

Rechnernetze und verteilte Systeme

Peter Buchholz

Informatik IV

Praktische Informatik – Modellierung und Simulation

Koordinaten:

- Tel: 755 4746
- Email: peter.buchholz@cs.tu-dortmund.de
- OH 16, R. 216
Sprechstunde Do. 10.00 –11.30 und n.V.
- URL: <http://ls4-www.cs.tu-dortmund.de/~buchholz>

Rechnernetze und verteilte Systeme

Rechnernetz

Zusammenschluss autonomer (teilweise sehr heterogener)
Rechner (inkl. eingebetteter Systeme etc.)

Typische Beispiel: Internet

Verbindung der Rechner über
Koxialkabel, Lichtwellenleiter, Funk, Satelliten,

Vorlesung beschäftigt sich damit, wie ein solcher
Zusammenschluss funktioniert
und stellt einen Ausschnitt aus einem sehr umfangreichen
Gebiet vor!

Literatur

Zentrale Literatur

- **J. F. Kurose, K. W. Ross: Computer Networking, 6th Ed., Pearson 2013**
bzw. die ältere deutsche Ausgabe J. F. Kurose, K. W. Ross:
Computernetzwerke, 5te Auflage; Pearson Studium 2012
(6. Auflage 2013 mit kleineren Änderungen)

Weitere Empfehlungen

- A. Tanenbaum/D. J. Wetherall: Computer Networks, 5th Edition; Pearson Studium 2011.
- L. L. Peterson, L. S. Davie. Computer Networks. Morgan Kaufmann, 5th Edition, 2012.

Folien

Zusammenstellung aus folgenden Quellen:

- Foliensätze der Vorlesungen
verfügbar auf der Vorlesungsseite
http://ls4-www.cs.tu-dortmund.de/cms/de/lehre/2016_ws
(nicht auf der Seite der Gruppe RvS, dort sind die Folien vom vorletzten Jahr!)
- Wesentliche Vorlage:
Foliensatz zum Buch „*J. F. Kurose, K. W. Ross: Computernetze; Pearson Studium 2002 & 2007 & 2009 & 2013*“
die meisten Graphiken wurden von den Folien übernommen
weitere Quellen: Folien zu den Büchern von
Tanenbaum/Wetherall und Peterson/Davie.

Organisatorisches

Bachelor: Schriftliche Fachprüfung RvS 60 Minuten

Voraussichtliche Termine (unter Vorbehalt):

1. Mittwoch 15.2.2017, 8.00 Uhr
2. Dienstag 4.4.2017, 16.00 Uhr

Voraussetzung zur Klausurteilnahme:
erfolgreiche Teilnahme an den Übungen!

Informationen zu den Übungen am Ende der Vorlesung

Gliederung und Ablauf

- 1 Einführung, Internet und Protokolle
- 2 Internet und Protokolle
- 3 Anwendungsschicht
- 4 Anwendungsschicht
- 5 Transportschicht
- 6 Transportschicht
- 7 Transportschicht
- 8 Vermittlungsschicht
- 9 Vermittlungsschicht
- 10 Das Netz der Informatik
- 11 Sicherungsschicht
- 12 Sicherungsschicht
- 13 Multimedia
- 14 Sicherheit in Netzen
- 15 Netzmanagement, Abschluss

Kapitel 1: Einführung/Übersicht

Ziele:

- Ein Gefühl für Aufbau von Netzen bekommen und die Terminologie kennen lernen
- Details später
- Ansatz:
 - Internet als Beispiel

Übersicht:

- Was ist das Internet?
- Was ist ein Protokoll?
- Rand des Netzes: Hosts, Zugangsnetz, physikalische Medien
- Kern des Netzes: Paket-/Leitungsvermittlung, Struktur des Internets
- Leistung: Verlust, Verzögerung, Durchsatz
- Sicherheit
- Protokollschichten, Dienstmodelle
- Historie

Rechnernetze und verteilte Systeme

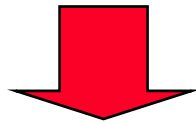
- ◆ **Rechnernetz:** ←
Durch Telekommunikationssystem verbundene autonome Rechnerknoten
- ◆ **Telekommunikationssystem:** ←
System, das Teilnehmern Kommunikationsdienste anbietet (in der Regel selbst durch Rechnernetz implementiert)
- ◆ **Verteiltes System:**
Anwendung, deren Komponenten sich an verschiedenen Orten befinden,
Komponenten sind in Rechnernetz installiert, werden lokal von den Rechnerknoten ausgeführt und kommunizieren miteinander mit Hilfe eines Telekommunikationssystems.

Besonderheiten verteilter Systeme

- Kommunikation

- **unzuverlässig, teuer, langsam**

← Räumliche Entfernung →



- Lose Kopplung

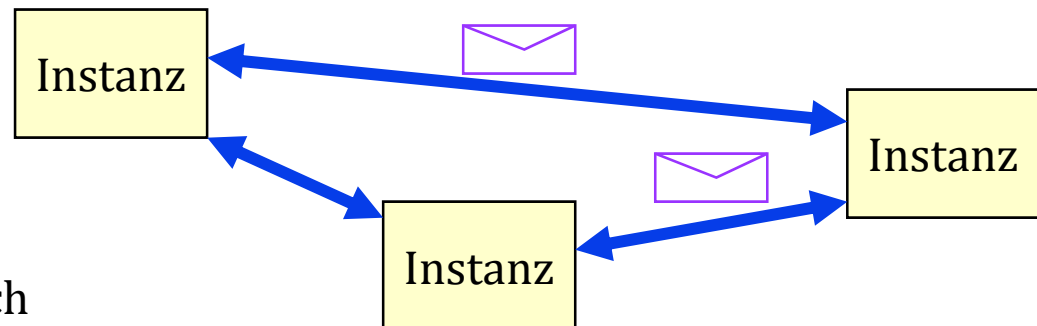
- Kommunikation selten
 - Synchronisation schwach
 - Fehlertoleranz

- Nebenläufigkeit (Concurrency)

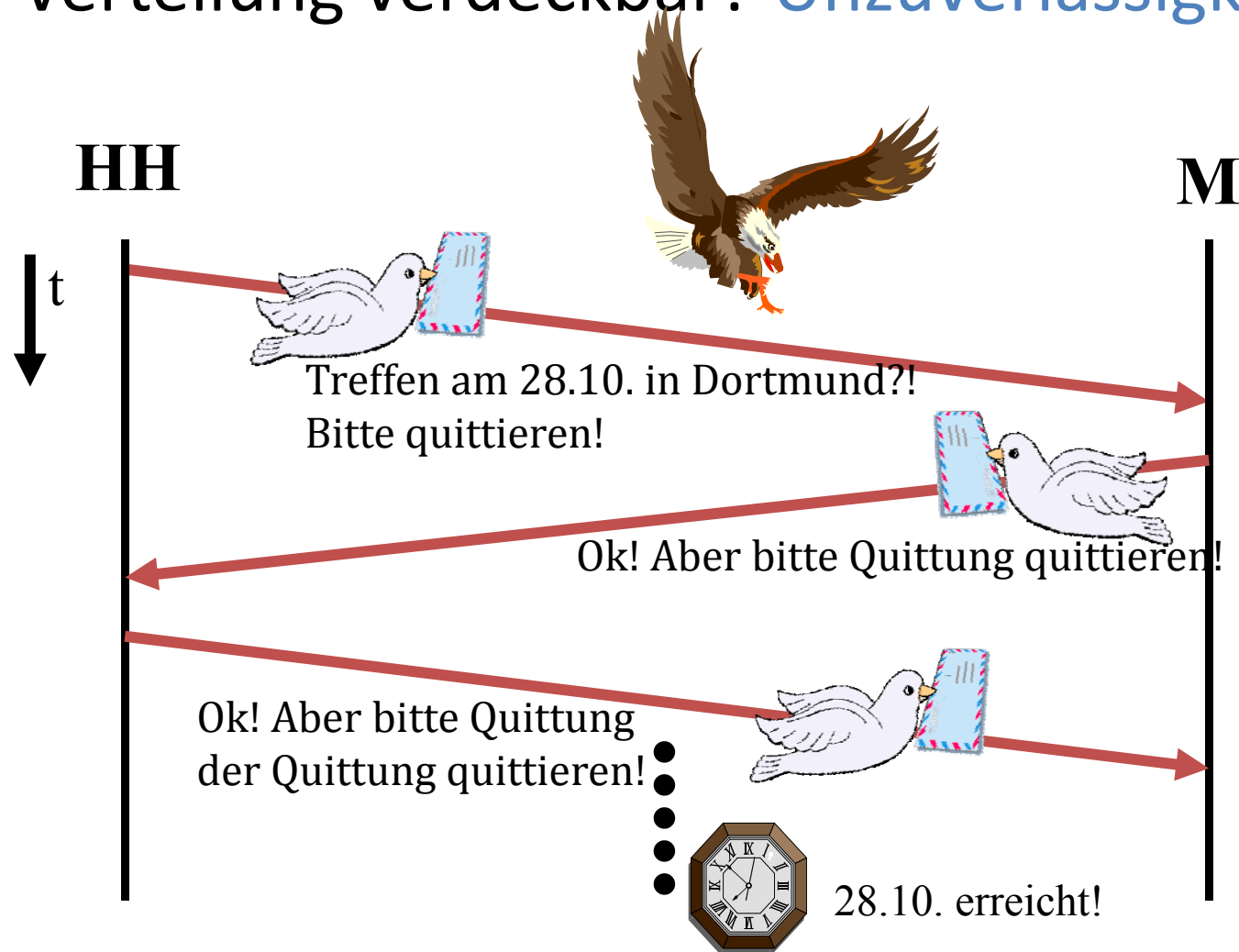
- weitgehend unabhängige Fortschritte

- Dezentrale Kontrolle

- weitgehende Autonomie
 - lokale Kontrolle auf Basis partieller Sichten
 - vollständige Sicht des globalen Systemzustands wird vermieden, da das zu teuer ist (Einfrieren)



Verteilung verdeckbar? Unzuverlässigkeit!



Vollständig zuverlässige Übereinkunft unter Fristsetzung ist nicht möglich!

Das Internet

- Millionen miteinander verbundener Computer:



PC



Server



Laptop



Mobiltelefon

*PCs, Workstations, ... =
Endsysteme*

– auf denen
Netzwerkanwendungen
laufen

□ *Kommunikationsleitungen*



Zugangspunkt

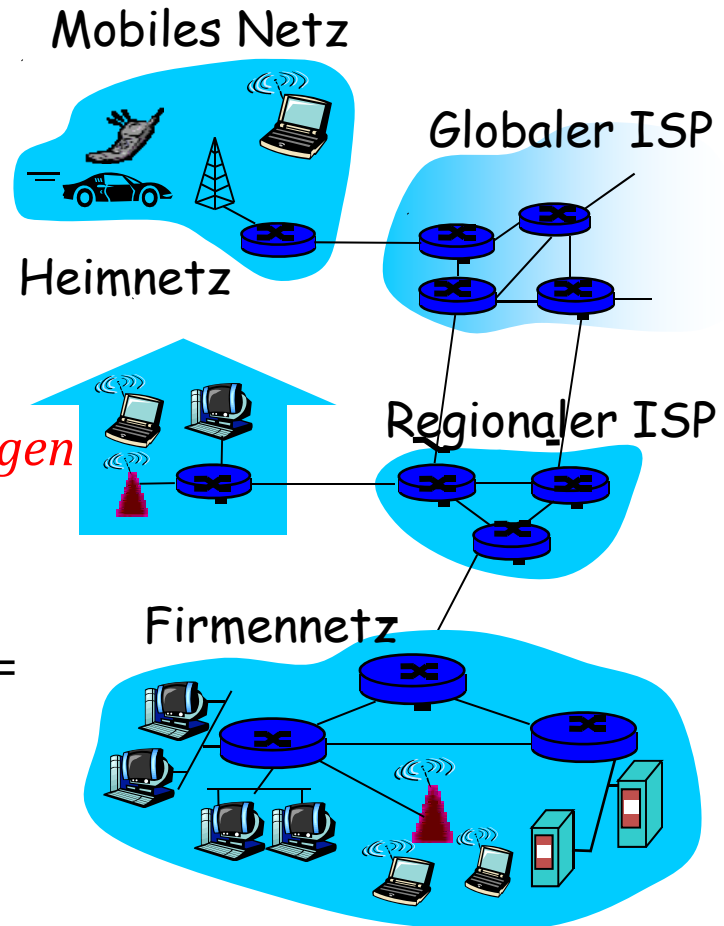
— Drahtgebundene/
drahtlose
Verbindungen

- ❖ Fiberglas, Kupfer, Radio, Satellit
- ❖ Übertragungsrate =
Bandbreite

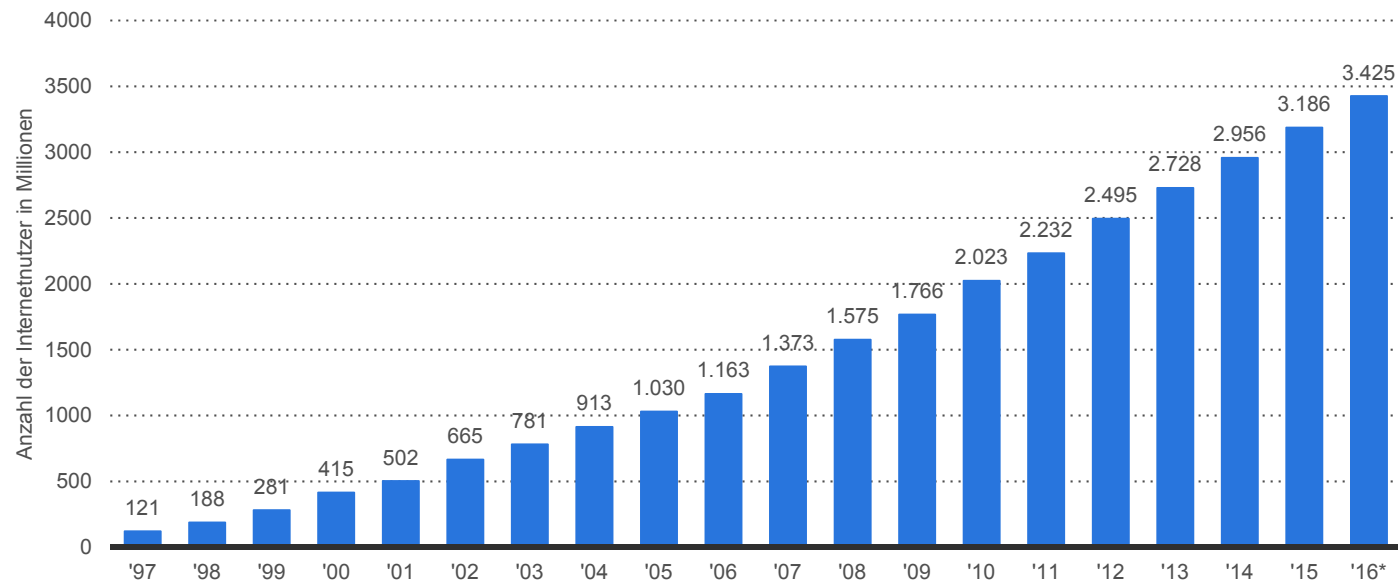


Router

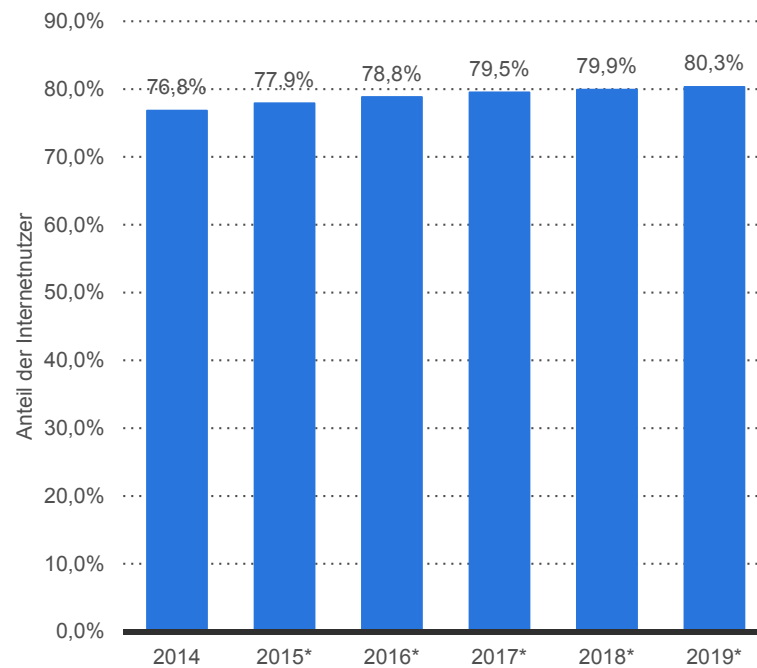
□ *Router*: Weiterleitung von
Paketen (Informations-
/Datenmengen)



© Kurose/Ross 2009



© Statista 2016, Internet live stats



© Statista 2016, Internet live stats

Internetanwendungen

Typische Anwendungen im Internet:

- Kommunikation
E-Mail, Telefonie (VoIP), Messaging, Videokonferenzen, ...
- Information
WWW, soziale Netze, Video-Streaming, Bewertungsportale, ...
- Nutzung externer Ressourcen
Datenspeicherung (in der Cloud), Remote Login, Dateitransfer, ...
- Geschäftsmodelle
Online-Shops, Buchungsportale, Auktionen, Call Center, ...
- Steuerung und Überwachung
Home Automation, Fernwartung, Anlagensteuerung, ...
- Verteilte Arbeitsprozesse
Heimarbeit, virtuelle Büros,

Internetanwendungen

Zukünftige Anwendungen:

- e-Health
Telemedizin, Gesundheitsüberwachung,
- Smart Cities
personalisierte und lokalisierte Dienste, ...
- Internet der Dinge
individualisierte Produktion und Lieferung, ...
-

Prognosen sind schwierig, besonders wenn sie die Zukunft betreffen
(Mark Twain oder Niels Bohr oder Karl Valentin ...)

