Einführung in die Wirtschaftsinformatik I

WS 2024/25

Verteilte Systeme und Rechnernetze

Dr. Rainer Wieching

Gliederung – Teil 2

1. Verteilte Systeme

- Motivation
- Eigenschaften
- Architekturen

2. Netzwerke

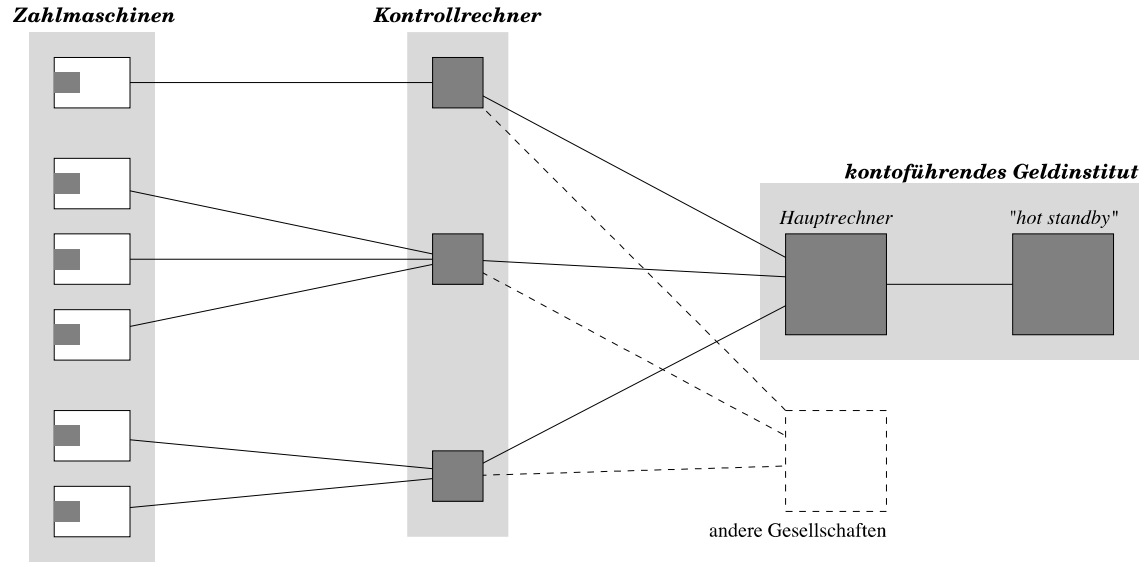
- Arten
- Vermittlungstechniken
- Schichtenmodell

Motivation

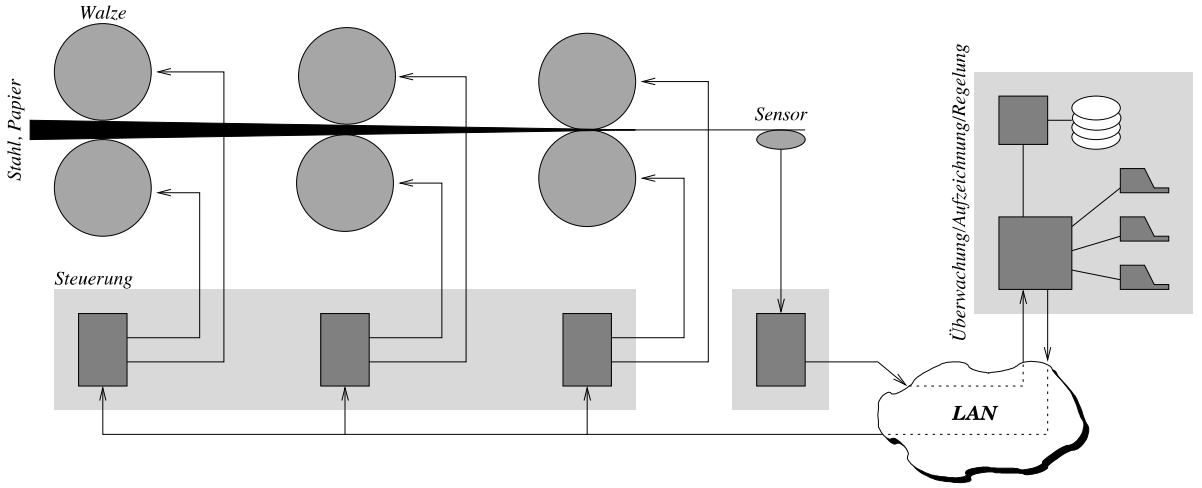
Gemeinsame Nutzung von Betriebsmitteln wie beispielsweise {Druck, Datenbank, Datei, Namens…}dienste

Geographisch **verteilte, kooperative Anwendungen** wie beispielsweise Chat, Bildtelefonie, Fernwartung, …

Transaktionssysteme - Geldautomaten



Industrieanlagen - Walzwerk



Definitionen

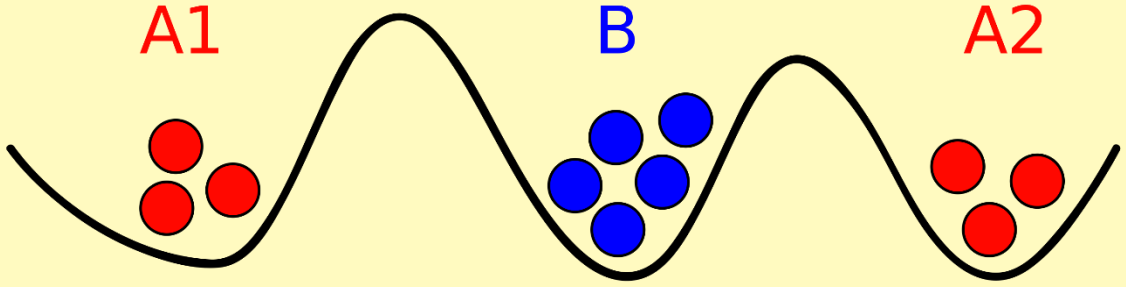
„Ein verteiltes System ist eine Kollektion unabhängiger Computer, die den Benutzern als Einzelcomputer erscheinen” – A. Tannenbaum

Mehrere, physikalisch bzw. logisch verteilte, autonome Prozesse, die über (unzuverlässige) Kanäle/(offene) Netzwerke kommunizieren bzw. sich koordinieren

Definitionen

„Ein verteiltes System ist eine Kollektion unabhängiger Computer, die den Benutzern als Einzelcomputer erscheinen” – A. Tannenbaum

Mehrere, physikalisch bzw. logisch verteilte, autonome Prozesse, die über (unzuverlässige) Kanäle/(offene) Netzwerke kommunizieren bzw. sich koordinieren



Beispiel “The Two Generals’ Problem”

Um die blaue Armee koordiniert anzugreifen, müssen die zwei Generäle der roten Armee Boten durch das Tal schicken, dass von der blauen Armee kontrolliert wird

Eigenarten verteilter Systeme

Es ist die Eigenart verteilter Systeme, dass es auf Dauer keine zwei Prozesse gibt, die zur gleichen Zeit, die gleiche zutreffende Sicht des Systems haben.

Keine gemeinsame Uhr: Uhrensynchronisation aufgrund nicht bekannter Verzögerungszeiten bei der Kommunikation (meist Nutzung logischer statt physikalischer Uhren).

Kein gemeinsamer Speicher: Kein einzelner Knoten kennt den vollständigen globalen Zustand. Es ist daher schwierig, globale Eigenschaften des Systems zu beobachten.

Keine akkurate Ausfallerkennung: Es ist in einem asynchronen verteilten System (d.h. keine obere Schranke für Kommunikationszeiten bekannt) unmöglich, langsame von ausgefallenen Prozessen zu unterscheiden.

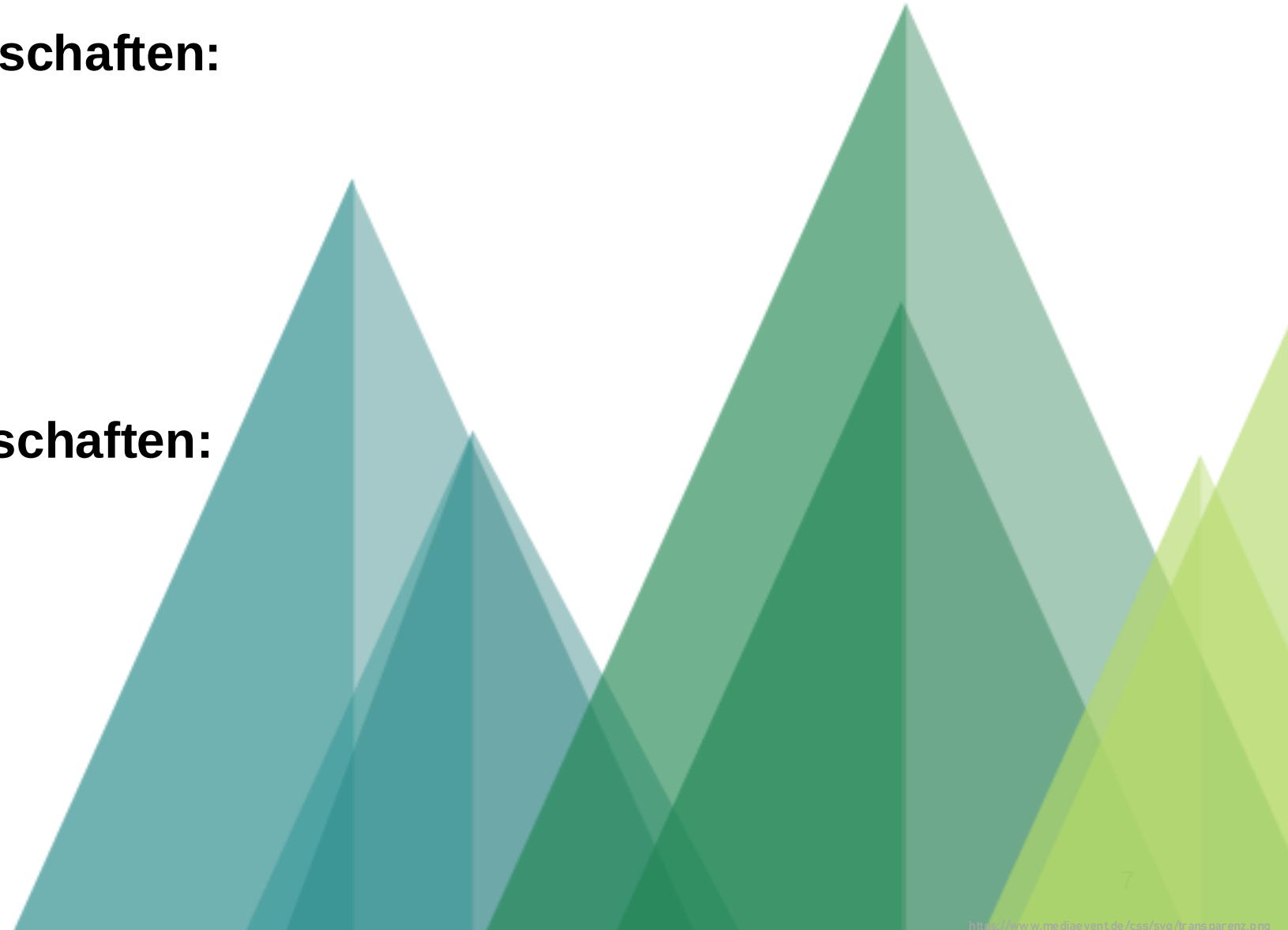
Weitere Eigenschaften

Charakteristische Eigenschaften:

- Heterogenität
- Nebenläufigkeit
- Fehlerverarbeitung

Wünschenswerte Eigenschaften:

- Sicherheit
- Skalierbarkeit
- Offenheit
- Transparenz



Heterogenität

Bereiche von Heterogenität

- Netzwerke und Kommunikations-protokolle
- Prozesse und Betriebssysteme
- Personen und Organisationen
- …

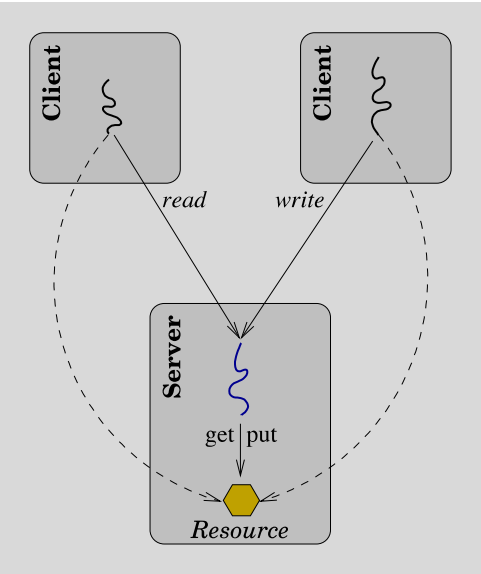
Umgang Heterogenität

- Nutzung gemeinsamer, offener Standards
- Nutzung von Middleware zum Verbergen von Heterogenität
- Virtuelle Maschinen und mobiler Code

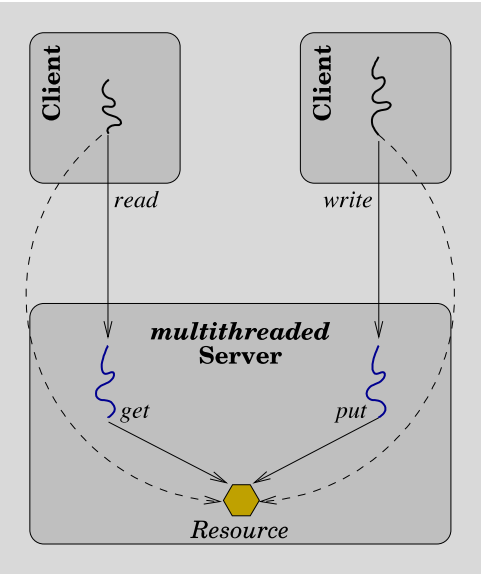
Nebenläufigkeit

Koordination unabhängiger Prozesse bzw. Zugriff auf gemeinsame Ressource

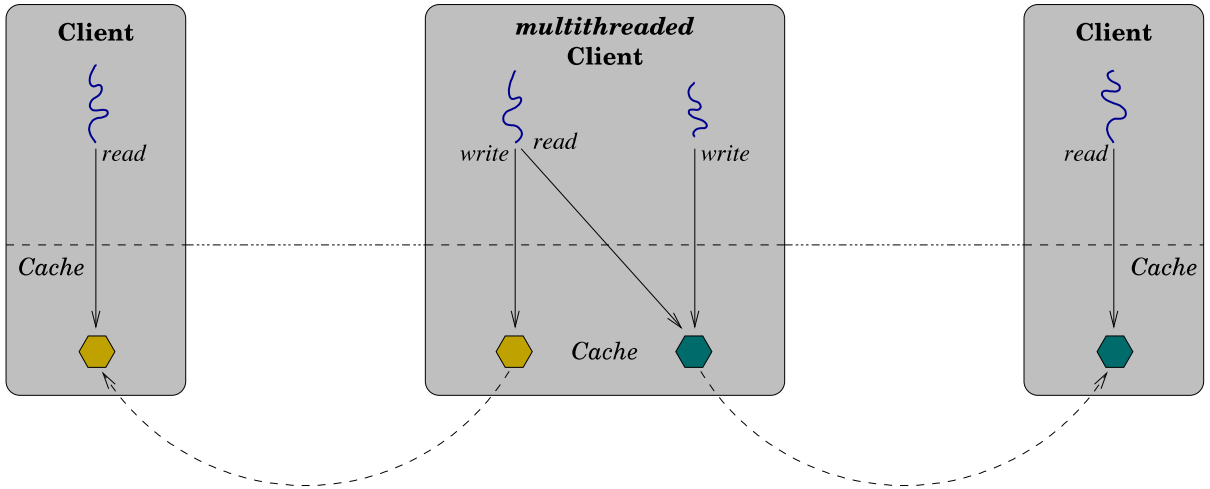
- Gestaltungsoptionen
- Exklusive Nutzung
- Parallele Nutzung
- Nutzung von Replikaten (Caching)



Exklusive Nutzung



Parallele Nutzung



Nutzung von Replikaten

Fehlerverarbeitung

Fehler

- *An error is a manifestation of a fault in a system, which can lead to system failure.*

Failure (Funktionsausfall)

- Keine Diensterbringung bzw. weicht von Spezifikation ab

Error (Fehler)

- Systemzustand der zu einem Funktionsausfall führen kann

Fault (Fehlerursache)

- Fehlerhafte Software/Hardware

Fehlerverarbeitung

- Fehler erkennen, z.B. durch Prüfsummen-Check

Maskieren/Verbergen

- Erkannte Fehler nach außen verbergen (z.B. verlorene Nachrichten wiederholen) oder abschwächen (z.B. fehlerhafte Nachrichten verwerfen).

Tolerieren

- Nicht erkannte bzw. maskierte Fehler sollten toleriert werden können

Fehlerarten

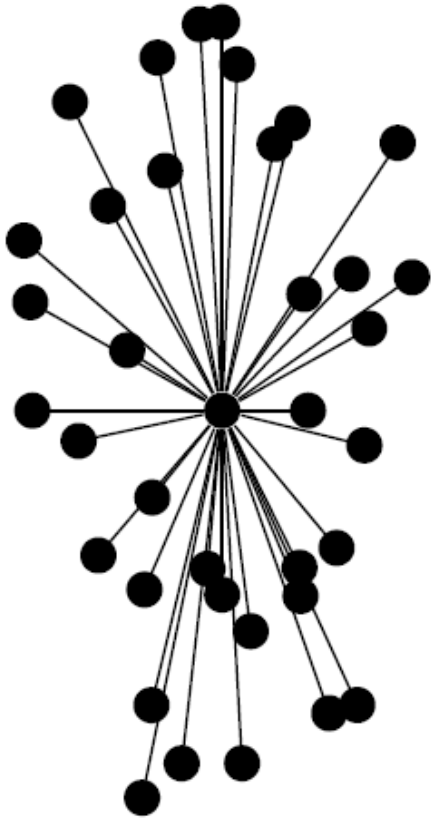
Gutmütige Fehler (benign faults)

- Crash Stop
  - Prozess bzw. der Zugriff darauf fällt komplett aus
- Fail Stop
  - Dienst wird funktionsunfähig und signalisiert dies
- Fail Silent
  - Dienst „rührt sich nicht mehr“ (evtl. schwierig erkennbar)

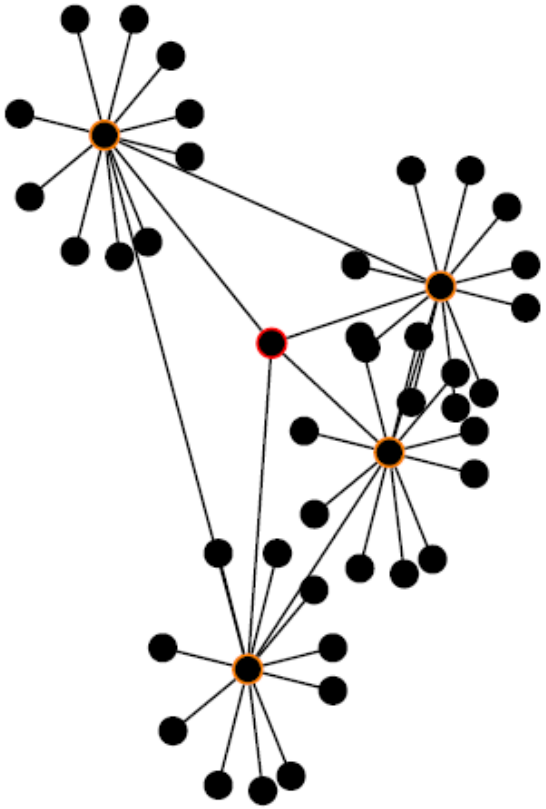
Bösartige Fehler (malicious / byzantine faults)

- Prozess/Kanal läuft fehlerhaft weiter und weist zufälliges Verhalten auf
- Fehlerhafte Prozesse können beliebige Aktionen (koordiniert) ausführen
- Umfasst sämtliche Arten von Fehler, z.B. auch gezielte Angriffe von außen auf das System

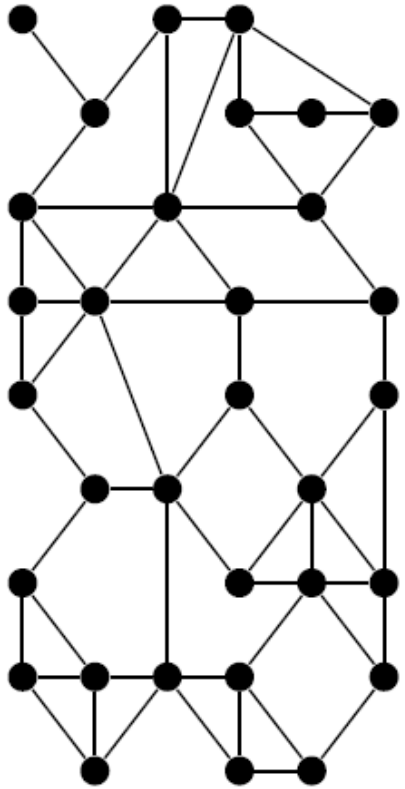
Verteilungsarten



Centralised



Decentralised



Distributed

Sicherheit

Motivation

- Datenübertragung über öffentliche Netze, sowie
- Nutzung fremder Dienste bzw. öffnen von Diensten für Fremde erhöht das Risiko der missbräuchlichen Nutzung

Beispiele:

- Nachrichten können abgefangen, verfälscht bzw. gefälscht und/oder mehrfach geschickt werden (z.B. Kontoüberweisungen)
- Dienste und Nutzer können vorgetäuscht werden (z.B. Onlinebank-Attrappe)

Schutziele CIA

- **C**onfidentiality (Vertraulichkeit)
  - nur Berechtigte dürfen auf Daten zugreifen
- **I**ntegrity (**I**ntegrität)
  - keine unbemerkte Veränderung der Daten
- **A**vailability (Verfügbar)
  - Daten müssen dann verfügbar sein, wenn ein autorisierter Benutzer diese benötigt

Skalierbarkeit

Definition

- Ein System skaliert, wenn es bei steigender Anzahl an Ressourcen und Benutzer effizient bleibt.

Kernprobleme beim Entwurf skalierbarer verteilter Systeme

- Kostenkontrolle für die physischen Ressourcen: Bei steigender Nachfrage soll eine Erweiterung zu vernünftigen Kosten möglich sein
- Kontrolle des Leistungsverlustes und Vermeidung von Leistungsengpässen: Hierarchische Lösungen (Beispiel DNS) bevorzugen, so dass die Menge zu ladender/verarbeitender Daten nicht zu groß wird
- Erschöpfung der SW-Ressourcen verhindern: Ressourcen so anlegen, dass sie für zukünftige Erweiterungen voraussichtlich ausreichen werden. Beispielproblem: Umstellung von 32-Bit Internetadressen auf 128-Bit

Offenheit

Definition

- Offenheit beschreibt den Grad, zu dem neue Dienste hinzugefügt und zur Verwendung von unterschiedlichen Clients bereitgestellt werden

Offene verteilte Systeme

- basieren auf dem Vorhandensein eines einheitlichen Kommunikationsmechanismus und veröffentlichten Schnittstellen für den Zugriff auf gemeinsam genutzte Betriebsmittel;
- Können aus heterogener Hard- und Software aufgebaut sein, die insbesondere auch von unterschiedlichen Herstellern stammen können.

