

Rechnerkommunikation III

1. Protokolle und Dienste der Vermittlungsschicht

- Dienstklassen der Vermittlungsschicht
 - Verbindungslose Dienste (Datagramm Teilnetz → Postsystem)
 - Verbindungsorientierte Dienste (Virtuelle Verbindung, Virtual Circuit → Telefonsystem)

1.1 Routing

1.1.1 Routing-Algorithmen

- Verfahren zur Bestimmung von Wegen, die ein Datenpaket vom Sender zum Empfänger nehmen soll.
- Routing-Algorithmen verarbeiten *Wegewahlinformationen*, mit Hilfe derer der Weg festgelegt wird (→ *statische / dynamische* Routing-Algorithmen)
- Beispiele für Routing Verfahren
 - **Fluten:**
(Datenpakete werden vom Router repliziert und auf allen anderen Wegen weitergeschickt → hoher Netzverkehr)
 - **Shortest Path Routing**
(Kürzester Weg berechnet nach: Anzahl der Teilstrecken / Entfernung in km / ...)
 - **Distance Vector Routing**
(Jeder Router verwaltet eine Tabelle, die für jedes Ziel die bestmögliche Entfernung und die zu verwendende Ausgangsleitung enthält)
 - **Link State Routing**
(Routing der Pakete nach Zustand der Leitungen → gleichmässigerer Netzauslastung)

- Routing mittels Wegewahltabellen (verbindungsloser Dienst)

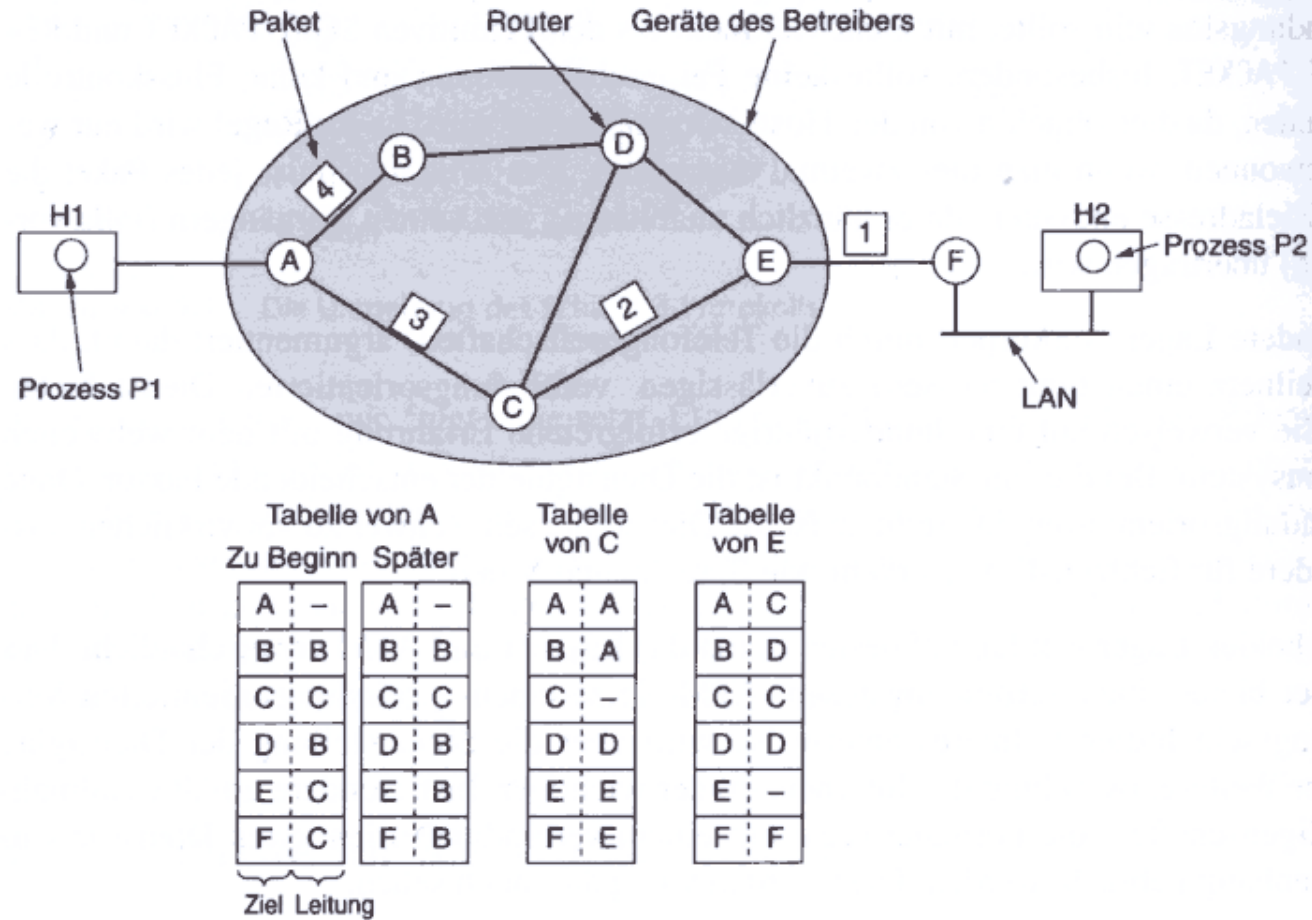


Abbildung 5.2: Routing in einem Datagramm-Teilnetz

- Routing mittels Wegewahltabellen (verbindungsorientierter Dienst)