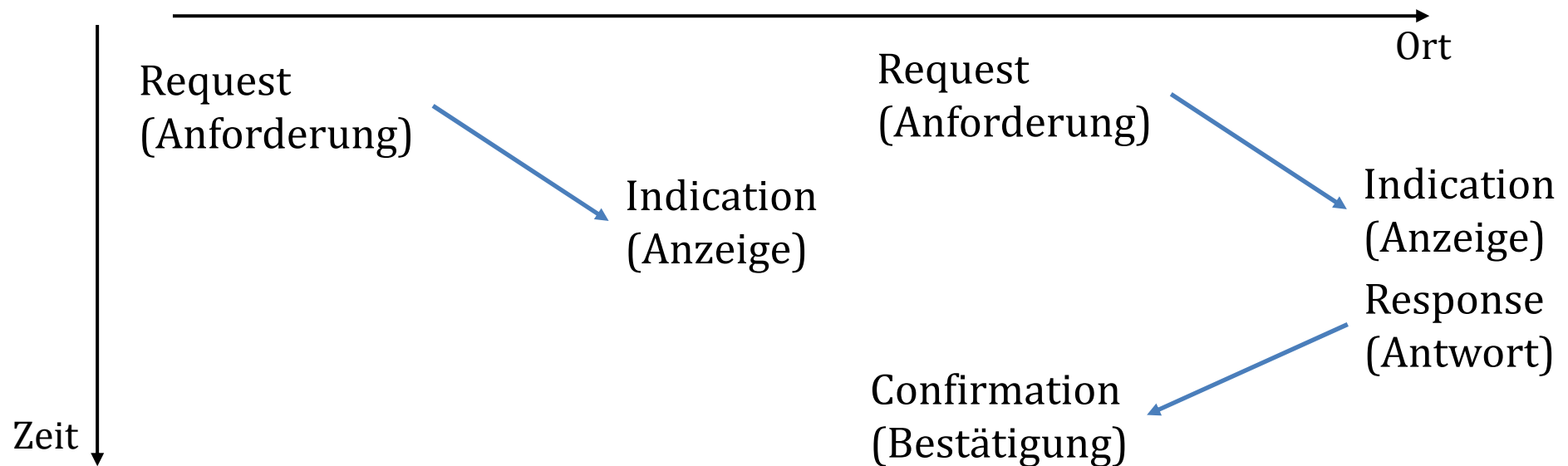
Dienste

Zentraler Idee zur Nutzung von Ressourcen in Rechnernetzen:

➤ Anbieten und aufrufen von Diensten

Dienstnehmer (Initiator) ruft einen Dienst auf, der von Dienstanbieter bereit gestellt wird

Man unterscheidet unbestätigte und bestätigte Dienste



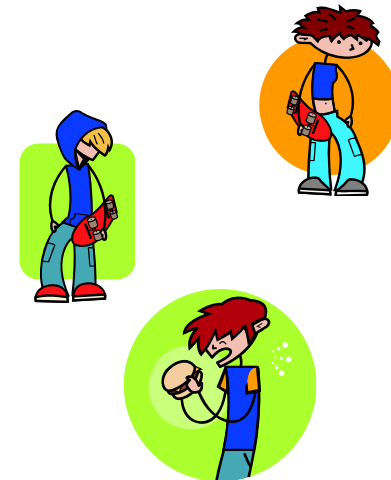
Kommunikationsdienste

Kommunikationsformen

Unicast (2 Partner)



Broadcast (an alle)



Multicast (an eine Gruppe)



Kommunikationsdienste

Kommunikation ohne Kontext

Dienst enthält alle benötigten Informationen

z.B. Brief, Telegramm, UDP-Datagramm



Kommunikation im Kontext

Verbindung wird aufgebaut,
Kommunikation entlang der Verbindung,
Verbindung wird abgebaut

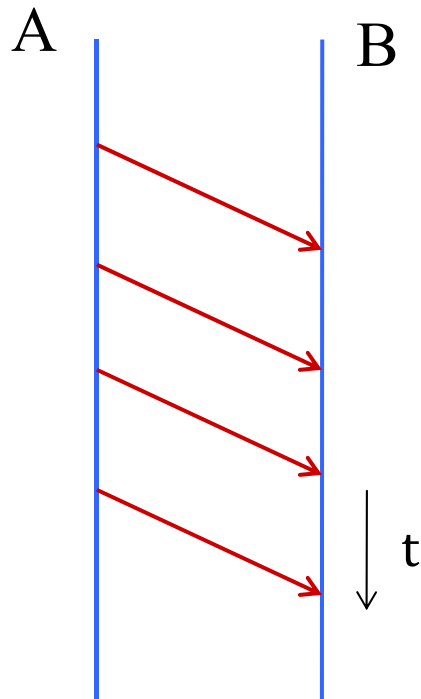
z.B. Telefon, TCP-Verbindung



Kommunikationsdienste

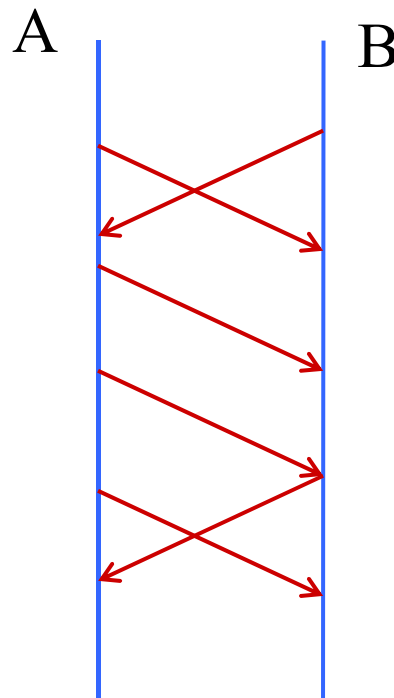
Richtungsbetrieb

simplex



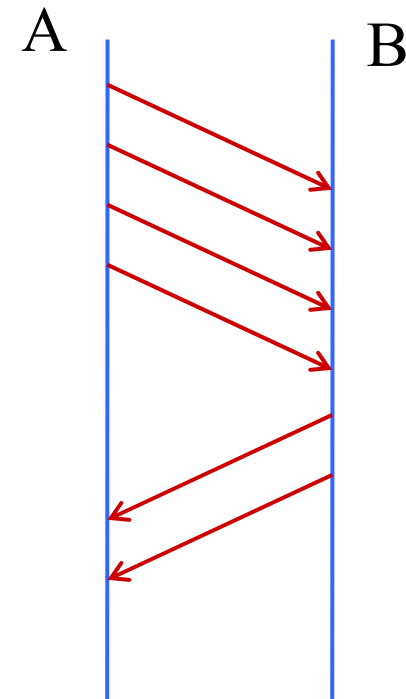
Z.B. Feuermelder,
Sensoren

duplex



Z.B. Telefon

halbduplex



Z.B. Wechselsprech-
anlage

Dienstleistende Systeme

➤ Instanzen:

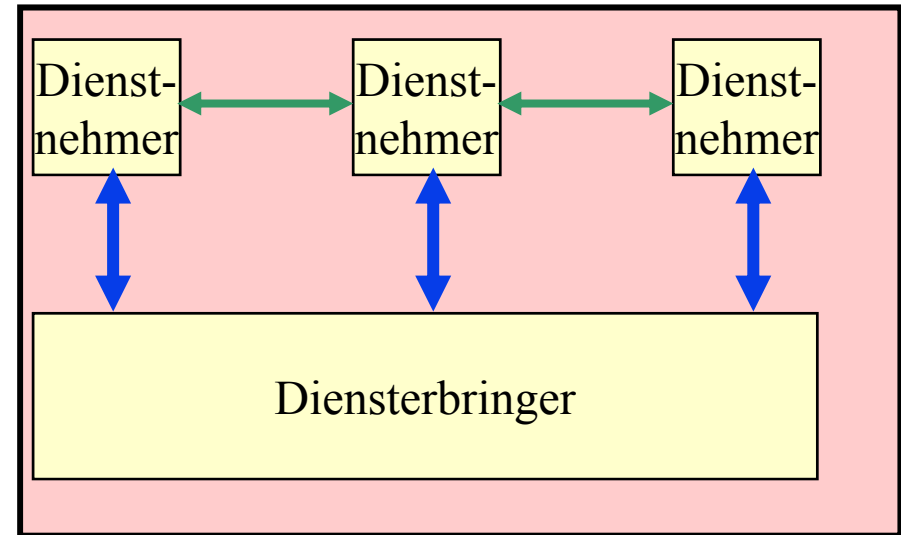
- Menge von Dienstnehmern
- Dienstbringer (offenes Subsystem)

➤ Kommunikation:

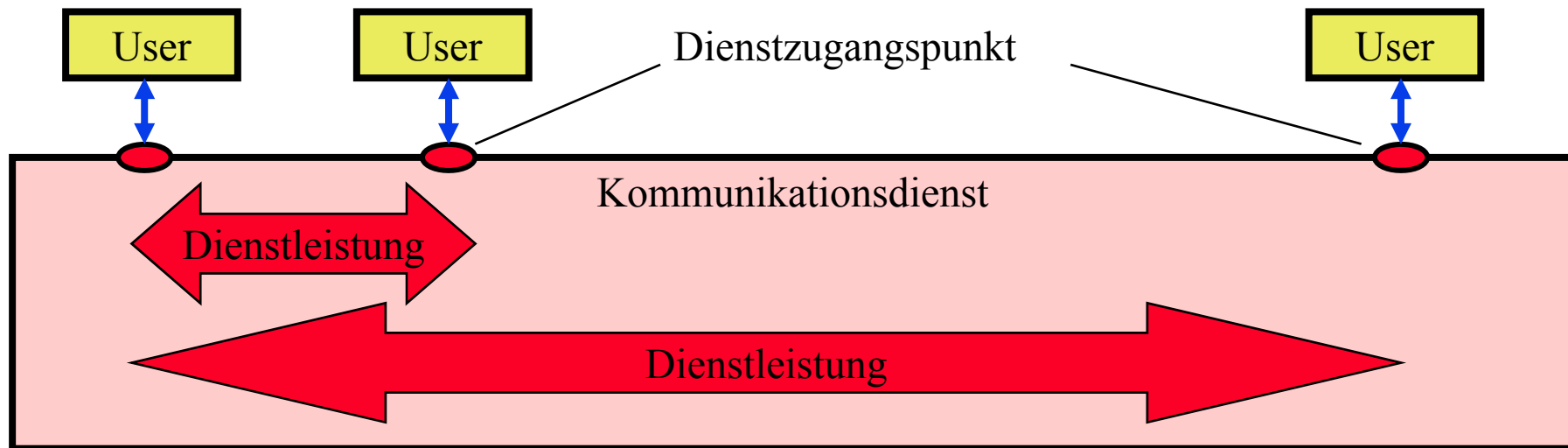
- vertikale Kommunikation
 - » Abwicklung von Dienstleistungen
- horizontale Kommunikation
 - » zwischen Dienstnehmern

➤ Kommunikationssysteme:

- in der Zeit Datenhaltungssystem
- im Raum Telekommunikationssystem
 - » Dienstleistungen dienen dem Nachrichtenaustausch zwischen Dienstnehmern
 - » Dienstbringer interpretiert Nachrichten nicht



Kommunikationsdienste



Ein Kommunikationsdienst bietet Teilnehmern Dienstleistungen zum Nachrichtenaustausch an. Wichtige Eigenschaften der Dienstleistungen betreffen:

- Partneradressierung
- Datagramme (verbindungslose Kommunikation, z.B. UDP)
- Verbindungsorientierung: Verbindungen und virtuelle Verbindungen (z.B. TCP)
- Zwei- / Mehrpartner-Kommunikation (Uni- / Multi- / Broadcast)
- Richtung (Simplex, Duplex, Halbduplex)

Kommunikationsdienst - Sichten

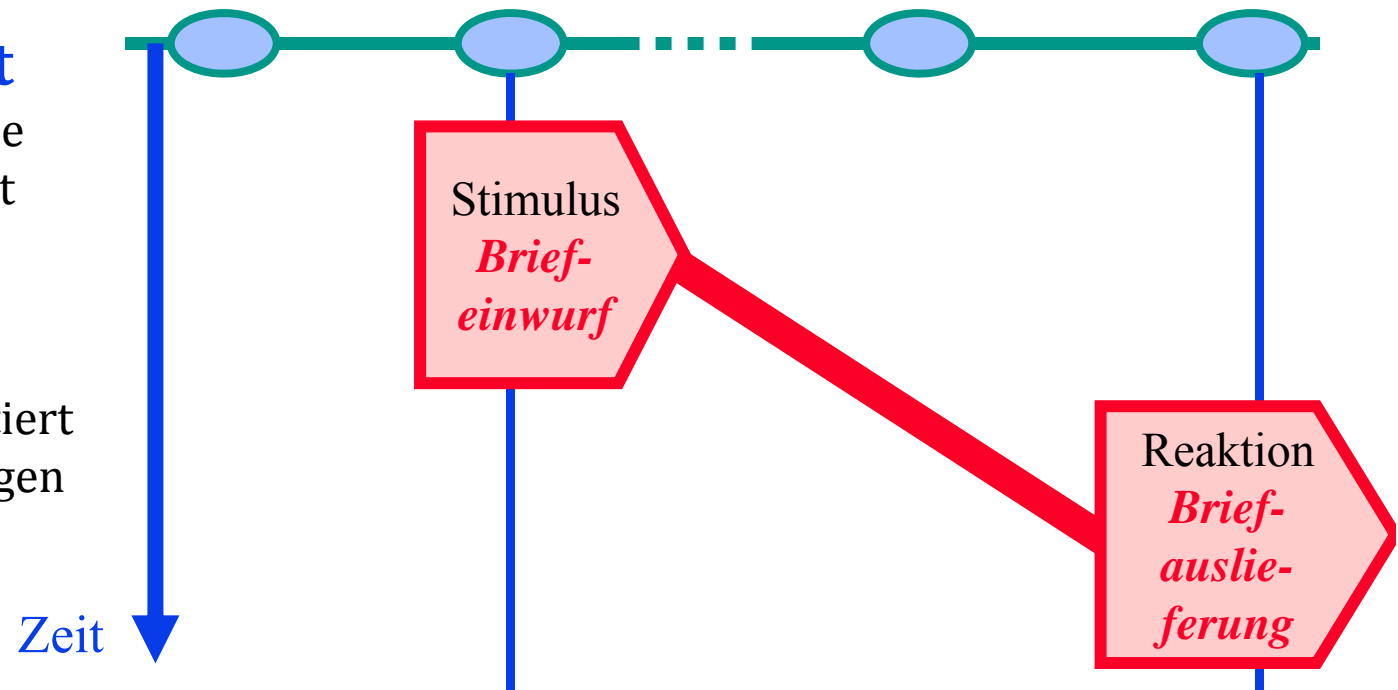
Statische Sicht

Die Dienstschnittstelle, ist gegliedert in Dienstzugangspunkte, welchen Dienstadressen zugeordnet sind.

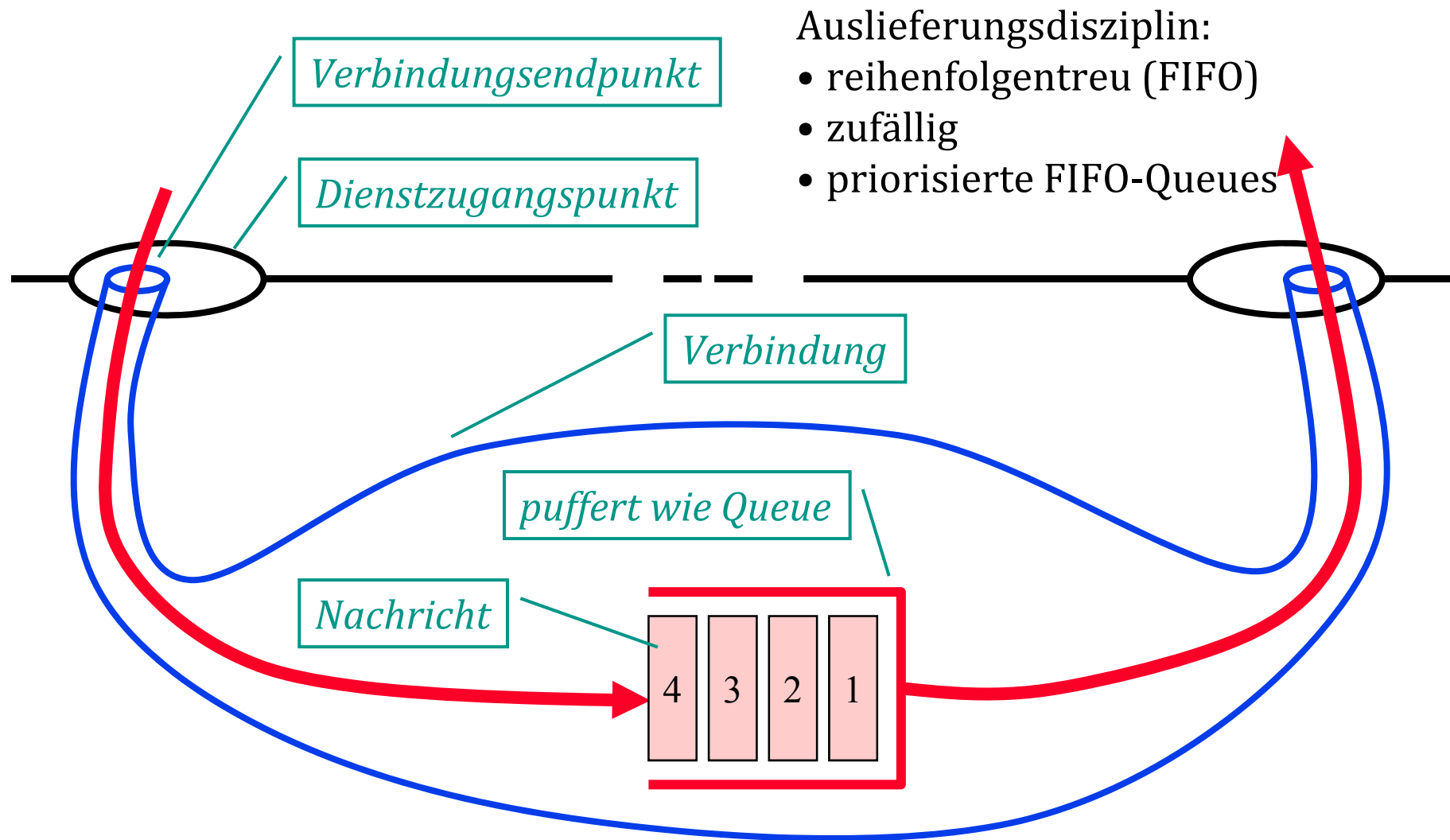


Dynamische Sicht

An der Dienstschnittstelle treten im Verlauf der Zeit Ereignisse auf:
Die Anforderung und Ausführung einer Dienstleistung repräsentiert sich in zusammengehörigen Dienststimuli und Dienstreaktionen

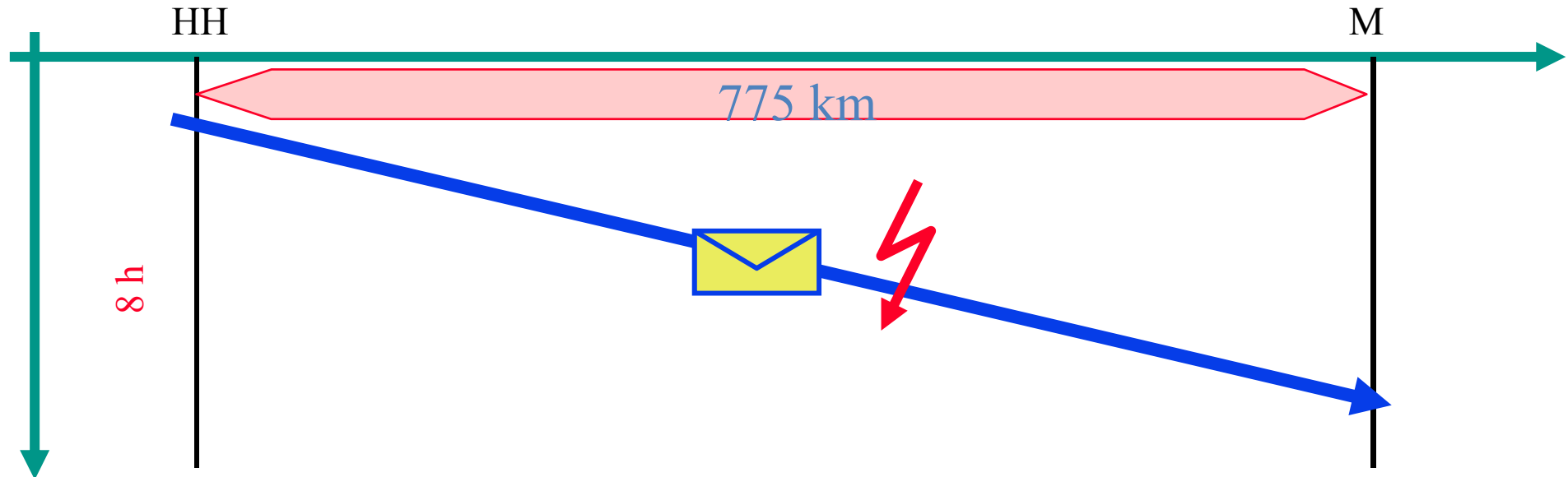


Kommunikationsdienst: Nachrichtenreihenfolge



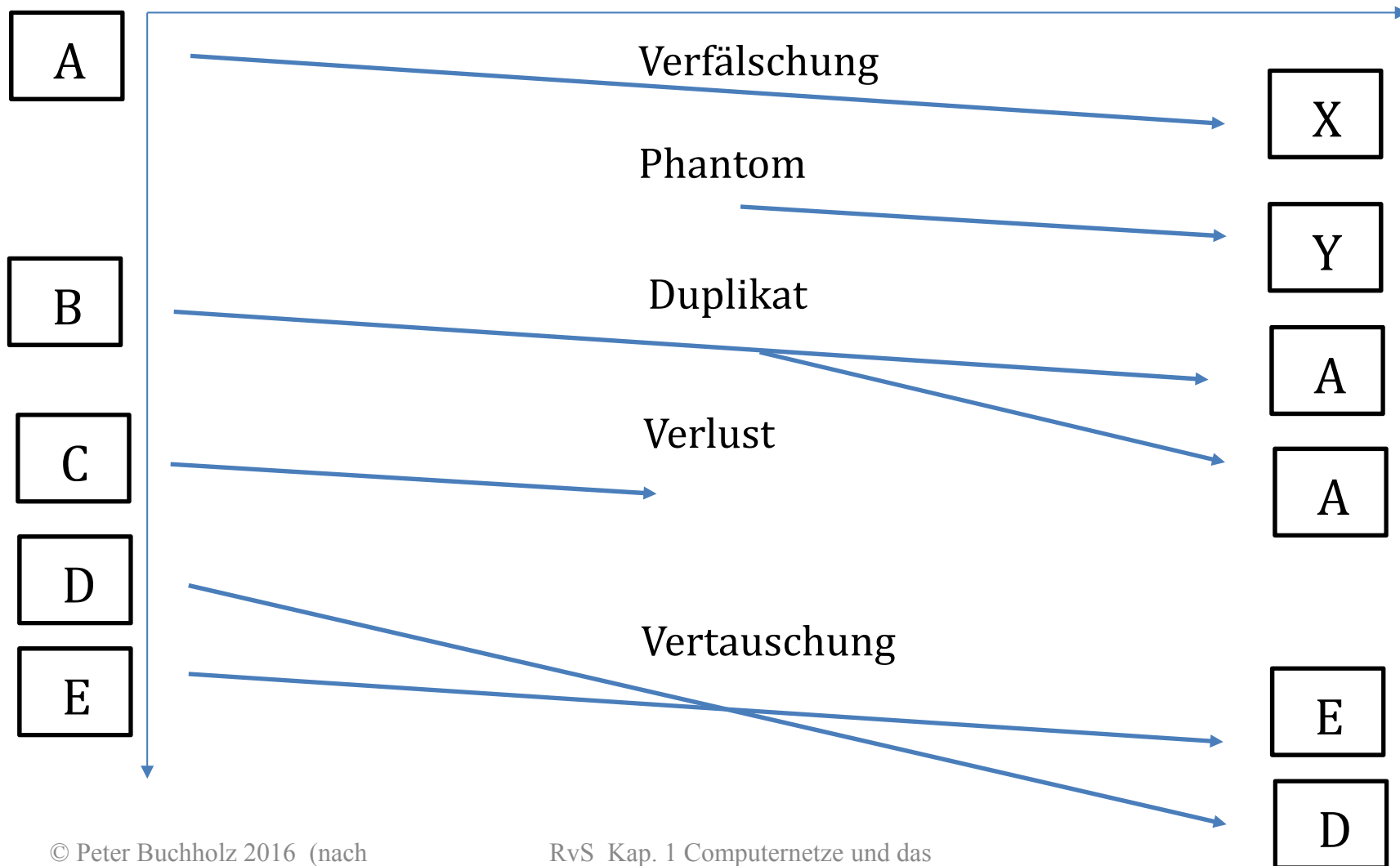
Kommunikationsdienst: Qualität

- Leistung
 - *Nachrichtenlaufzeit, Verzögerung*
 - *Durchsatz (Bandbreite, Bitrate)*
 - *Entfernung*
- Zuverlässigkeit
 - *Verfügbarkeit*
 - *Fehler*
 - *Verlust, Verfälschung, Vertauschung, ...*
- Kosten
 - *Grundkosten*
 - *Dienstleistungskosten*
- Datensicherheit
 - *Verfälschung / Integrität*
 - *Vertraulichkeit*
 - *Zurechenbarkeit*
 - *...*