Beispiel Internet-Protokolle

- RFC-Dokumente (Requests For Comment), laufend nummeriert, enthalten Diskussionen und Spezifikationen (siehe www.ietf.org/rfc.html)

Transparenz

Das verteilte System wird vom Anwender/Programmierer als einheitliche/lokale Einheit wahrgenommen und nicht als Sammlung voneinander unabhängiger, verteilter Komponenten.

Acht Formen der Transparenz (ANSI/ISO):

1. **Zugriffs-T.** ermöglicht den Zugriff auf lokale und entfernte Ressourcen unter Verwendung identischer Operationen.

2. **Positions-T.** (Ortstransparenz) erlaubt den Zugriff auf die Ressourcen, ohne dass man ihre Position/ihren Ort kennen muss.

3. **Nebenläufigkeits-T.** erlaubt, dass mehrere Prozesse gleichzeitig mit denselben gemeinsam genutzten Ressourcen arbeiten, ohne sich gegenseitig zu stören.

Transparenz

4. **Replikations-T.** erlaubt, dass mehrere Instanzen von Ressourcen verwendet werden, um die Zuverlässigkeit und die Leistung zu verbessern, ohne dass die Benutzer oder Applikationsprogrammierer wissen, dass Repliken verwendet werden.

5. **Fehler-T.** erlaubt das Verbergen von Fehlern, so dass Benutzer und Applikationsprogrammierer ihre Aufgaben erledigen können, auch wenn Hardware- oder Softwarekomponenten ausgefallen sind.

6. **Mobilitäts-T.** erlaubt das Verschieben von Ressourcen und Clients innerhalb eines Systems, ohne dass die Arbeit von Benutzern oder Programmen dadurch beeinträchtigt wird.

7. **Leistungs-T.** erlaubt, dass das System neu konfiguriert wird, um die Leistung zu verbessern, wenn die Last variiert.

8. **Skalierungs-T.** erlaubt, dass sich Systeme und Applikationen vergrößern, ohne dass die Systemstruktur oder die Applikationsalgorithmen geändert werden müssen.

Gliederung

1. Verteilte Systeme

- Motivation
- Eigenschaften
- **Architekturen**

2. Netzwerke

- Arten
- Vermittlungstechniken
- Schichtenmodell

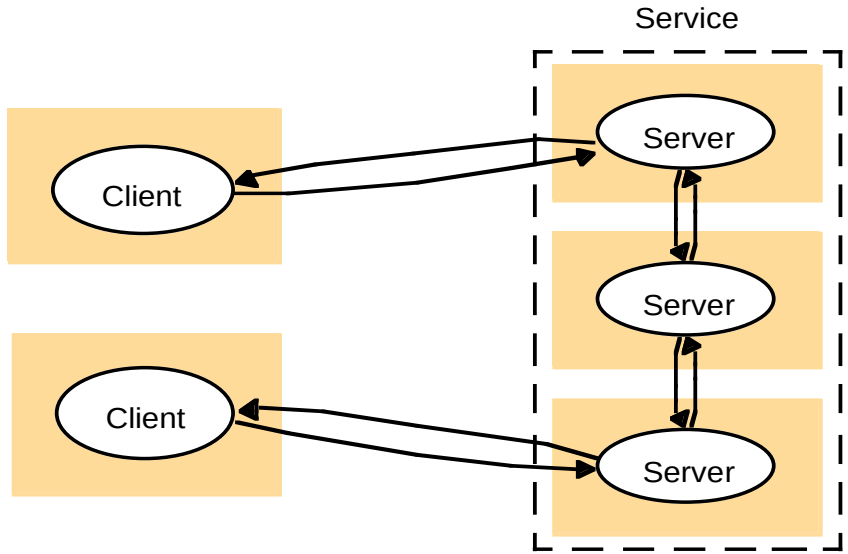
Client/Server sind Rollen von Prozessen innerhalb einer Diensterbringung eines verteilten Systems.

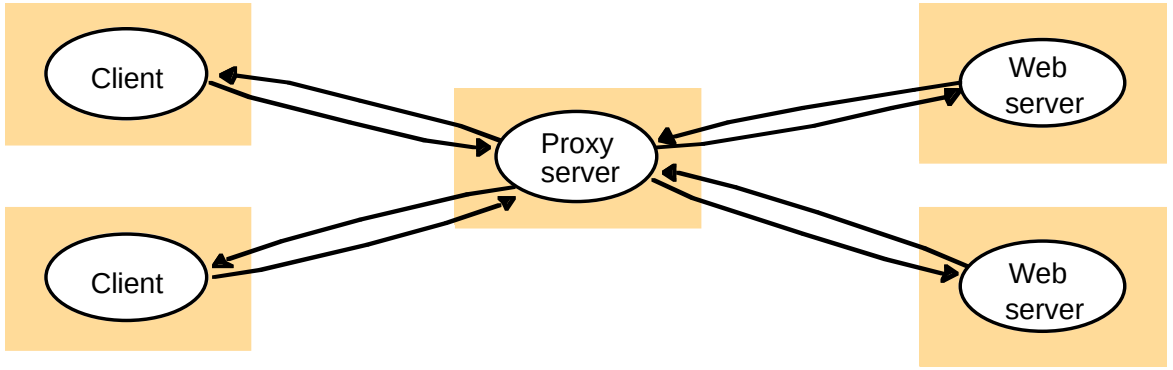
Server: Reagierender Prozess

- bearbeitet Anfragen
- ständige Ausführung
- Adresse bekannt
- Beispiel: Webshop, Anrufbeantworter

Client: Initiierender Prozess

- stellt Anfragen
- Beispiel: Webshop Kunde, Anrufer

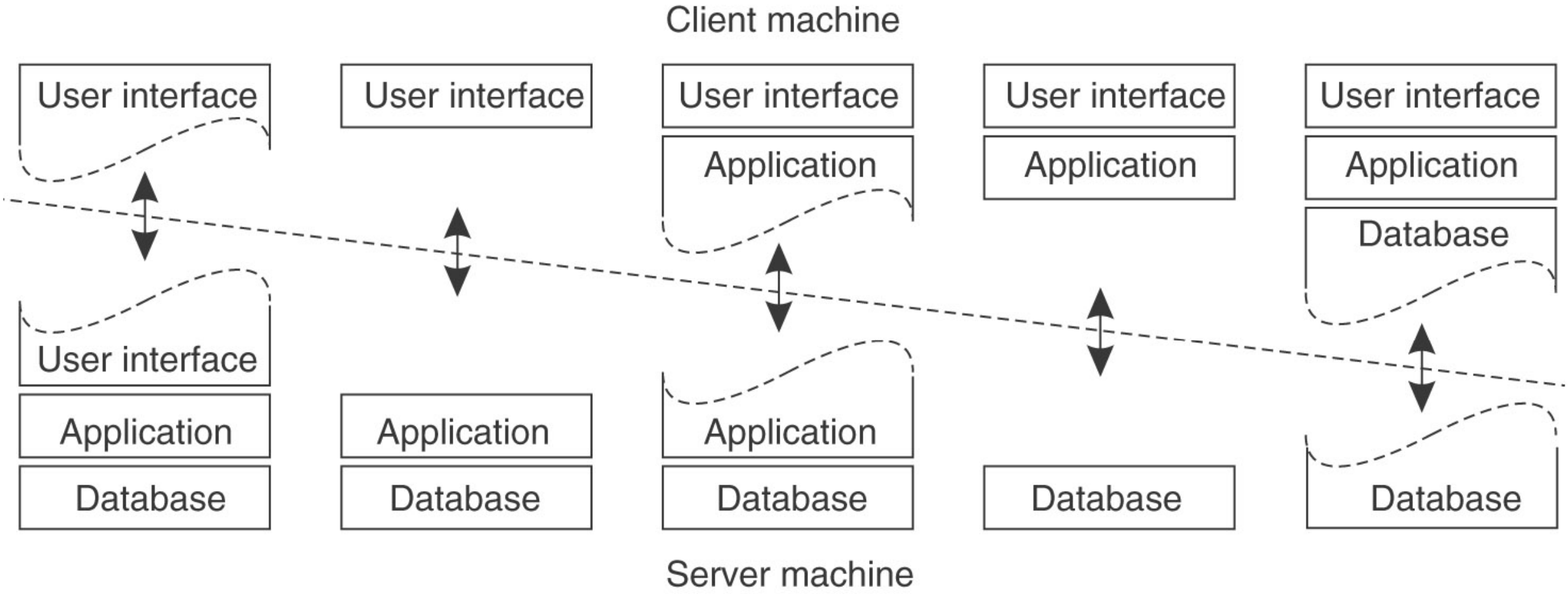




Drei-Ebenen-Architektur: „three-tier“

Präsentation	• Kommuniziert mit dem Anwender
Fachlogik	• Führt die Geschäftsregeln aus, verwaltet Prozessinformationen
Datenbank-management	• Datenzugriff und Datenspeicherung

Ebenen im Client/Server Modell



Thin Client ⟷ Fat Client

Gleichrangige Prozesse

Aufgaben der Peer-Prozesse

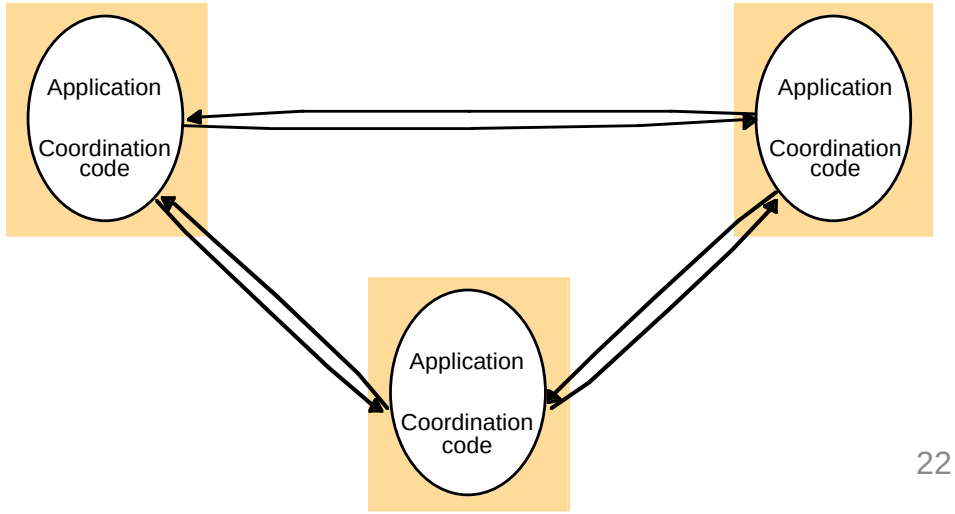
- Konsistenz der Ressourcen auf Anwendungsebene
- Synchronisation der Aktivitäten auf Anwendungsebene

Eigenschaften

- Vermeidet Flaschenhals-Prozesse
- Meist höhere Komplexität

Beispiele

- File-Sharing-Systeme: Jedes System teilt den anderen Peer-Prozessen mit, welche Dateien zur Verfügung stehen
- P2P basierte Groupware (z.B. Groove, Skype): Nachrichten eines Gruppenchats werden vom initiierenden Prozess an alle Teilnehmer geschickt



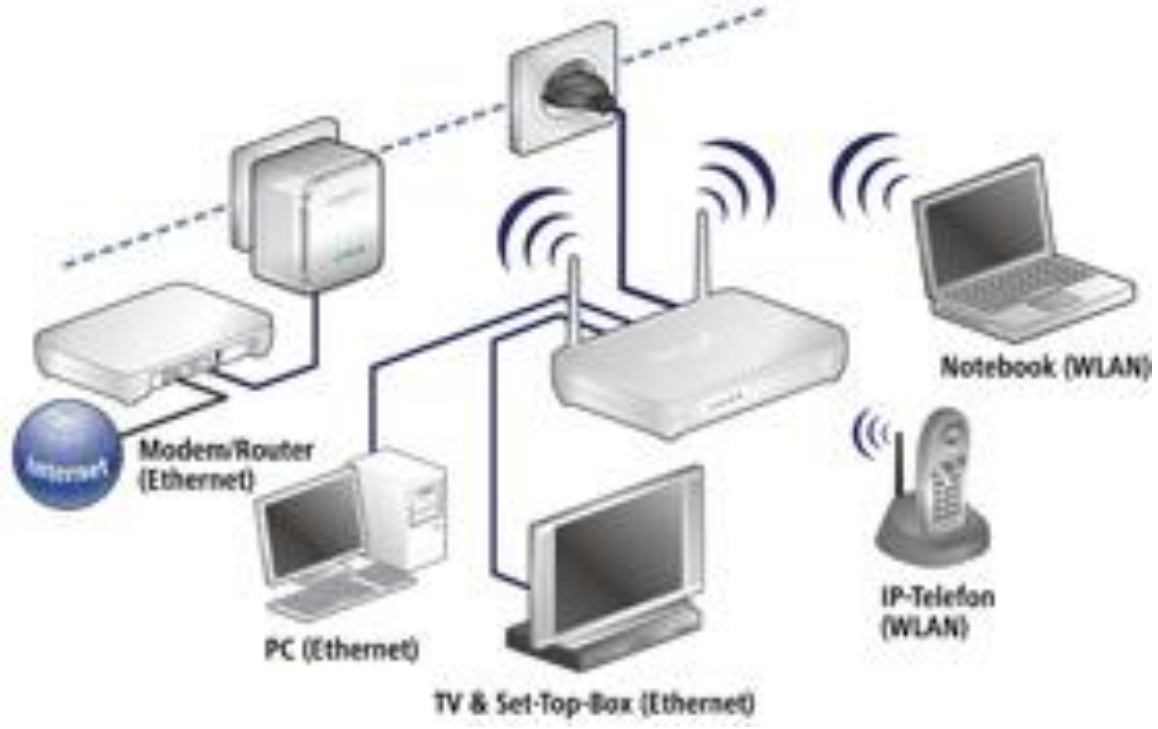
Gliederung

1. Verteilte Systeme
    - Motivation
    - Eigenschaften
    - Architekturen

2. Netzwerke
    - Arten
    - Vermittlungstechniken
    - Schichtenmodell

Rechnernetz

„Ein Rechnernetz besteht aus mehreren autonomen Rechnern (Computern), welche zum Zweck des Datenaustauschs miteinander verbunden sind" – Enzyklopädie der Wirtschaftsinformatik



Beispiel: Powerline basiertes Heimnetzwerk

Es gibt lokal begrenzte Netze und Weitverkehrsnetze.

Typen

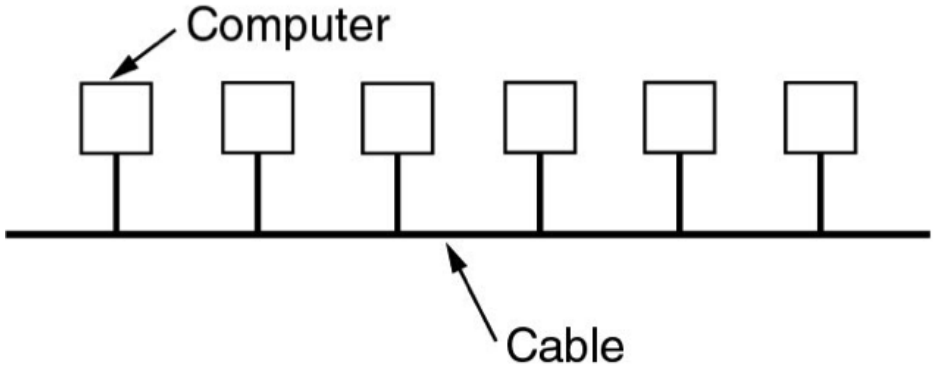
- Personal Area Networks (PAN)
- Local Area Networks (LAN)
- Metropolitan Area Networks (MAN)
- Wide Area Networks (WAN)
- Inter-Networks

Merkmale

- Übertragungsweg
  - Wired
  - Wireless
- Kennzahlen
  - Latenz
  - Bandbreite
  - Jitter

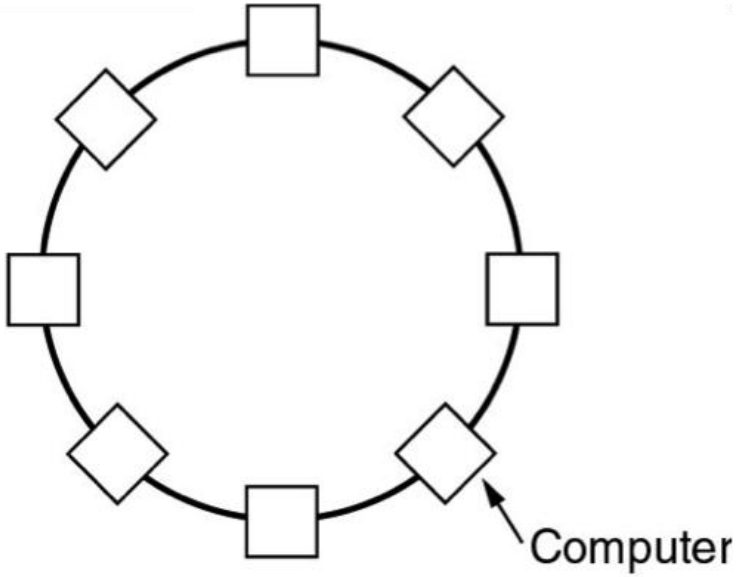
Local Area Networks (LAN)

Ein **LAN** ist ein lokales Netz, dass Endsysteme innerhalb eines oder benachbarter Gebäude verbindet. Häufig basieren lokale Netze dabei auf Ethernet oder drahtlosen Technologien.



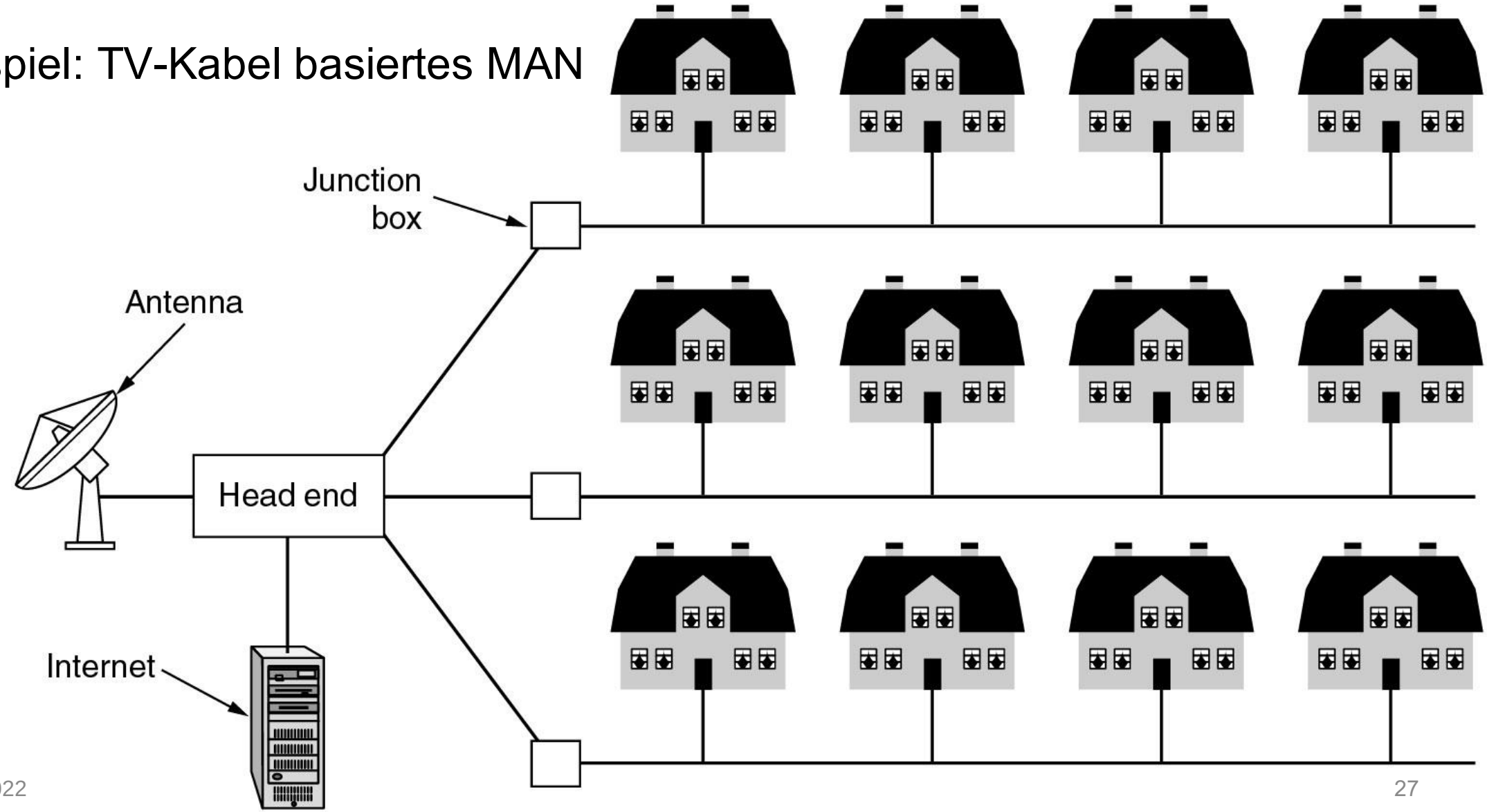
Netzwerktopologien

- Bus (z.B. Ethernet)
- Ring (z.B. Token Ring)



Metropolitan Area Network (MAN)

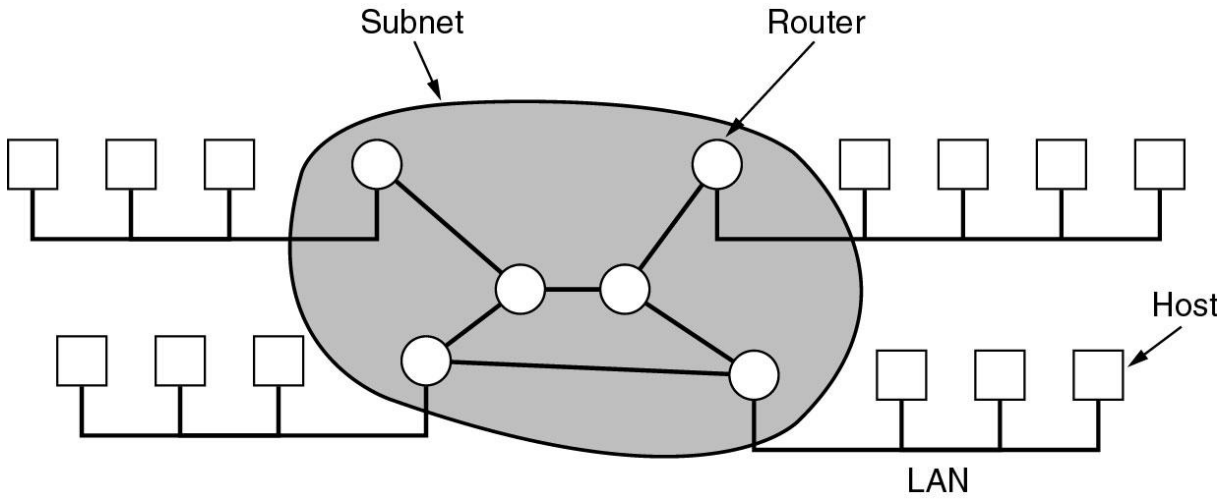
Beispiel: TV-Kabel basiertes MAN



Wide Area Networks (WAN)

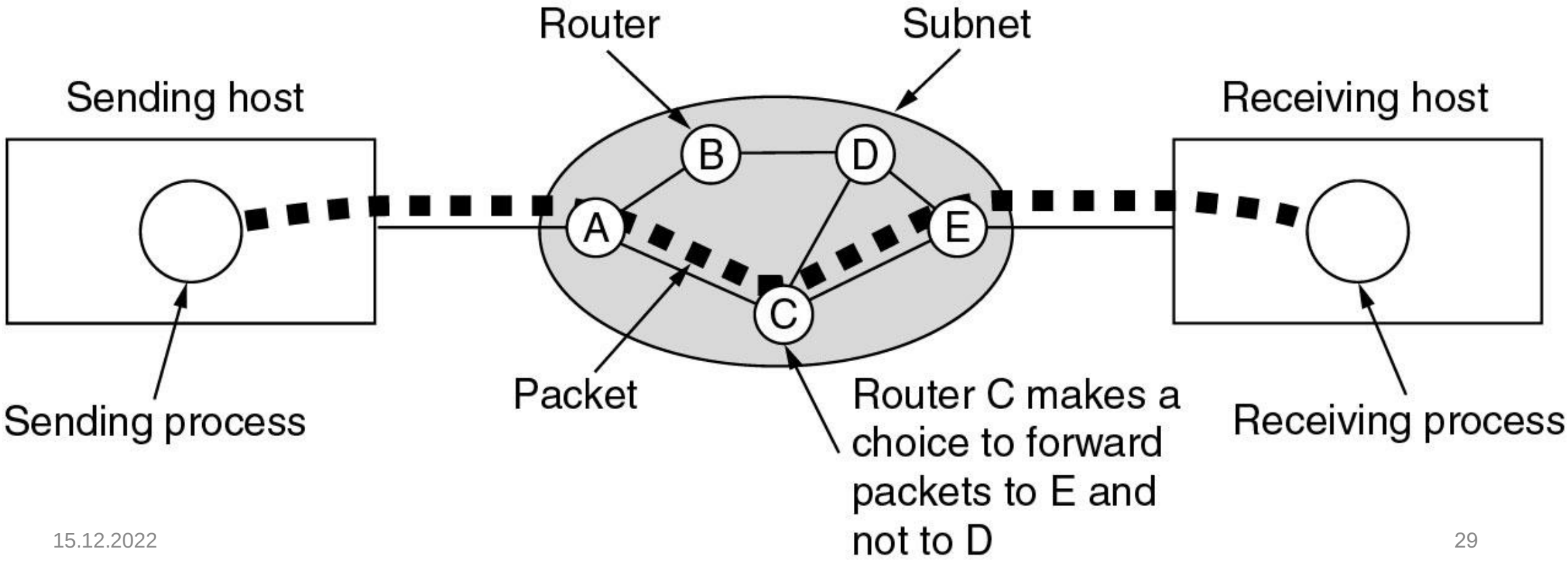
Ein Weitverkehrsnetz (WAN) ist ein Rechnernetz, dass

- einen sehr grossen geografischen Bereich (Land, Kontinent oder die ganze Welt) abdeckt.
- oft setzt es sich aus vielen einzelnen, kleineren, von mehreren Organisationen betriebenen Rechnernetzen zusammen,
- die über Vermittlungssysteme miteinander verbunden werden.