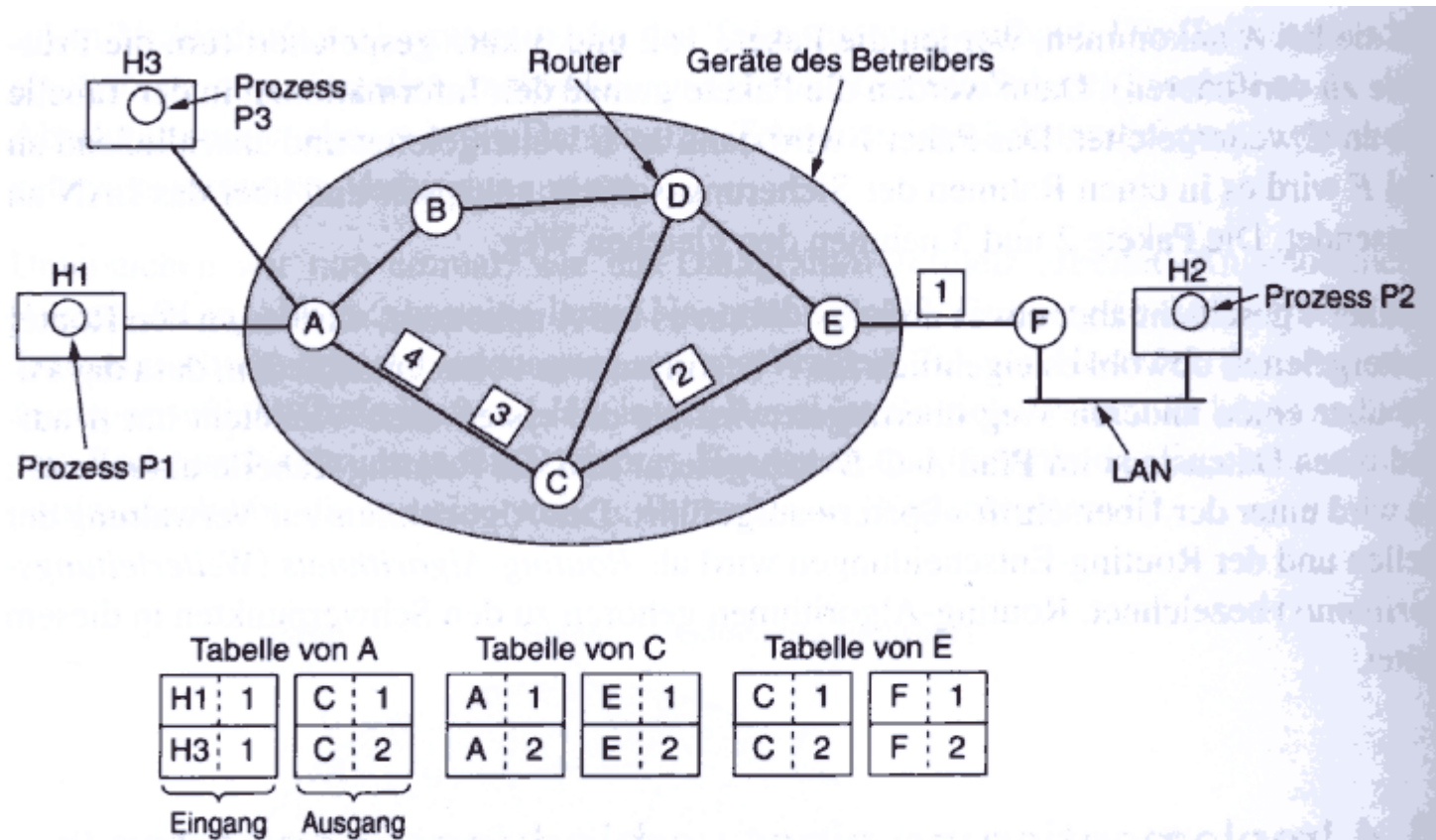


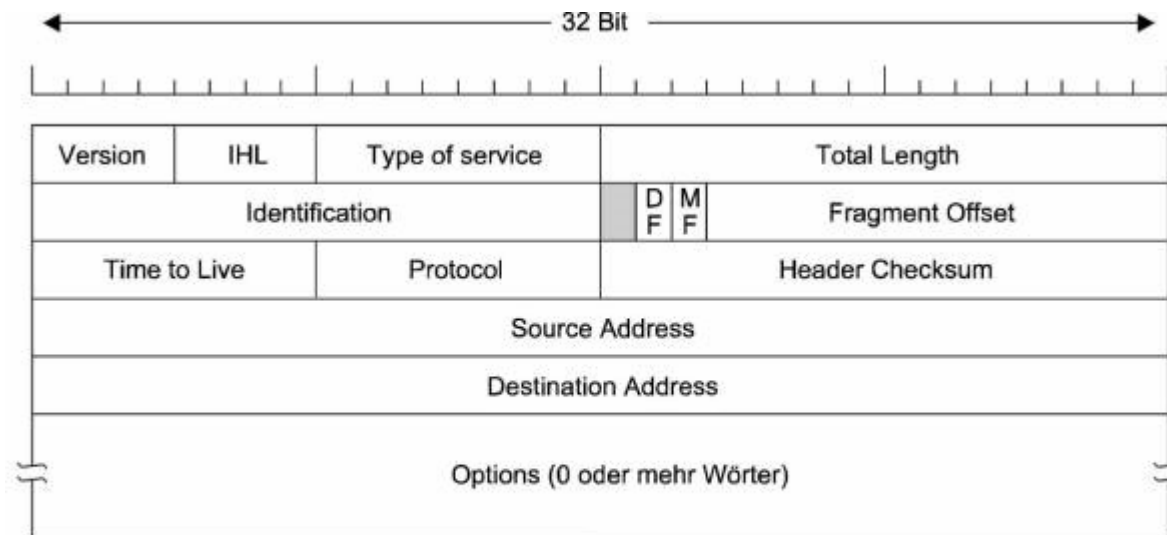
Abbildung 5.3: Routing in einem Teilnetz aus virtuellen Verbindungen

Rechnerkommunikation III

1.2 Die Vermittlungsschicht im Internet

1.2.1 Internet Protocol (IP)

- IPv4 ist definiert in RFC 791, IPv6 in RFC 2460, 2466.
- IPv4: Aufbau:



(2)

Abb. 5.45: Der Header des IP-Protokolls

(Abb. In dieser Präsentation aus: 1. Abeck et al.: Verteilte Informationssysteme, 2. Tanenbaum, A.: Computernetzwerke, 3. Kurose, J. u. Ross, K.: Computernetze)

Rechnerkommunikation III

IPv4 Charakteristik

- Besteht aus einem **Header-** (20 Byte feste Länge + optionaler Abschnitt mit variabler Länge (max. 40 Byte)) und **Textteil**.
- **Header+Text** bilden zusammen das **Datagramm**.
- Max. Gesamtlänge eines Datagramms: 65.536 Byte.
- Elementare Fragmenteinheit: 8 Byte.
- **Header:**
Mehrere festgelegte Felder kodieren verschiedene Basisinformationen (Version des Protokolls, Länge, ... (s. Abb. 5.45)) und zusätzliche optionale Informationen (Sicherheit, Striktes Source-Routing... (s. Abb 5.46))
- **Verbindungsloses**, relativ unzuverlässiges Protokoll: keine Bestätigung der Zustellung/ Verlust eines Pakets; keine Überlastkontrolle

Rechnerkommunikation III

IPv4 Header: Optionen

Option	Beschreibung
Sicherheit (<i>Security</i>)	Bezeichnet, wie geheim das Datengramm ist
Striktes Source-Routing (<i>Strict Source Routing</i>)	Bestimmt den kompletten Pfad
Loses Source-Routing (<i>Loose Source Routing</i>)	Gibt eine Liste von Routern aus, die nicht zu verfehlen sind
Routenaufzeichnung (<i>Record Route</i>)	Veranlaßt jeden Router, seine IP-Adresse anzuhängen
Zeitstempel (<i>Time Stamp</i>)	Veranlaßt jeden Router, seine Adresse und einen Zeitstempel anzuhängen