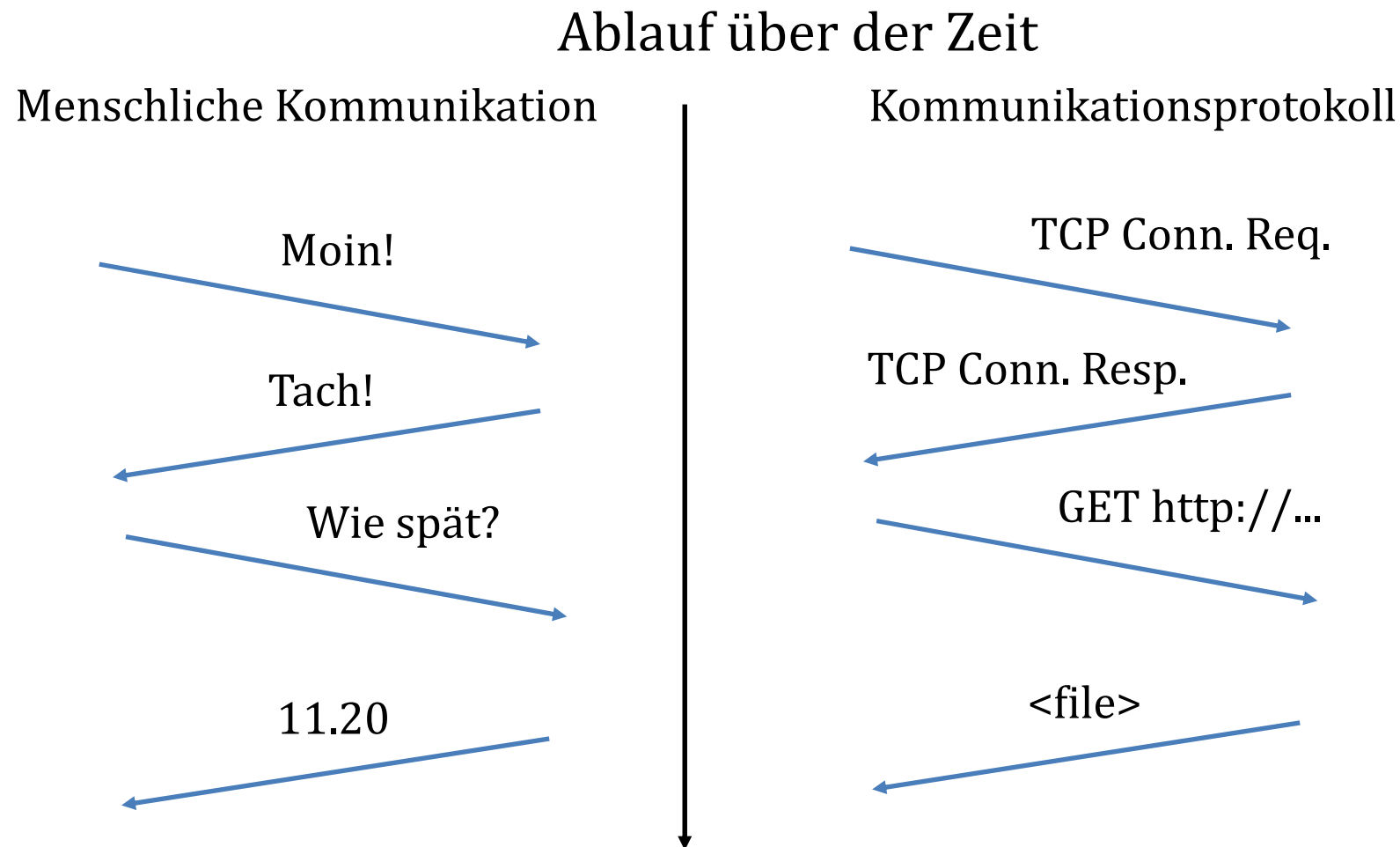
Kommunikationsdienst: Zuverlässigkeit/Fehler/Störung

Fehlerklassen bei der Kommunikation

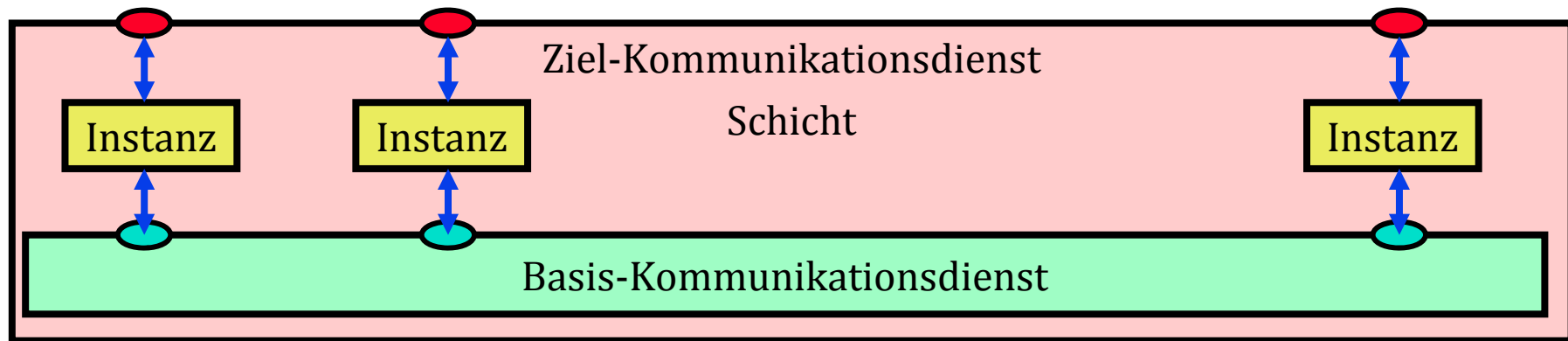


Kommunikationsprotokoll

Regeln zur Kommunikation !



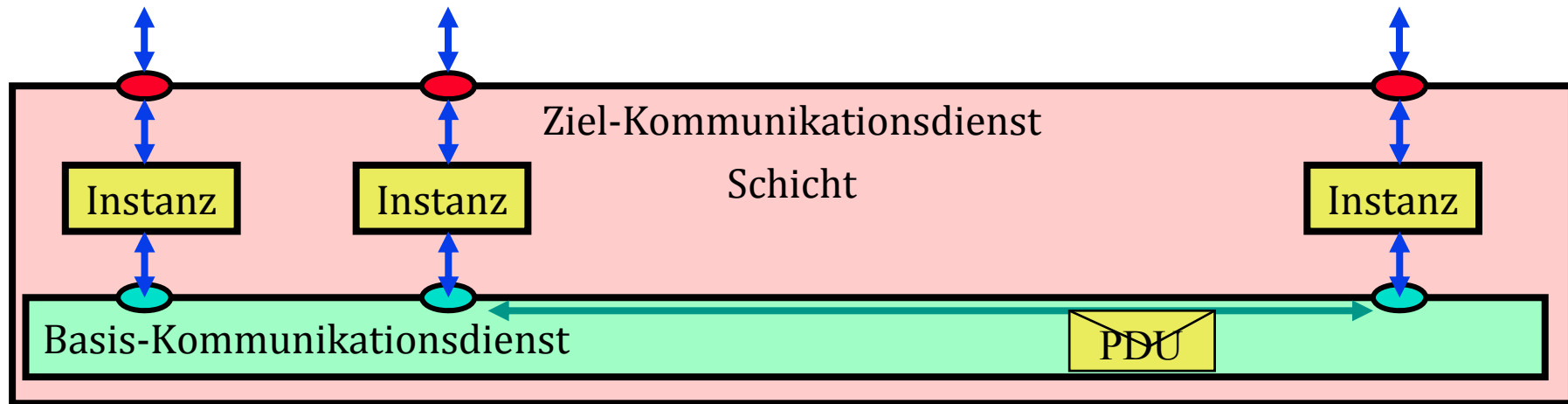
Kommunikationsprotokolle



Definition

- Ein Protokoll ist eine Menge von Regeln und Formaten (semantisch und syntaktisch), die das Kommunikationsverhalten von Instanzen zur Ausführung von Funktionen regelt (ISO 7498)
- Alle Kommunikationsaktivitäten im Internet werden von Protokollen bestimmt
- Protokollstandards ermöglichen die Offenheit des Internets für Komponenten unterschiedlicher Bauart

Kommunikationsprotokolle



Ein Kommunikationsprotokoll definiert das Kommunikationsverhalten von Instanzen, welche einen Basis-Kommunikationsdienst nutzen, um einen (höherwertigen) Ziel-Kommunikationsdienst zu erbringen. Es wird definiert über:

- Zieldienst
- Basisdienst
- Instanzenverhalten
- PDU-Formate

Kommunikationsprotokolle

Kommunikation kann nur funktionieren, wenn man die Regeln festlegt und sich daran hält, auch in heterogenen Systemen (\Rightarrow Festlegung/Definition eines Protokolls)

- Proprietäre Protokolle

Kommunikation in homogenen Systemen

Schnittstellen müssen nicht offen gelegt werden

- De-facto Standards

Industriestandards, die durch vielfache Nutzung zu Standards werden

Schnittstellen müssen offen gelegt werden

- Offizielle Standards

durch internationale Standardisierungsorganisation festgelegt

Schichtung von Diensten & Protokollen

Schicht 3:

- erbrachter Dienst
- Instanzen und Protokoll der Schicht

Schicht 2:

- erbrachter Dienst
- Instanzen und Protokoll der Schicht

Schicht 1:

- erbrachter Dienst
- Instanzen und Protokoll der Schicht

Basisdienst – Medium (Schicht 0)

Schichtenmodelle

➤ ISO/OSI

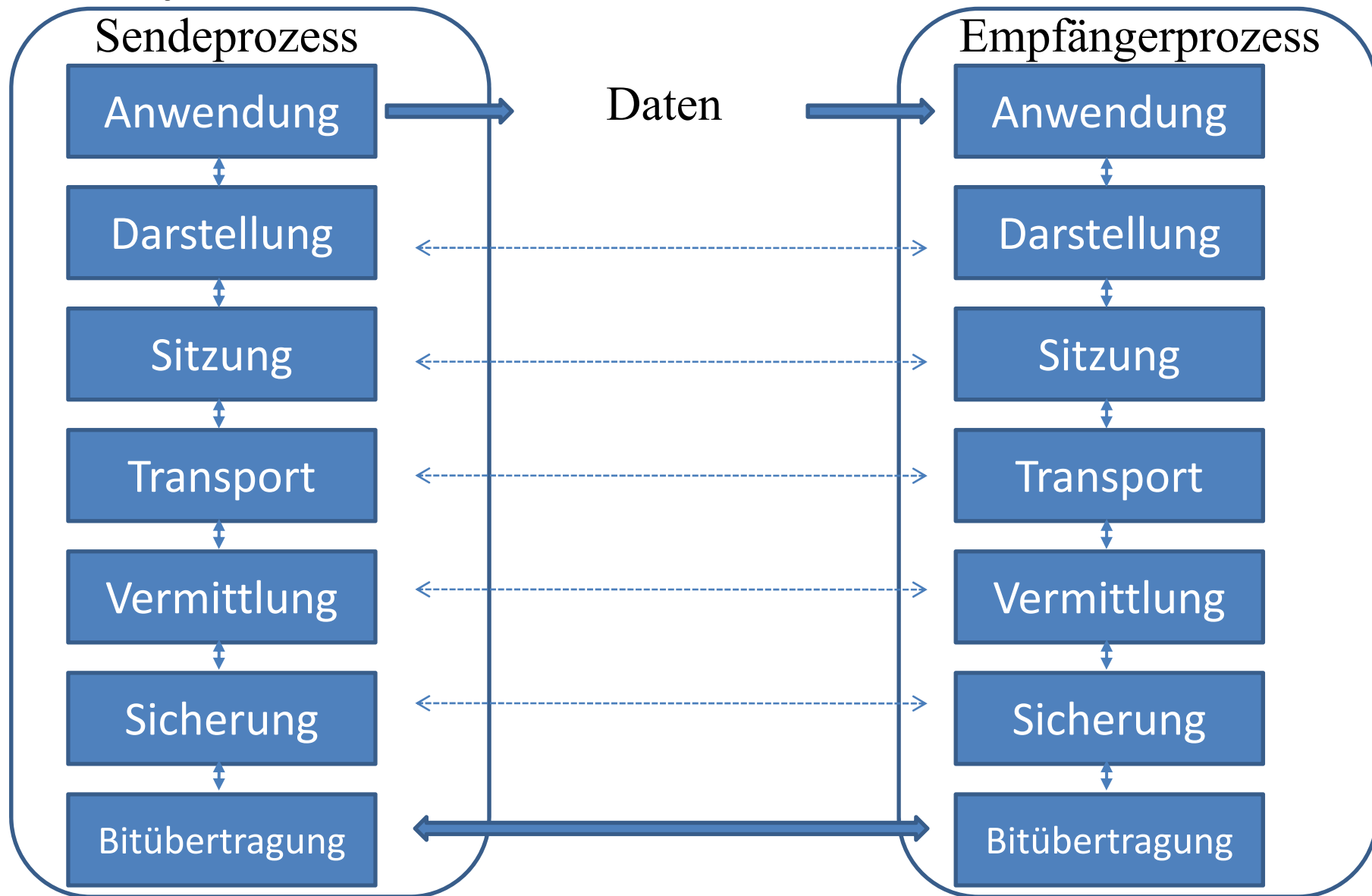
- Kommunikation Offener Systeme – Basis-Referenzmodell
- allgemeines Modell, das sich auf die logische Architektur konzentriert
(Welche Funktionen können in welchem Zusammenhang in einer Kommunikation auftreten?)
- (ISO 7498)

➤ TCP/IP

- Internet-Protokollstack
- Für (beinahe) alle Systeme implementiert.
- (RFCs, IEEE-Normen)



ISO/OSI-Schichtenmodell



ISO/OSI-Schichtenmodell

- **Anwendungsschicht (Application Layer)**
 - höchste Ebene, stellt die Kommunikationsdienstleistungen bereit, die direkt von einer Anwendung benötigt werden
 - Beispiel: „**Übertrage das Kommando eine Datei zu öffnen**“
- **Darstellungsschicht (Presentation Layer)**
 - reicht die Dienstleistungen des Session-Dienstes weiter.
 - stellt Dienstleistungen bereit, mit denen sich Anwendungsprozesse über das Format der Nachrichten abstimmen können.
- **Kommunikationssteuerungsschicht (Session Layer)**
 - bietet Dienstleistungen an, die zur Eröffnung, Durchführung und Beendigung einer Kommunikationsbeziehung (Session) nötig sind.
 - Dienstleistungen zur Realisierung anwendungsnaher Fehlerbehandlungsmaßnahmen: **Synchronisation, Wiederaufsetzen, Stornieren, Unterbrechen, Wiederaufnehmen**

ISO/OSI-Schichtenmodell

◆ Transportschicht (Transport Layer)

- erweitert Endsystemverbindungen (Rechner–Rechner) zu Anwenderverbindungen (Anwender–Anwender)
- Anwender = Anwendungsprozesse
- behandelt Ende-zu-Ende-Qualitätsaspekte

} bildet
Trans-
port-
system

◆ Vermittlungsschicht (Network Layer)

- unterstützt beliebige Konnektivität im Netz

} bildet
Daten-
netz

◆ Sicherungsschicht (Data Link Layer)

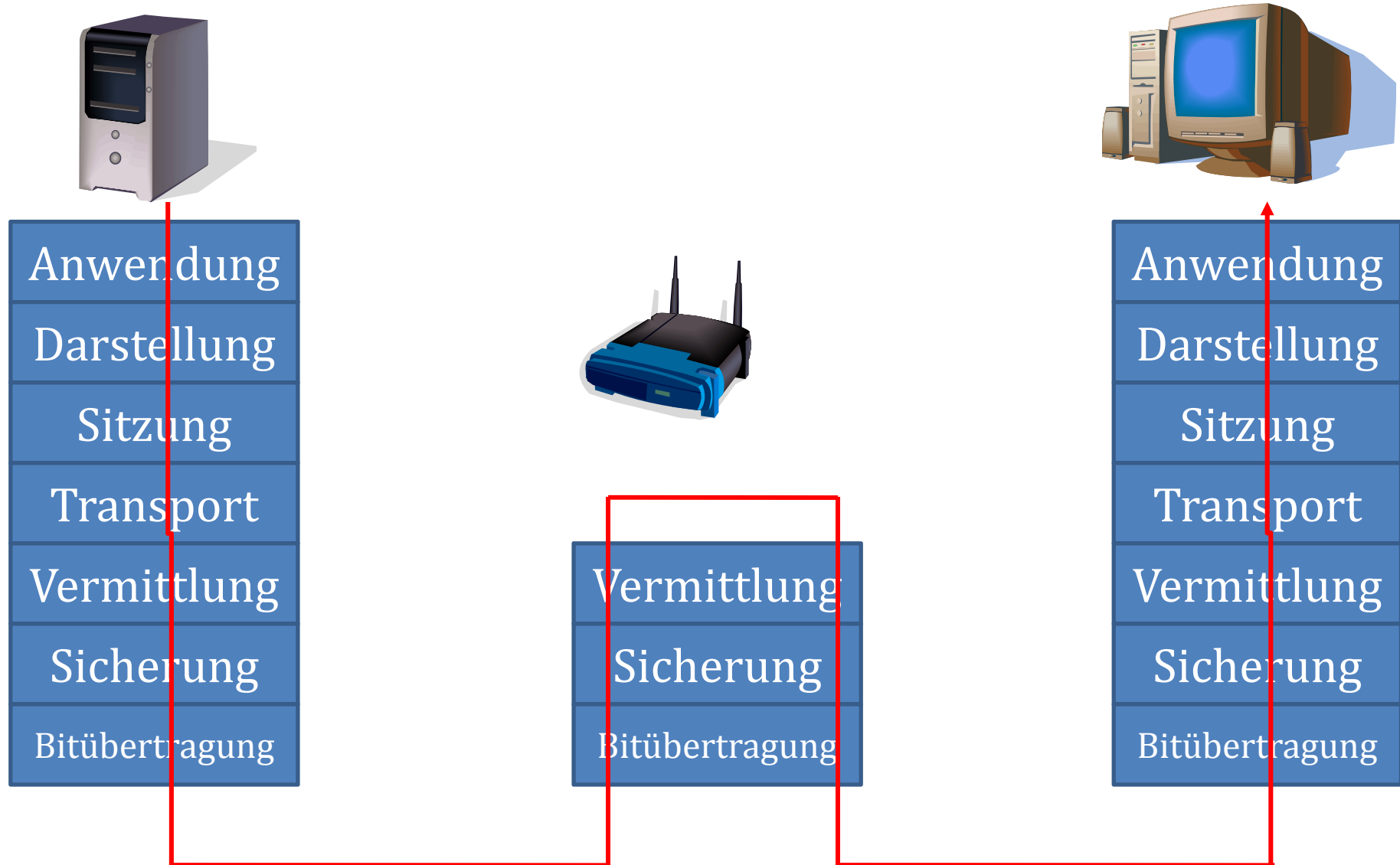
- stellt zuverlässige Links zur Verfügung
- Flusskontrolle, Fehlererkennung und -korrektur