WAN - Vermittlungssysteme

Weiterleitung eines Paket-Strom (stream of packets)
vom Sender zum Empfänger.



Gliederung

1. Verteilte Systeme
    - Motivation
    - Eigenschaften
    - Architekturen

2. Netzwerke
    - Arten
    - **Vermittlungstechniken**
    - Schichtenmodell

Vermittlung (Switching)

Leitungsvermittlung (circuit-switching)

- Zu Beginn wird eine Leitung zwischen Sender und Empfänger aufgebaut. Die Leitung dient dann zur Übertragung von Datenströmen (Synchrone Übertragung, zeitorientierte Tarife, geringes Jitter)
    - Beispiel: Analoges Telefon (früher)

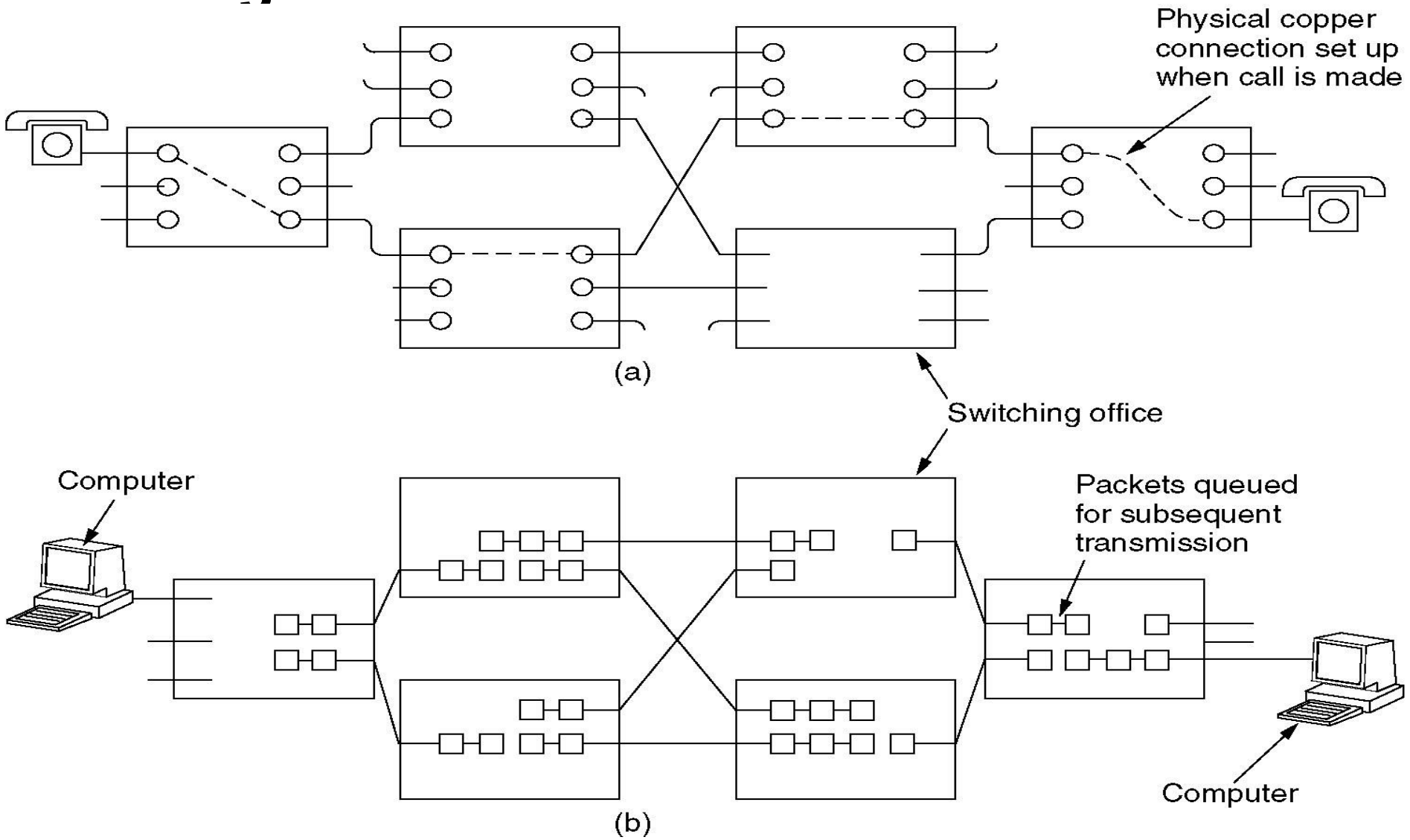
Paketvermittlung (packet-switching)

- Aufteilung der Nachricht in Pakete, die unabhängig voneinander zum Ziel geschickt werden. Sie müssen nicht die gleiche Route nehmen (Asynchrone Übertragung, volumenorientierte Tarife, hohes Jitter)
    - Beispiel: TCP/IP, Voice over IP (VoIP)

Nachrichtenvermittlung (message-switching)

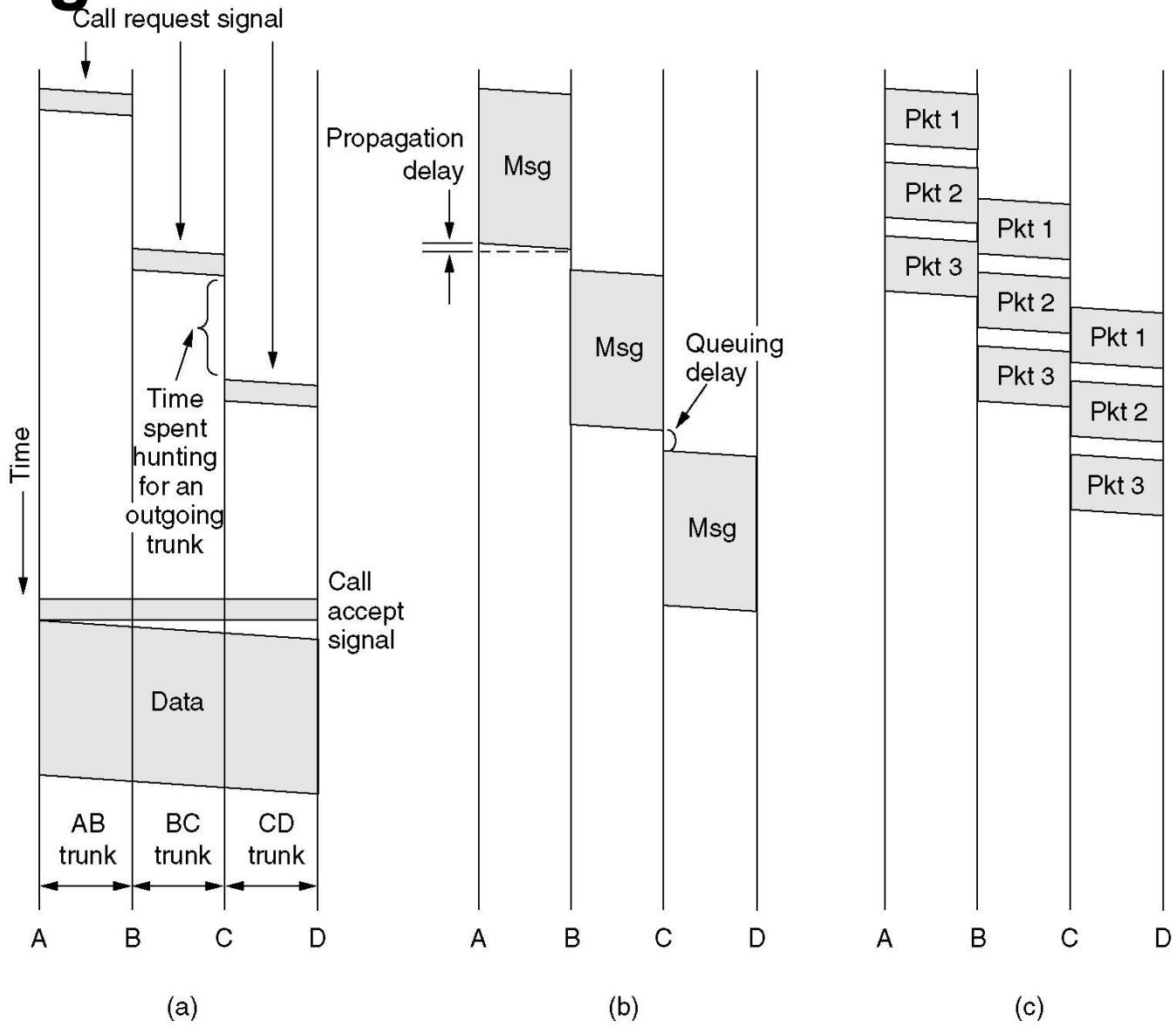
- Nachricht wird als ganzes verschickt

Strukturdiagramm



(a) Leitungsvermittlung (b) Paketvermittlung

Strukturdiagramm



(a) Leitungsvermittlung (b) Nachrichtenvermittlung (c) Paketvermittlung

Vergleich

Item	Circuit-switched	Packet-switched
Call setup	Required	Not needed
Dedicated physical path	Yes	No
Each packet follows the same route	Yes	No
Packets arrive in order	Yes	No
Is a switch crash fatal	Yes	No
Bandwidth available	Fixed	Dynamic
When can congestion occur	At setup time	On every packet
Potentially wasted bandwidth	Yes	No
Store-and-forward transmission	No	Yes
Transparency	Yes	No
Charging	Per minute	Per packet

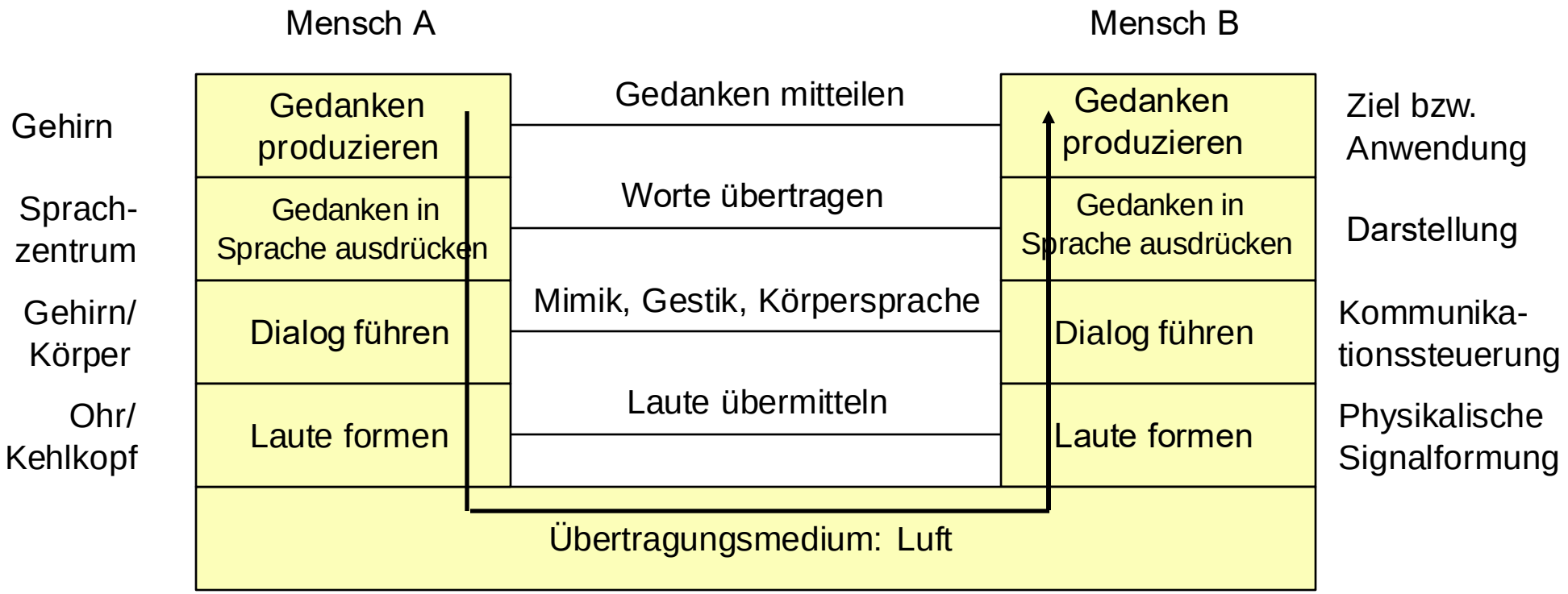
Gliederung

1. Verteilte Systeme
    - Motivation
    - Eigenschaften
    - Architekturen

2. Netzwerke

- Arten
- Vermittlungstechniken
- **Schichtenmodell**

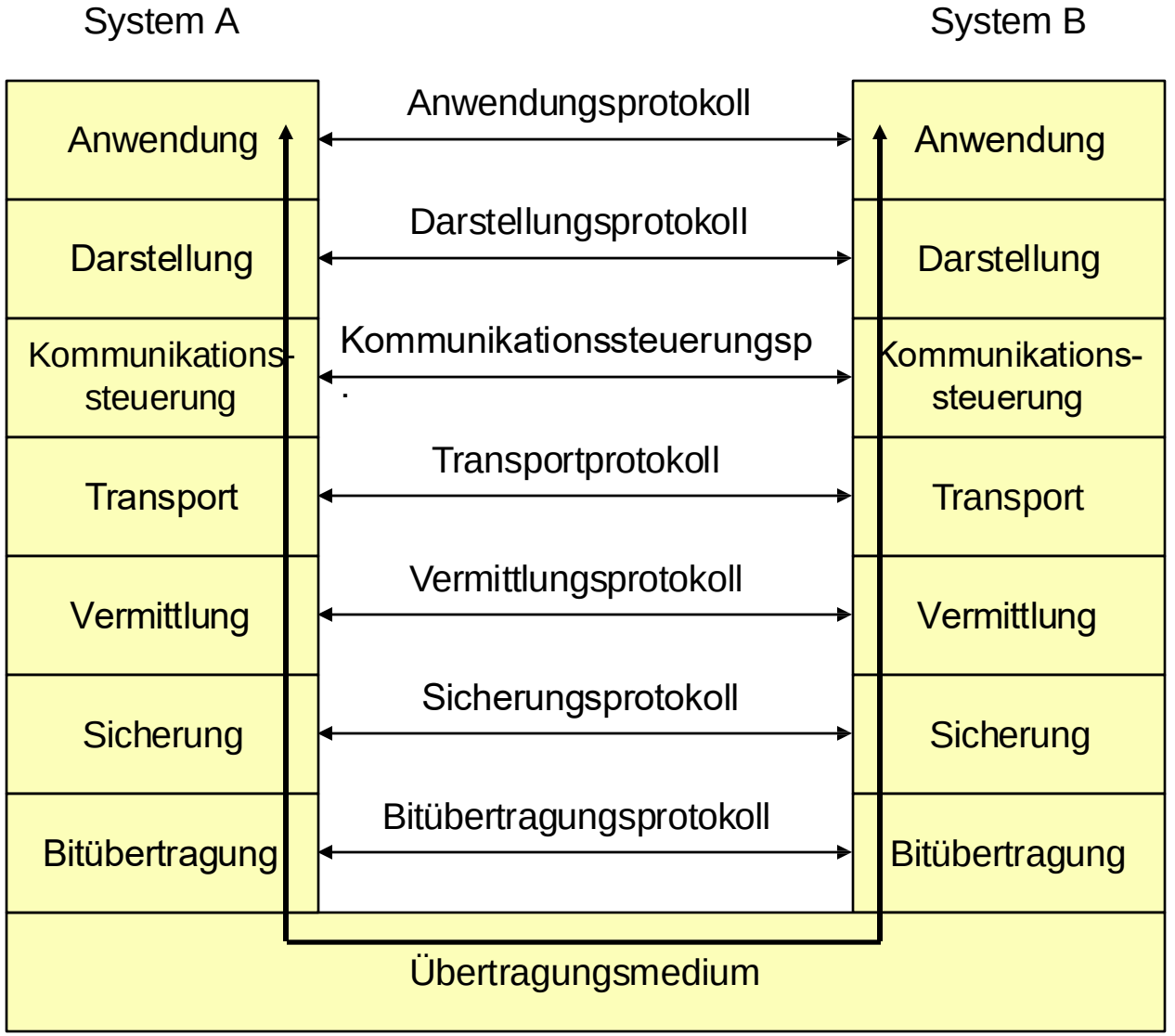
Ebenen-Modell der Mensch-zu-Mensch-Kommunikation



Das OSI-Referenzmodell der ISO (International Standards Organization) ermöglicht Kommunikation in offenen Systemen.

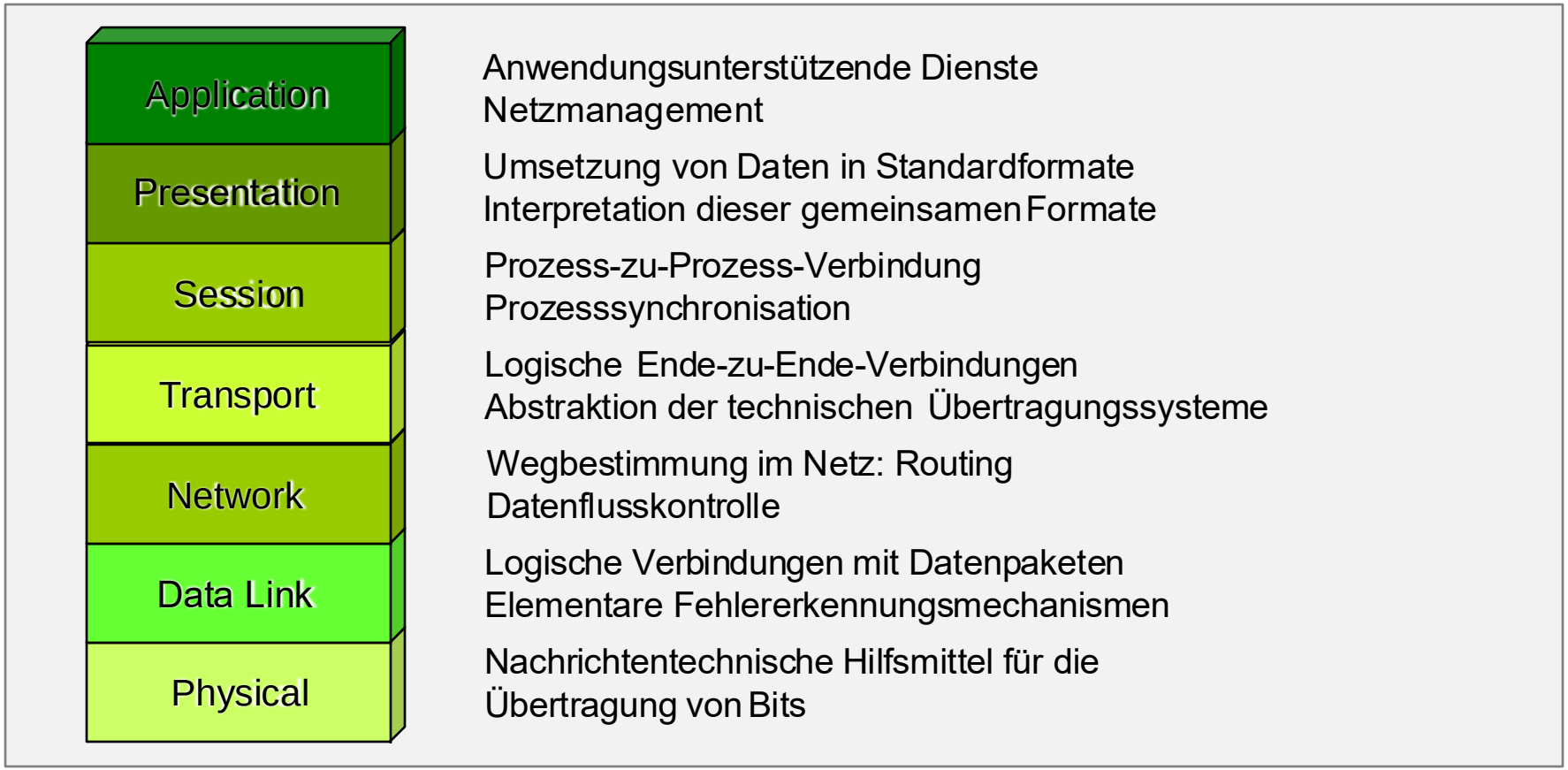
Open Systems Interconnection (OSI) Reference Model