Abb. 5.46: IP-Optionen

Rechnerkommunikation III

IPv4 Adressierung und früher verwendete Netzklassen

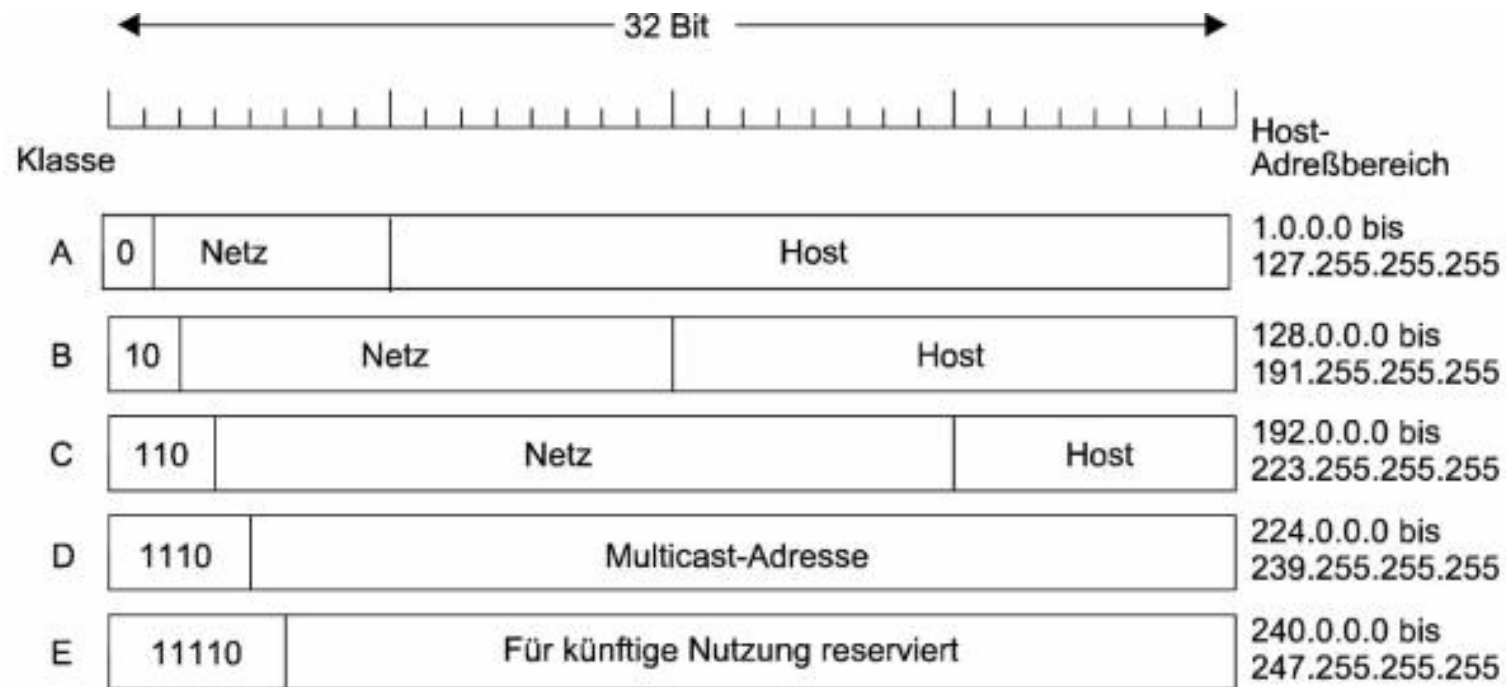


Abb. 5.47: IP-Adreßformate

Rechnerkommunikation III

Teilnetze

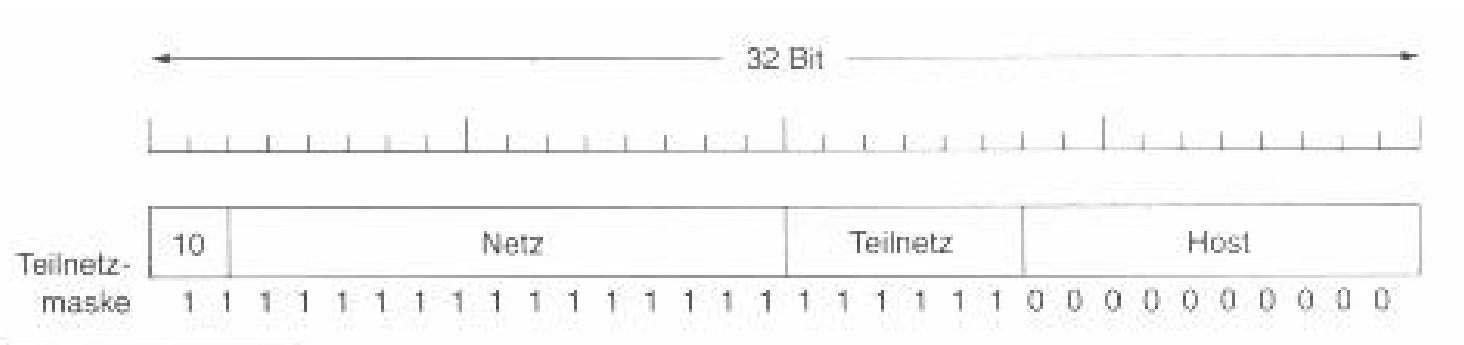


Abbildung 5.58: Klasse-B-Netz, das in 64 Teilnetze unterteilt ist

255.255.252.0

255.255.252.0/22

Rechnerkommunikation III

Classless InterDomain Routing (CIDR)

- **Netzklassen sind nicht mehr in Gebrauch, IP-Adressen werden nach CIDR vergeben!**
- CIDR (Classless Interdomain Routing) (RFC 1519) soll das Problem der "ausgehenden" IP-Adressen lösen:
- Die verbleibende Netze werden in Blöcken vergeben, unabhängig von Klassen:
- Adressen 194.0.0.0 bis 195.255.255.255 für Europa
- Adressen 198.0.0.0 bis 199.255.255.255 für Noramerika
- ...

Rechnerkommunikation III

IPv6 Charakteristik

- **IPv6** wurde eingeführt, um vor allem **die Anzahl der zu vergebenden IP-Adressen zu vergrößern**; dabei soll zusätzlich das Protokoll aufgrund von mit IPv4 gemachten Erfahrungen verbessert werden; neue Anwendungen (Multimediaanwendungen) und veränderte technologische Rahmenbedingungen (Realisierung hoher Datenraten) sind weitere Gründe.
- Die **Größe der IP-Adresse** wurde von **32** auf **128 Bit** erhöht.
Nicht mehr vorhanden sind (vor allem aus Gründen des Zeitaufwandes bei der Verarbeitung):
 - Fragmentierung/Reassemblierung findet jetzt nur noch bei Quelle und Ziel statt, nicht aber bei dazwischen liegenden Routern
 - Prüfsumme: aufgrund des TTL-Feldes musste in jedem Router die Prüfsumme neu berechnet werden
 - Optionen verschoben in „nächsten Header“

Notation der 16-Byte Adressen:

- X:X:X:X:X:X:X

z.B.: **FEDC:BA98:7654:3210:FEDC:BA98:7654:3210** (in Hex-Format)

Rechnerkommunikation III

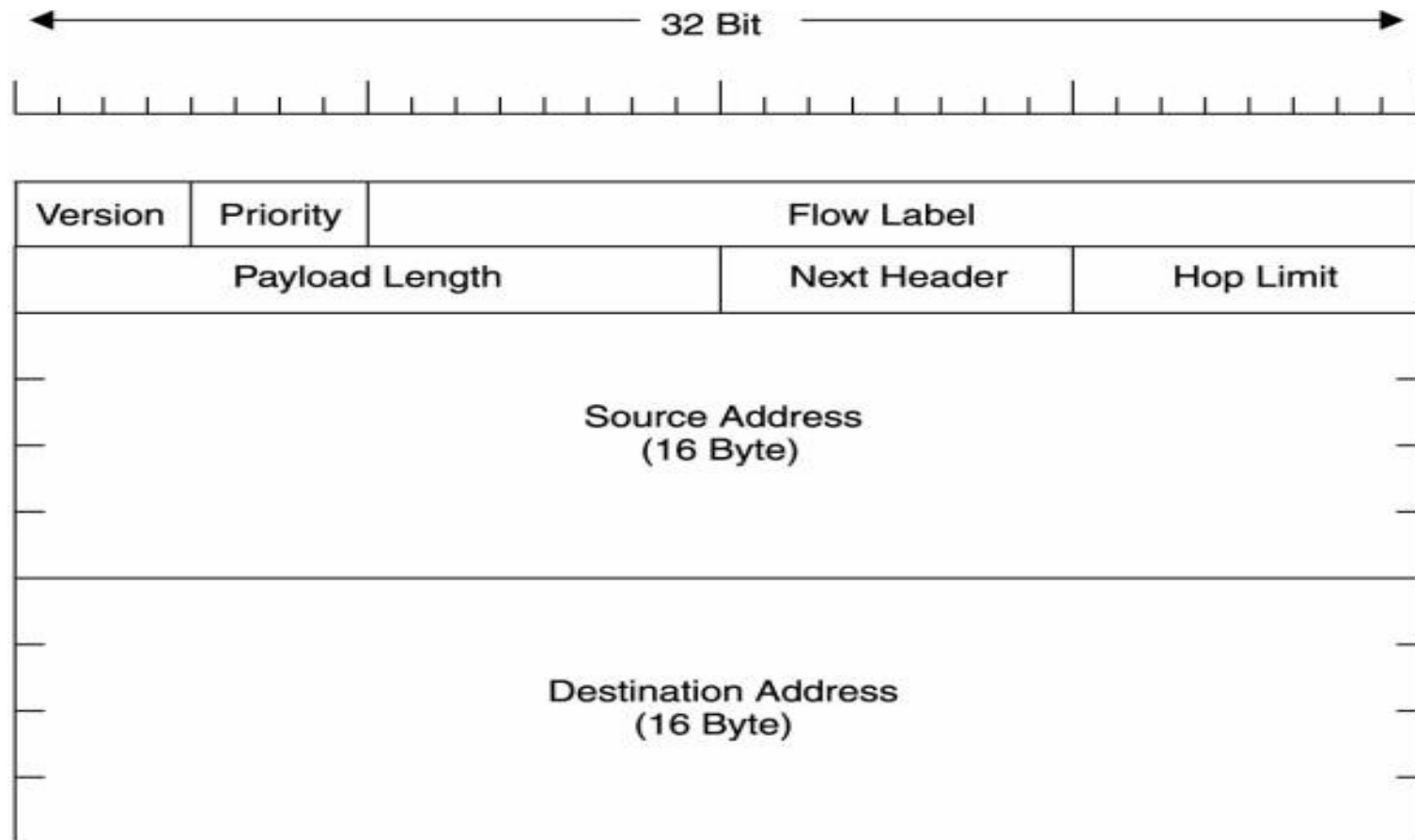


Abb. 5.56: Der feste IPv6-Header (zwingend)

Rechnerkommunikation III

5.1.4 Die Transportschicht (Transport Layer)

- Abstrahiert von unterschiedlichen *Vermittlungsschichtdiensten*; Aspekte des eigentlichen Nachrichtenaustauschs bleiben somit dem Dienstbenutzer verborgen.
- Die Dienste der Transportschicht sorgen dafür, dass Daten in Datenpakete zerlegt werden bzw. die einzelnen Datenpakete wieder korrekt zusammengefügt werden, so dass sie von Anwendungen verarbeitet werden können.
- Echte **Endpunkt-zu-Endpunkt-Schicht**, weil Quell- und Zielmaschine direkt miteinander kommunizieren, während auf den niedrigeren Schichten eine Maschine immer nur mit dem unmittelbaren Nachbarn kommuniziert.
- Bsp.: **TCP** (Transmission Control Protocol), **UDP** (UserDatagram Protocol)