◆ Bitübertragungsschicht (Physical Layer)

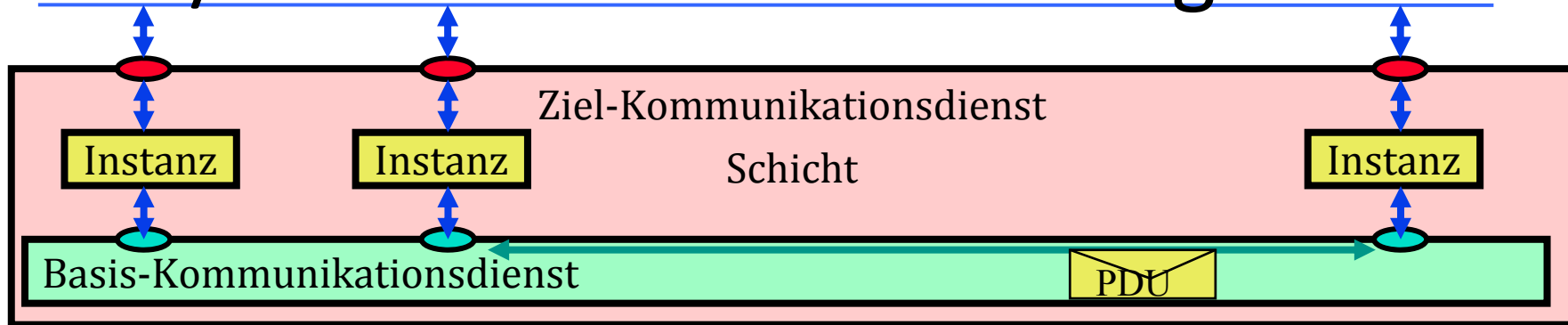
- stellt ungesicherte Links für die Übertragung von Bitfolgen zur Verfügung.

} je Link

ISO/OSI-Schichtenmodell



ISO/OSI-Schichtenmodell: Begriffe



(N)-Schicht *(N)-layer*

Alle Instanzen einer Hierarchie-Ebene (*peer-entities*). Diese kommunizieren über den Basiskommunikationsdienst (N-1)-Dienst und erbringen den Zielkommunikationsdienst (N)-Dienst.

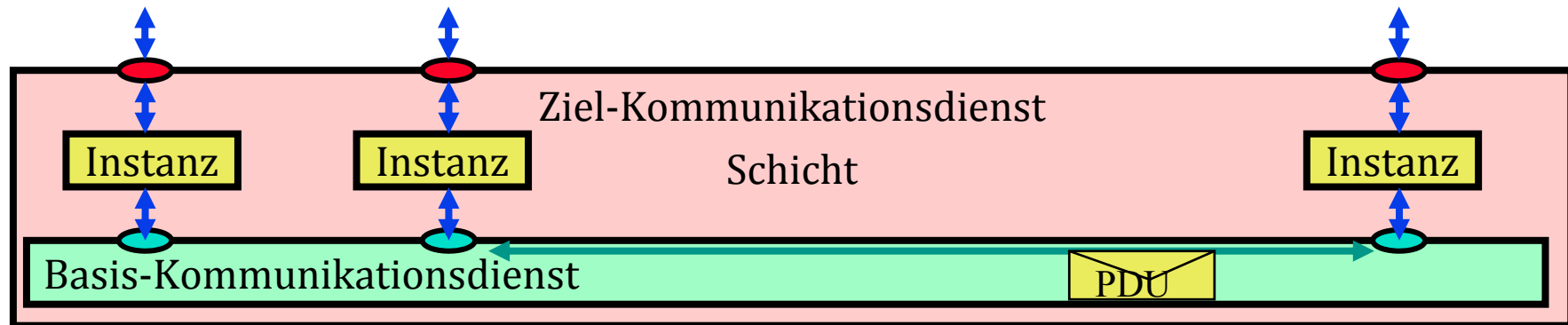
(N)-Dienst *(N)-service*

Fähigkeit der (N)-Schicht (und der Schichten darunter), die der (N+1)-Schicht an der Grenze zwischen (N)-Schicht und (N+1)-Schicht zur Verfügung gestellt wird.

(N)-Protokoll *(N)-protocol*

Verhaltens- und Formatfestlegungen (semantisch und syntaktisch) zum Kommunikationsverhalten der (N)-Instanzen.

ISO/OSI-Schichtenmodell: Begriffe



(N)-Dienstzugangspunkt *(N)-service-access-point*

Punkt, an dem der (N)-Dienst den (N+1)-Instanzen (oder Nutzern) zur Verfügung gestellt wird.

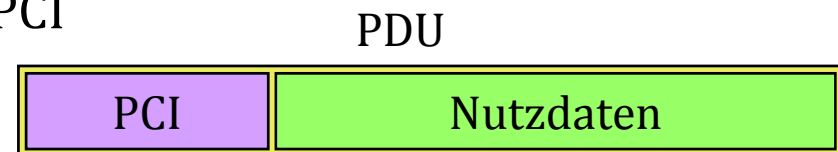
(N)-Adresse *(N)-address*

Kennung, zur Identifikation eines (N)-Dienstzugangspunkts.

(N)-Protokolldateneinheit *(N)-PDU (N)-protocol data unit*

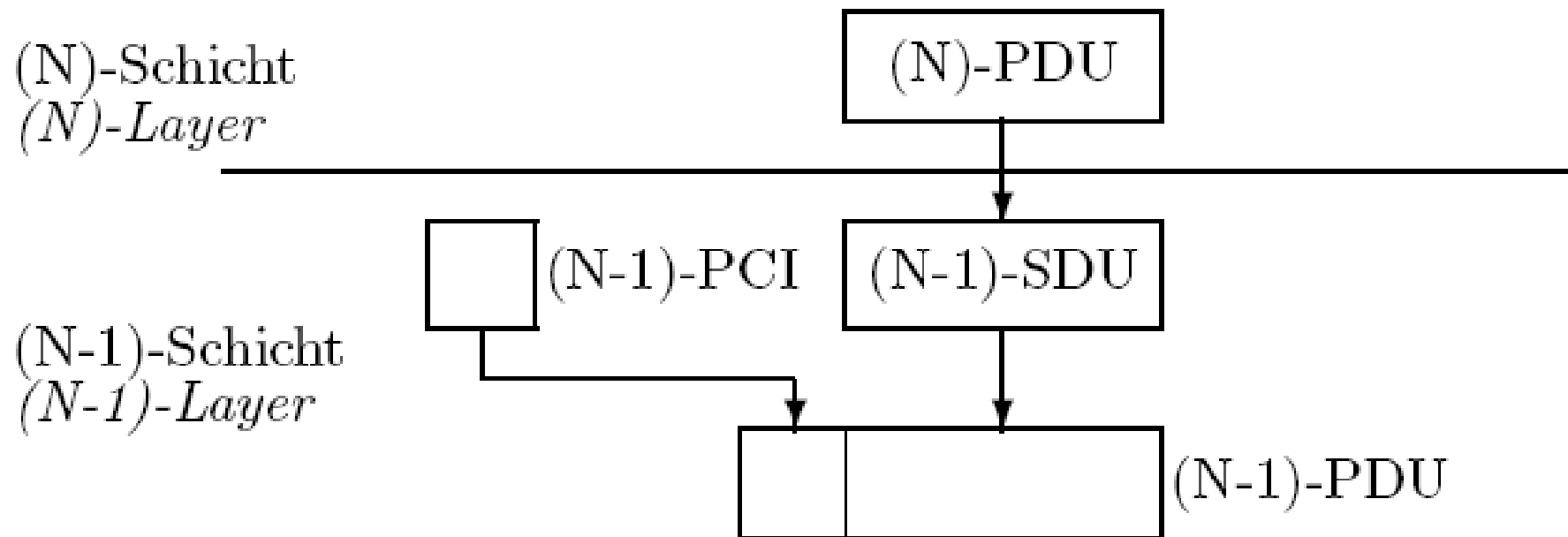
Nachricht, welche (N)-Instanz gemäß (N)-Protokoll einer anderen (N)-Instanz sendet, besteht aus

- (N)-Protokollkontrollinformation: (N)-PCI
- Nutzdaten der (N+1)-Instanzen



ISO/OSI-Schichtenmodell

Dateneinheiten

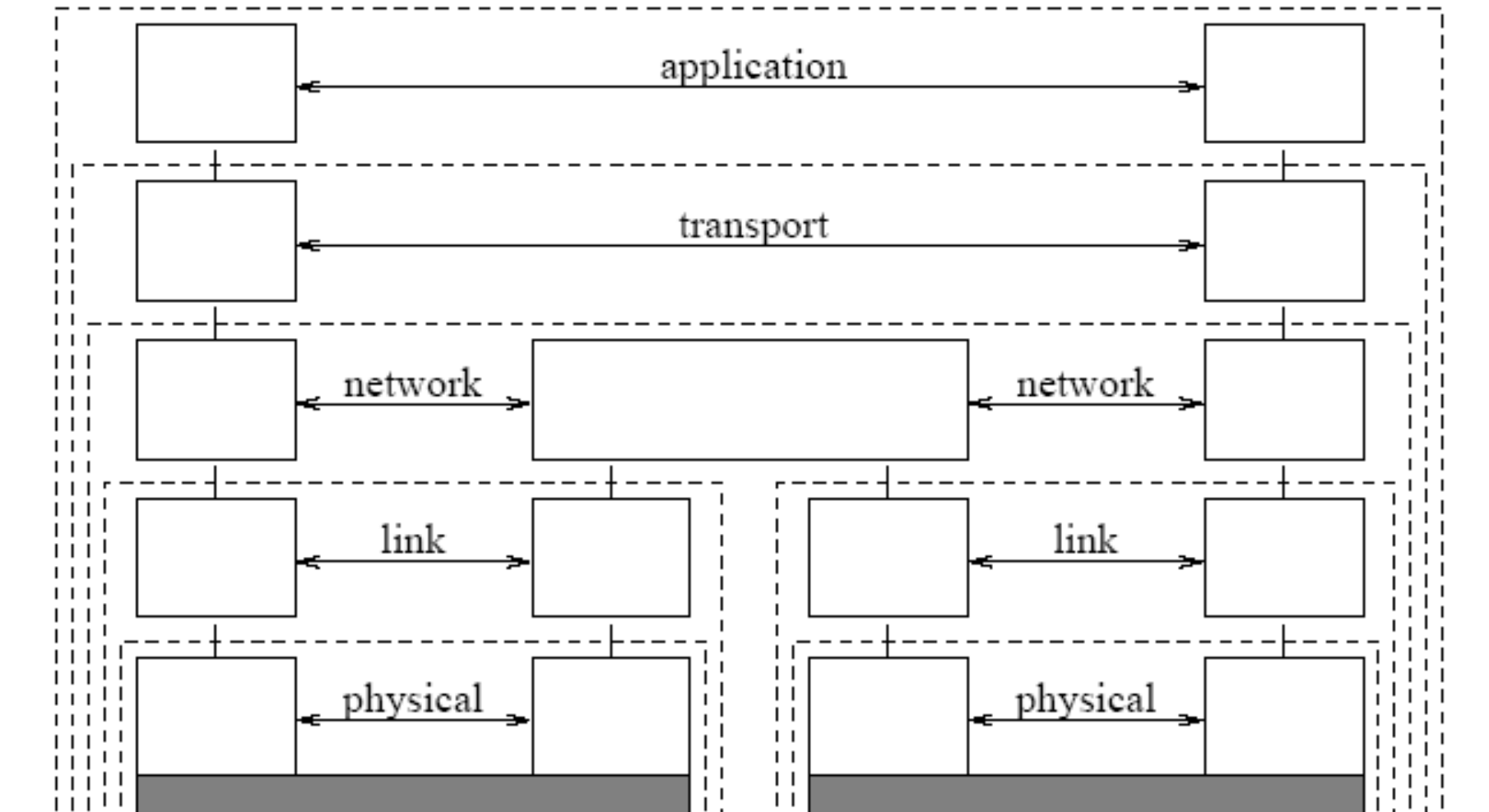


PDU Protokolldateneinheit (*protocol-data-unit*)

SDU Dienstdatenheinheit (*service-data-unit*)

PCI Protokollkontrollinformation (*protocol-control-information*)

TCP/IP Protokollstapel (Protocol Stack)



TCP/IP Protokollstapel

application layer

- unterstützt verteilte Applikationen (*umfasst die ISO/OSI-Schichten 5, 6 und 7*)
- Anwendungsprotokolle FTP, SMTP, HTTP, SNMP, DNS, ...

transport layer

- Datenübertragung von Anwendung zu Anwendung (Port zu Port)
- Transportprotokolle TCP, UDP

network layer

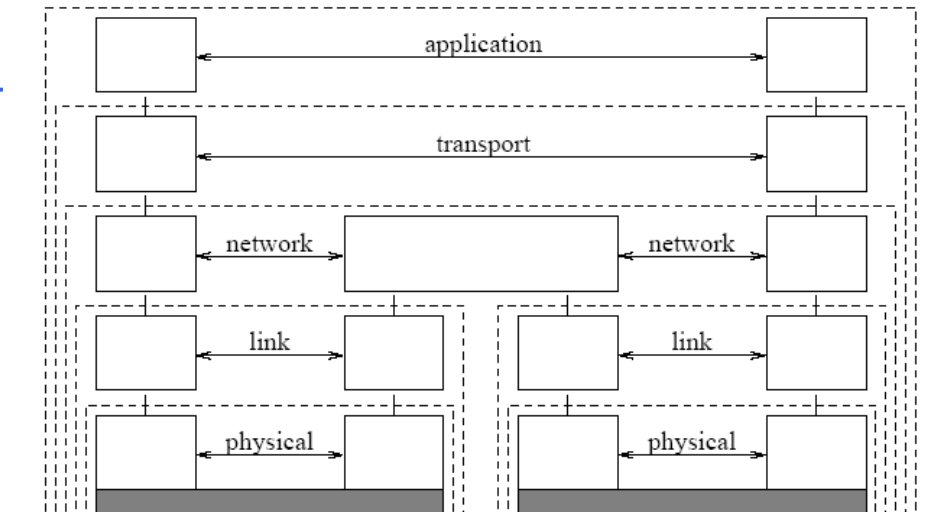
- transportiert (routet) Datagramme von Endsystem zu Endsystem
- Internet-Protokoll IP, Routing-Protokolle

data link layer

- Datentransfer zwischen benachbarten Systemen
- PPP, Ethernet, ...

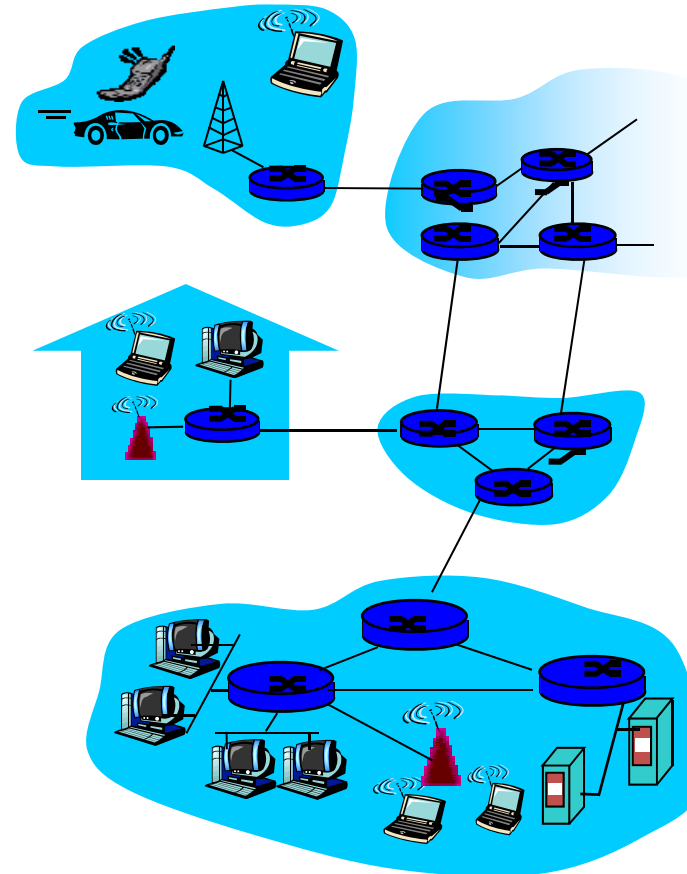
physical layer

- Bitübertragung auf der Leitung oder im Funkkanal
- RS-232, Ethernet, ...



