HOCHSCHULE DER MEDIEN

NETZE

Prof. Dr. Wolf-Fritz Riekert
Hochschule der Medien (HdM) Stuttgart
University of Applied Sciences

mailto:riekert@hdm-stuttgart.de
http://v.hdm-stuttgart.de/~riekert

NETZE

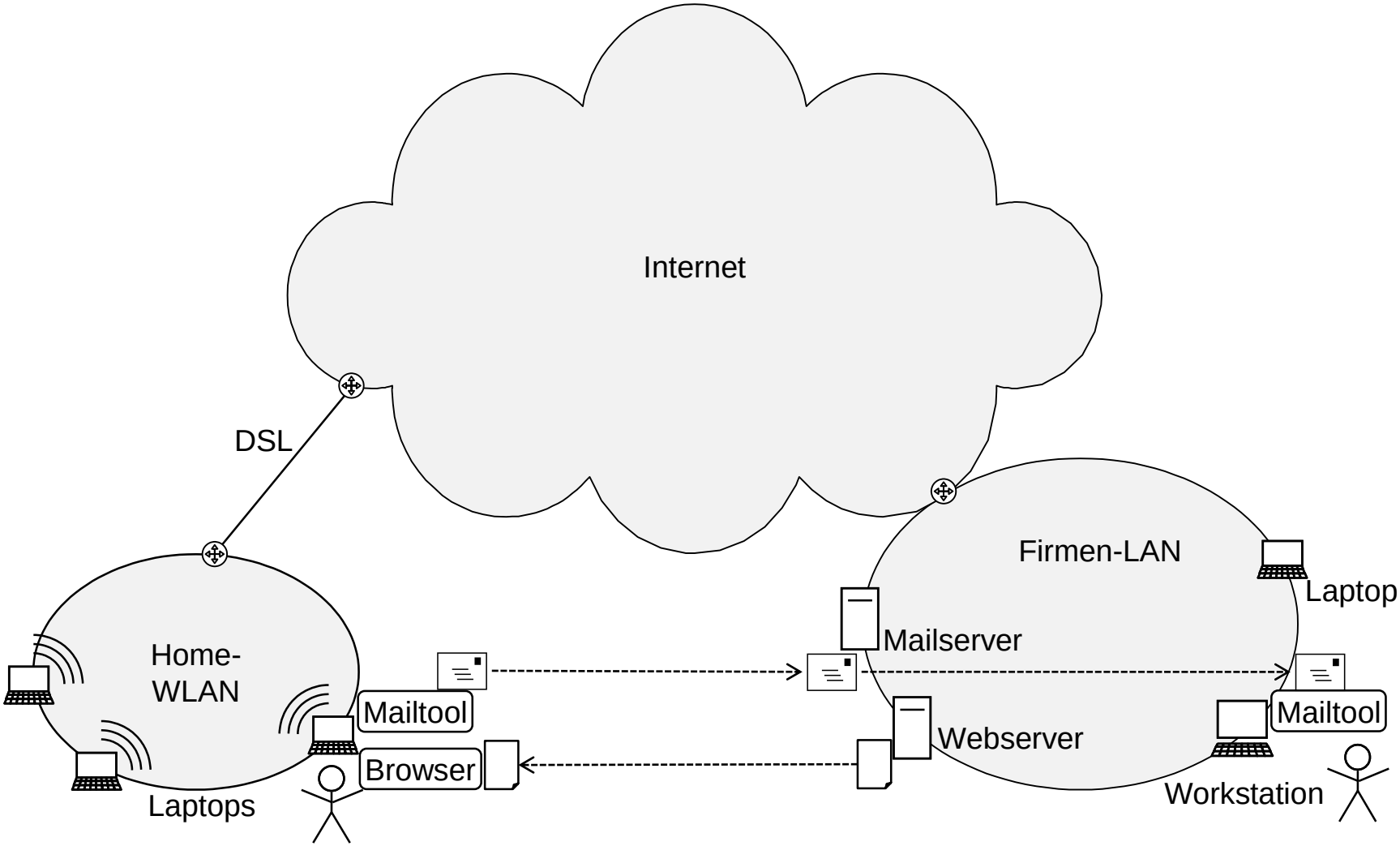
Definition Netze (im Sinne von Computernetze, Rechnernetze):

- Zusammenschluss elektronischer Systeme (Computer, elektronische Geräte, Mobilgeräte etc.)
- über Kommunikationskanäle (Kabel, Funk, Lichtwellen)

Ziele:

- Gemeinsame Nutzung von Ressourcen (Geräte, Programme, Daten)
- Fernbedienung, Überwindung räumlicher Distanzen
- Kommunikation zwischen Menschen, Zusammenarbeit
- Elektronischer Handel (E-Commerce)
- Informationsbeschaffung, -bereitstellung
- Unterhaltung (Multimedia)