Rechnerkommunikation III

2. Dienste und Protokolle der Transportschicht

2.1 Dienste

- Instanzen der **Vermittlungsschicht** arbeiten gemäß unterschiedlicher **Vermittlungsschichtprotokolle**.
Dementsprechend bieten sie **unterschiedliche** Dienste an.
- Die **Transportschicht** soll einen **zuverlässigen** Datentransferdienst für die Anwendungsprozesse bereit stellen, unabhängig von der verwendeten Netztechnologie in den Schichten unterhalb → zusätzliche Robustheit

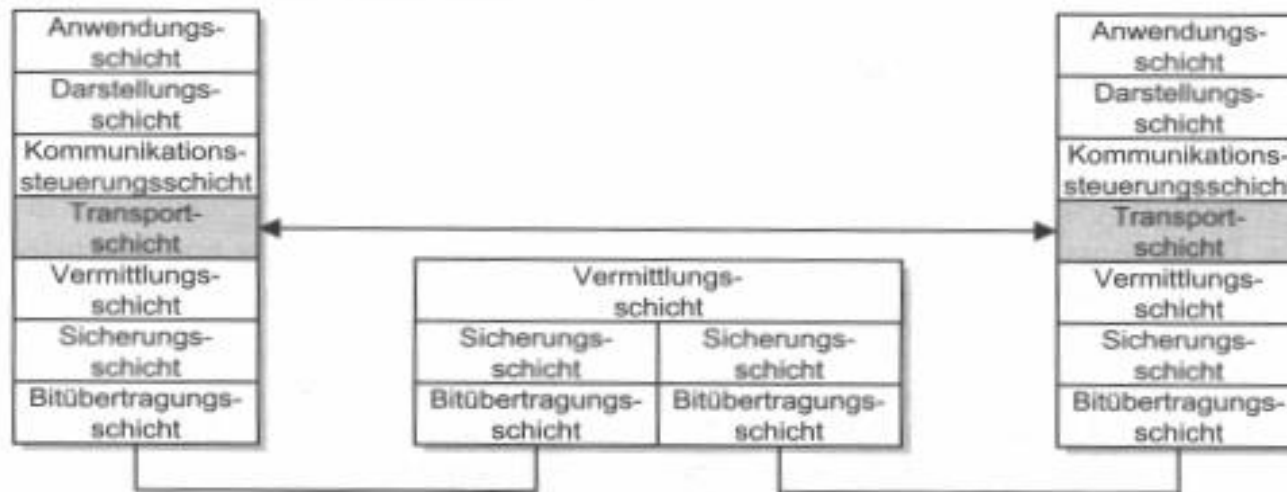


Abb. 9-1 Einordnung der Transportschicht

Rechnerkommunikation III

- **Bereitstellung von *Dienstgüte*:**
Die Anwendungsprozesse als Dienstnehmer der Transportschicht können **unterschiedliche Qualitäten** eines Transportschichtdienstes in Anspruch nehmen.

Diese werden über folgende ***Dienstqualitätsparameter*** spezifiziert:

- Zuverlässigkeit
- Übertragungsverzögerung
- Jitter (**Puffern** z.B. bei Video- oder Audioübertragung → erhöht aber die Verzögerung)
- Bandbreite

Anwendung	Zuverlässigkeit	Übertragungsverzögerung	Jitter	Bandbreite
E-Mail	Hoch	Niedrig	Niedrig	Niedrig
Dateiübertragung	Hoch	Niedrig	Niedrig	Mittel
Webzugriff	Hoch	Mittel	Niedrig	Mittel
Entfernte Anmeldung	Hoch	Mittel	Mittel	Niedrig
Audio on Demand	Niedrig	Niedrig	Hoch	Mittel
Video on Demand	Niedrig	Niedrig	Hoch	Hoch
Telefonie	Niedrig	Hoch	Hoch	Niedrig
Videokonferenzen	Niedrig	Hoch	Hoch	Hoch

Abbildung 5.30: Erforderliche Dienstgüte für verschiedene Anwendungen

Rechnerkommunikation III

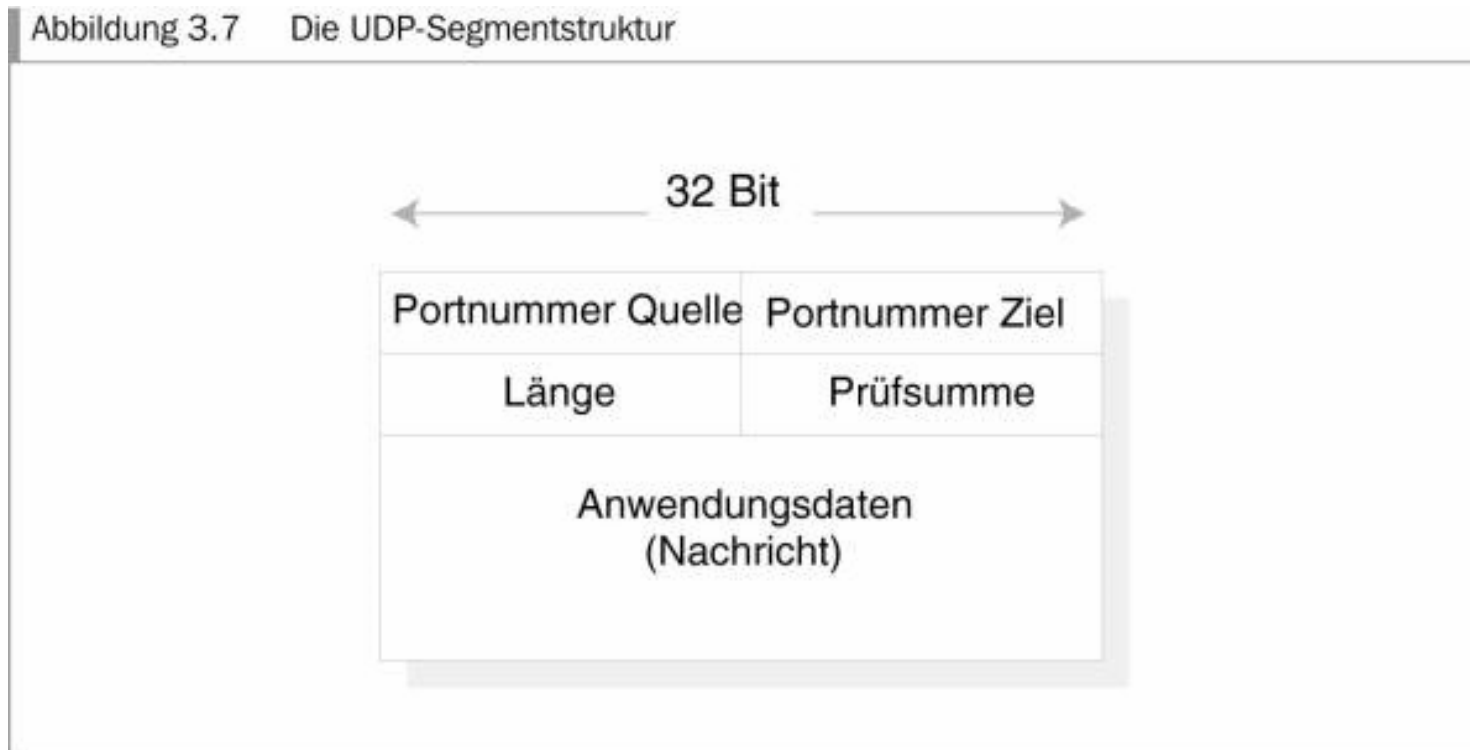
2.2 Protokolle der Transportschicht

2.2.1 User Datagram Protocol (UDP)

- Definiert in RFC 768.
- Verbindungsloses Protokoll
- Bietet einen einfachen, unbestätigten Datagramm-Dienst.
- Unterstützt also nicht Flusskontrolle, Fehlerkontrolle oder erneutes Senden
- Max. Größe einer UDP-PDU: 64 KB.
- Schnelle, einfache Übertragung
- Verwendung: z.B.: Multimediaanwendungen, kurze Anforderungen