Struktur des Internets

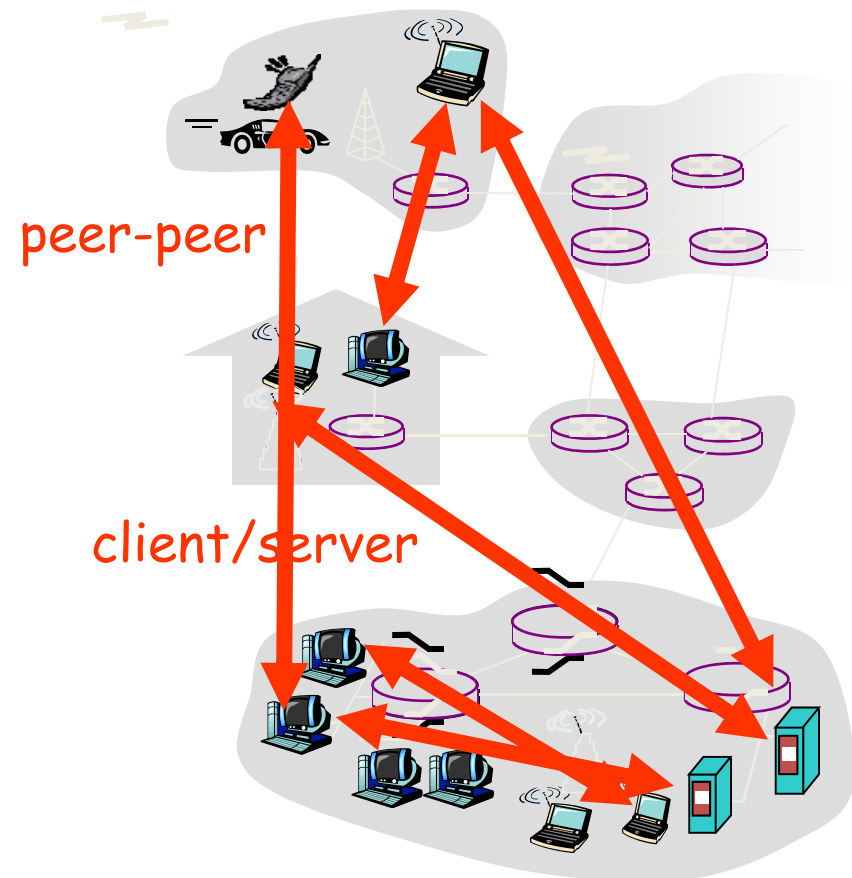
- Netz-Peripherie:
End-Systeme
(PCs, Server, ..)
- Übertragungsmedien:
drahtgebunden oder
drahtlose Verbindungen
- Kernnetz:
 - Verbundene Router
 - Netz von Netzen
(Subnetze, Teilnetze)



© Kurose/Ross 2009

Internet - Peripherie

- End-Systeme (Hosts)
 - beherbergen Applikationen und Server-Programme
 - sind Endpunkte der Verbindung
 - z.B. Mail, Web-Browser
- Client-Server-Modell
 - Client stellt Anfragen und erhält Service
 - Server ist "immer" verfügbar
 - Mail Client/Server, Web-Browser/Server
- Peer-To-Peer-Modell
 - keine dedizierten Server
 - z. B. Skype, BitTorrent



© Kurose/Ross 2009

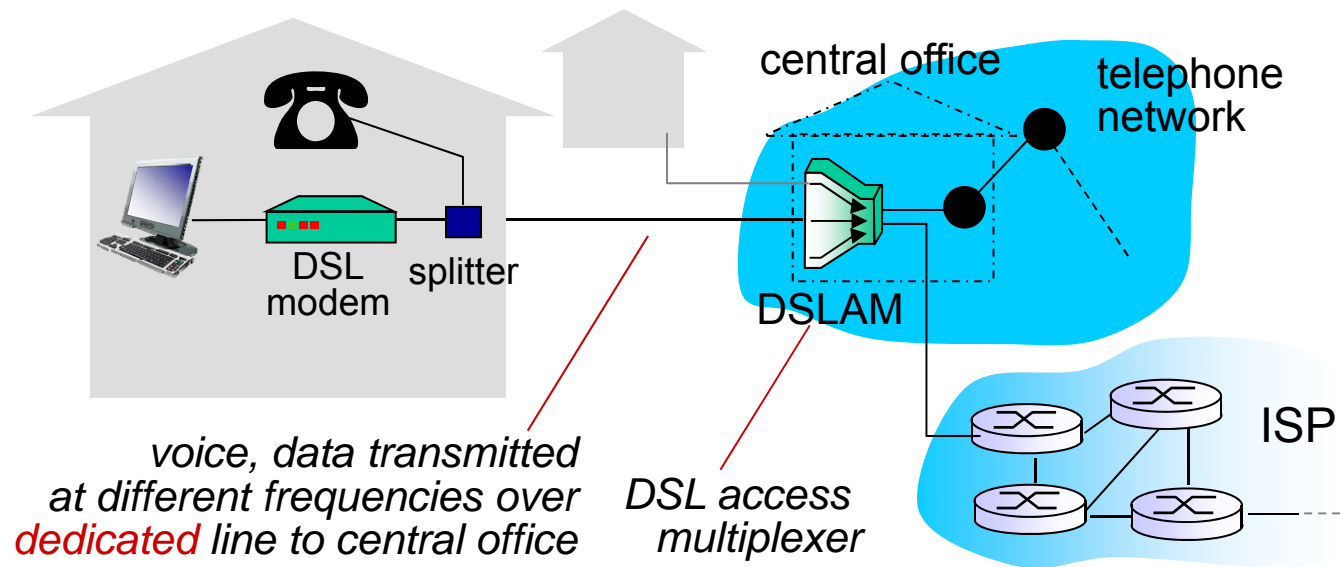
Physikalische Übertragung

Basis jeder Kommunikation:
Physikalische Datenübertragung
zwischen verbundenen Partner!

- Verdrillte Adernpaare (geschirmt, ungeschirmt)
- Koaxialkabel
- Glasfaser
- Funkkanäle (erdgebunden, Satelliten)

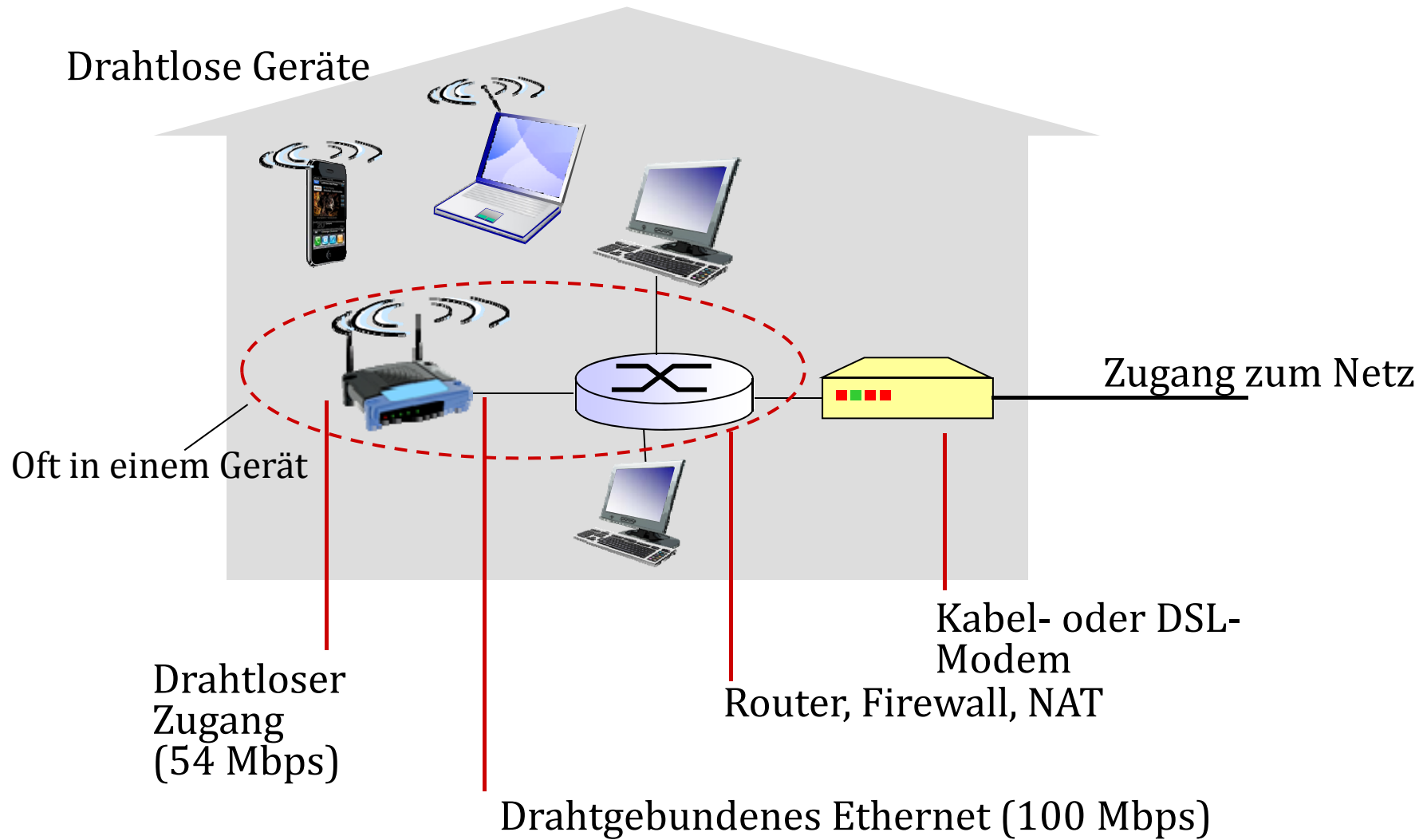


Zugangsnetz: digital subscriber line (DSL)



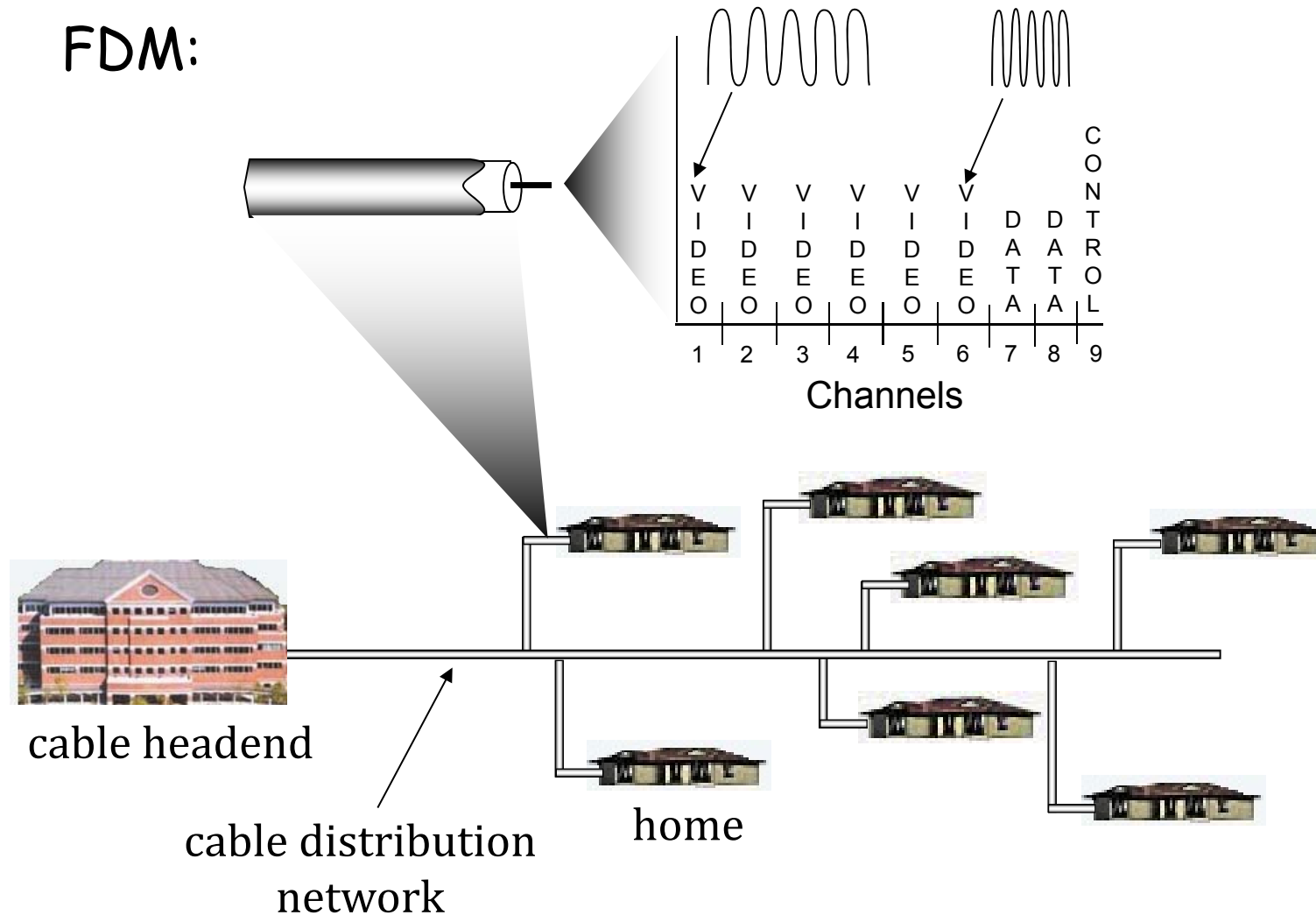
- Nutzung der vorhandenen Telefonleitung zur Datenübertragung zur zentralen Schaltstelle (DSLAM)
 - Daten werden zum Internet weitergeleitet
 - Sprache wird zum Telefonnetz weitergeleitet (bisher!)
- < 2.5 Mbps Übertragungsrate aufwärts (typisch < 1 Mbps)
- < 24 Mbps Übertragungsrate abwärts (typisch < 10 Mbps, VDSL < 50 Mbps)

Zugangsnetz im Haus



Struktur drahtgebundener Netzzugänge

FDM:



© Kurose/Ross 2009

Verbindungen im Netz

Geflecht von verbundenen Routern

Wie werden die Daten durch das Netz übertragen?

- Leitungsvermittlung
(circuit switching)
 - pro Verbindung eine Leitung (Telefonnetz)
- Paketvermittlung (packet switching)
 - Daten werden in einzelnen Paketen durch das Netz geschickt (Briefpost)

Leitungsvermittlung

Ressourcen für eine Verbindung werden von einem Ende bis zum anderen reserviert (End-to-End):

- Bandbreite, Vermittlungskapazität
- reservierte Ressourcen,
keine Nutzungskonkurrenz durch andere Verbindungen
- von der Leitung abhängige aber garantierte Leistung
- Zustand der Verbindung an jedem Transferknoten gespeichert

Multiplexing

Benutzung einer Verbindungsleitung durch mehrere Verbindungen

- Die Netz-Ressource (z. B. Bandbreite) wird aufgeteilt.
- Die "Teile" werden einzelnen Verbindungen zugeteilt.
- Keine Mitbenutzung unbenutzter "Teile" durch andere Verbindungen

Die Aufteilung der Bandbreite erfolgt durch

- Frequenzmultiplexing (frequency division)

oder

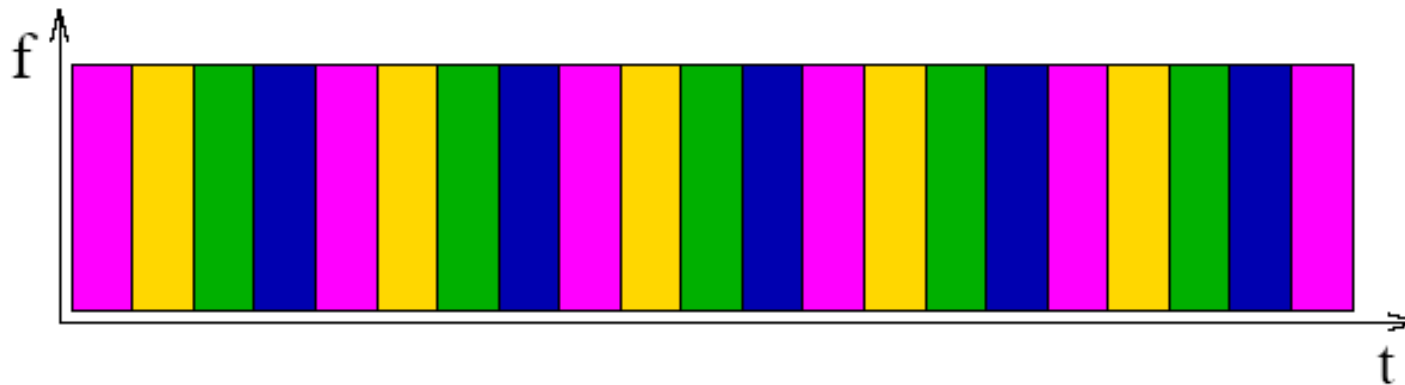
- Zeitmultiplexing (time division).

Multiplexing

Frequenzmultiplex



Zeitmultiplex



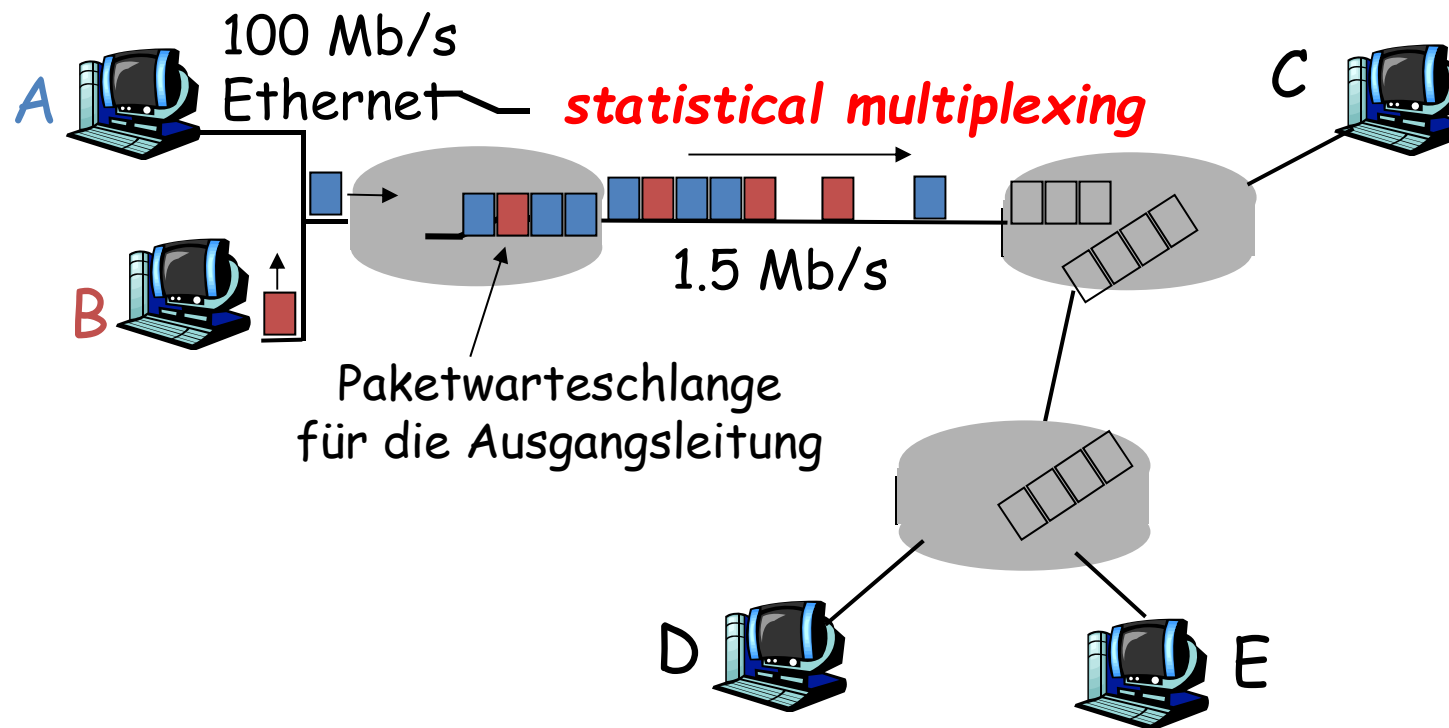
Paketvermittlung

Der Datenstrom wird in separat zu transportierende Pakete aufgeteilt.



- Mehrere Verbindungen teilen sich eine Leitung.
- Jedes Paket nutzt die volle Bandbreite.
- Die Ressourcen werden nach Bedarf genutzt.
- Keine garantierte Bandbreite für den Datenstrom.
 - Die Summe der benötigten Ressourcen kann die Summe der vorhandenen übersteigen.
- Pakete im Puffer warten auf freie Ressource (Store and Forward - Prinzip).

Paketvermittlung: Statistisches Multiplexen



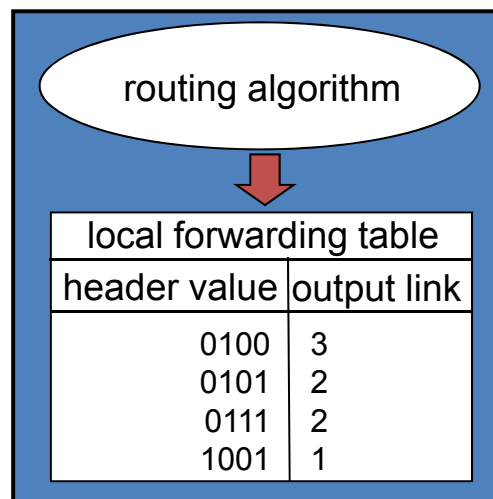
Sequenz von A & B Paketen, die zufällig eintreffen,
Bandbreite wird nach Bedarf verteilt
→ ***statistical multiplexing***.

TDM: jeder Host bekommt feste Slots zugeteilt.