- 1979 entwickelt
- 1983 ISO Standard Referenzmodell
- Unterteilt Aufgaben in sieben aufeinander aufbauende Schichten (layers)



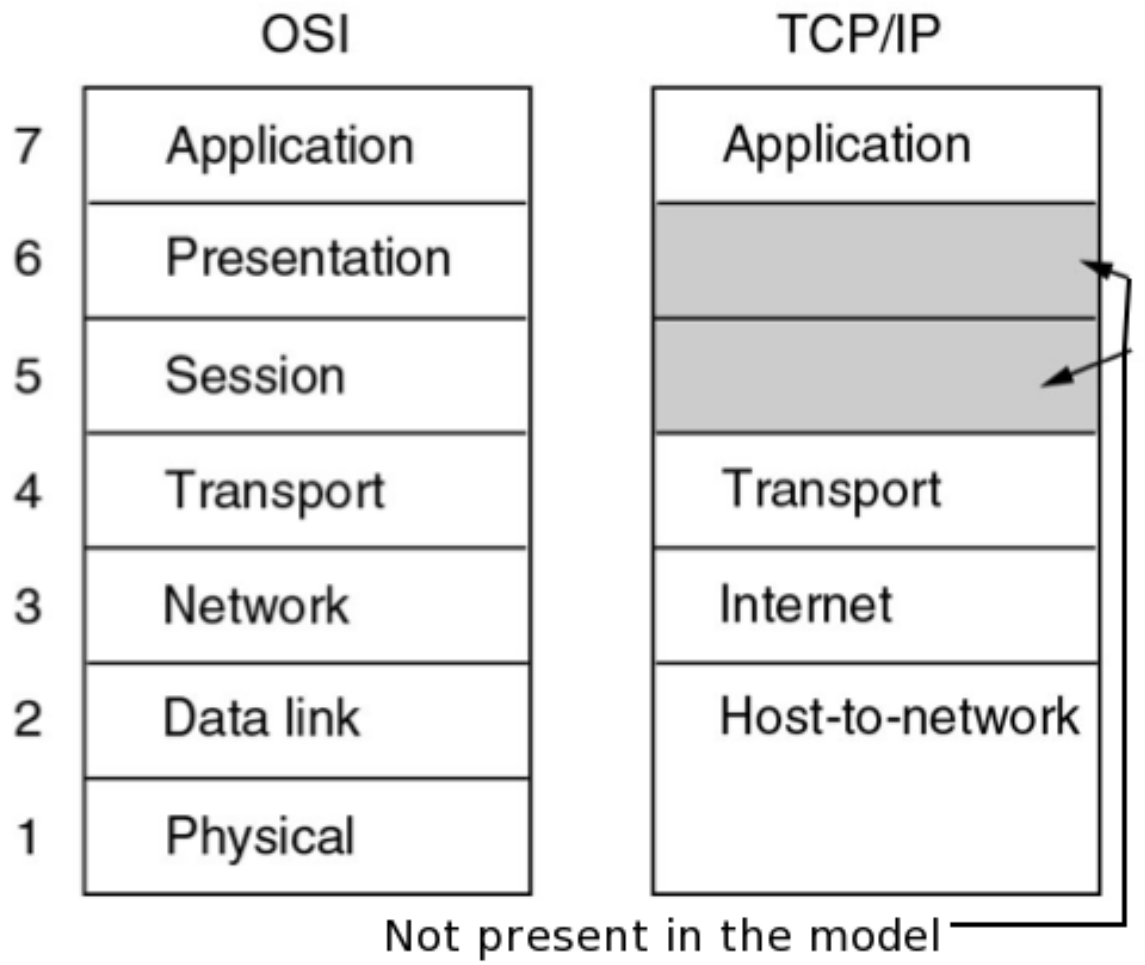
OSI: Open Systems Interconnection

Idee: Separation of Concerns. Jede Schicht übernimmt spezifische Aufgaben, sodass man sich in höheren Schichten nicht darum kümmern muss.



TCP/IP Modell

- Familie von Netzwerkprotokollen
- Grundzüge bereits 1974 festgelegt
- Version 4 bis 1981 in den RFCs definiert
- Hardware-unabhängig (implementiert für alle gängigen OS)



(L1) Bitübertragungsschicht

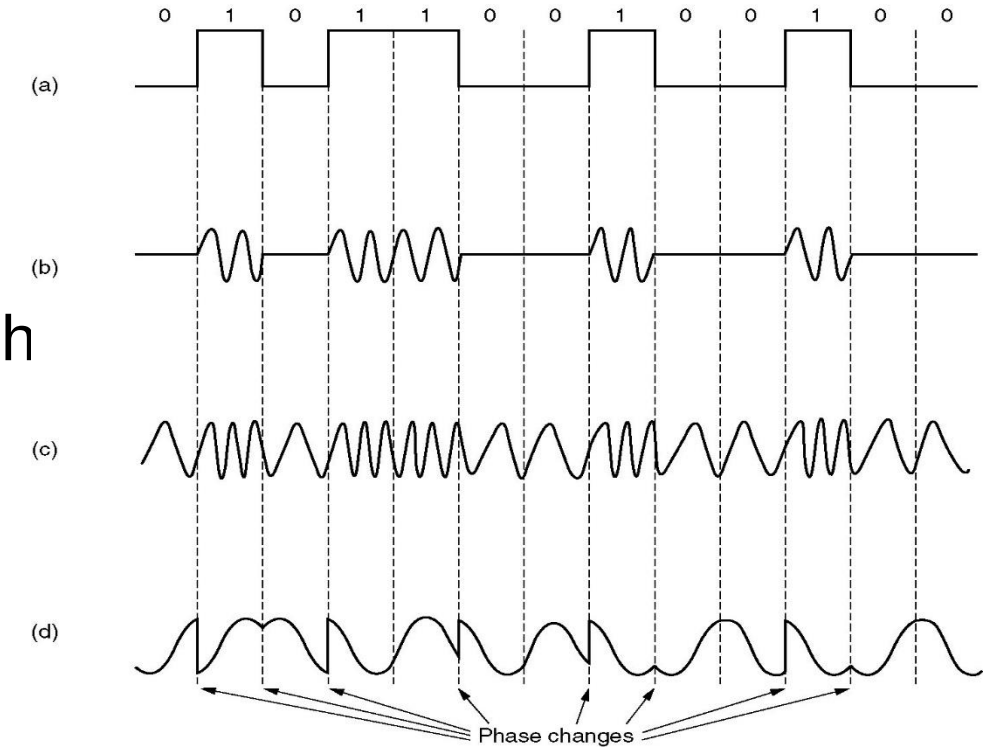
Kodieren des digitalen Datenstrom und übertragen durch Modulation physikalisch /elektromagnetischer Signale

Techniken:

- Leitungsbasiert
- Funkbasiert
- Satellitenbasiert

Regelung des Datenverkehr

- Technische Maßnahmen
- Politische Maßnahmen



(a) A binary signal
(b) Amplitude modulation
(c) Frequency modulation
(d) Phase modulation

Modulation

- Variation von Frequenz, Amplitude und/oder Phase einer Welle
- Zur Überlagerung der (Träger-)Welle mit dem Nutzsignal z.B. bei Funk, Modem, Breitbandkabel, ...

Leitergebundene Übertragungstechnik Beispiel

Twisted-Pair-Kabel

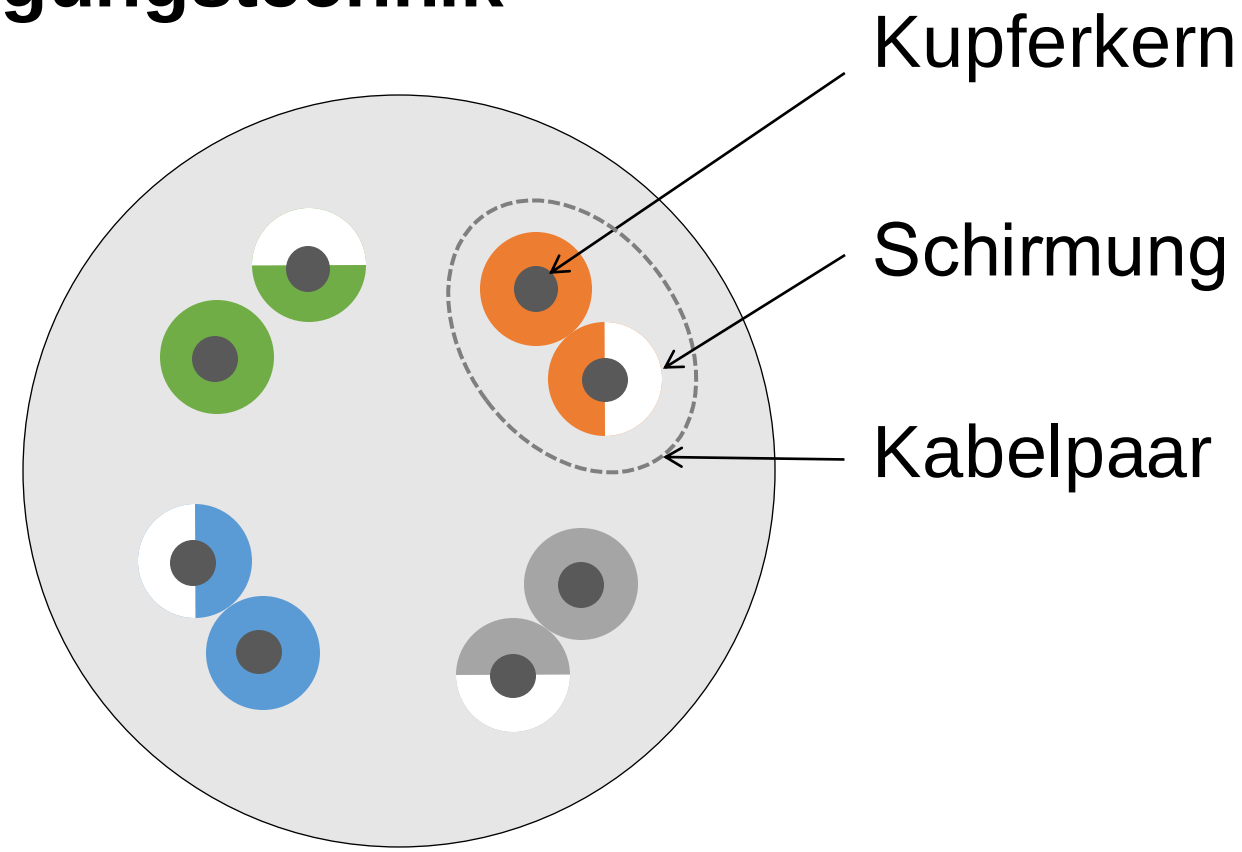
- 4 Kabelpaare
- Jedes Kabelpaar ist verdreht

Geschwindigkeit

- Ca .10-Gbit/s

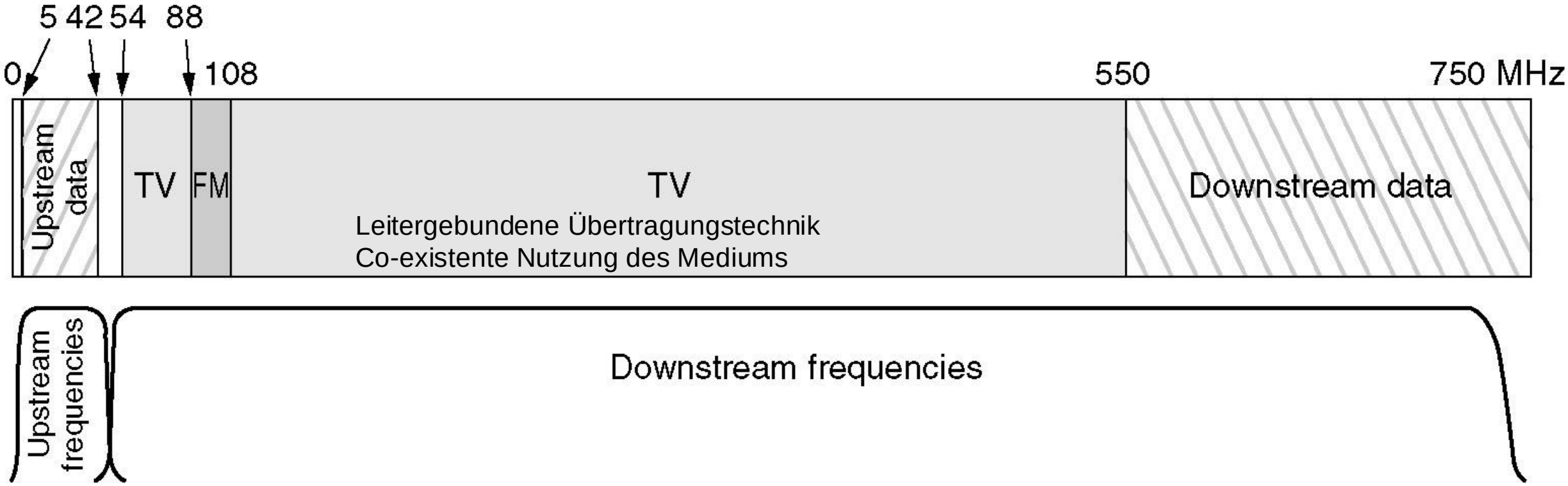
Eigenschaften

- Getrennte Sendekanäle
- Full-Duplex möglich



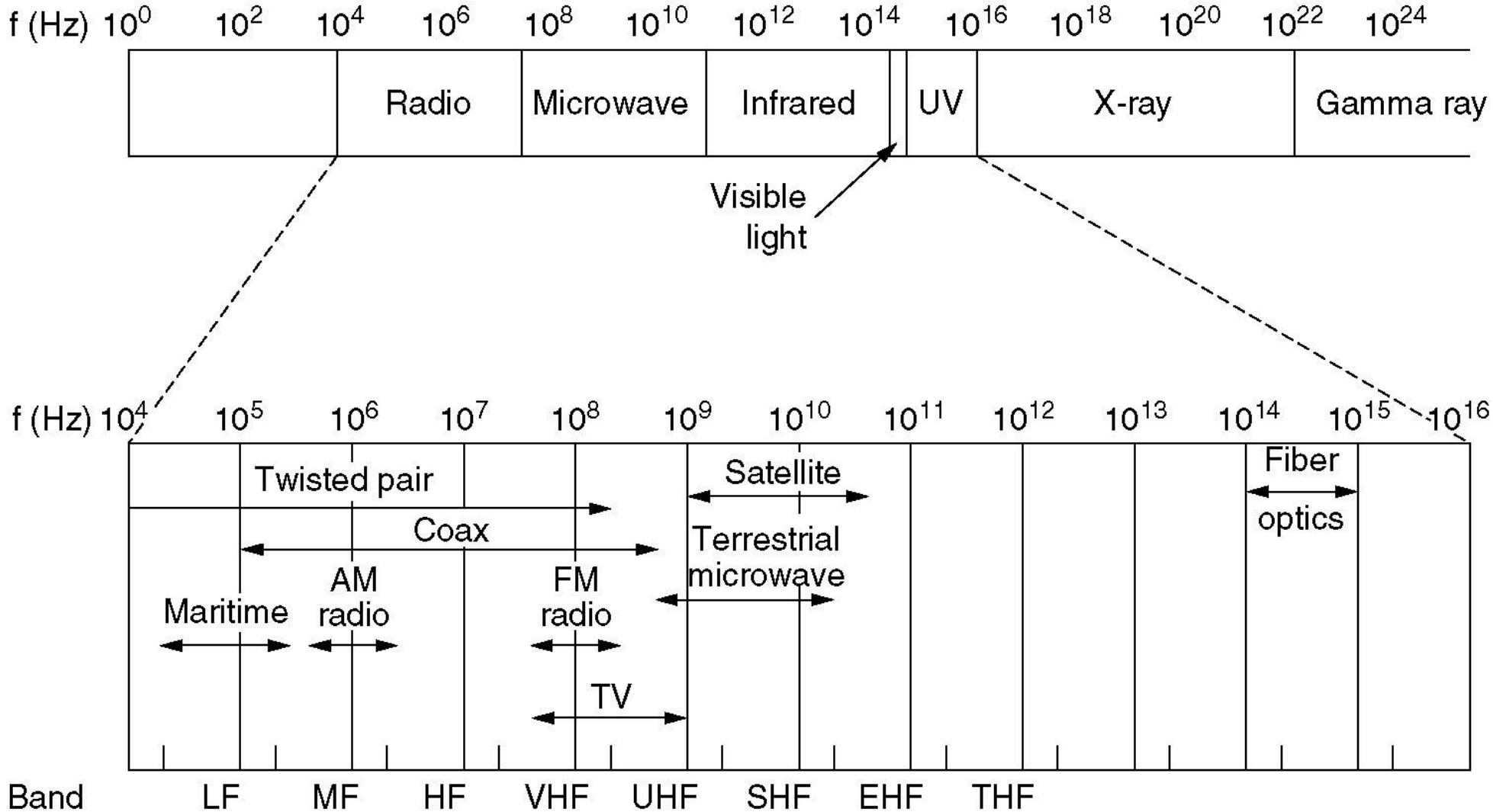


Leitergebundene Übertragungstechnik – Co-existente Nutzung des Mediums



Fequenzmultiplexing: Typische Aufteilung der Frequenzen US-amerikanischen TV-Kabels zur Internet-Nutzung

Elektromagnetisches Spektrum und seine Nutzung zur Kommunikation



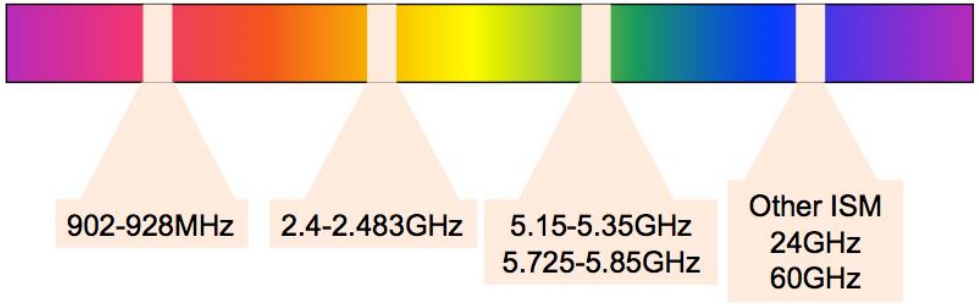
Politische Regelung – ISM Bänder

Ein ISM-Band (Industrial Scientific and Medical band) ist ein Frequenzbereich, der nicht der staatlichen Regulierung unterliegt und lizenzfrei für industrielle, wissenschaftliche und medizinische Anwendungen genutzt werden darf.

Jedoch müssen Auflagen bezüglich der Sendeleistung und der Störung benachbarter Frequenzbereiche eingehalten werden.

Beispiel:

- Aufstellen eines WiFi-Routers (genehmigungsfrei)
- Aufstellen eines UKW Senders (genehmigungspflichtig)



Nutzung der ISM Frequenzbandbereiche:

- 900MHz ISM band – cordless phones, some WAN, proprietary LAN, industrial heating
- 2.4GHz – government & military radio link, cordless phones, Bluetooth, 802.11b (Wi-Fi), HomeRF, microwave ovens
- 5GHz – mobile satellite, 802.11a, HiperLAN, HiperPAN, 802.15.3 (proposed), microwave ovens (future), fixed wireless

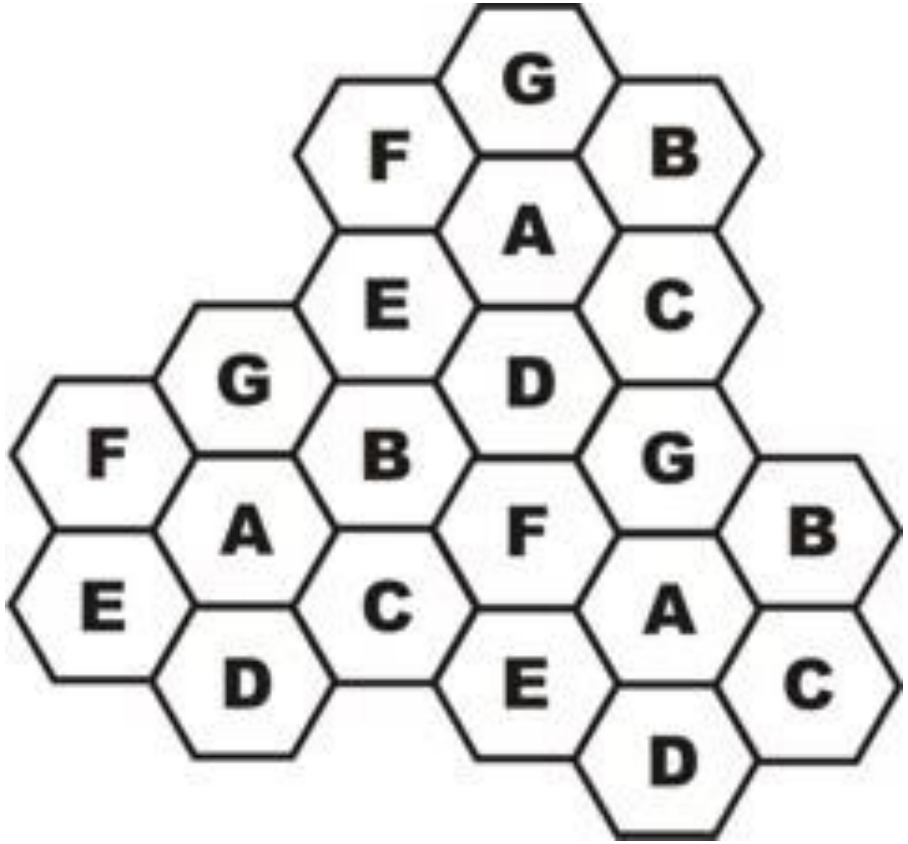
Mobilfunksystem

Zellulares Konzept

- für gleichmäßige gute Abdeckung wird der Raum in Zellen aufgeteilt
- Idealisiert: hexagonale Zelle mit jeweils ein Sendemast im Zentrum

Herausforderung

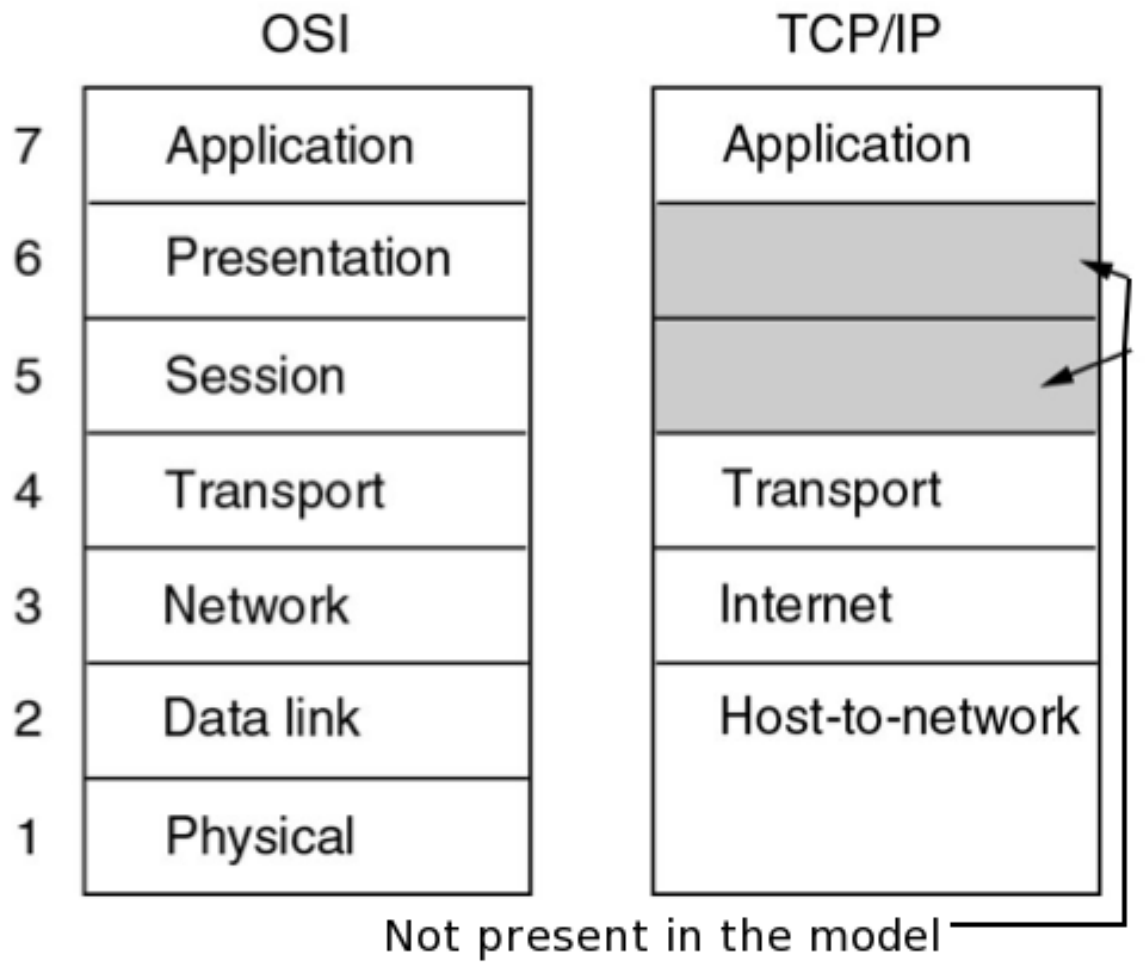
- Begrenzte Anzahl von Frequenzen bzw. Kanäle, gleichzeitig möglichst viele Mobilfunknutzer bedienen
- Wechsel eine Mobilfunkteilnehmers zu benachbarten Zelle möglichst Unterbrechungsfrei
- Funkverkehr der einzelnen dürfen sich nicht gegenseitig stören



Benachbarte Zellen verwenden unterschiedliche Frequenzen, nicht benachbarte dürfen gleiche verwenden

TCP/IP Modell

- Familie von Netzwerkprotokollen
- Grundzüge bereits 1974 festgelegt
- Version 4 bis 1981 in den RFCs definiert
- Hardware-unabhängig (implementiert für alle gängigen OS)



Die Sicherungsschicht (L2) bietet Schutz vor Übertragungs-fehlern und übernimmt die Übertragungssteuerung.