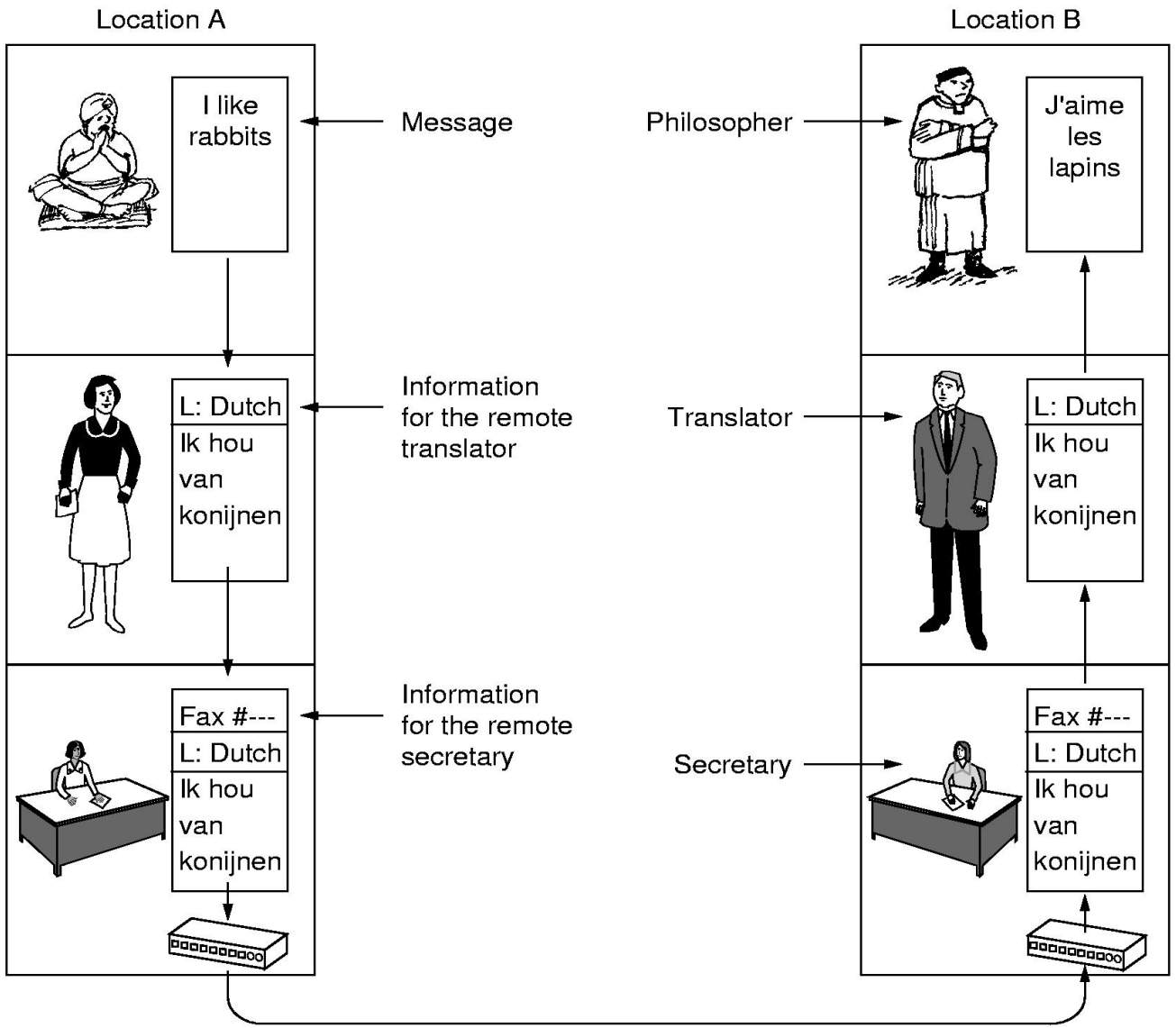
BEISPIELSZENARIO



BEDEUTUNG DER SOFTWARE FÜR NETZE

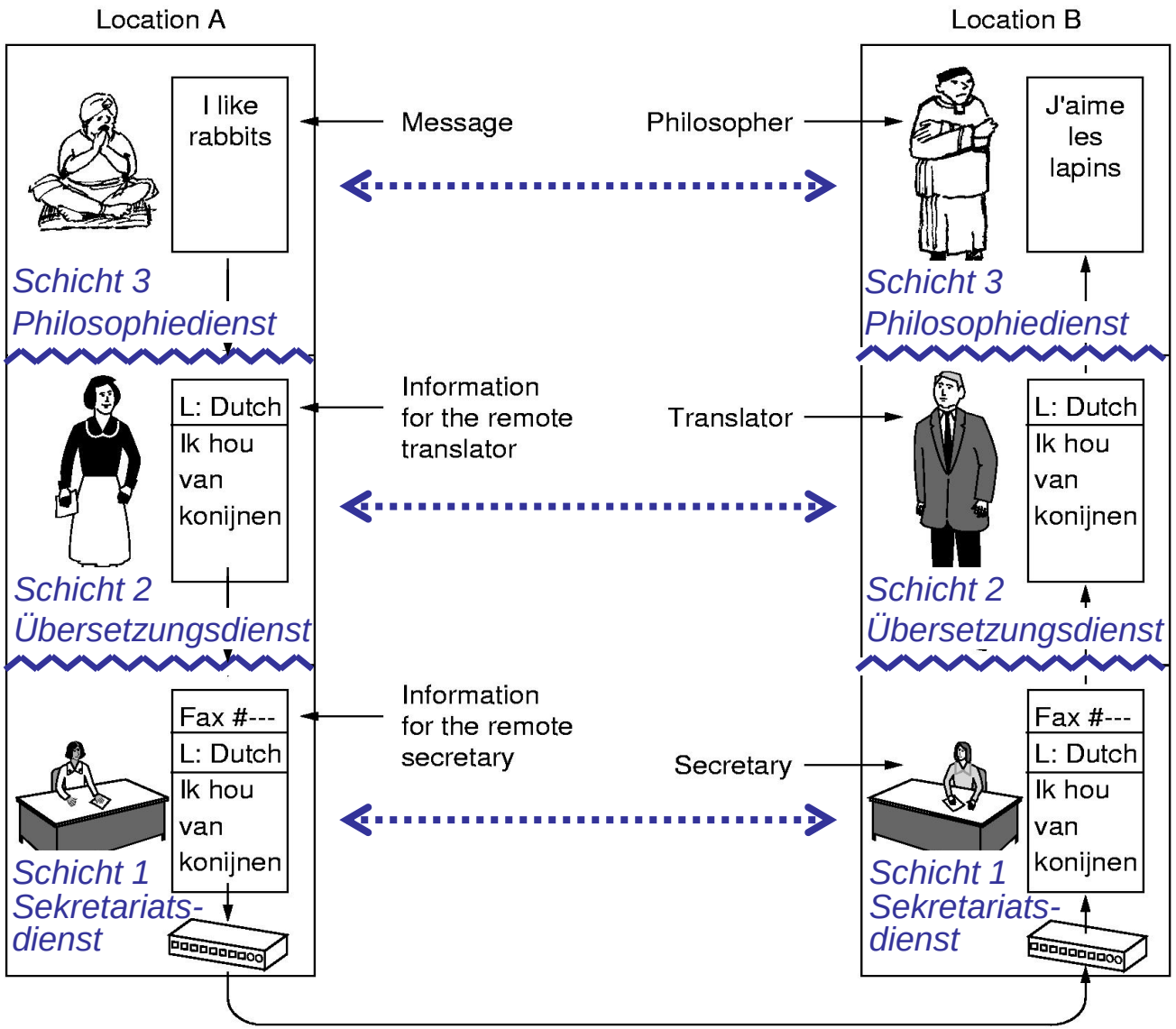
- Software ist inzwischen die entscheidende Komponente zur Bereitstellung von Netzwerkdiensten geworden
- Der überwiegende Teil dieser Vorlesung ist mit Netzwerksoftware befasst.
- Netzwerksoftware: ein komplexes Feld, das einer besonderen Strukturierungstechnik bedarf
  - ⇨ Strukturierung in Form von Schichten oder Ebenen

BEISPIEL KOMMUNIKATION ZWEIER PHILOSOPHEN: SCHICHTENMODELL



Quelle: Tanenbaum & Wetherall (2012)

SCHICHTEN, DIENSTE, PROTOKOLLE, SCHNITTSTELLEN AM BEISPIEL



Legende:

Protokoll

Schnittstelle

basiert auf: Tanenbaum & Wetherall (2012)

WARUM SCHICHTEN?

- **Modularisierung** der Netzwerksoftware. Jede Schicht ist ein eigener Modul. Zwischen den Modulen gibt es feste **Schnittstellen**. Für das Verständnis des Ganzen ist es nicht wichtig, wie ein Modul intern funktioniert, er kann als „Blackbox“ betrachtet werden. Dies dient der **Reduzierung der Komplexität** und vereinfacht die Arbeit für die Systementwickler.
- Schichten sind vertikal geordnet. Jede Schicht hat **nur Schnittstellen mit der unmittelbar darüber und** der unmittelbar **darunter liegenden Schicht**. Dies hat eine weitere Reduzierung der Komplexität zur Folge.
- Die festen Schnittstellen erlauben es, **Schichten auszuwechseln**, ohne die darüber oder darunter liegenden Schichten zu beeinflussen (Beispiel: Übergang von einem Ethernet-LAN zu einem WLAN).