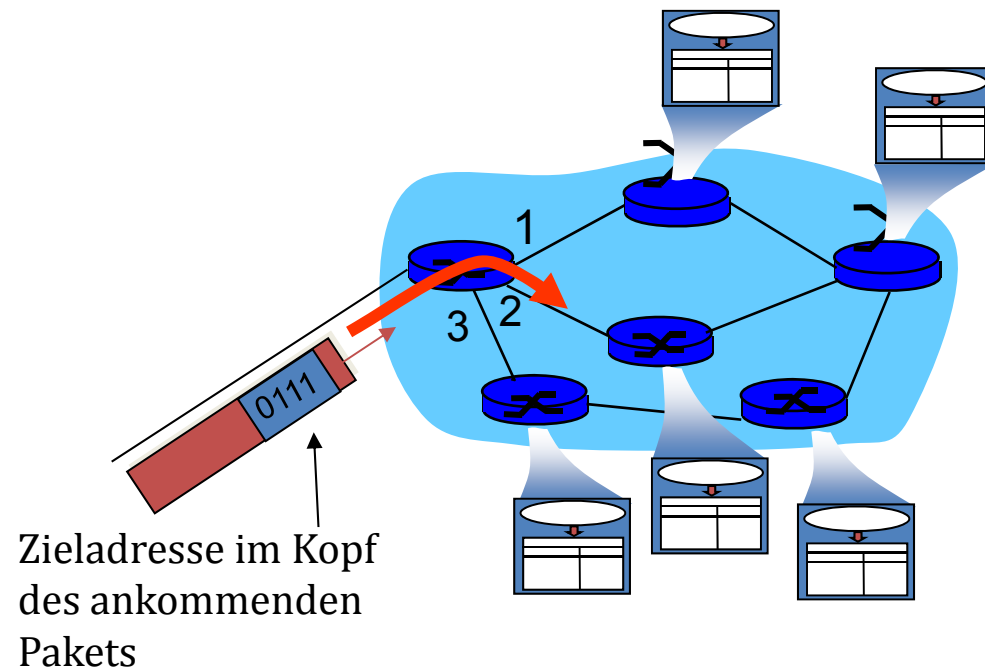
Funktionen des internen Netzes

Routing: Bestimmung der Route durch das Netz vom Start zum Ziel

- *Routing Algorithmus*



Weiterleitung: Schicke Pakete vom Ausgang eines Routers zum Eingang eines anderen Routers



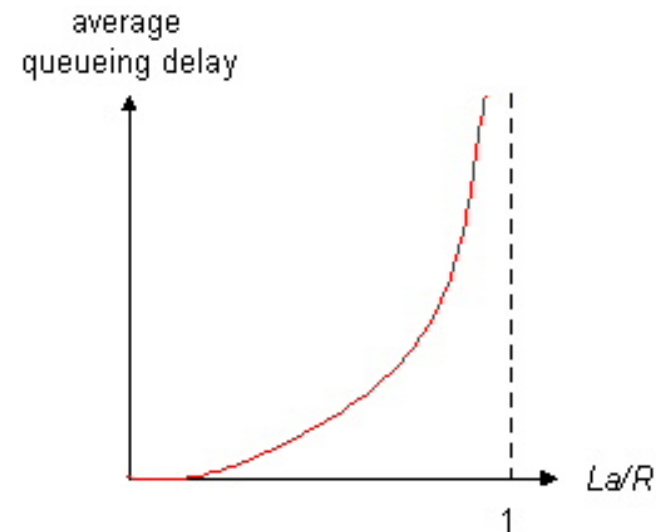
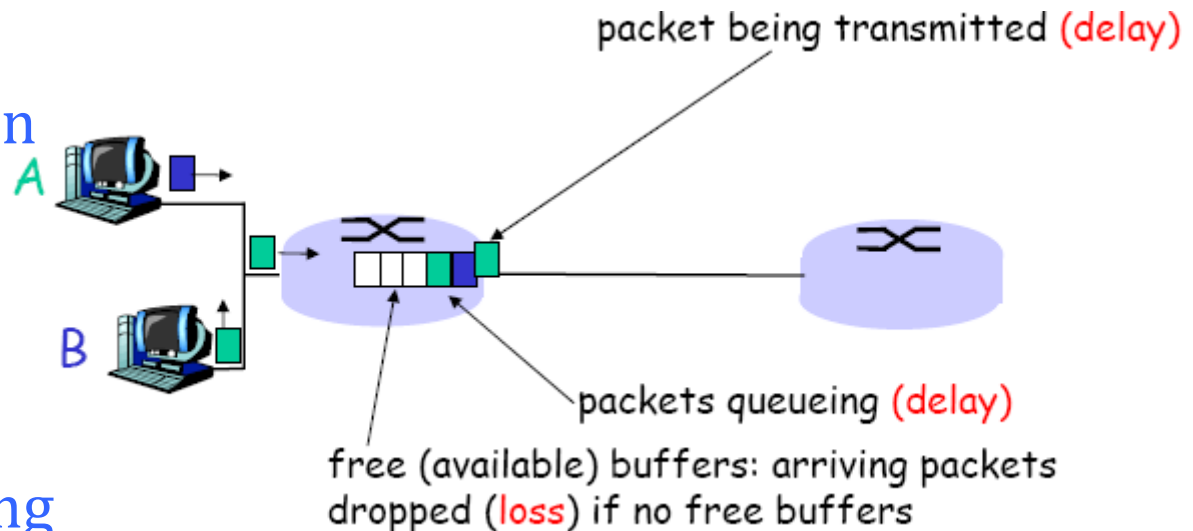
Leistungsgrößen

Übertragungsmedien
sind

Ressourcen, die

- nur beschränkt verfügbar sind
- für die Übertragung Zeit benötigen

Abhängigkeit der
Übertragungszeit von der
Last ist nichtlinear!!



Leistungsgrößen

Verzögerungszeiten bei der Übertragung zwischen Knoten

- Knoten-Verarbeitung
- Warteschlangen-Aufenthalt
- Übertragungsverzögerung
(Paketlänge und Übertragungsrate)
- Signalverzögerung
(Ausbreitungsgeschwindigkeit der Signale in Medium)

Ende-zu-Ende Verzögerung

- Kumulierte Verzögerung in allen Schritten

Leistungsgrößen

Programme zur Messung von Übertragungszeiten

tracert ftp.uni-dortmund.de

```
1  gb5-gw-ls4 (129.217.16.20) 0.635 ms 0.469 ms 0.322 ms
2  mh-sw1-vl26.HRZ.Uni-Dortmund.DE (129.217.129.231) 0.460 ms 0.459 ms 0.323 ms
3  ftp.hrz.uni-dortmund.de (129.217.153.143) 0.324 ms 0.374 ms 0.308 ms
```

ping -s www.scilab.org

PING www.scilab.org: 56 data bytes

64 bytes from frioul.inria.fr (128.93.12.139): icmp_seq=0. time=28. ms

64 bytes from frioul.inria.fr (128.93.12.139): icmp_seq=1. time=28. ms

64 bytes from frioul.inria.fr (128.93.12.139): icmp_seq=2. time=28. ms

...

64 bytes from frioul.inria.fr (128.93.12.139): icmp_seq=9. time=27. ms

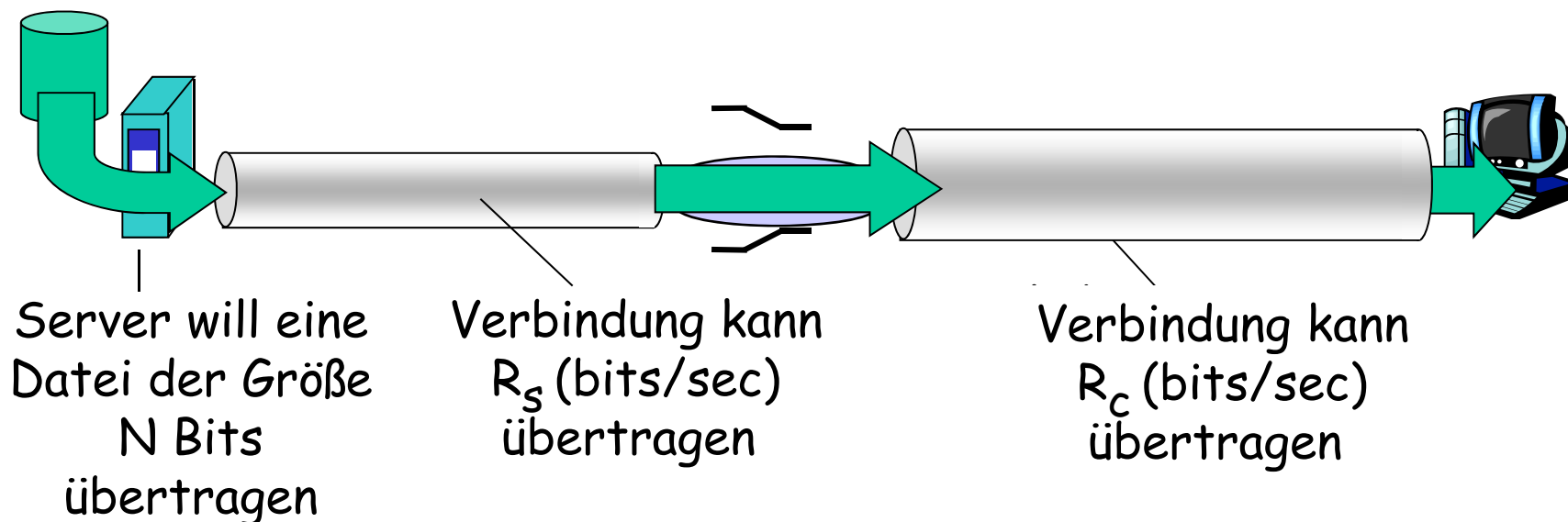
----www.scilab.org PING Statistics----

10 packets transmitted, 10 packets received, 0% packet loss

round-trip (ms) min/avg/max = 27/27/28

Leistungsgrößen

- **Durchsatz:** Rate (bits/Zeiteinheit) mit der Daten zwischen Sender und Empfänger übertragen werden
 - *momentan:* Rate zu einem Zeitpunkt
 - *durchschnittliche:* Rate über einen längeren Zeitraum



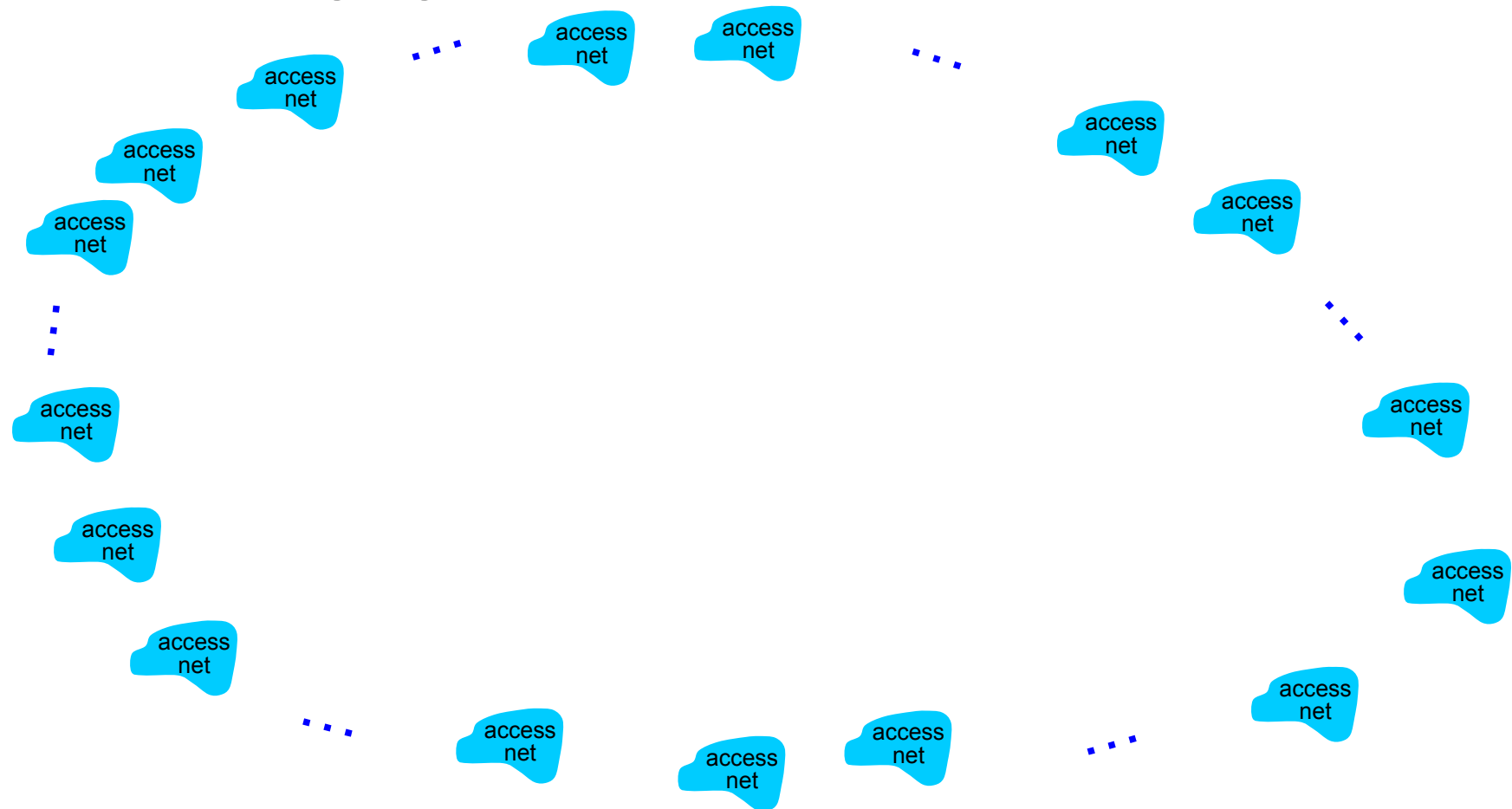
Leistungsgrößen

Verluste und Verfälschungen von Paketen durch

- Pufferüberläufe
- Ausfall von Komponenten
- Übertragungsfehler
- Absichtliche Verfälschungen

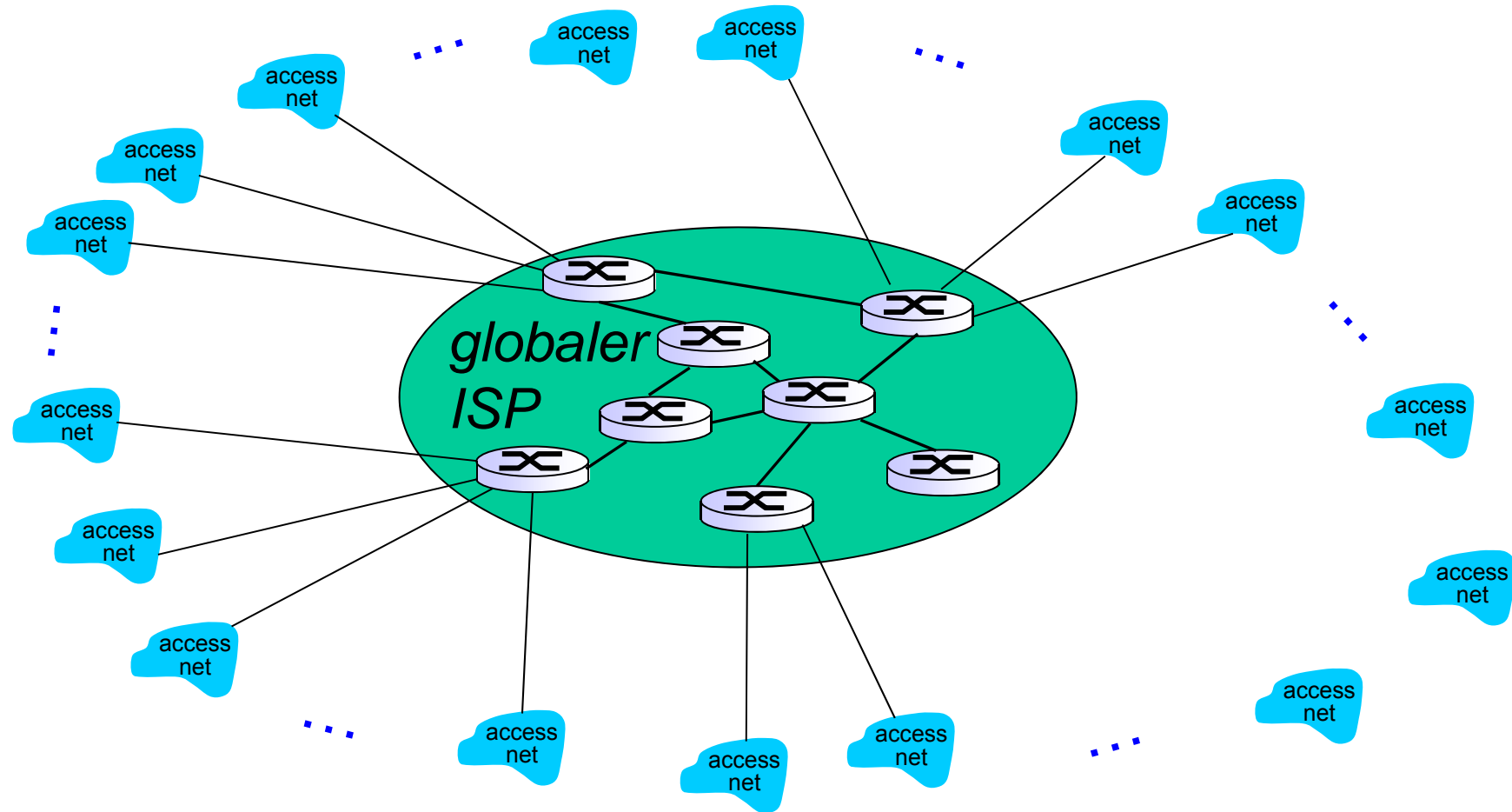
Struktur des Internets: Netz von Netzen

Wie kann man Millionen von ISPs (Internet Service Provider) mit Ihren Zugangsnetzen miteinander verbinden?



Struktur des Internets: Netz von Netzen

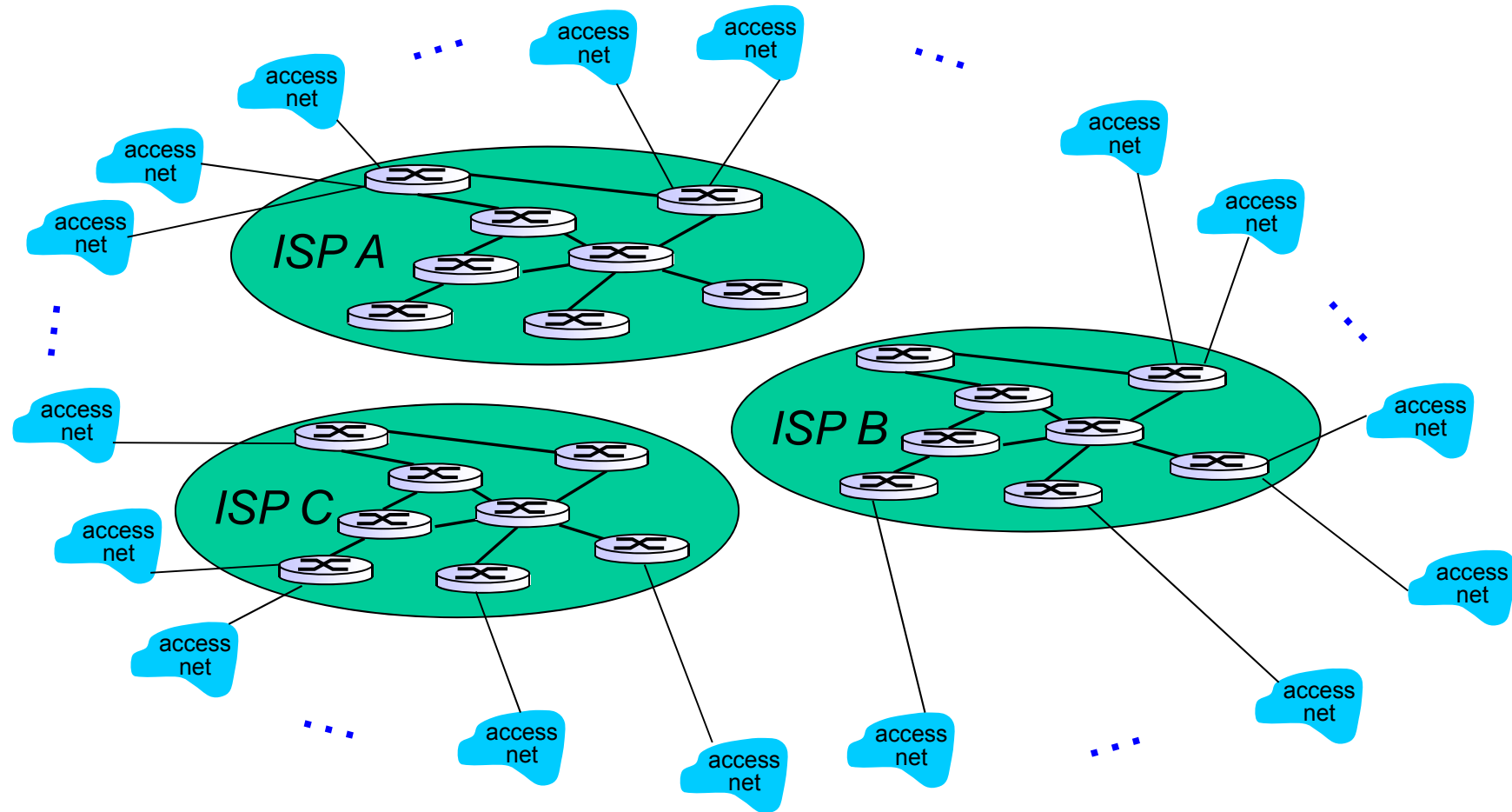
*Nutzung eines globale ISPs, um die Verbindung herzustellen
Kunden und Anbieter (Provider) ISP schließen Verträge*