Gestaltungsaufgaben

- Wohldefinierte Dienste der Netzwerkschicht anbieten
  - insb. zuverlässige Datenübertragung
- Zugriff auf das Übertragungsmedium regeln
- Fehlerkontrolle
  - Erkennen und Korrigieren
- Überlastkontrolle
  - Senderate an aktuell verfügbare Bandbreite anpassen
  - Verlust von Daten verhindern

Datenübertragungs-Dienste

1. Verbindungslose Dienste ohne Bestätigung
2. Verbindungsorientiere Dienste ohne Bestätigung
3. Verbindungsorientiere Dienste mit Bestätigung
4. …

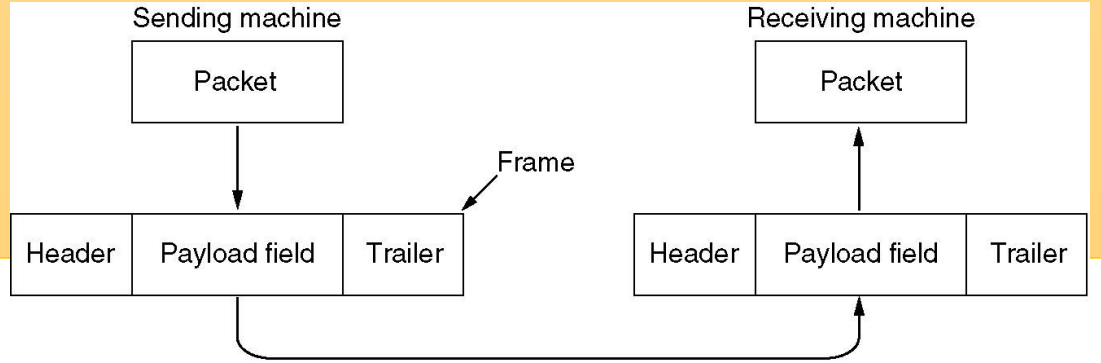
Datenübertragung

Arbeitsweise

1. Nutzdaten von der Quelle entgegennehmen
2. Empfänger und Sender entsprechend der Protokollspezifikation adressieren
3. Nutzdaten in Frames einpacken (Framing)
4. Frames an Ziel-Maschine übertragen
5. Nutzdaten auspacken und an obere Ziel-Sicht weiterleiten

Frames

- Bitmuster im Header und Trailer signalisieren Beginn und Ende
- Nutzdaten (Payload) im Payload field verpacken
- Zusätzliche Kontrollinformation im Header/Trailer
  - Sender, Empfänger
  - Frametypen, Fehlerkontrollinformation, …



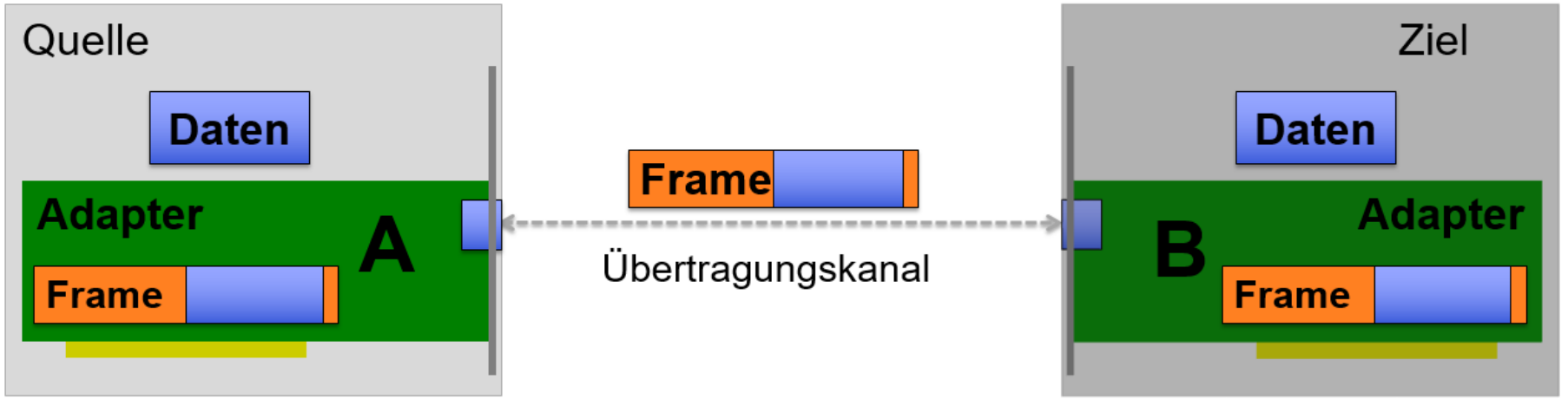
Datenübertragung - Beispiel

Arbeitsweise

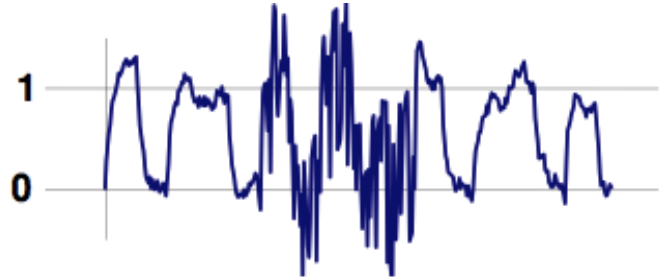
- Netzwerkkarte
  - Implementiert die Netzzugangsschicht
  - Adapter zwischen physikalischer und Datenverbindungs-Schicht

Frames

- Adapter Senderseite
  - Fügt Daten in einen Rahmen (Frame) ein
  - Fügt zusätzliche Daten zum Rahmen hinzu (z.B. für Fehlererkennung)
- Empfängerseite
  - Überprüft die empfangenden Daten
  - Leitet Daten an die obere Schicht weiter

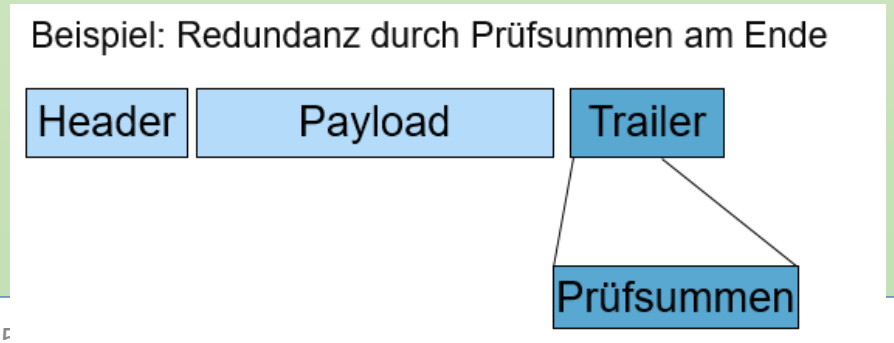


Fehlerkontrolle



Arbeitsweise

- Ursachen
  - Frames können verfälscht werden (z.B. Bits können während der Übertragung gekippt werden)
  - Frames können verloren gehen (z.B. Kollision, Empfänger überlastet)
- Allgemeiner Lösungsansatz
  - Einfügen von Redundanz



Frames

- Grundprinzipien der Fehlerbehandlung
  - **Error Correction**
    Fehlerkorrektur beim Empfänger
  - **Error Detection**
    Fehlererkennung beim Empfänger und Wiederholung der fehlerhaft übertragenen Informationen (retransmission).

Durch Störeinflüsse können ein oder mehrere Bits einer Nachricht falsch übertragen werden.

Es gibt drei Fehlerarten:

```
Original                        00010010 11010101 10111101 01111001
Einzelfehler:                   00010011 11010001 10111101 01111101
Unabhängige Mehrfachfehler:     00010010 11010101 11111001 01111001
Bursts:                         00010*** ******** 10111101 01111001
```

Durch Hinzufügen von Paritätsbits lassen sich Einzelfehler innerhalb einer Nachricht erkennen.

Parität: Nachricht wird ergänzt um zusätzliches Prüfbit P

Beispiel: ($x_1\, x_2\, x_3\, P$) mit $P = x_1+x_2+x_3 \pmod 2$

- Anzahl der Einsen in x_i ist gerade: $P=0$, sonst: $P=1$
- Es gilt: $0 = x_1+x_2+x_3+P \pmod 2$

Das Kreuzsicherungsverfahren ermöglicht dem Empfänger in den meisten Fällen einen Fehler selbständig zu korrigieren.

	1	2	3	4	5	6	7	8	VRC
BYTE 1	0	1	0	1	0	1	0	1	0
BYTE 2	1	0	1	0	0	0	1	1	0
BYTE 3	1	1	0	0	1	1	1	0	1
BYTE 4	0	1	1	1	1	0	1	0	1
BYTE 5	1	0	0	1	1	0	0	0	1
BYTE 6	1	1	0	1	0	0	0	1	0
BYTE 7	0	1	0	0	1	0	0	0	0
LRC	0	1	0	0	0	0	1	1	1

Datenbit gestört

	1	2	3	4	5	6	7	8	VRC
BYTE 1	0	1	0	1	0	1	0	1	0
BYTE 2	1	0	1	0	0	0	1	1	0
BYTE 3	1	1	0	0	0	1	1	0	1
BYTE 4	0	1	1	1	1	0	1	0	1
BYTE 5	1	0	0	1	1	0	0	0	1
BYTE 6	1	1	0	1	0	0	0	1	0
BYTE 7	0	1	0	0	1	0	0	0	0
LRC	0	1	0	0	0	0	1	1	1

Paritätsbit gestört

	1	2	3	4	5	6	7	8	VRC
BYTE 1	0	1	0	1	0	1	0	1	0
BYTE 2	1	0	1	0	0	0	1	1	0
BYTE 3	1	1	0	0	1	1	1	0	0
BYTE 4	0	1	1	1	1	0	1	0	1
BYTE 5	1	0	0	1	1	0	0	0	1
BYTE 6	1	1	0	1	0	0	0	1	0
BYTE 7	0	1	0	0	1	0	0	0	0
LRC	0	1	0	0	0	0	1	1	1

Die Übertragungssteuerung ist erforderlich, um Kollisionen durch gleichzeitiges Senden zu vermeiden.

Jeder Knoten (Sender/Empfänger) hat eine eindeutige 48 bit MAC-Adresse

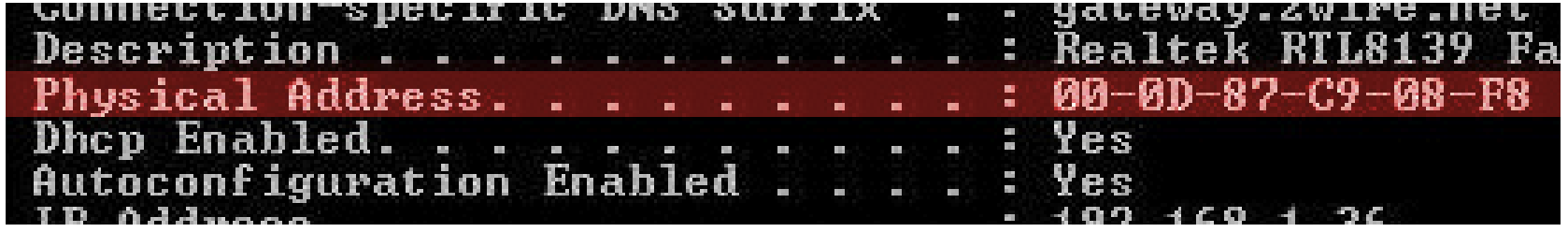
Vergabe von MAC-Adressen

- Vergabe durch die IEEE (Institute of Electrical and Electronics Engineers, Inc.) um Eindeutigkeit zu sichern
- Hersteller von Hardware kaufen Teile der Adressen (erste 24 Bits dienen als Herstellerkennung)

Eigenschaften: Flache Adressierung

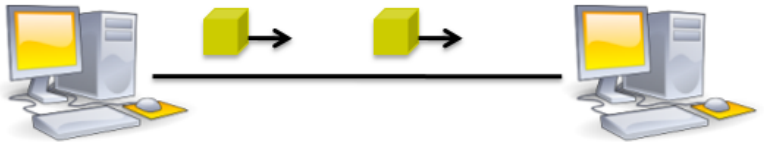
- Nachteil bei Skalierung da kein hierarchisches Routing möglich ist (wie z.B. bei IP-Adressen)
- Vorteil bei mobilen Geräten da Standortwechsel problemlos möglich ist, ohne Adresse zu ändern

Anzeige der MAC Adresse bei MS Windows

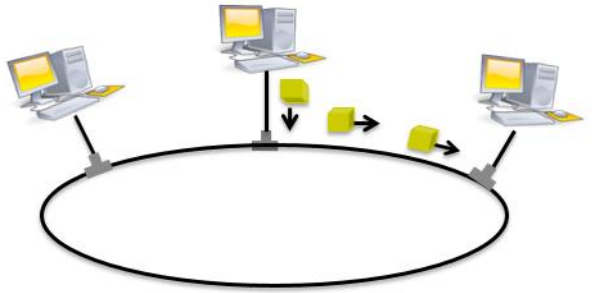


Gemeinsames Medium - Logische Topologien

Punkt zu Punkt: Nur zwei Knoten teiler sich das Medium, z.B. serielles Kabel zwischen 2 Rechnern



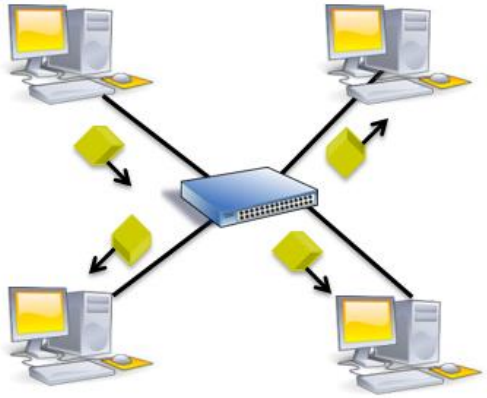
Ring: Gerichtete Ausbreitung, z.B. Token Ring



Bus: Mehrere Knoten teilen sich das Medium, Ausbreitung in 2 Richtungen, z.B. Ethernet mit Koaxialkabel



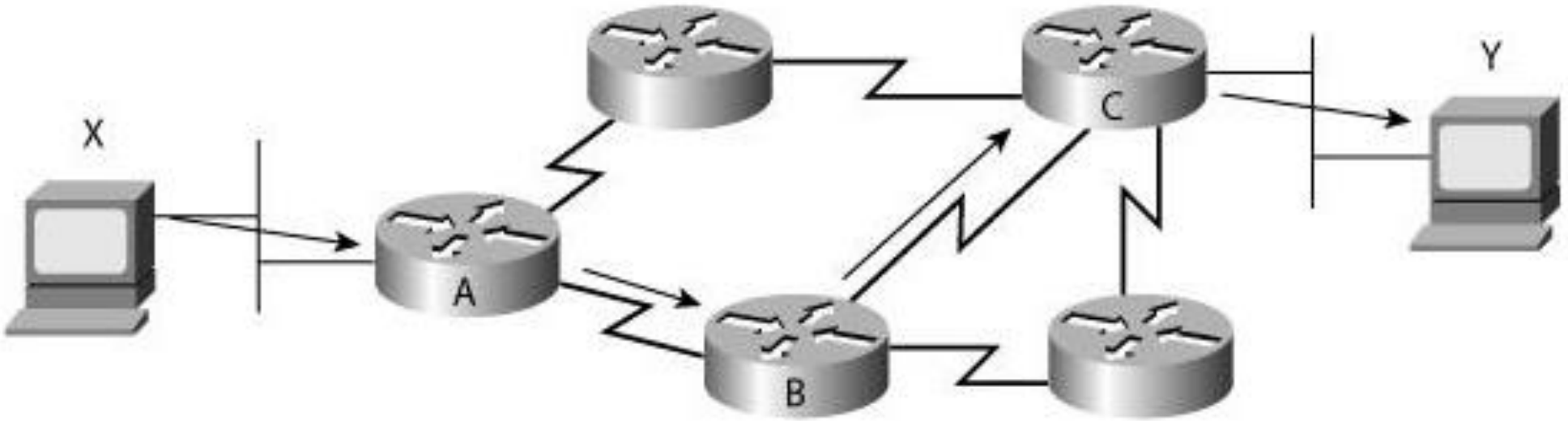
Stern: Mehrere Knoten teilen sich das Medium; Ausbreitung über zentralen Knoten, z.B. Ethernet mit Twisted Pair



Die Vermittlungsschicht (L3) stellt ein Adressierungsschema und Routingmechanismen (Wegewahl Sender/Empfänger) bereit.

Effiziente und **skalierbare Datenübertragung** zwischen heterogenen LAN/MAN/WAN Netzen zu ermöglichen

Heterogenität der Netze vor den höheren Schichten verstecken



https://www.tecchannel.de/i/detail/artikel/434734/5/347915/il-74722955636310194/

Die Vermittlungsschicht (L3) stellt ein Adressierungsschema und Routingmechanismen (Wegewahl Sender/Empfänger) bereit.