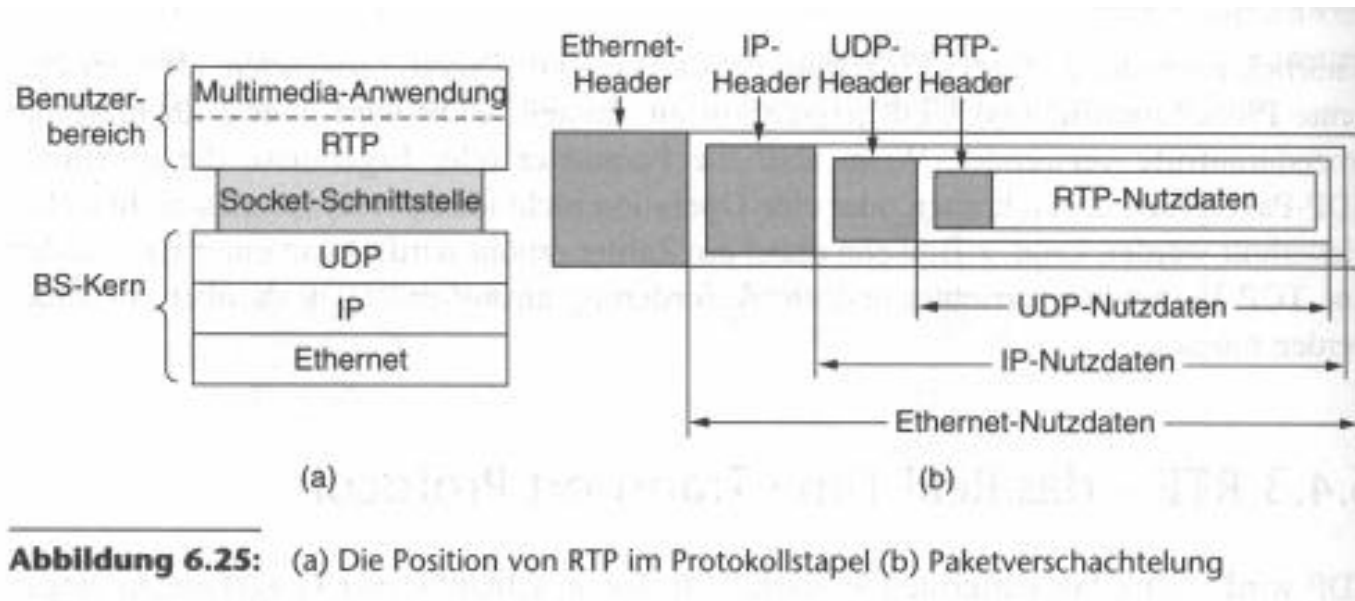
Rechnerkommunikation III

- Aufbau der UDP- PDU:



2.2.2 Realtime Transport Protocol (RTP)

- Definiert in RFC 3550, (1889).
- Protokoll für Echtzeit-Multimedia-Anwendungen (*Internettelefonie, Audiostreaming, ...*).
- RTP ist ein Protokoll das sich nicht exakt in eine Schicht einordnen läßt, da es ein Transportprotokoll ist, das in der Anwendungsschicht implementiert ist; es verwendet wiederum UDP als Transportmedium
- Bietet **keine** Fehlerkorrektur, da Pakete, die erneut gesendet werden würden, ohnehin zu spät eintrüfen.



- RTP hat auch ein Kontrollprotokoll: RTCP. RTCP kann z.B. Informationen über Übertragungsverzögerung, Jitter (Abweichungen in der Paketübermittlungszeit), Bandbreite liefern.

SW: Jitter-Kontrolle

- **Jitter („Zittern“):**
Standardabweichung bei den Paketankunftszeiten während eines Transports.
- hoher Jitter kann zu *Qualitätsschwankungen* bei der Wiedergabe von Echtzeitanwendungen führen; der Verzögerungsbereich für Pakete muss also in einer konstanten Spanne gehalten werden.
- **Strategie:**
Router überprüfen, um wie weit ein Paket von einer Standardübertragungszeit für eine Wegstrecke abweicht. Die Information wird im Paket gespeichert und an jeder Teilstrecke überprüft und aktualisiert. Entsprechend der Abweichung kann der Router das Paket zurückhalten oder versuchen, es schneller weiterzugeben

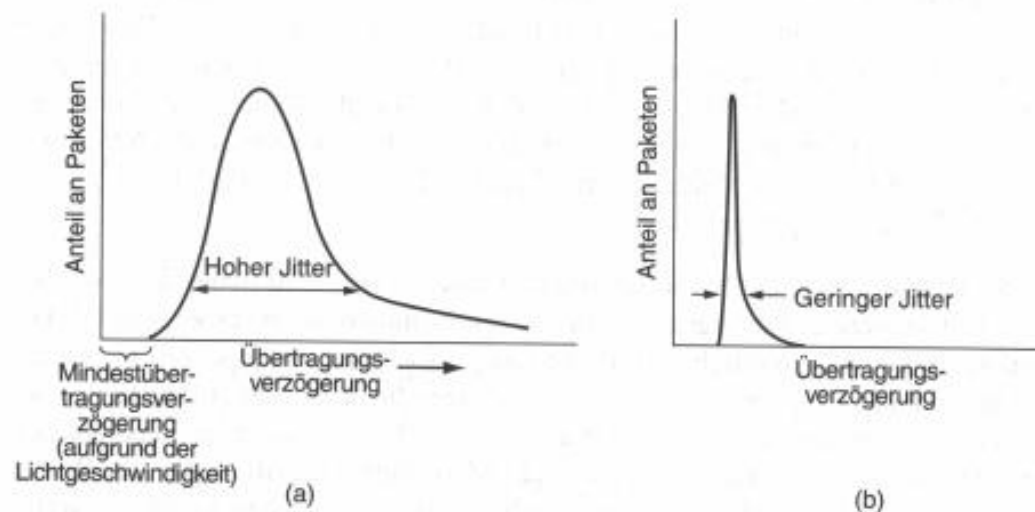


Abbildung 5.29: (a) Hoher Jitter (b) Geringer Jitter

Rechnerkommunikation III

2.2.3 Transmission Control Protocol (TCP)

- Definiert in RFC 793.
- Verbindungsorientiertes Protokoll
- TCP ist **zuverlässig** (alle Datenpakete kommen **redundanzfrei, vollständig** und in **richtiger Reihenfolge** an) und **verbindungsorientiert** (stellt virtuellen Kanal über Sockets her)
- **Multiplexen/ Demultiplexen:**
 - Um Daten zwischen mehreren Prozessen auszutauschen, müssen sie multiplext/demultiplext werden, d.h. die Daten müssen einzelnen Prozessen zugeordnet werden.
 - Die Aufgaben der Übertragung der in einem Transportschichtsegment enthaltenen Daten an den richtigen Anwendungsprozess heißt *Demultiplexen*.
 - Die Aufgabe des Einsammelns von Daten aus verschiedenen Anwendungsprozessen, die Vervollständigung der Daten mit Header-Informationen, um Pakete zu bilden, und die Weiterleitung der Pakete an die Vermittlungsschicht heißt *Multiplexen*.

Rechnerkommunikation III

- TCP unterstützt Vollduplex-Datenübertragung
- TCP- Aufbau: Header + Payload (Nutzdaten, z.B. die Protokolle der Anwendungsschicht HTTP, FTP,...) = TCP- PDU.