Struktur des Internets: Netz von Netzen

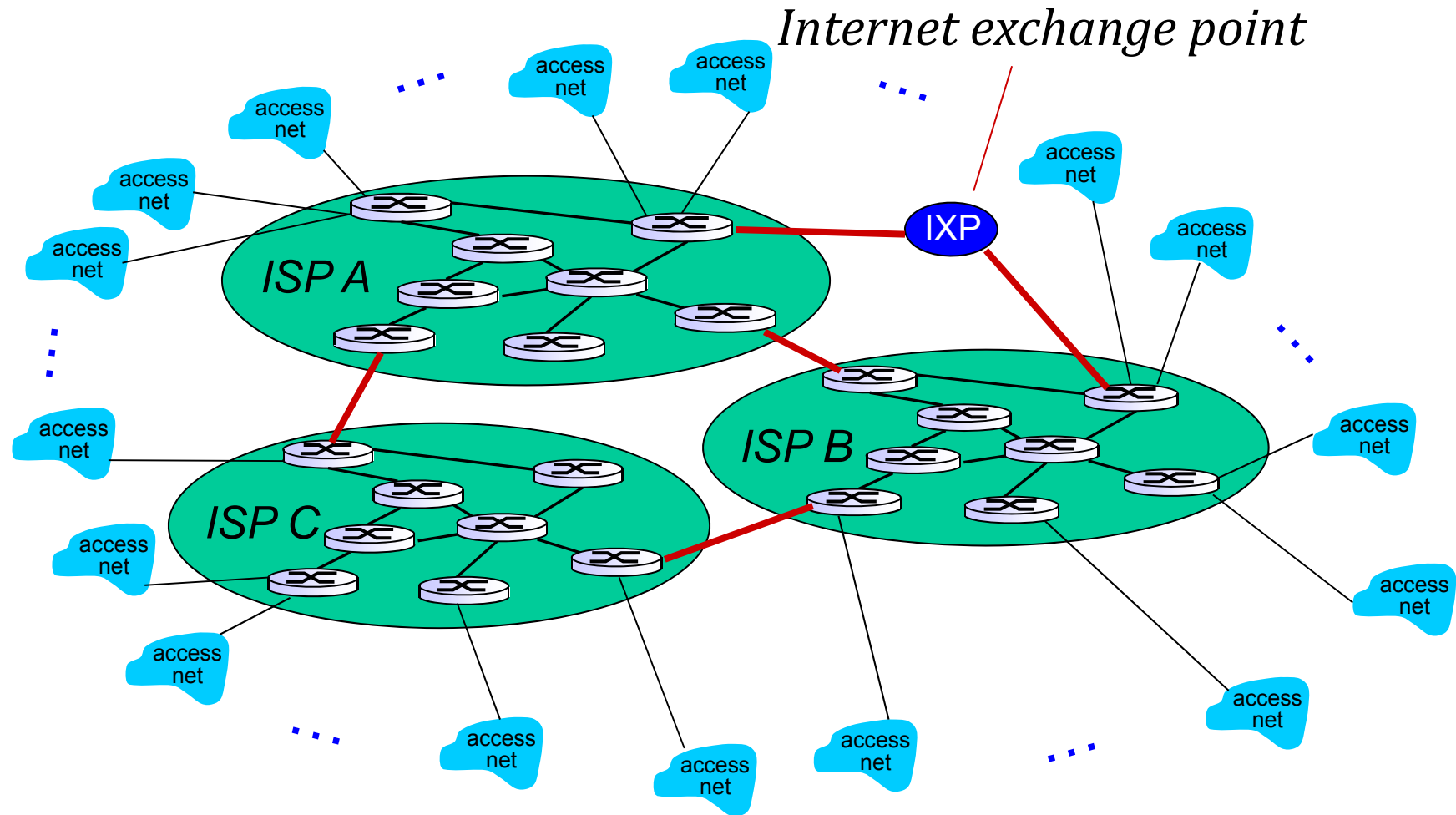
Ein Monopolist wäre nicht gut für den Wettbewerb und die Kunden, deshalb mehrere Anbieter..

Aber wie kommunizieren Kunden unterschiedlicher Anbieter?



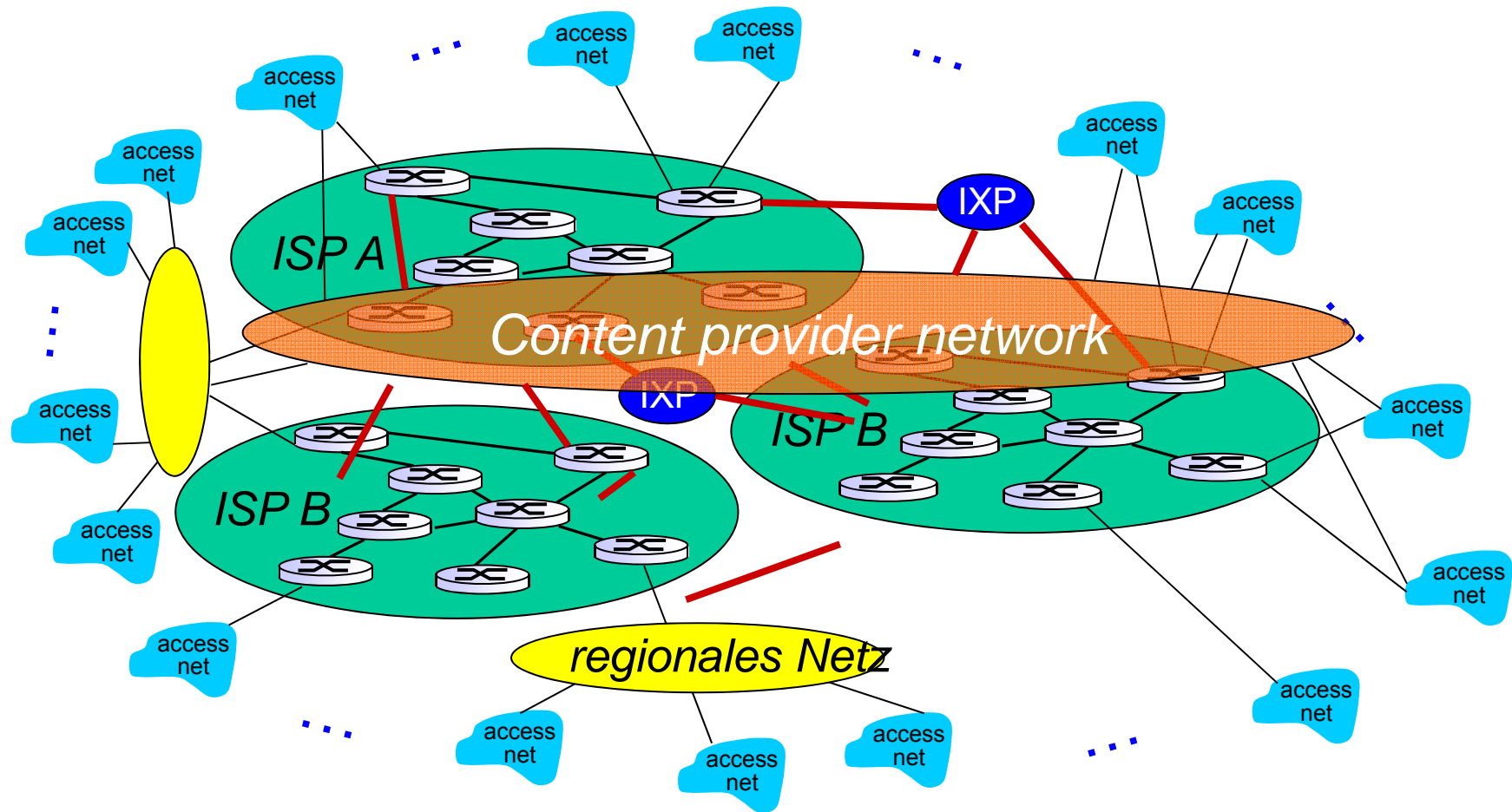
Struktur des Internets: Netz von Netzen

Austausch zwischen den zentralen ISPs

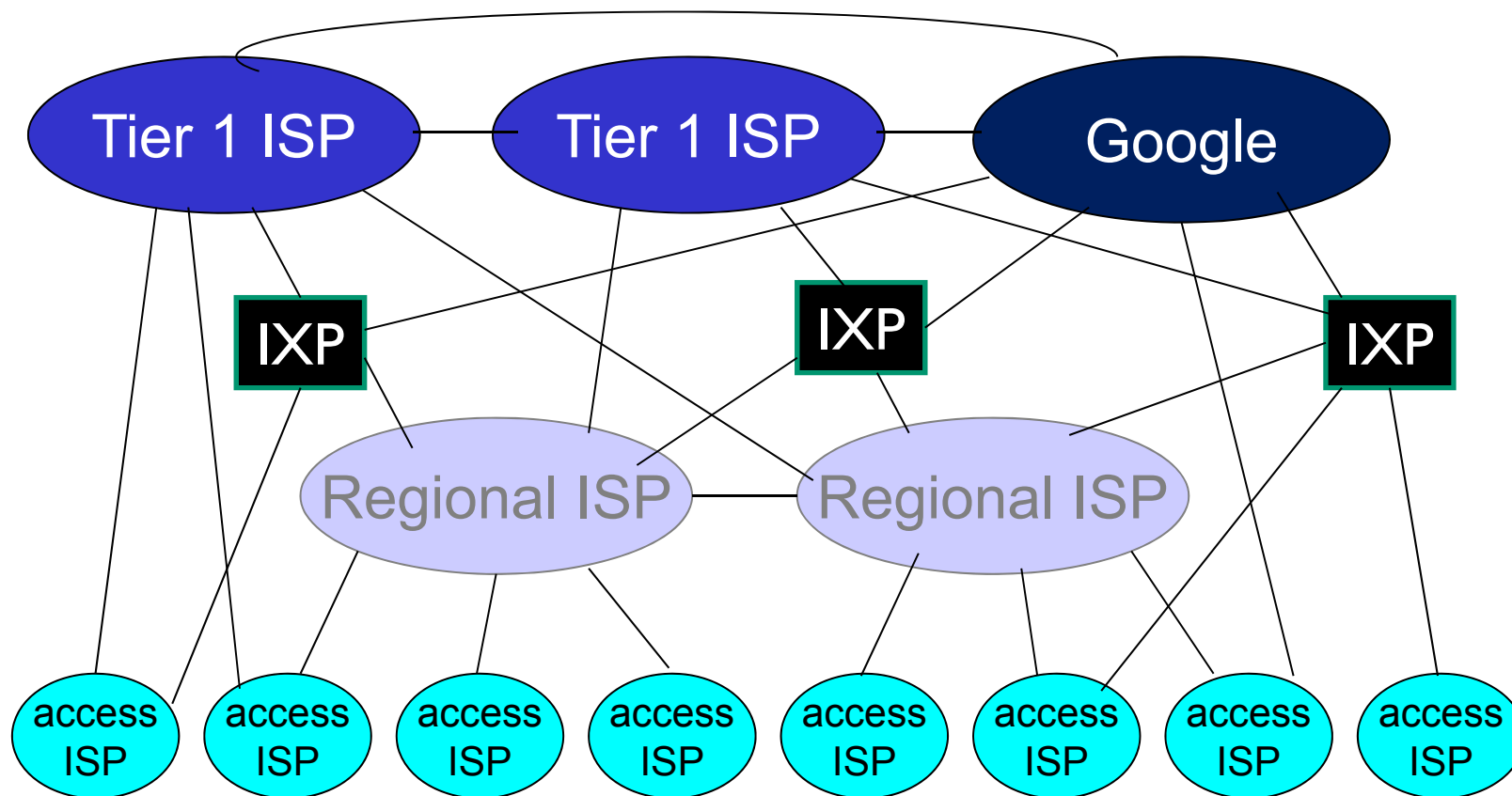


Struktur des Internets: Netz von Netzen

Eigentlich geht es noch weiter...

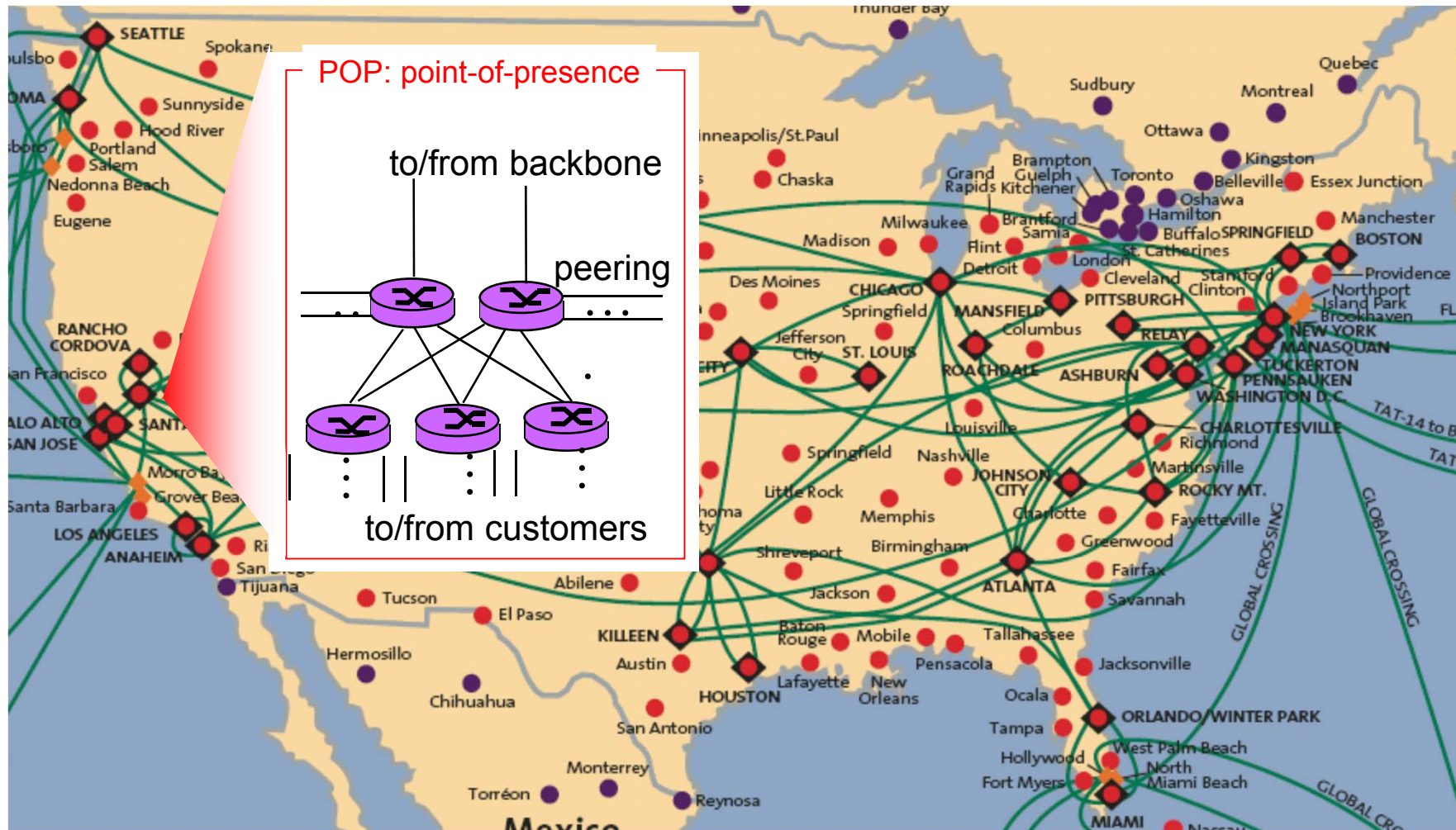


Struktur des Internets: Netz von Netzen



- Obere Ebene: kleine Menge gut verbundener Netze
 - **“tier-1” kommerzielle ISPs** (e.g., Level 3, Sprint, AT&T, NTT), nationale & internationale Abdeckung
 - **content provider Netze** (z.B. Google): private Netze, die eigene Datenzentren verbinden und die “tier 1 ISPs” umgehen

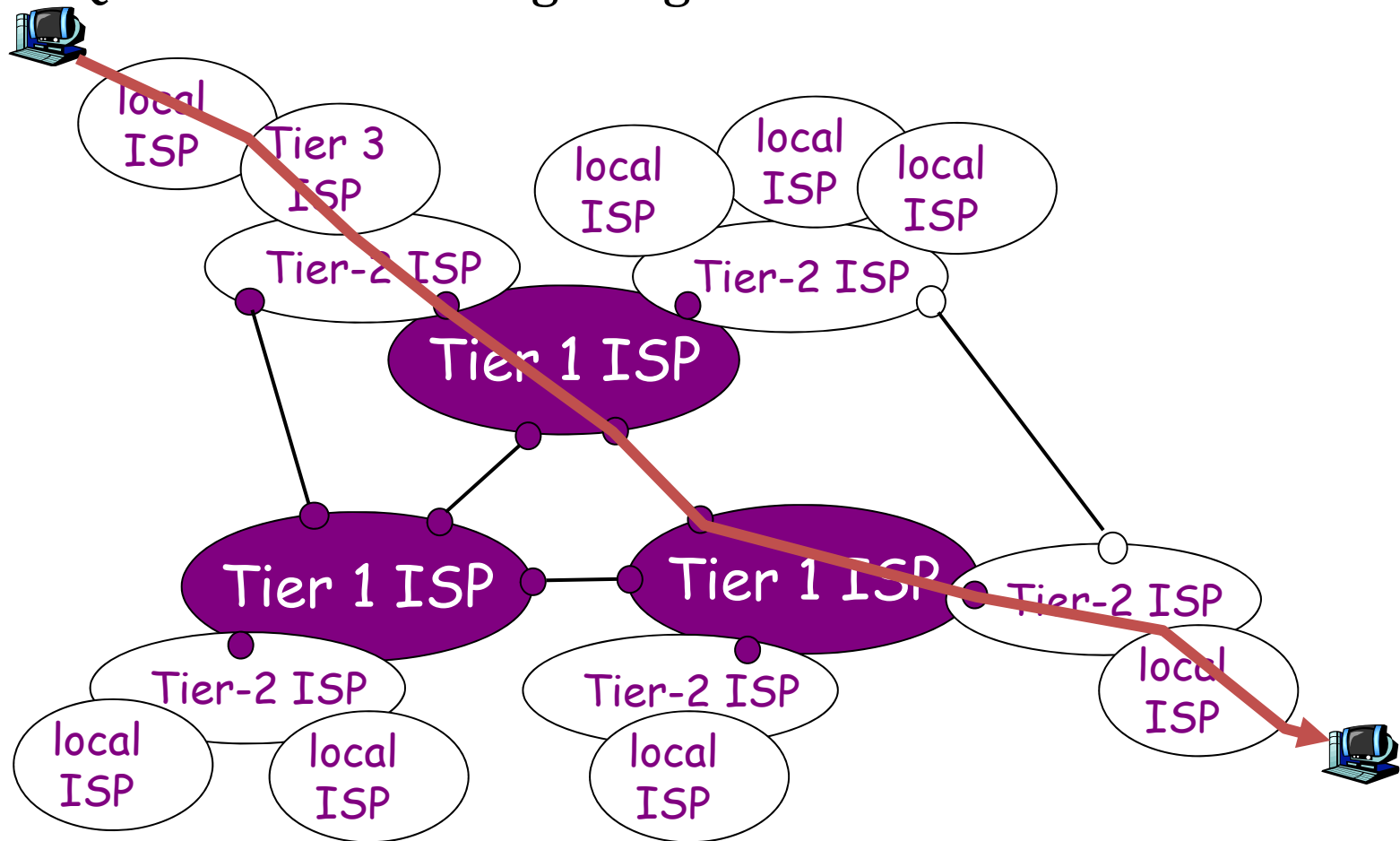
Tier-1 ISP z.B. Sprint



© Kurose/Ross 2009

Routing

- Ein Paket muss seinen Weg durch viele Netze nehmen, um von der Quelle zum Ziel zu gelangen



Routing

Paket muss seinen Weg zum Ziel über Zwischenknoten (Hops) finden (\Rightarrow Routingalgorithmus)

➤ **Datagramm-Netz**

- Die Zieladresse bestimmt den nächsten Hop.
- Verschiedene Pakete desselben Datenstroms können unterschiedliche Wege nehmen.