Aufgaben

Netzwerkübergreifende Dienste bereitstellen

- Senden von Paketen
- Aufbau “virtueller” End-to-End Verbindungen

Netzwerkübergreifende Adressräume bereitstellen

- z.B. IP-Adressen
- Adressen auflösen
  - z.B. IP-Adresse -> MAC-Adressen)

Netzwerkübergreifende Datenübermittelung

- Wegesuche (Routing)
  - Routingtabellen aufbauen und aktualisieren
  - Pakete an lokalen Empfänger oder fremden Router weiterleiten

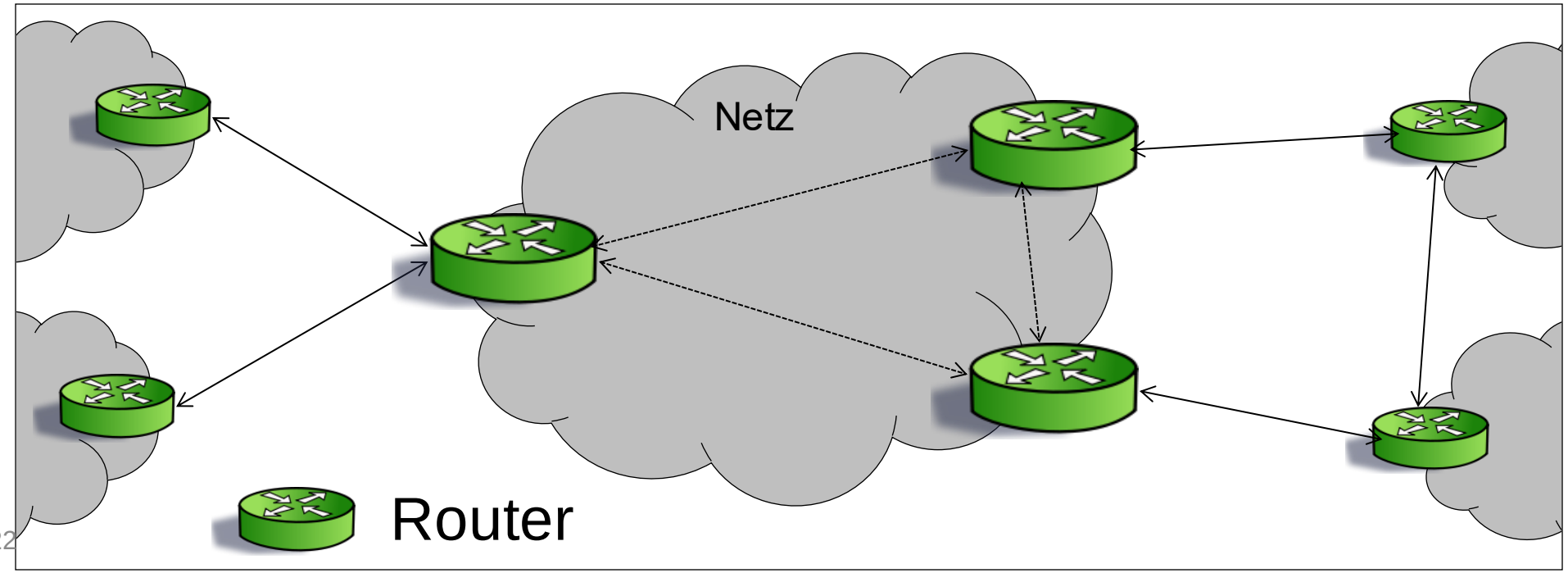
Aufteilen (Fragmentierung) von Pakete in Frames

- z.B. IP-Pakete -> Ethernet-Frames

Router – „Die Schnittstelle ins Netz“

Aufgaben eines Routers:

- Ins Netz eingehende Daten in das interne Netz leiten (und umgekehrt)
- Den Status des Netzes überwachen (optional)
- Erreichbare Netze und die Kosten für Weiterleitung bekanntgeben (optional)



Anforderungen an das Routing

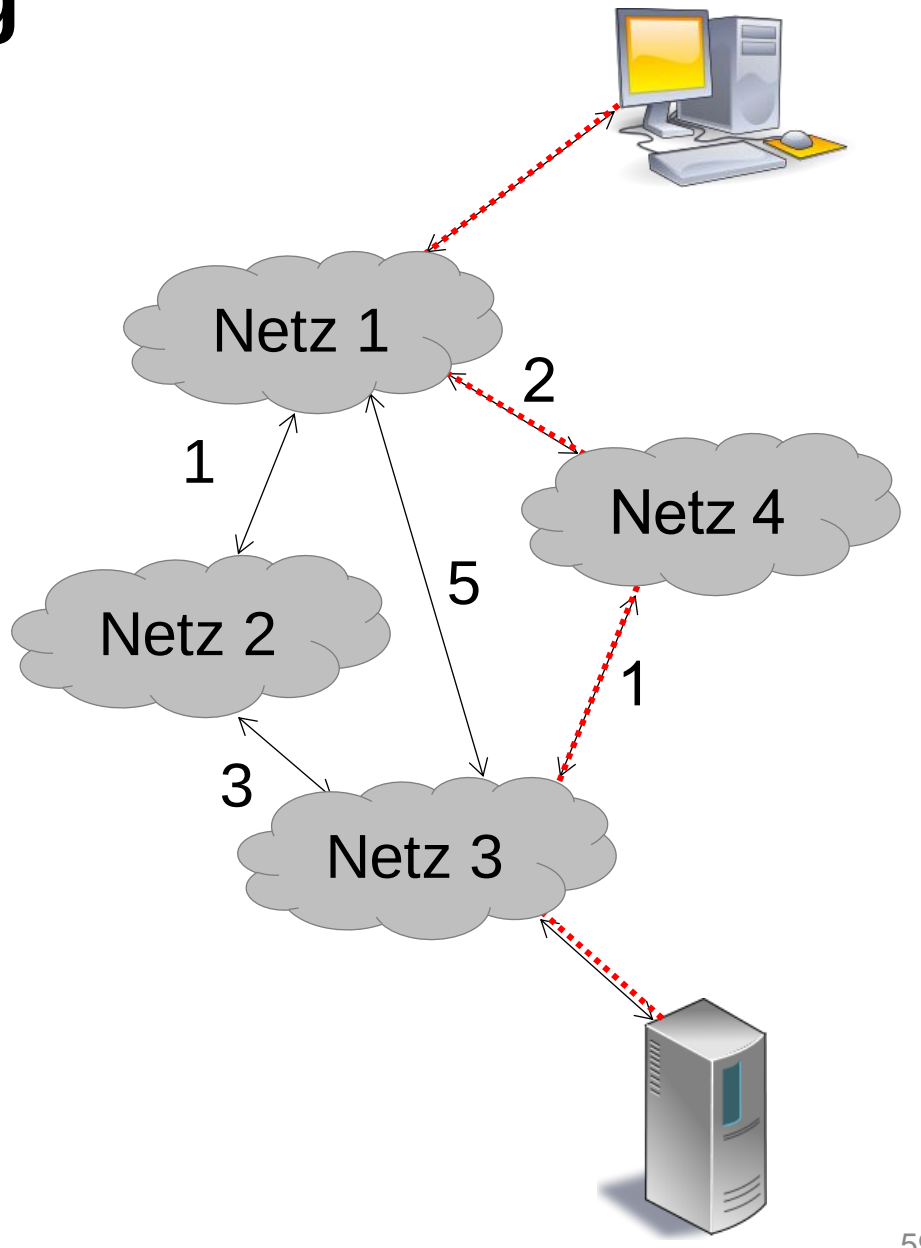
Einfachheit: Router besitzen wenig Speicher und Leistung; Wegewahl soll wenig Zeit kosten

Stabilität: Router sollen lange laufen

Robustheit: Router sollen alternative Wege bei Ausfall einer Route finden

Fairness: Alle Anfragen sollen an die Reihe kommen

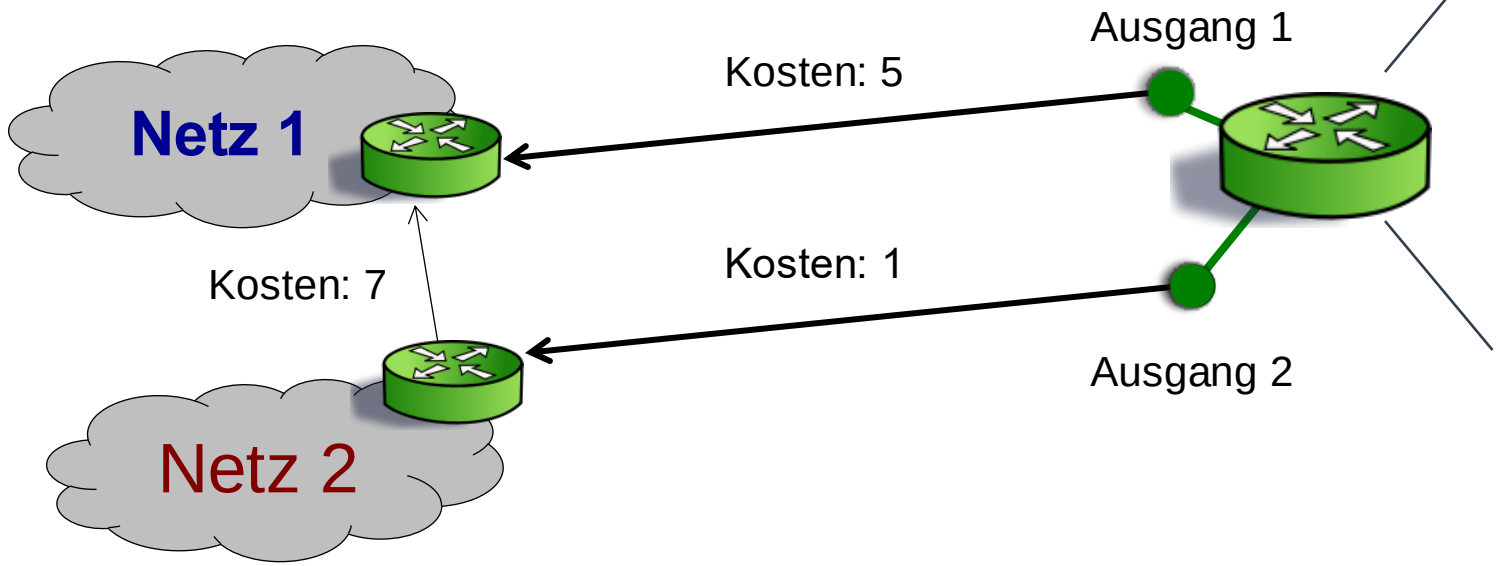
Optimalität: Bei Auslastung sollen Pakete warten



Routing Strategien: Statisches Routing

Funktionsweise: Router hat eine Routingtabelle in der beschrieben wird, welches Netz durch welche Ausgangsleitung erreicht werden kann. Dabei können Alternativen mit Prioritäten versehen werden.

Problem: Routen werden manuell festgelegt -> Aktualisierung aufwändig, lange Reaktionszeiten



Ziel Netz	Ausgang	Priorität
1	1	1
2	1	2
2	2	1

Routing Strategien: Dynamisches Routing

Funktionsweise

- Benachbarte Router tauschen dynamisch Tabellen aus
- Aus den Informationen werden jeweiligen Transportkosten berechnet

Theoretischer Hintergrund

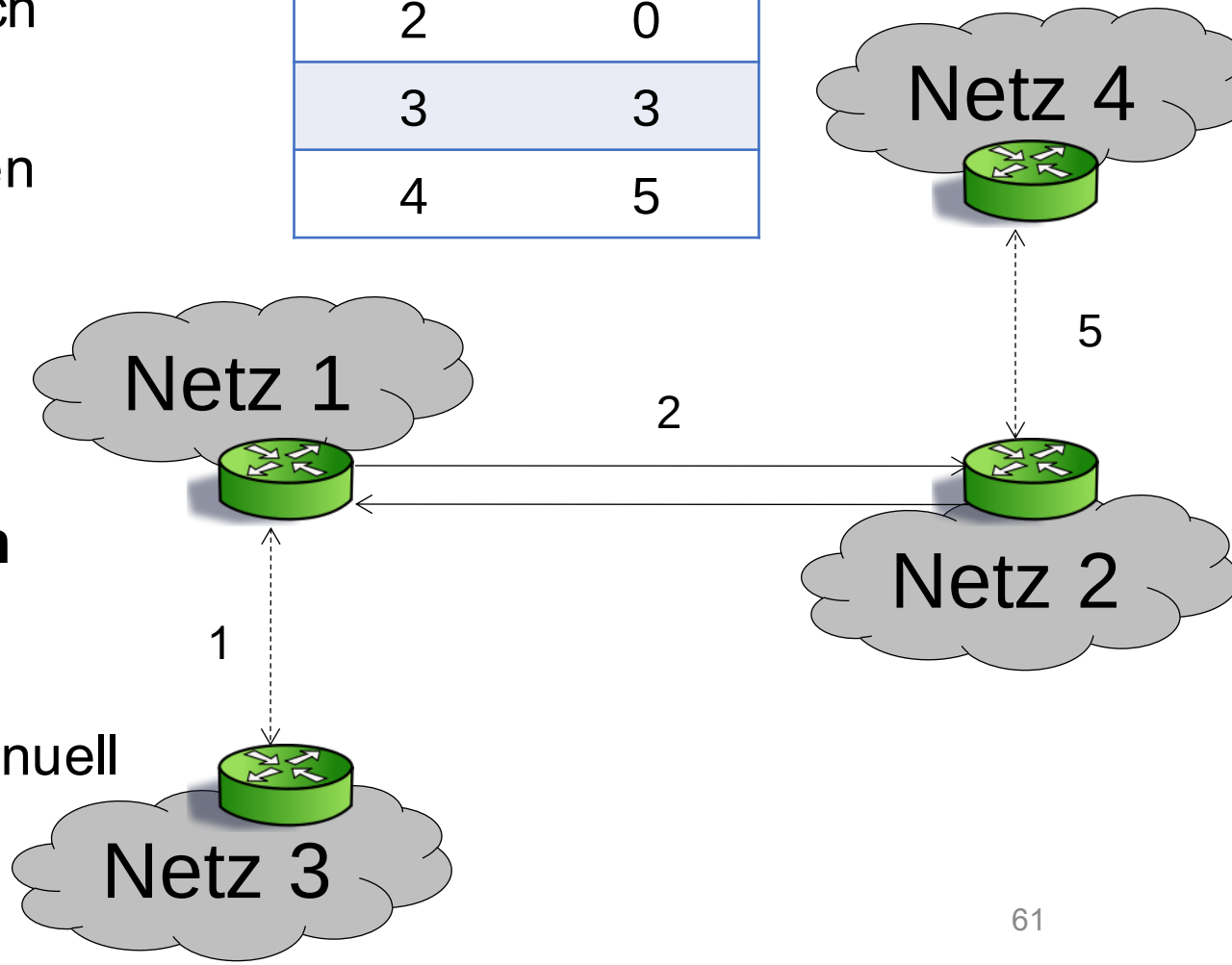
- Graphentheorie

Vorteil dynamischer Aktualisierungen

- Schnelle Reaktion bei Ausfällen
- Bei Ausfall müssen die Routen nicht manuell neu gesetzt werden

Netz 2:

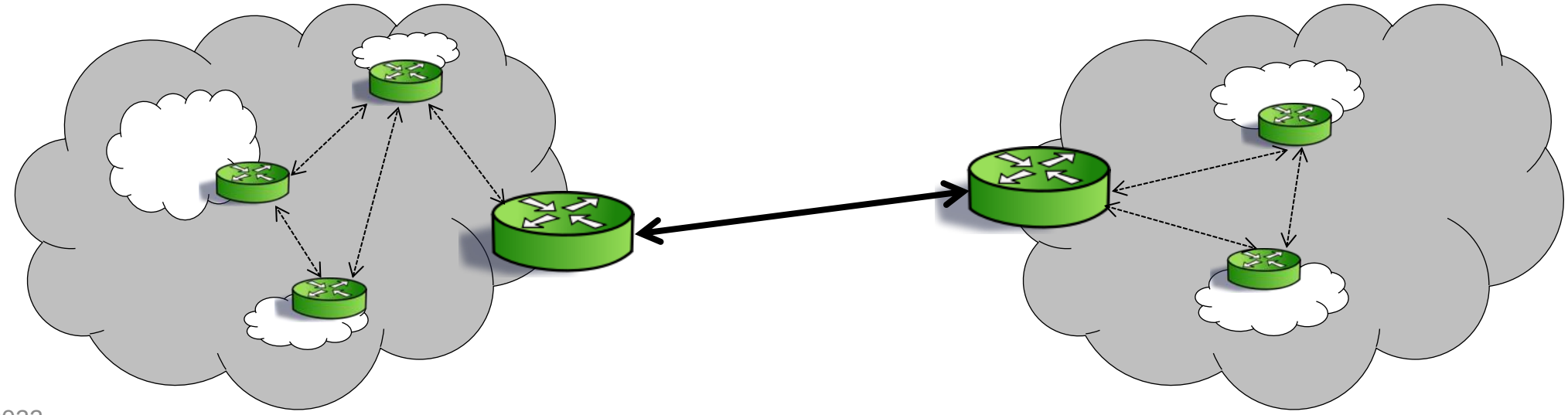
Ziel	Kosten
1	2
2	0
3	3
4	5



Routing Strategien: Hierarchisches Routing

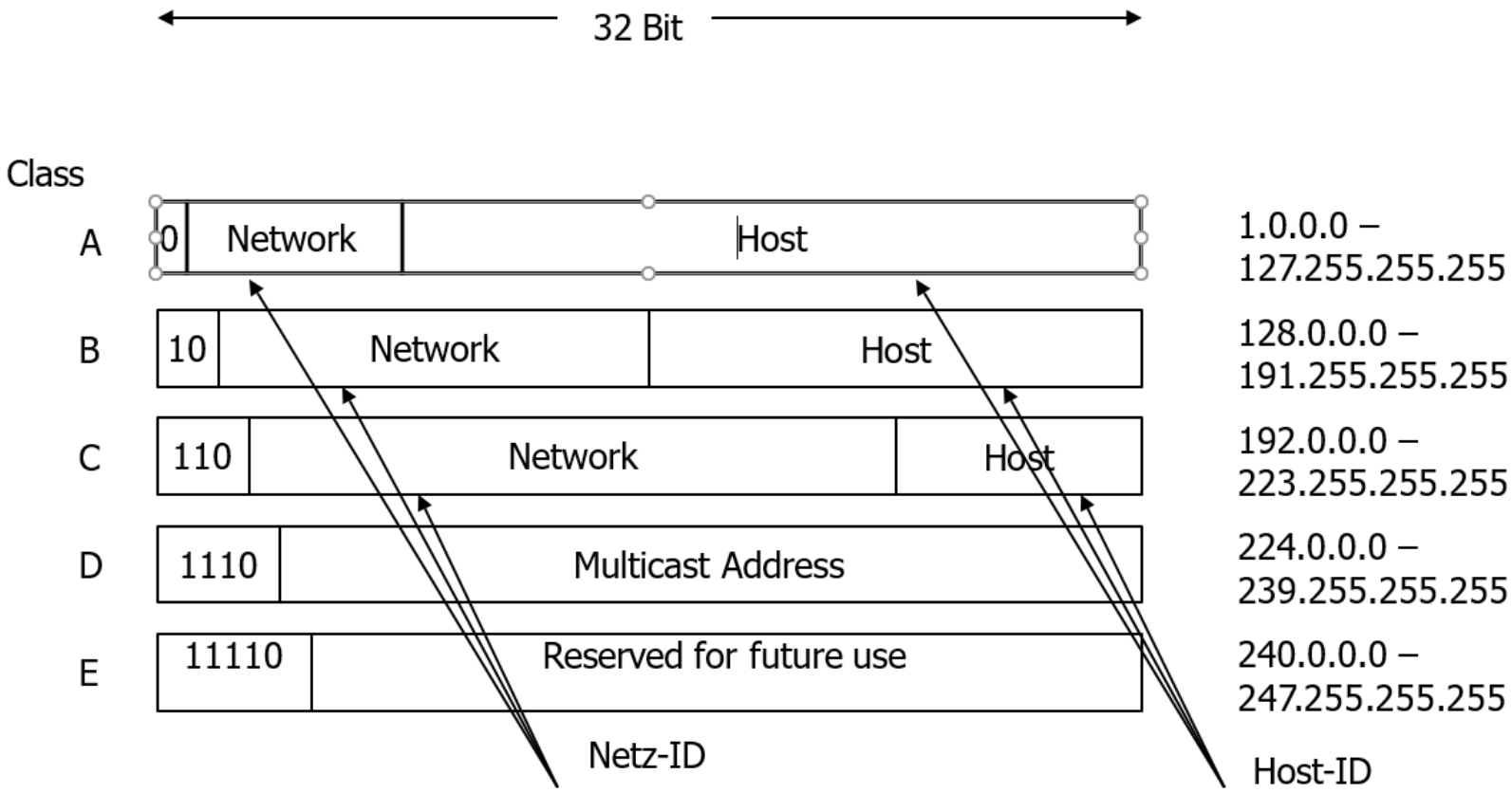
Motivation: Es gibt viele kleine Netze und der Austausch der Routing-Informationen für alle Netze ist nicht möglich. Die Verwalter der Netze wollen Routing selbst steuern/kontrollieren.

Prinzip: Das Routing findet auf mehreren Ebenen statt. Die Router werden in Regionen aufgeteilt Router weiß wie Daten in seiner Region geroutet werden müssen. Für externe Ziele wird ein spezieller Router verwendet.



Im Internet: Adressierung mittels IP-Adressen. Das IP-Protokoll stellt einen Paketvermittlungsdienst zur Verfügung.

IP-Adresse: 4 Byte, die als durch Punkte voneinander getrennte Dezimalzahlen notiert werden, z.B. 131.66.215.7



IPv6-Adressen haben 128 Bit und eine andere Syntax, z.B. fe80::a9a4:18c:ca16:4dae

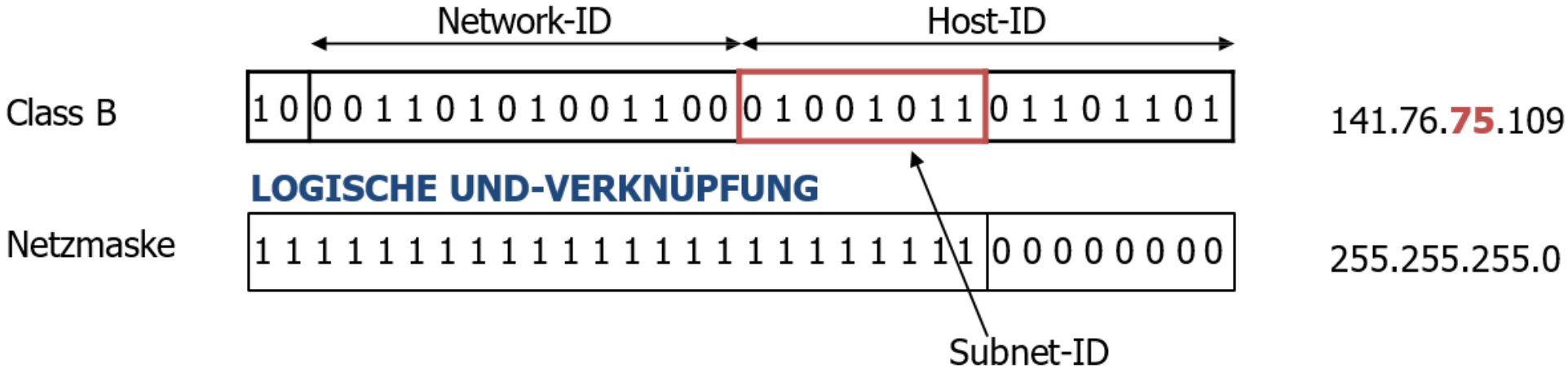
Es ist üblich, ein Netz in logisch voneinander separierte Subnetze zu teilen. Dazu verwendet man eine Subnetz-Maske.

Vorteile der Subnetze:

Dezentralisierung: Verwaltung des Adressraums unterliegt der jeweiligen Struktureinheit

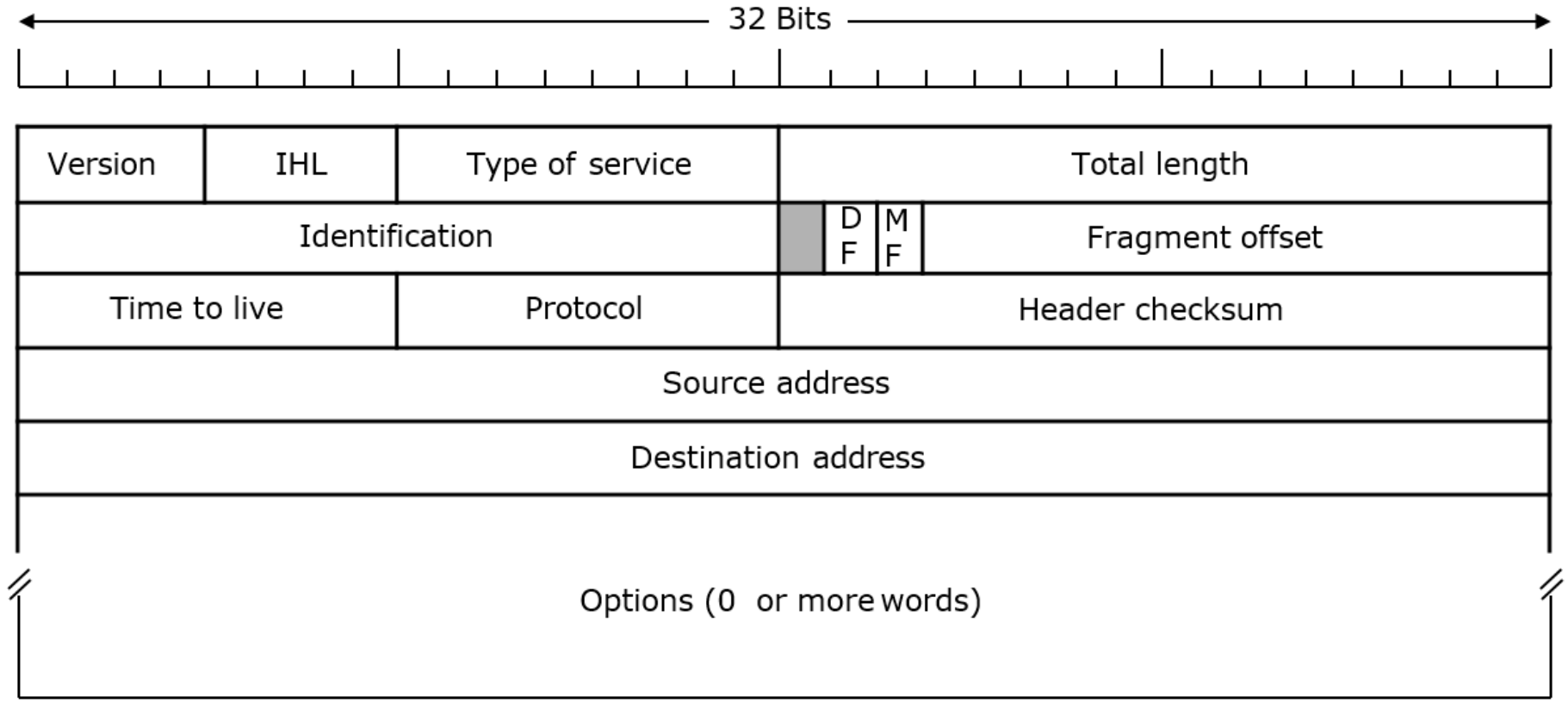
Lastverteilung: Reduktion der Verkehrslast am zentralen Router (bei interner Kommunikation)

IP Address:	141.76.75.109
Subnet Mask:	255.255.255.0
Router:	141.76.75.1



Das Konzept der „Classes“ wurde vom Classless Inter-Domain Routing (CIDR), das auf Netzmasken basiert, abgelöst.