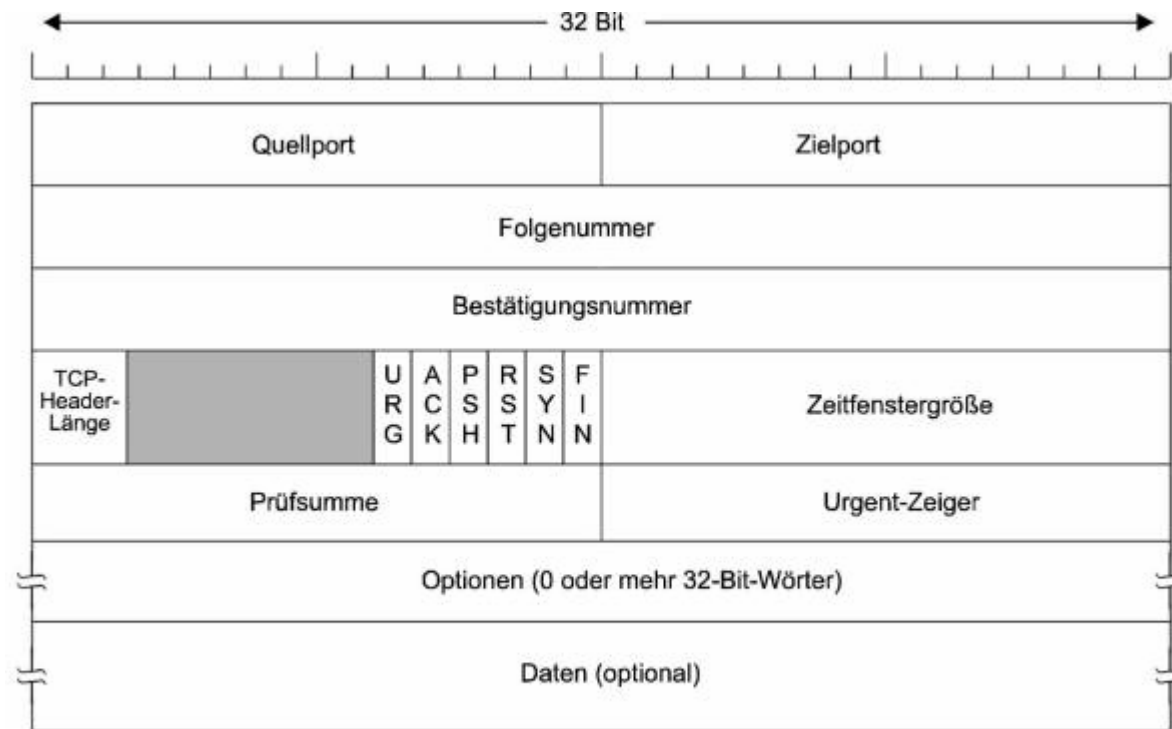


Abb. 6.24: Der TCP-Header

Rechnerkommunikation III

- 3. Protokolle und Dienste der Anwendungsschicht
- 3.1 E-Mail

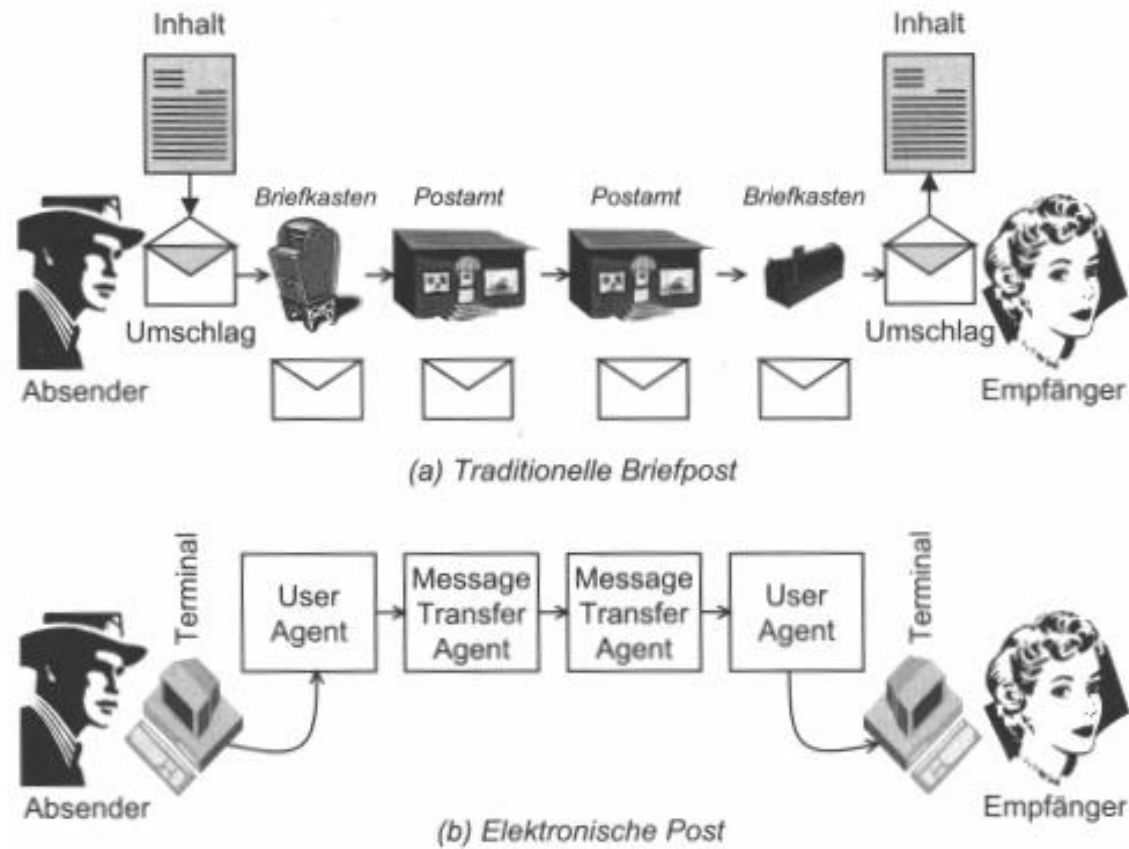


Abb. 10-5 Vergleich Briefpost und elektronische Post

Rechnerkommunikation III

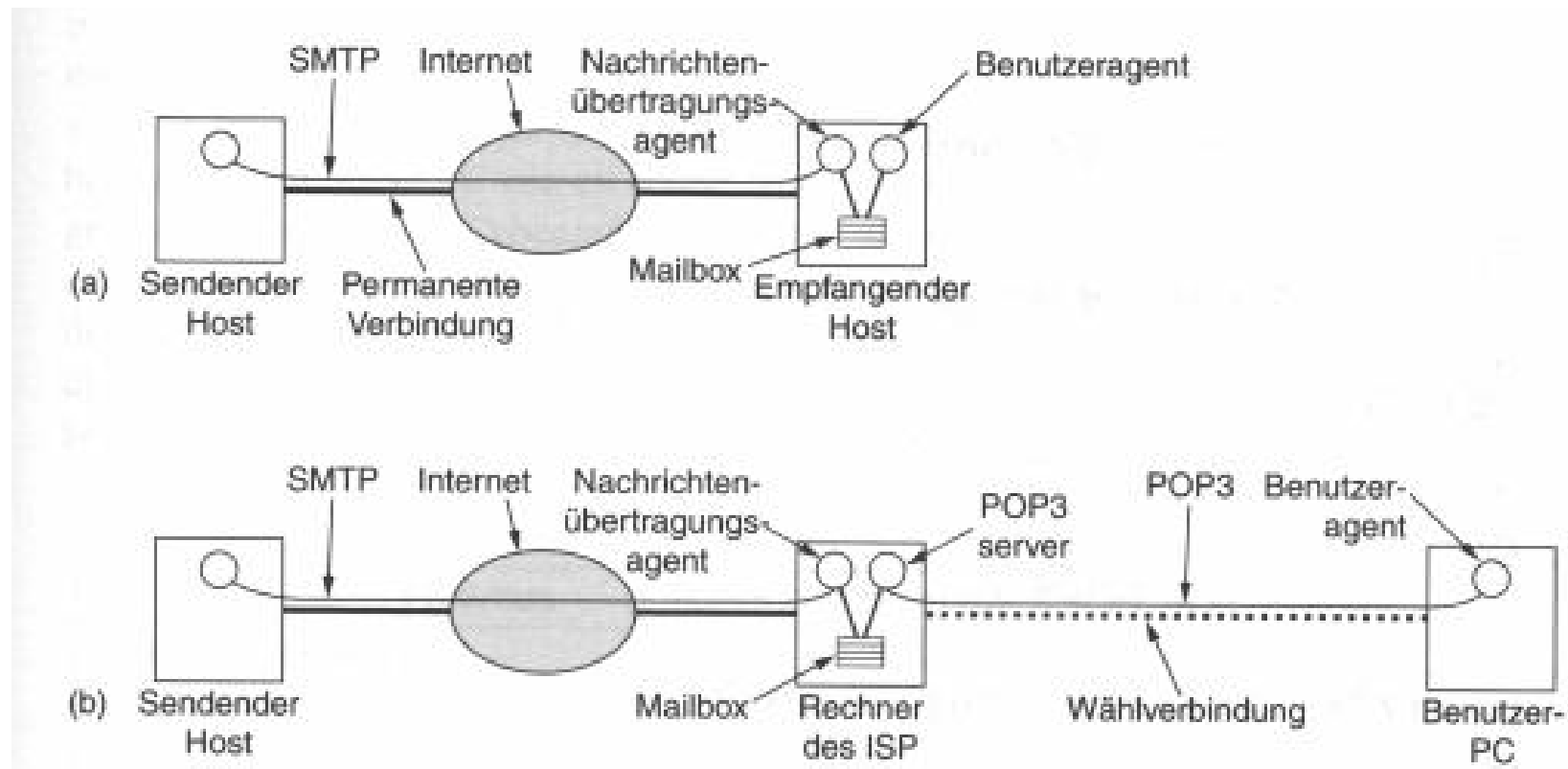
- **User Agent:** Unterstützt den Benutzer bei der Erstellung und den Versand seiner Nachricht; er ist ein Anwendungsprozeß, über den Dienstleistungen des Übermittlungssystems dem Benutzer verfügbar gemacht werden. (= Mailprogramm)
- **Message Transfer Agent:** Diese übernehmen die Nachricht vom User Agent oder anderen MTAs und vermitteln sie so an den Empfänger; sie realisieren also das eigentliche Nachrichtenübermittlungssystem.
- Bei der Übermittlung von Nachrichten können verschiedene Protokolle zum Einsatz kommen: SMTP, POP3, IMAP...