➤ **Virtual-Circuit Netz** (VC, virtuelles Leitungsnetz)

- Jedes Paket hat eine Marke (*Tag*), die den nächsten *Hop* bestimmt.
- Pfad wird beim Verbindungsaufbau festgelegt.
- Router speichern Verbindungsdaten.

Internet – verbindungsorientiert

Ziel: Datentransfer zwischen End-Systemen

- Bestätigter Verbindungsaufbau (Handshaking)
 - Vorbereitung auf die Datenübertragung
 - Zustand der Verbindung wird in beiden Hosts gespeichert

TCP – Transmission Control Protocol [RFC793]

- Zuverlässiger Datentransfer in richtiger Reihenfolge (reliable in-order byte-stream data transfer)
 - Overhead durch Quittierung
- Flusskontrolle (flow control)
 - keine Überschwemmung des Empfängers durch den Sender
- Überlastkontrolle (congestion control)
 - Vermeidung von Staus im Netz

Internet - verbindungslos

Ziel: Datentransfer zwischen End-Systemen

- Keine Vorbereitung des Transfers (kein Handshaking)
 - zustandlos, separate Übertragung einzelner Daten-Pakete

UDP – User Datagram Protocol [RFC768]

- Unzuverlässiger Datentransfer (unreliable data transfer)
- keine Flusskontrolle (no flow control)
- keine Überlastkontrolle (no congestion control)
- Daten-Pakete können verloren gehen

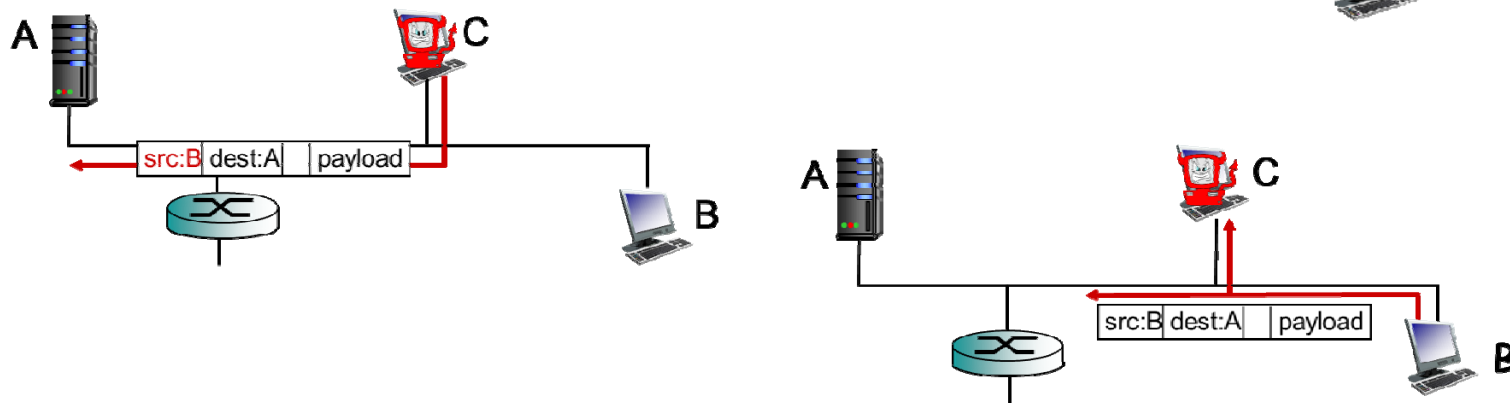
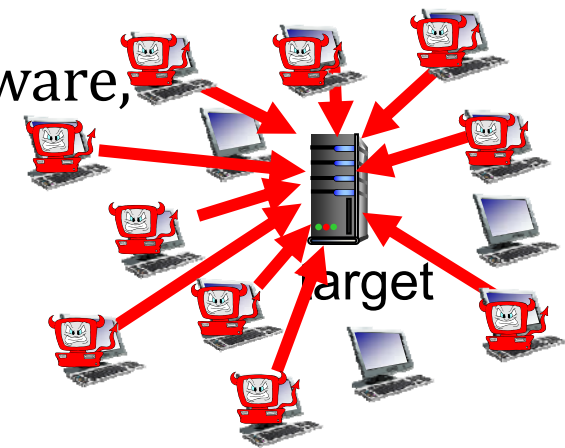
Sicherheit im Internet

- Gebiet der Netzwerksicherheit beschäftigt sich mit:
 - möglichen Angriffen auf Computernetze
 - Verteidigungsstrategien gegen Angriffe
 - dem Aufbau sicherer Netzwerke
- Sicherheit spielte in den Anfangsjahren des Internets keine Rolle:
 - *ursprüngliche Vision*: “eine Gruppe Nutzer, die sich vertrauen und in transparenter Weise das Netz nutzen”
😊
 - Internet-Protokolle wurden und werden genutzt, um die fehlende Sicherheit beim Design des Netzes auszugleichen
 - Sicherheitsüberlegungen heute auf allen Ebenen

Sicherheit im Internet

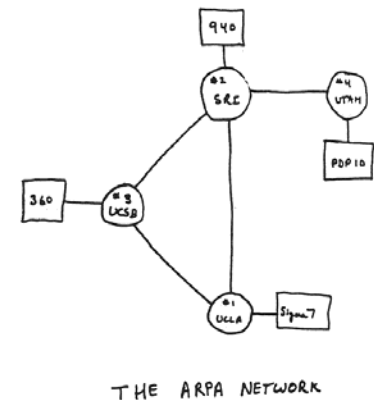
Typische Bedrohungsszenarien:

- Malware in Form von Virus und Würmern (ausspähen, Zerstörung von Daten & Hardware, Einbindung des Rechners in ein Botnet,...)
- Mitlesen oder einschleusen von Paketen



Historie des Internets

- 1961-72 Entwicklung Paketvermittlung bis hin zum ARF
- 1970 Aloha-Netz auf Hawaii
- 1974 Cerf und Kahn entwickeln Architektur zur Vernetzung von Netzen (Basis des Internets)
- 1976 Ethernet (Xerox Park)
- 70er Jahre viele proprietäre Netze (DECNET, SNA,...)
- 1982 SMTP Email-Protokoll
- 1983 TCP/IP, DNS
- 1985 FTP
- 90er Entwicklung von Web-Anwendungen (1994 Mosaic)
- Seit Beginn der 90er kommerzielle und wissenschaftliche Nutzung vereinfacht (offenes System)



Beschreibung von Kommunikationsprotokollen

Entwurf und Spezifikation von Protokollen erfolgt oft auf Basis von Automaten

- Einzelne Protokollinstanzen werden durch einen Automaten dargestellt
 - Endliche Automaten sind nicht mächtig genug, um reale Protokolle zu beschreiben \Rightarrow Einsatz von erweiterten Automatenmodellen (erweiterte Mealy-Automaten)
- Kommunizierende Automaten beschreiben den Protokollstapel

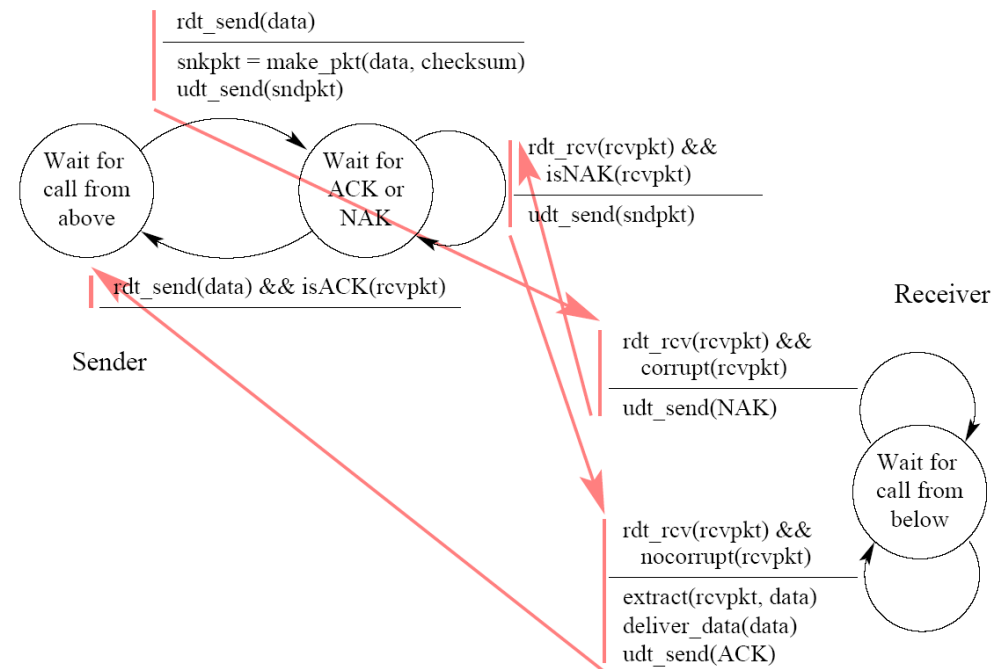
Folgende Darstellung ist nicht im Buch von Kurose und Ross zu finden!

Mealy-Automaten

Erweiterter Mealy Automat,

*wie er oft zur Definition von Kommunikationsprotokollen
(genauer des Verhaltens von Protokollinstanzen) eingesetzt wird*

Szenario mit Fehlern



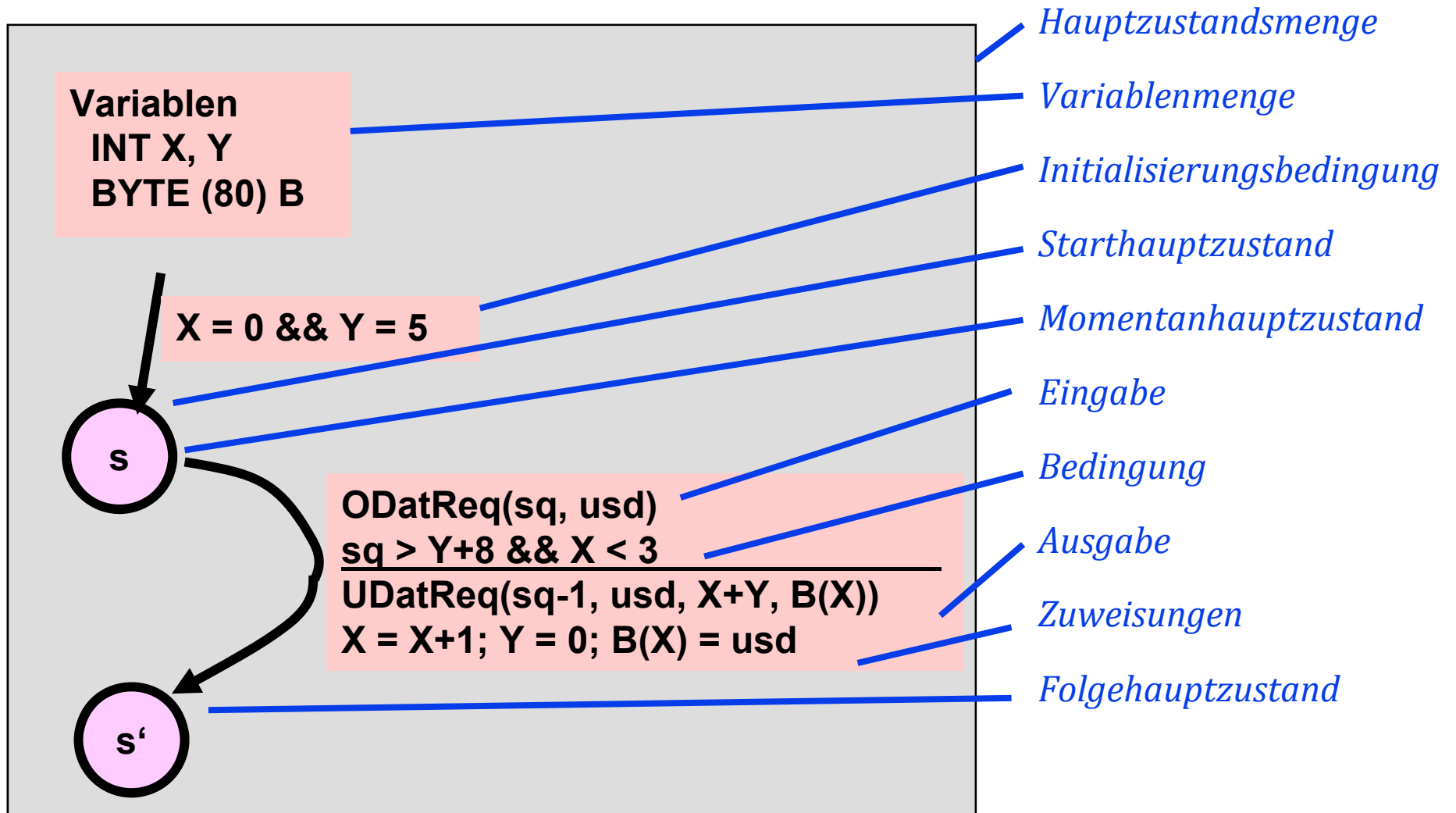
Mealy-Automaten

➤ Definiert durch

- Menge von Variablen V_1, \dots, V_n mit Wertebereichen W_1, \dots, W_n
- Menge von Eingaben E_1, \dots, E_m jeweils mit Parametern EP_{i1}, \dots, EP_{im}
- Menge von Ausgaben A_1, \dots, A_p jeweils mit Parametern AP_{i1}, \dots, AP_{ip}
- Menge von Hauptzuständen HS
- Ein ausgezeichnete Start-Hauptzustand hs_0
- Initialisierungsbedingung als boolescher Ausdruck über Variablen
- Menge von Transitionsklausen TK_1, \dots, TK_q ,
jeweils definierend eine Menge von Transitionen T_1, \dots, T_q
 - » Momentanhauptzustand: $s \in HS$
 - » Eingabe $e(w_1, w_2, \dots)$: Term aus E_i über Eingabeparametern
 - » Bedingung: Boolescher Ausdruck über Eingabeparametern und Variablen
 - » Folgehauptzustand: $s' \in HS$
 - » Ausgabe $a(u_1, u_2, \dots)$: Term aus A_j über E_i -Eingabeparametern und Variablen
 - » Variablenzuweisungen $V_k = \text{aus}_k$, Term über E_i -Eingabeparametern und Variablen

➤ Ergibt Mealy-Automaten mit großen Mengen von Zuständen, Eingaben, Ausgaben und Transitionen

Mealy-Automaten



Mealy-Automat

Unvollständigkeit

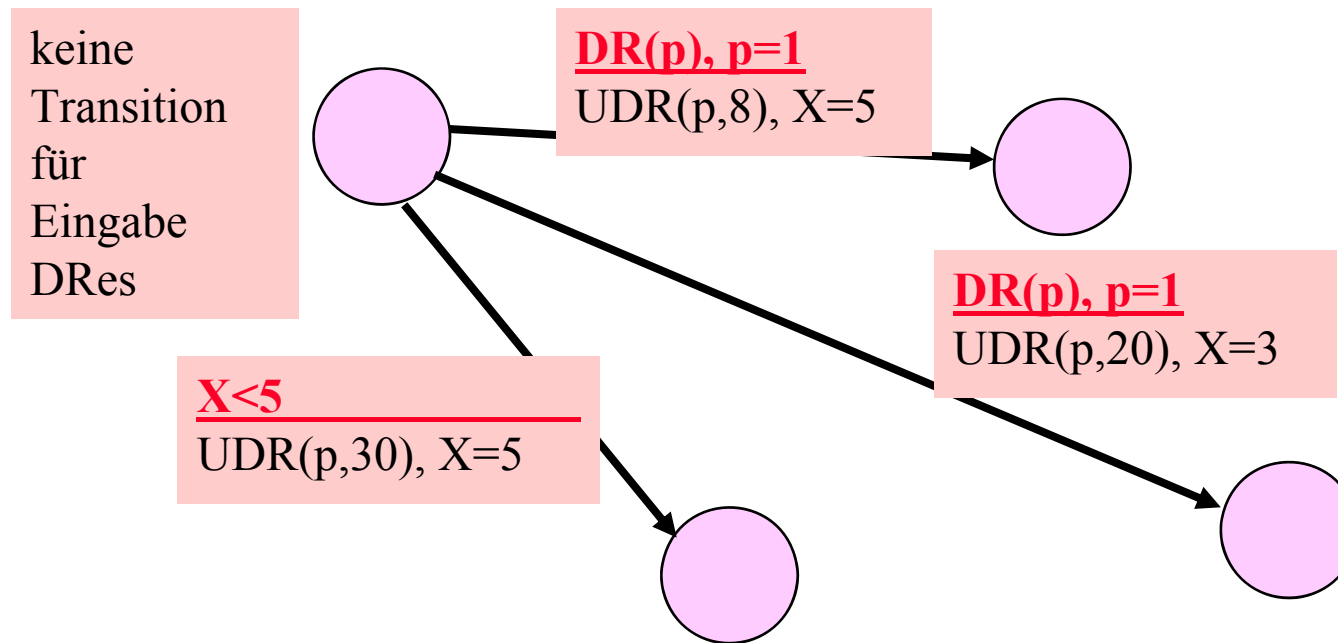
Nicht in jedem Zustand ist für alle Eingaben eine Transition vorhanden

Nichtdeterminismus

Es gibt u.U. pro Momentanzustand-Eingabe-Kombination mehr als eine Transition

Spontane Transitionen

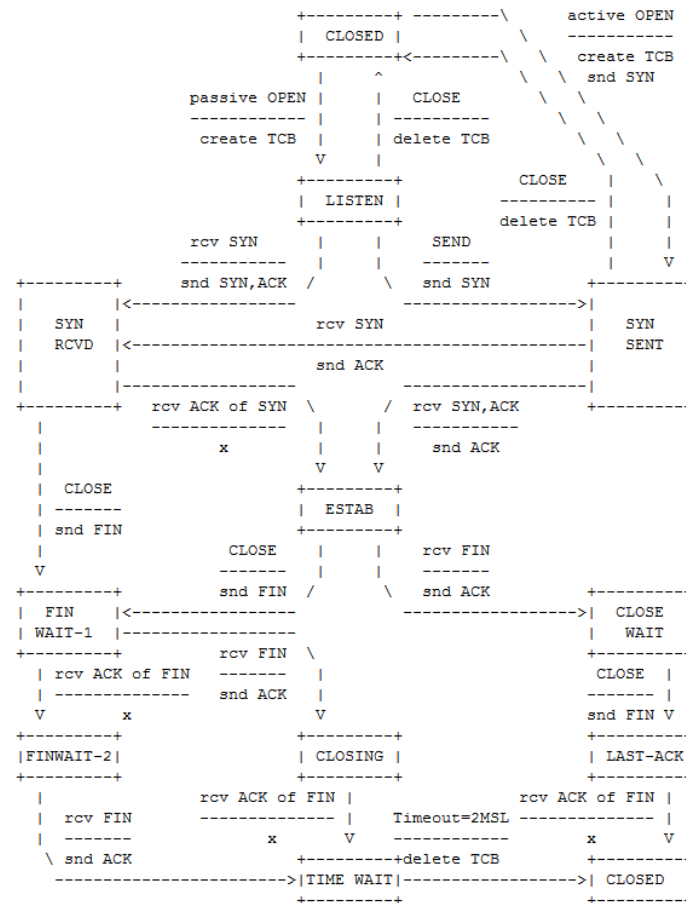
Es gibt u.U. Transitionen ohne Eingabe



TCP-Verbindungsaufbau (Mealy-Automat)

September 1981

Transmission Control Protocol
Functional Specification



TCP Connection State Diagram
Figure 6.

Mealy-Automat zur Beschreibung
des Verbindungsaufbaus in TCP aus
RFC 793 (Sept. 1981)