Der Header eines IP-Pakets enthält am Anfang v.a. Angaben zur Größe des Pakets.



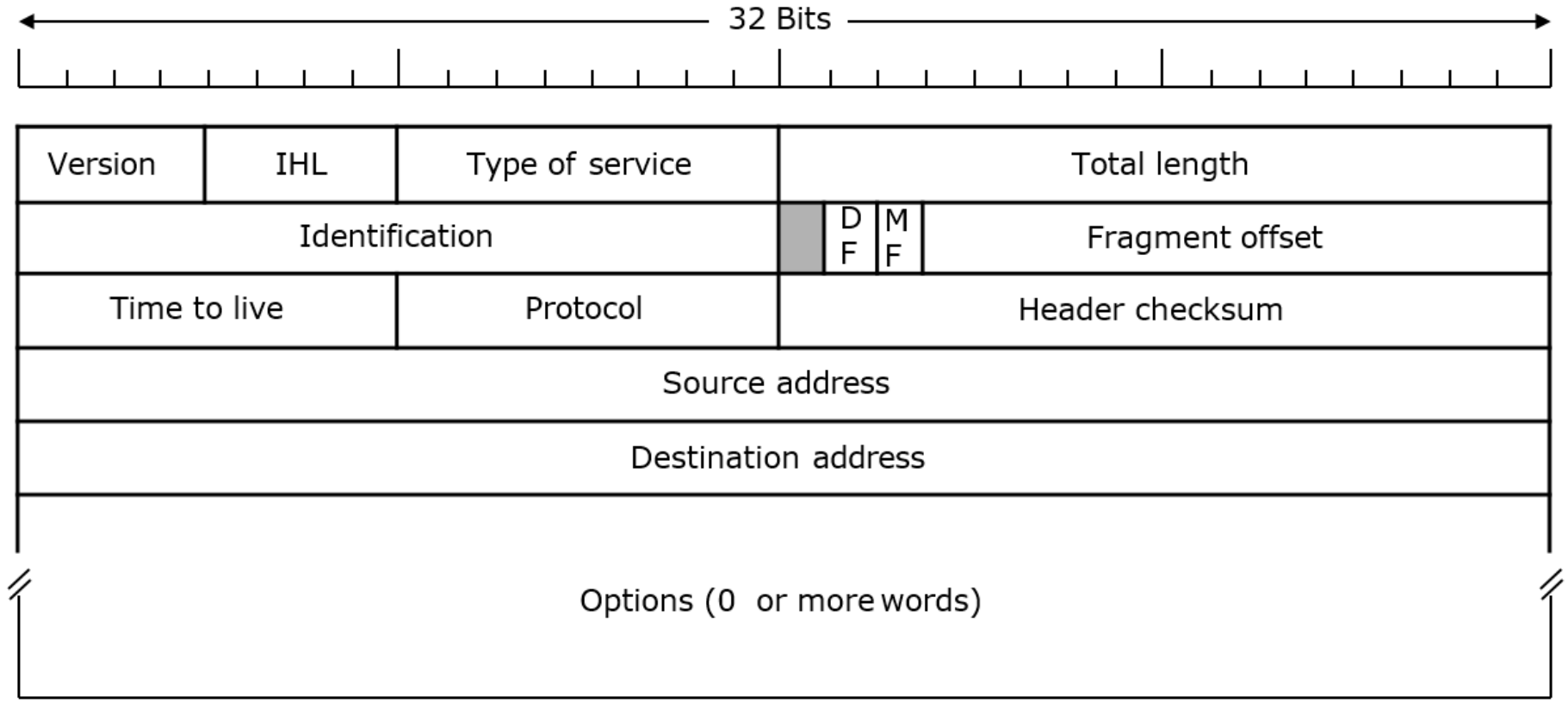
Version (4 Bit): v4 oder v6

IHL=Headerlänge (4 Bit) in 32-Bit-Worten: maximale Länge des Headers 15*32Bit = 60 Byte

Type of Service (8 Bit): Prioritätslevel (erste 3 Bit), Quality of Service-Merkmale, meist ignoriert

Total length in Byte: maximale Länge eines Pakets: 64 Kbyte

Je nach Fähigkeiten der darunterliegenden Schicht kann es zur Fragmentierung großer IP-Pakete beim Transport kommen.



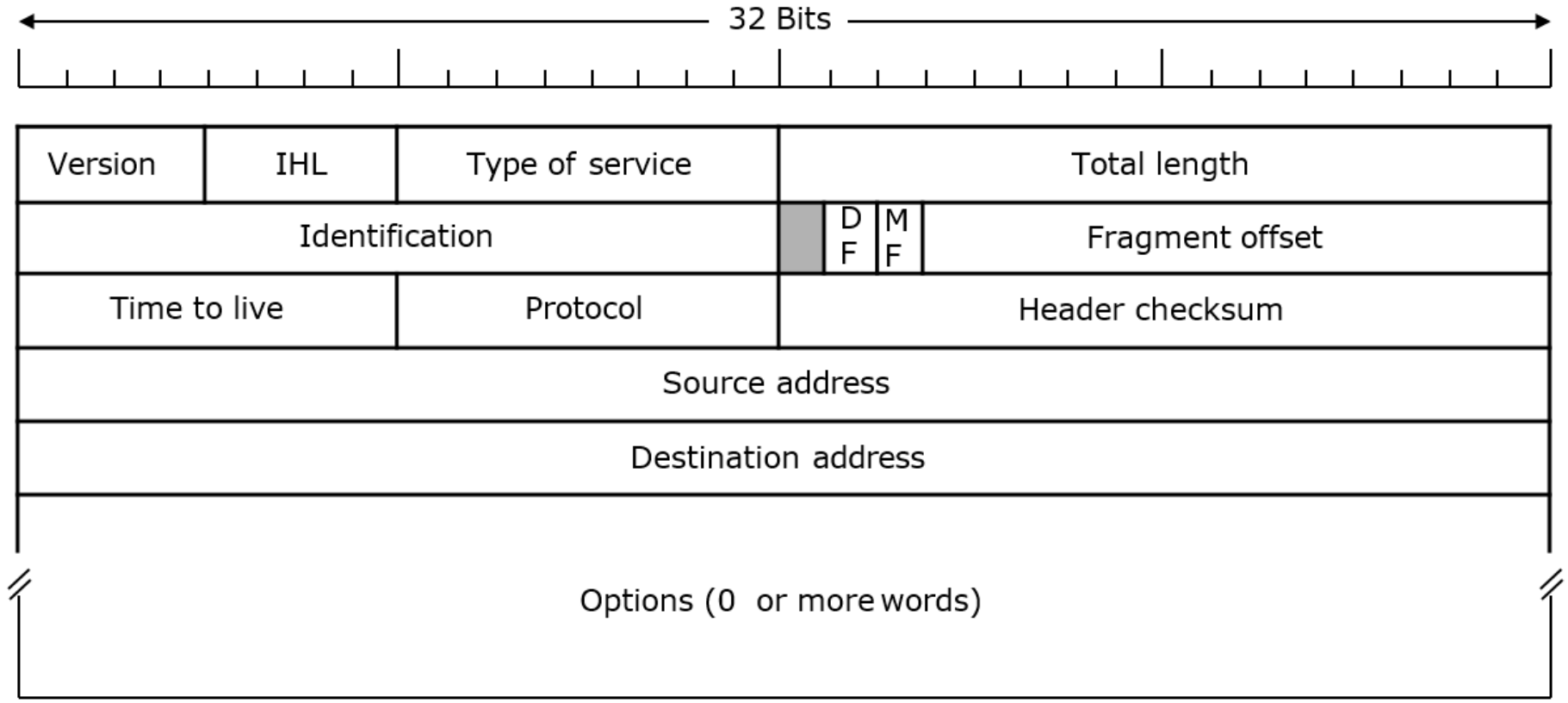
Identification (16 Bit): dient der Zusammensetzung fragmentierter Pakete

DF (1 Bit): Do-Not-Fragment-Flag (1=Fragmentierung nicht erlaubt)

MF (1 Bit): More-Flag: (1=weitere Fragmente folgen)

Fragment offset (13 Bit): Position des Fragments im unfragmentierten Datagramm als Vielfaches von 8 Bytes

Weiterhin werden „Schleifen“ verhindert und es wird das verwendete Transportschicht-Protokoll angegeben.



Time to live (TTL, 8 Bit): verhindert, dass Paket in einer Schleife innerhalb des Netzes feststeckt, als Hop-Count verwendet, d.h. Router verringert Wert um 1

Protocol (8 Bit): identifiziert das Transportprotokoll (17_{dez}=UDP, 6_{dez}=TCP)

Header checksum (16 Bit): Prüfsumme f.d. Header, muss neuberechnet werden, wenn TTL-Feld sich ändert

Wie bekommt eine Station ihre IP-Adresse?

Wie bekommt eine Station ihre IP-Adresse?

Der Nutzer kann sie manuell festlegen oder – wenn vorhanden – von einem Konfigurations-dienst (DHCP) festlegen lassen.

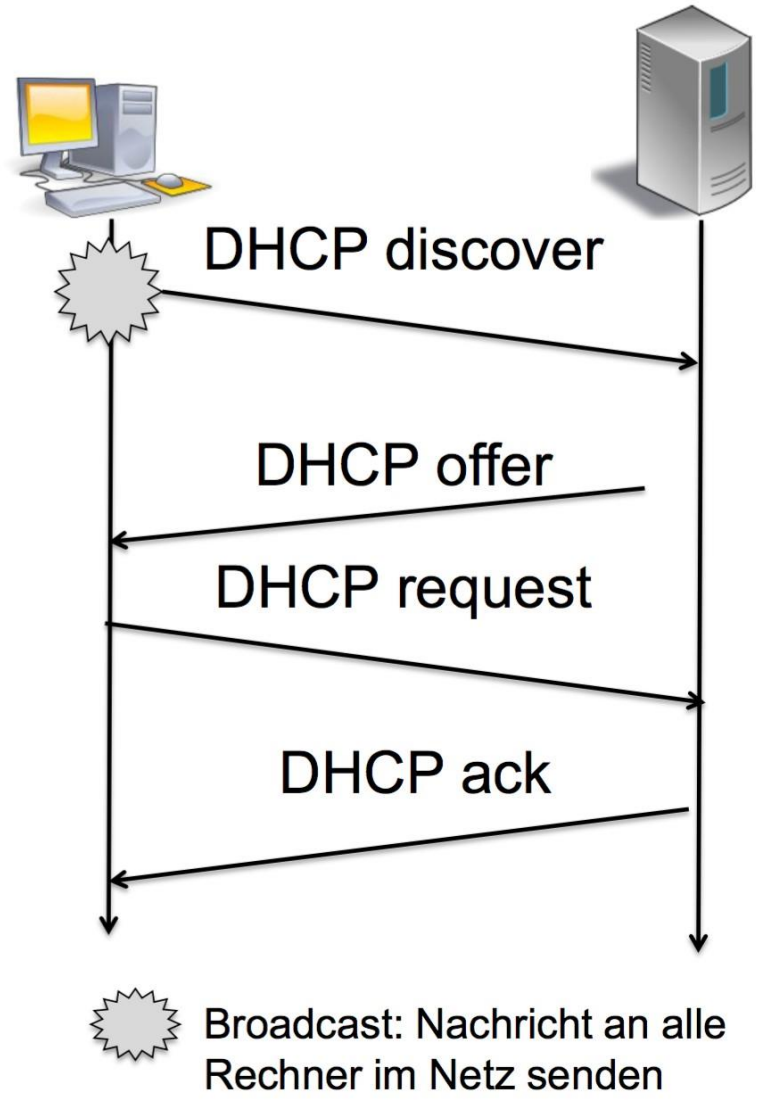
Das Dynamic Host Configuration Protocol erlaubt die Zuweisung von IP-Adressen im lokalen Netz.

1. Auffinden eines DHCP-Servers:
   Host broadcastet DISCOVER

2. Ein oder mehre DHCP-Server melden sich (DHCP-OFFER)

3. Host fordert Konfiguration mit DHCP-REQUEST von einem der Server an

4. DHCP-Server übermittelt eine freie IP-Adresse mit DHCP-ACK



Wie erfährt eine Station, an welche Ethernet-Adresse sie Pakete für eine bestimmte IP-Adresse schicken soll?

Zuordnung von MAC-Adresse und IP-Adresse durch das Address Resolution Protocol (ARP)

Dienst: Ermittlung der zu einer IP-Adresse zugehörigen lokalen MAC-Adresse

1. Anfrager schickt Broadcast im lokalen Netz:

   who-has <ip_address_dest> tell <ip_address_asker>

2. Adapter leiten die Anfrage an Internetschicht

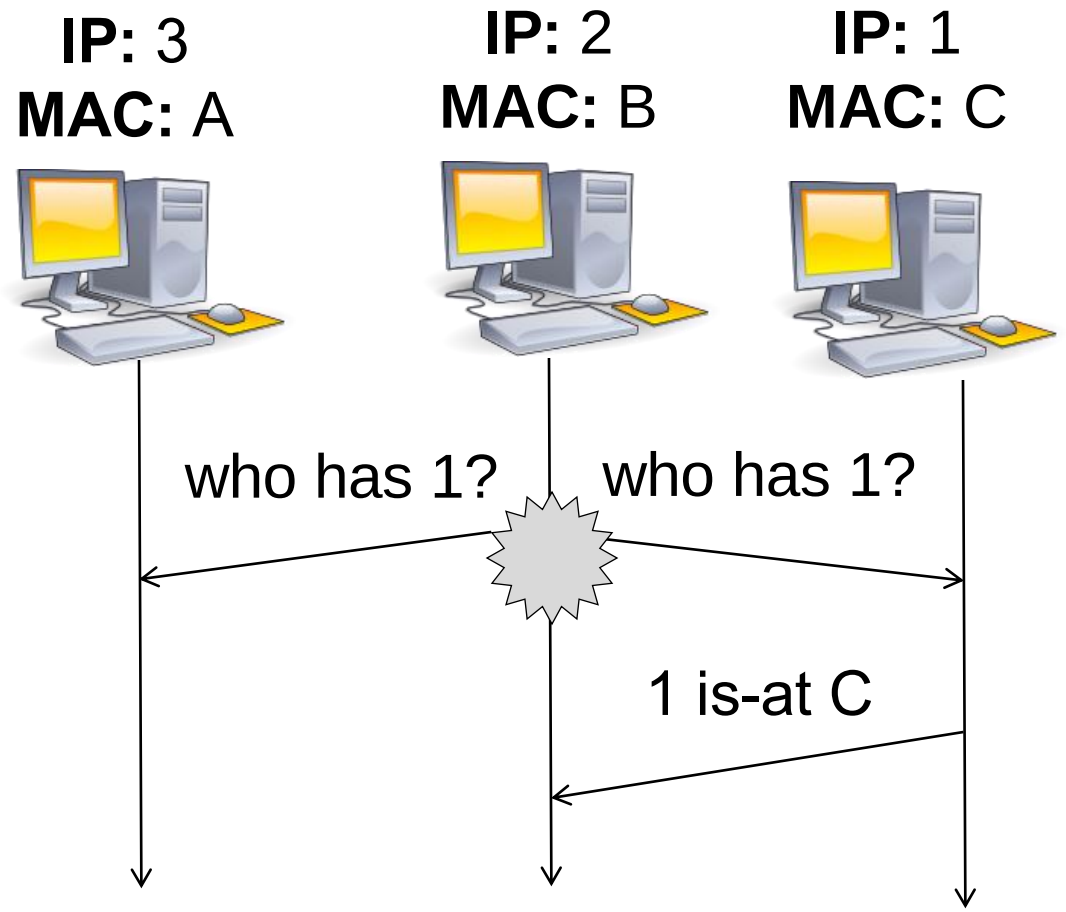
   Überprüfung, ob Adresse ein selbst zugeordnet ist

   Ergebnis wird Adapter mitgeteilt

3. Adapter mit passender IP-Adresse schickt MAC-Adresse an den anfragenden Adapter:

   reply <ip_address_dest> is at <mac_address_dest>

4. Anfrager speichert Zuordnung zwischen MAC- und IP-Adresse (temporär) in einer Tabelle

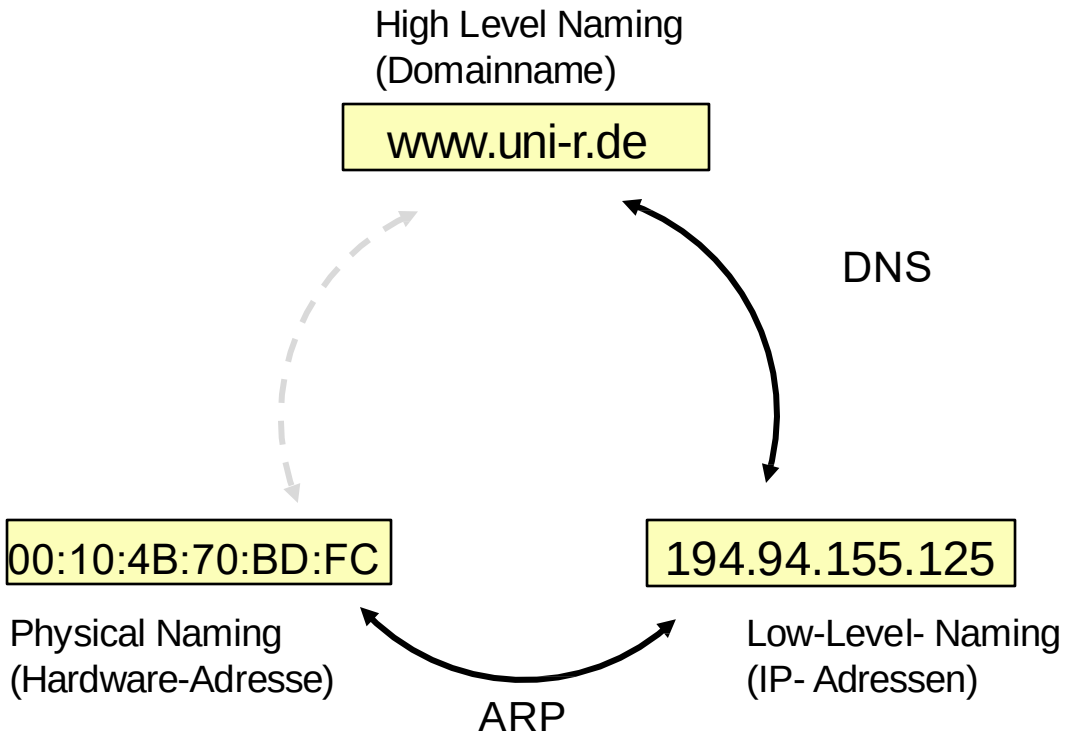


Woher erfährt ein Web-Browser die IP-Adresse des Webservers, an den er seine Anfrage senden soll?

Menschen nutzen üblicherweise Domains zur Adressierung. Die Umsetzung von Domains in IP-Adressen übernimmt das DNS.

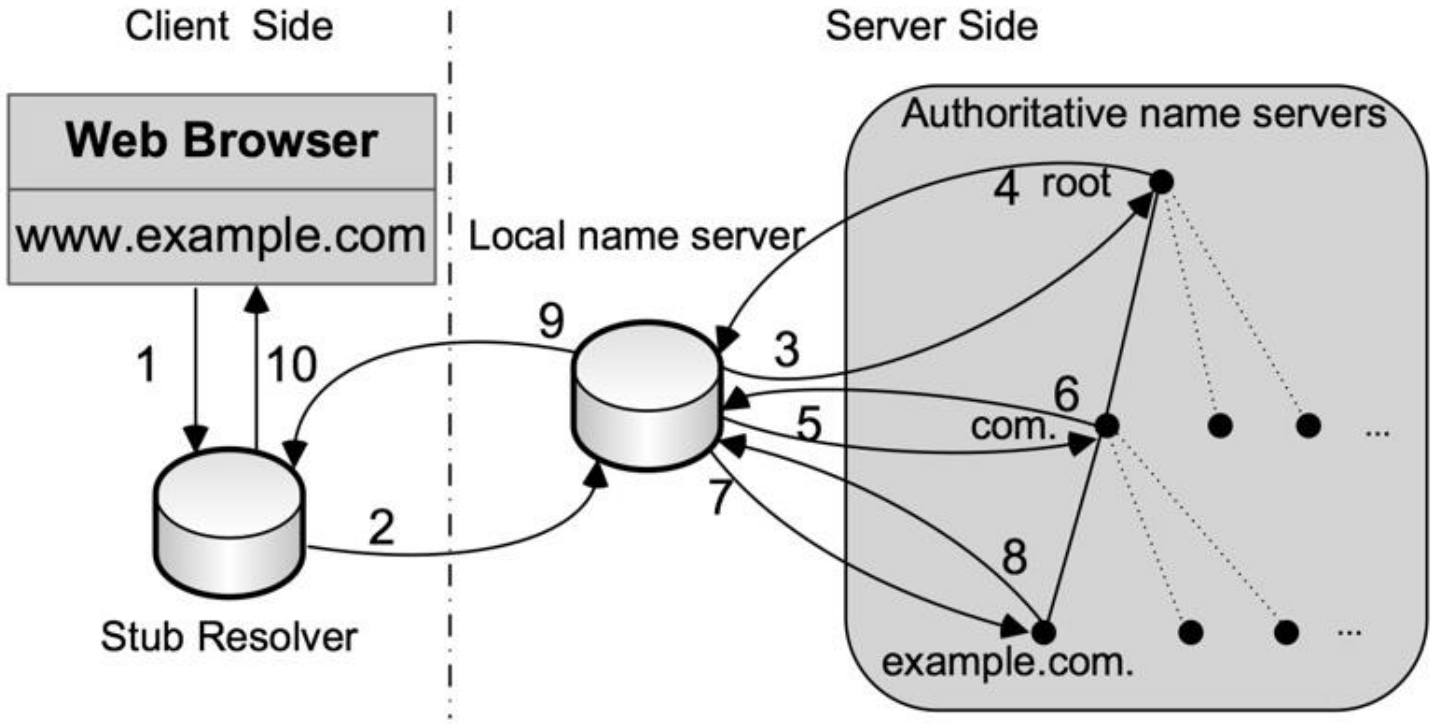
DNS: Domain Name System

- Abbildung des Rechnernamens auf IP-Adresse
- Anfrage an Nameserver
- typischerweise in WANs



Der DNS-Namensraum ist hierarchisch organisiert. Stationen können Informationen im Baum von Nameservern erfragen.