3.1.2 Simple Mail Transfer Protocol (SMTP)

- Im Internet wird Mail zugestellt, indem die Quelle eine TCP-Verbindung zu Port 25 des Ziels aufbaut.
- SMTP ist ein einfaches ASCII-Protokoll:
 - Nach dem Aufbau der TCP-Verbindung wartet der sendende Rechner (Client), bis der empfangende Rechner (Server) zuerst mit der Kommunikation beginnt.
 - Der Server beginnt durch Aussenden einer Textzeile, durch die er sich identifiziert und mitteilt, ob er Email annehmen kann
- SMTP funktioniert nur, wenn der Empfänger einer Mail an einem Rechner arbeitet, der Emails senden und Empfangen kann.
- Da dies normalerweise nicht der Fall ist (kaum jemand hat einen Rechner zuhause, der Tag und Nacht online ist, und auf dem ein Mailserver läuft!) musste eine andere Lösung gefunden werden, um der steigenden Zahl an Benutzern den Empfang von Email zu ermöglichen: **POP3**

3.1.3 Post Office Protocol 3 (POP3)

= Protokoll um Nachrichten, die auf einem Übertragungsagenten hinterlegt sind, lokal abzurufen.



Rechnerkommunikation III

- POP3 durchläuft nacheinander 3 Zustände:
 - Autorisierung: Senden des Benutzernamens und Passworts
 - Transaktion: Abruf der Nachrichten aus der Mailbox (Speicherort beim ISP)
 - Aktualisierung: Löschen der Nachrichten
- POP3 setzt wie SMTP auf TCP auf, d.h. zunächst errichtet die das Mailprogramm eine TCP-Verbindung über einen Port (hier idR 110) und führt dann das POP3 Protokoll aus.

Rechnerkommunikation III

3.1.4 Internet Message Access Protocol (IMAP)

Funktion	POP3	IMAP
Protokoll definiert in	RFC 1939	RFC 2060
Verwendeter TCP-Port	110	143
E-Mail gespeichert auf	Benutzer-PC	Server
Lesen von E-Mail	Offline	Online
Erforderliche Verbindungszeit	Viel	Wenig
Belegte Server-Ressourcen	Minimal	Erheblich
Mehrere Mailboxen	Nein	Ja
Wer sichert Mailboxen	Benutzer	ISP
Gut für mobile Benutzer	Nein	Ja
Benutzer hat Kontrolle über Download	Wenig	Sehr viel
Herunterladen von Teilnachrichten	Nein	Ja
Kann die Festplattenkapazität ein Problem werden	Nein	Eventuell im Laufe der Zeit
Einfache Implementierung	Ja	Nein
Verbreiteter Support	Ja	Zunehmend

Abbildung 7.17: Ein Vergleich von POP3 und IMAP

Rechnerkommunikation III

3.1.5 Nachrichtenformate

- RFC 822

Header	Bedeutung
To:	E-Mail-Adresse(n) des/der primären Empfänger(s)
Cc:	E-Mail-Adresse(n) des/der sekundären Empfänger(s)
Bcc:	E-Mail-Adresse(n) für blinde Kopien an Dritte
From:	Ersteller der Nachricht
Sender:	E-Mail-Adresse des tatsächlichen Absenders
Received:	Zeile, die von jedem Transferagenten auf dem Weg eingefügt wird
Return-Path:	Kann verwendet werden, um einen Pfad zurück zum Absender zu bezeichnen

Abbildung 7.9: Header-Felder nach RFC 822 für die Nachrichtenübertragung

Rechnerkommunikation III

- **Multimediale Nachrichten**
 - Standard-SMTP sieht nur die Übertragung von Nachrichten als ASCII-Text vor
 - deshalb wurde ein Standard für die Übertragung multimedialer Nachrichteninhalte definiert: **MIME** (Multipurpose Internet Mail Extensions)
 - neue Datenfelder im Headerteil einer Nachricht:
z.B.: Content-Type: video/mpeg
Content-Transfer-Encoding: base64

Rechnerkommunikation III

4. Domain Name System (DNS)

4.1 Begriffe

- = auf Domänen basierendes Benennungsschema für IP-Adressen (RFC 1034, 1035), das als verteiltes Datenbanksystem realisiert ist.
- Domain Name Server (Name Server): Programm oder Rechner, das /der die Information über die Struktur des DNS verwaltet und aktualisiert.
- DNS-Protokoll: Protokoll, das die Umwandlung von IP-Adressen in DNS-Namen regelt. Momentan wird für die Übermittlung von DNS-Anfragen UDP oder TCP verwendet
- Domain Name Service: Dienst, der das DNS realisiert.

Rechnerkommunikation III

4.2 DNS-Namensraum

- Top Level Domain, Second Level Domain, Subdomain
- 134.95.100.203 uni-koeln.de
- Jede Domäne bestimmt, wie die unter ihr liegenden Domänen zugewiesen werden

Bsp.: cs.yale.edu
cs.keio.ac.jp
hki.uni-koeln.de

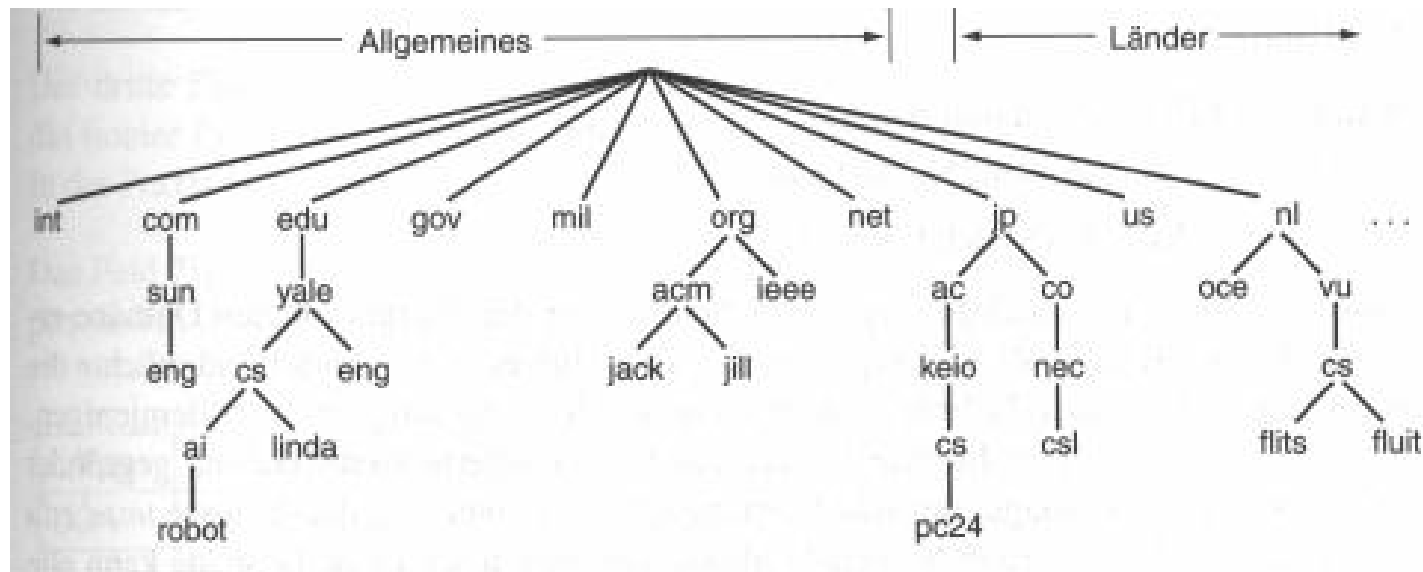


Abbildung 7.1: Teil des Namensraums der Internetdomänen

Rechnerkommunikation III

4.3 Zonen

- Der gesamte Namespace wird in Zonen, also Einheiten, die bestimmte, nicht-überlappende Teile des DNS-Baums zusammenfassen, aufgeteilt.