Autoritative Nameserver kennen die IP-Adresse von Domains bzw. verweisen auf Nameserver, die in der Hierarchie tiefer stehen. Da die Ermittlung der IP-Adresse mehrere Abfragen erzeugt, wird sie vom Client an seinen lokalen Nameserver (Resolver) delegiert.



Dienste der Transportschicht (L4) werden im Internet von den Protokollen TCP und UDP erbracht.

TCP (Transmission Control Protocol): stellt einen verbindungs- orientierten Dienst bereit, **UDP** (User Datagram Protocol) einen verbindungslosen.

Auf jedem Endgerät können mehrere TCP- und UDP-Dienste angeboten werden. Adressierung erfolgt mittels 16-bittiger Portnummer; teilw. standardisierte **well-known ports**: z.B. Port 25 (Mailserver), Port 53 (DNS-Server), Port 80 (Webserver).

Verbindungsorientiert: Datenstrom der Anwendung wird in einzelne Segmente zerteilt, die mit einer Sequenznummer versehen werden. Jedes Segment muss vom Empfänger bestätigt werden.

Vorteil von TCP: Rekonstruktion der ursprünglichen Reihenfolge möglich; Pakete können nicht „verloren“ gehen (Retransmission bei Verlust).

Vorteil von UDP: geringerer Overhead/Verzögerung

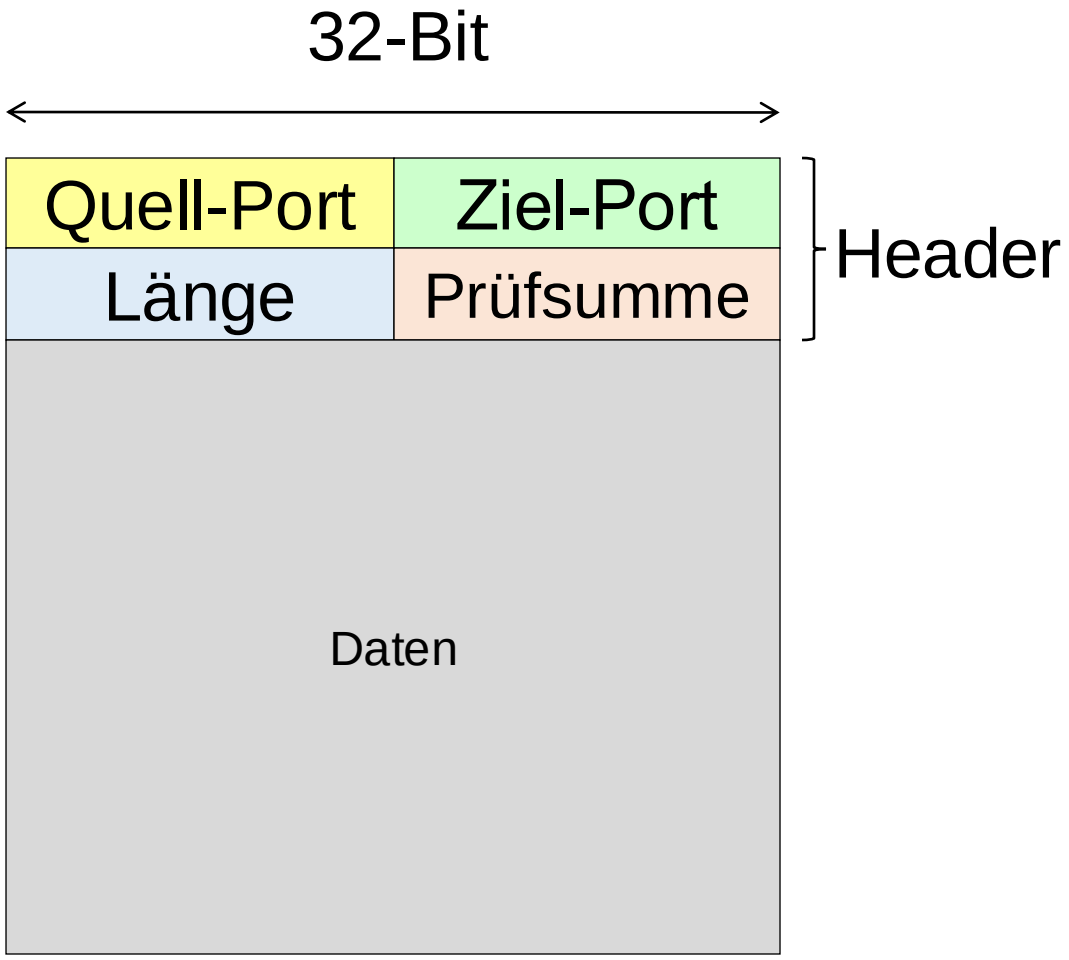
Transportdienst User Datagram Protocol – UDP

Eigenschaften:

- Einfach
- Schnell
- Zustandslos und Verbindungslos
- Pakete können verloren gehen
- Reihenfolge der Pakete nicht garantiert
- Broadcast möglich

Anwendung:

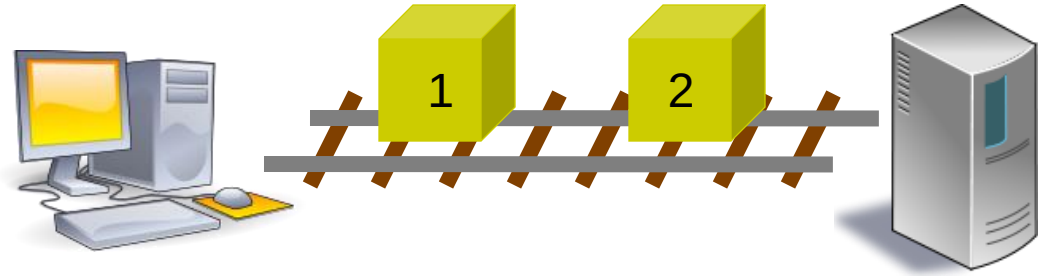
- Multimediaanwendungen
- DNS – Domain Name Server



Transportdienst TCP

Wichtigste Eigenschaften

- Verbindungsorientiert
- Ende-zu-Ende
  (kein Broadcast möglich)
- Verlässliche Übertragung
  - Reihenfolge der Pakete garantiert
  - Fehlerfreie Übertragung
  - Alle Daten werden übertragen
- Fairness durch Überlastungsschutz



Anwendung

- z.B. SMTP, HTTP, POP3 und IMAP

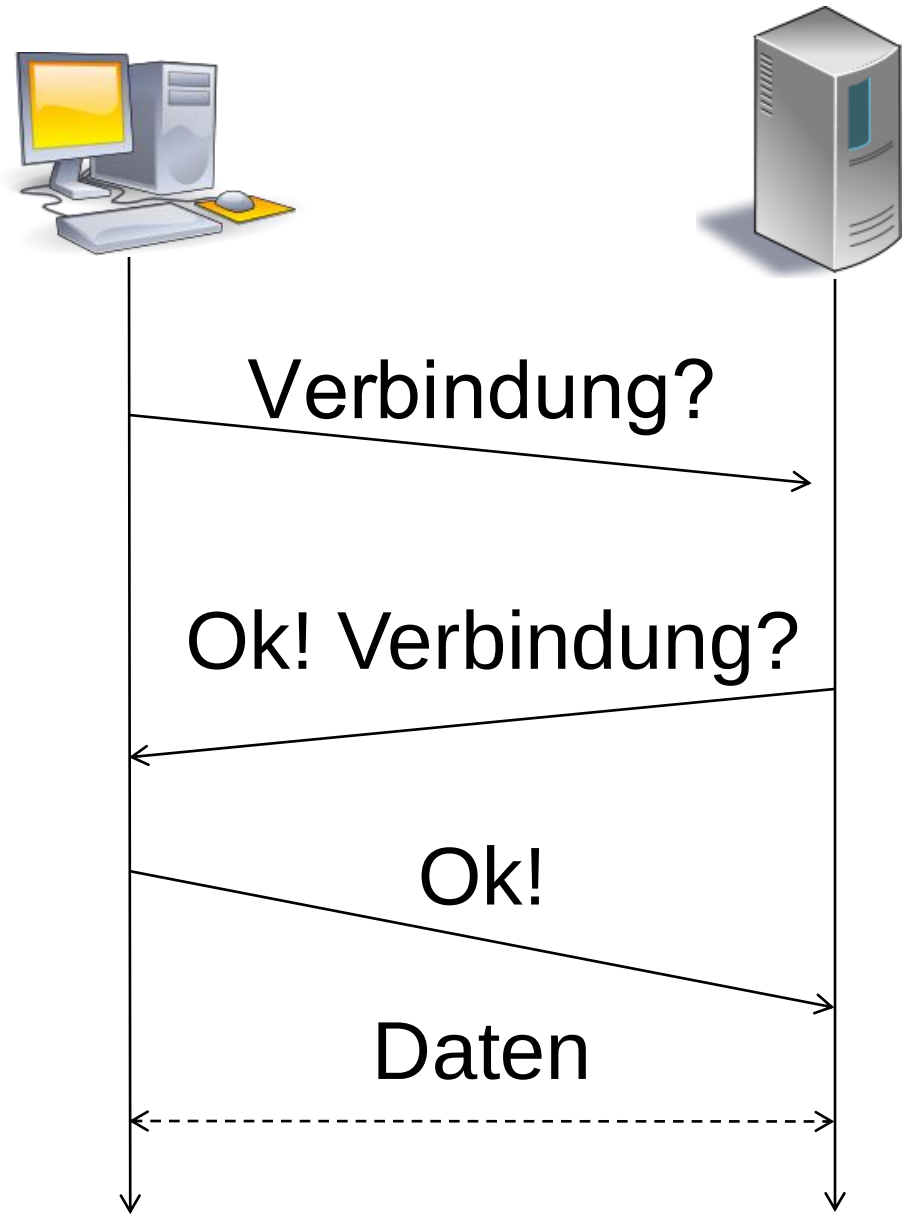
Transportdienst TCP

Ablauf 3-Wege-Handshake

1. Benutzer schickt eine Verbindungsanfrage an den geöffneten Port des Servers
2. Server sendet eine Bestätigung und eine eigene Anfrage an den Port des Benutzers
3. Benutzer bestätigt diese Anfrage
4. Daten können übertragen werden

Anmerkungen

- Nach Verbindungsaufbau können Daten übertragen werden
- Zusätzlich werden Eigenschaften der Verbindung während des Aufbaus ausgehandelt



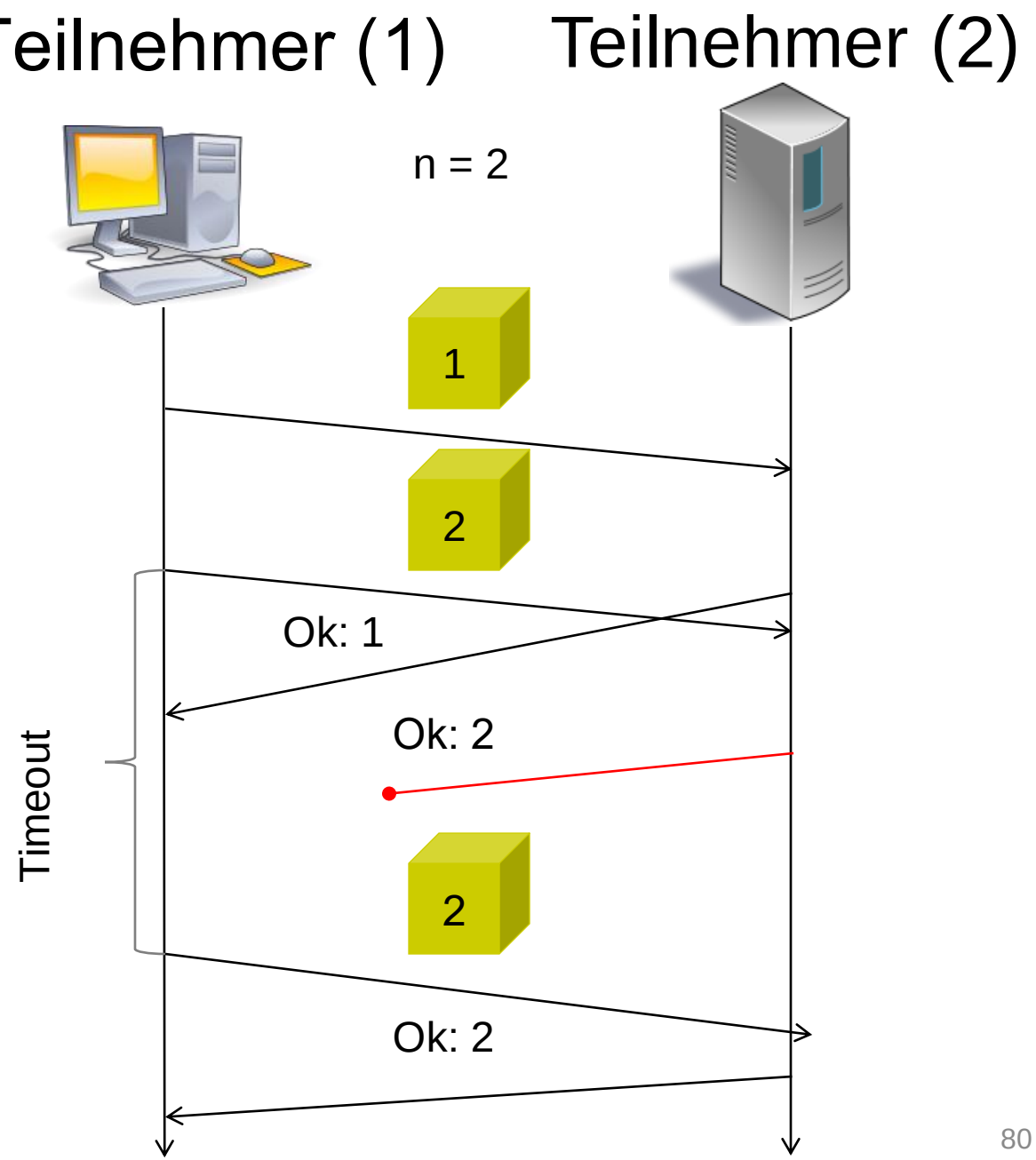
Transportdienst TCP

Fehlerfreiheit

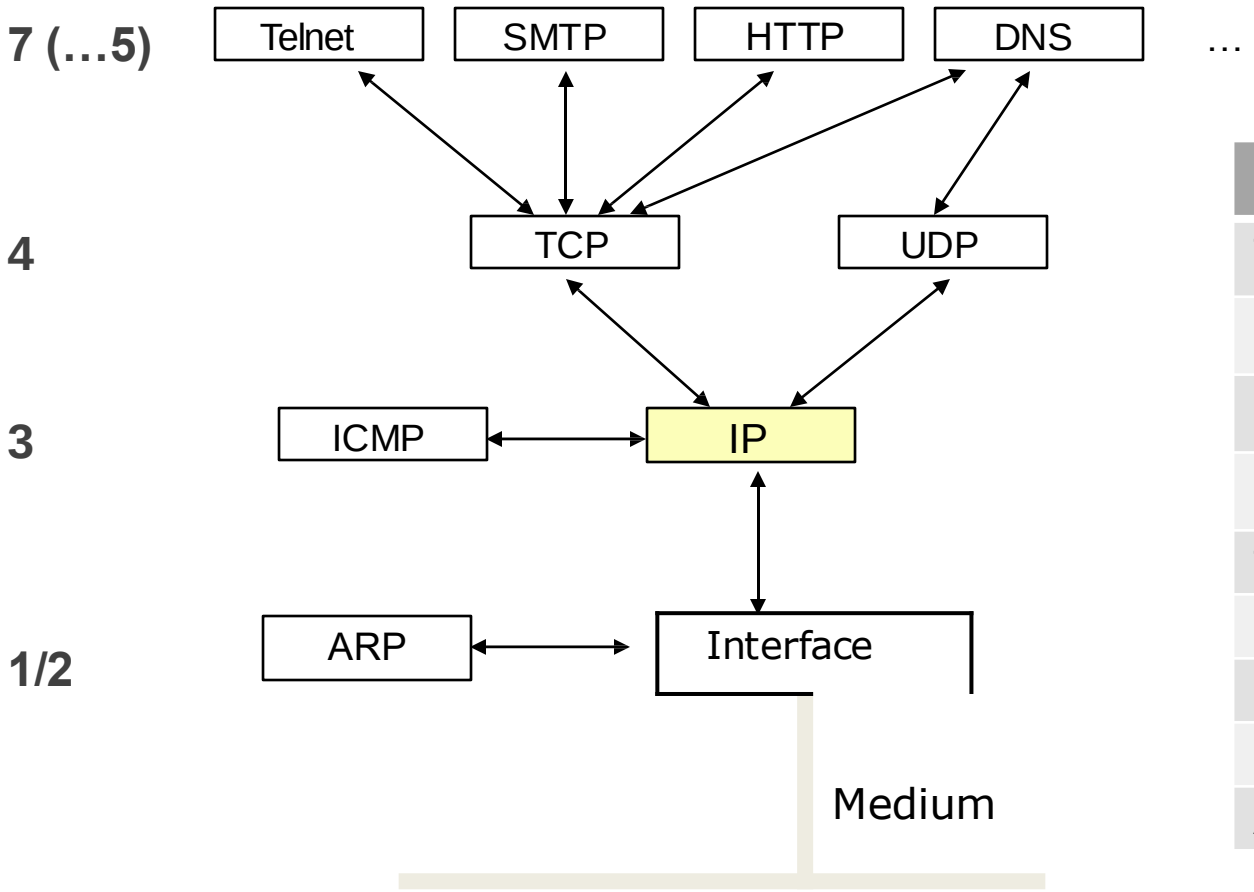
- Empfänger
  - Prüfe Checksumme
  - Korrigiere wenn möglich
  - Sonst nochmal schicken lassen

Verlustfreiheit

- Empfänger
  - Bestätige Empfang
- Sender
  - Falls keine Bestätigung, dann nochmal schicken



Die Aufgaben der höheren Schichten (L5–7) werden im Internet von Anwendungsprotokollen übernommen, zum Beispiel HTTP.

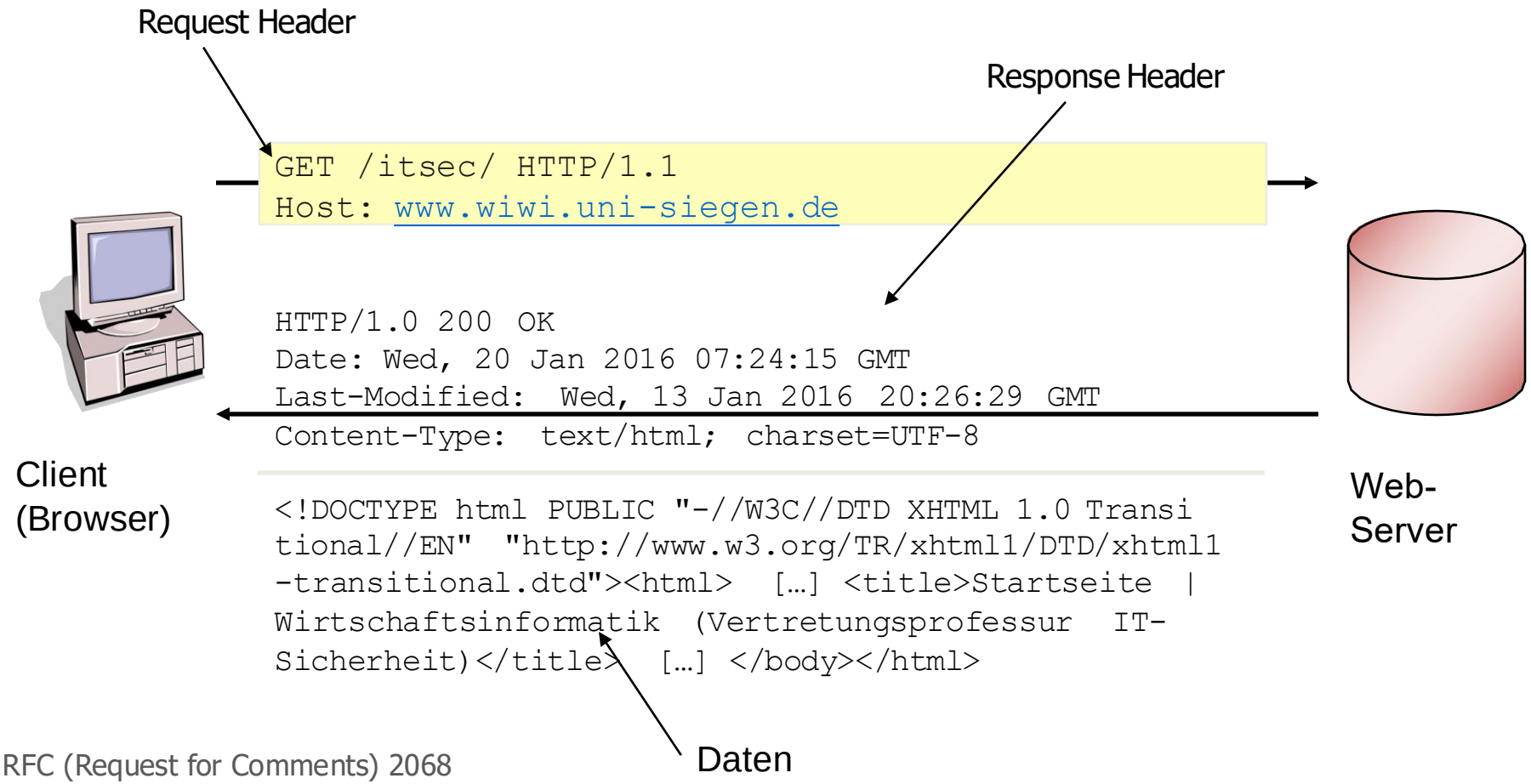


Bezeichnung	Protokollname
Telnet	Teletype Network
SMTP	Simple Mail Transfer Protocol
HTTP	Hypertext Transmission Protocol
DNS	Domain Name System
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
ARP	Adress Resolution Protocol

Höhere Schichten (L5-7) bilden die Anwendungsschicht und bauen auf den tieferliegenden Schichten auf.

Der Client baut eine TCP-Verbindung zum Server auf, sendet einen Request und empfängt die Response. Der Server schließt die Verbindung.

Viele Internetdienste nutzen HTTP (Webseiten, viele Apps, aber auch Spotify und YouTube).



Zusammenfassung

Rechnernetze ermöglichen den Entwurf **verteilter Systeme**, die offen, transparent und skalierbar gestaltet sein sollten.

Das **OSI-Schichtenmodell** definiert 7 Schichten für Rechnernetze, die jeweils dedizierte Aufgaben übernehmen.

Die Sicherungsschicht kümmert sich um **Fehlererkennung** bzw. **Fehlervermeidung** und Medienzugriffssteuerung.

IP beschreibt Adressen und Routing-Mechanismen im Internet. TCP und UDP sind Transportprotokolle für verbindungsorientierte bzw. verbindungslose Dienste.

ARP ist ein Protokoll, das IP- Adressen im lokalen Netz in MAC-Adressen übersetzt. Das **DNS** ist ein verteiltes und hierarchisch organisiertes System, das Domains in IP-Adressen übersetzt. DHCP wird zur Autokonfiguration verwendet.

HTTP und **SMTP** sind textbasierte Anwendungsprotokolle.

Nächste Termine

Nächste Vorlesung:

22.01.2025