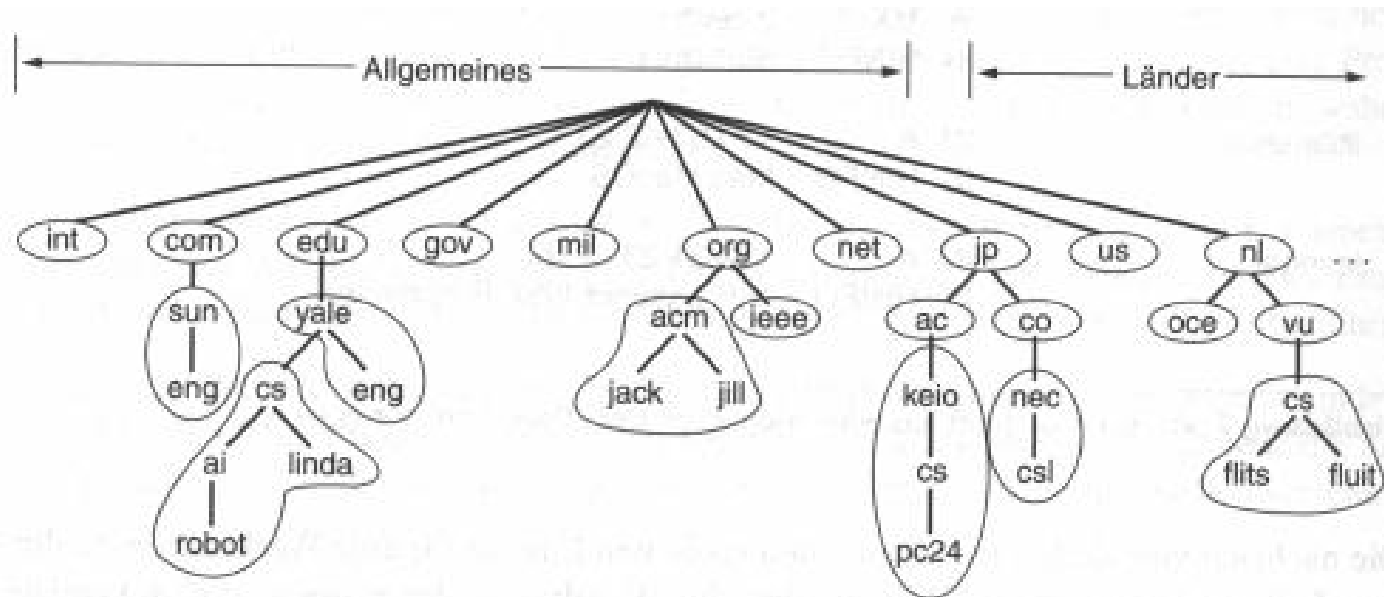


Abbildung 7.4: Teil des DNS-Namensraums mit der Aufteilung in Zonen

Rechnerkommunikation III

4.4 Nameserver

- Jede Zone enthält Nameserver, die Domänenanfragen beantworten und DNS-Einträge verwalten.

Man unterscheidet:

- *Autoritative Nameserver* : Daten, die von diesen stammen, gelten als absolut gesichert.
- *Nicht-Autoritative Nameserver*: Bezieht seine Daten von Nameservern außerhalb seiner Zone und speichert diese für eine gewisse Zeit im RAM (Cache-Nameserver)
- *Primary Nameserver*: Server, der eine Zone verwaltet; auf ihm befinden sich die Originaldateien.
- *Secondary Nameserver*: Server, die Kopien der Daten des Primary Nameservers enthalten.

Rechnerkommunikation III

4.6 Resolver

- Resolver stellen die Schnittstelle zwischen Anwendungsprogramm und Nameserver her. Sie können Informationen aus den Nameservern abrufen, z.B. Ressource Records um eine angeforderte IP-Adresse zu erhalten.
- **rekursive Anfrage:**
Der Resolver stellt eine Anfrage an den Nameserver seiner Domäne; dieser gibt einen Datensatz zurück oder eine „Negativmeldung“; ist der angefragte Datensatz auf einem anderen Nameserver, so übernimmt der angefragte Nameserver die Aufgabe der Informationsgewinnung.
- **Iterative Anfrage:**
Der Resolver erhält einen Datensatz zurück, der den „nächst entfernten“ Nameserver angibt; der Resolver startet darauf seine Anfrage neu an diesen Nameserver usw. bis er den Server, der die gewünschte Information hält, gefunden hat.

Beispiel

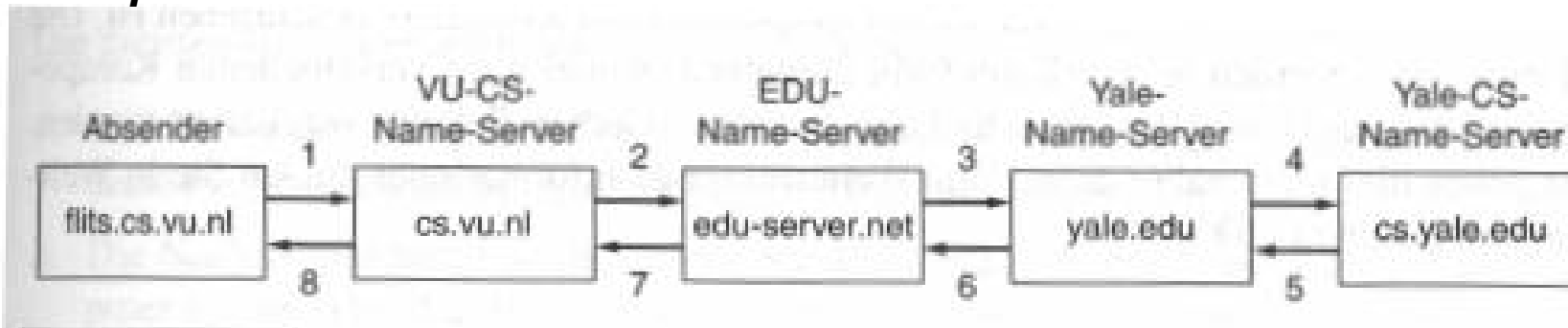


Abbildung 7.5: Suche nach einem entfernten Namen durch einen Resolver in acht Schritten

- Ein Resolver in **flits.cs.vu.nl** möchte die IP-Adresse des Hosts **linda.cs.yale.edu** wissen:
 1. Anfrage an seinen lokalen Name-Server (**cs.vu.nl**)
 2. Der lokale Server kennt die angefragte Adresse nicht und fragt einige in der Nähe befindliche Name-Server
 3. Danach dann Anfrage an den Name-Server von **.edu**. Dieser kennt die gesuchte Adresse auch nicht, kennt aber die Name-Server in seiner Zone und sendet eine Anfrage an **yale.edu**.
 4. Dieser leitet die Anfrage an **cs.yale.edu** weiter, der sich in seiner Zone befindet.
 5. Hier befinden sich die autoritativen Datensätze für diese Zone, so dass die Adresse für den gesuchten Host zurückgeliefert wird (Schritte 5-8)
 6. Kommen diese Datensätze wieder beim Name-Server **cs.vu.nl** an, werden sie dort im Cache verwahrt, falls Sie später nochmal benötigt werden. Dies sind dann aber keine autoritativen Datensätze mehr, weil eventuelle Änderungen in **cs.yale.edu** nicht auf alle Caches der Welt verteilt werden.

Rechnerkommunikation III

4.7 Was bietet/ ermöglicht DNS?

- Entkopplung von IP-Adresse
- dezentrale Verwaltung
- hierarchische Strukturierung des Namensraums in Baumform
- Eindeutigkeit der Namen
- Erweiterbarkeit
- Lastverteilung (durch Zuordnung mehrerer IP-Adressen zu einem Namen)
- Reverse lookup

Rechnerkommunikation III

Aufgaben

- 1) **Wiederholen** Sie den Stoff dieser Sitzung **bis zur nächsten Sitzung** (siehe dazu den Link zur Sitzung auf der HKI-Homepage). Informieren Sie sich zusätzlich durch eigene Literaturrecherche!
- 2) Beantworten Sie die Fragen aus der Sammlung „**beispielhafte Klausurfragen**“ zur Rechnerkommunikation (soweit in dieser Sitzung behandelt).