SCHICHTEN GLIEDERN
NETZWERKSOFT- UND HARDWARE

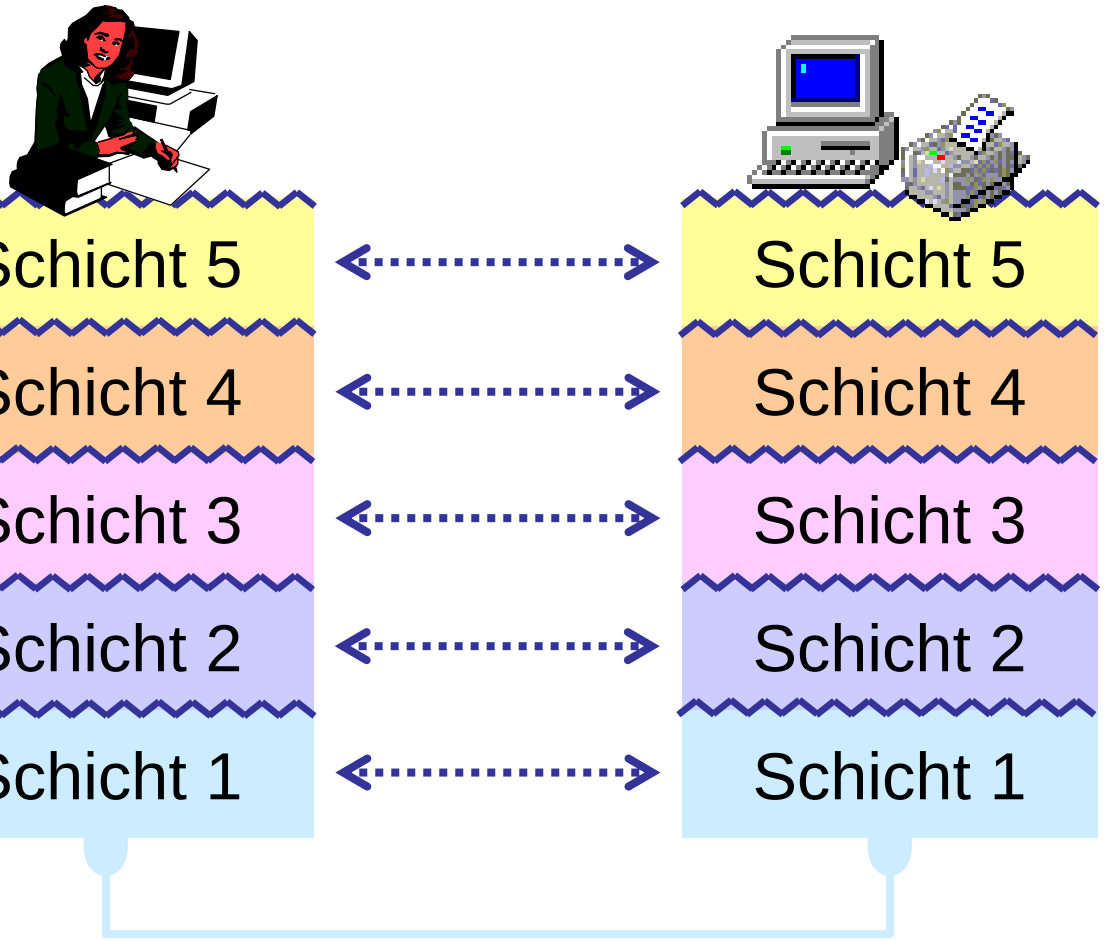
HOCHSCHULE DER MEDIEN

Legende:

Protokoll

Schnittstelle

Lokaler Computer *Ferner Computer*



Netzwerk-Software

Netzwerk-Hardware

SCHICHTEN, DIENSTE, PROTOKOLLE, SCHNITTSTELLEN (1)

Netzwerksoftware wird in Form von **Schichten** (layers) aufgebaut.

- Diese Schichten realisieren **(Netzwerk-)Dienste** (services), die aus **Dienstoperationen** bestehen.
- Schichten kommunizieren mit Schichten derselben Ebene (sogenannten Peers) auf fremden Computern. Diese Kommunikation befolgt **Protokolle** (= Regeln und Konventionen für die Kommunikation)
- Kommunikation erfolgt mittelbar (indirekt) über Dienstoperationen der nächsttieferen Schicht.
- Zwischen zwei angrenzenden Schichten existiert eine **Schnittstelle**. Diese legt fest, wie die Dienstoperationen der unteren Schicht von der oberen Schicht in Anspruch genommen werden können.

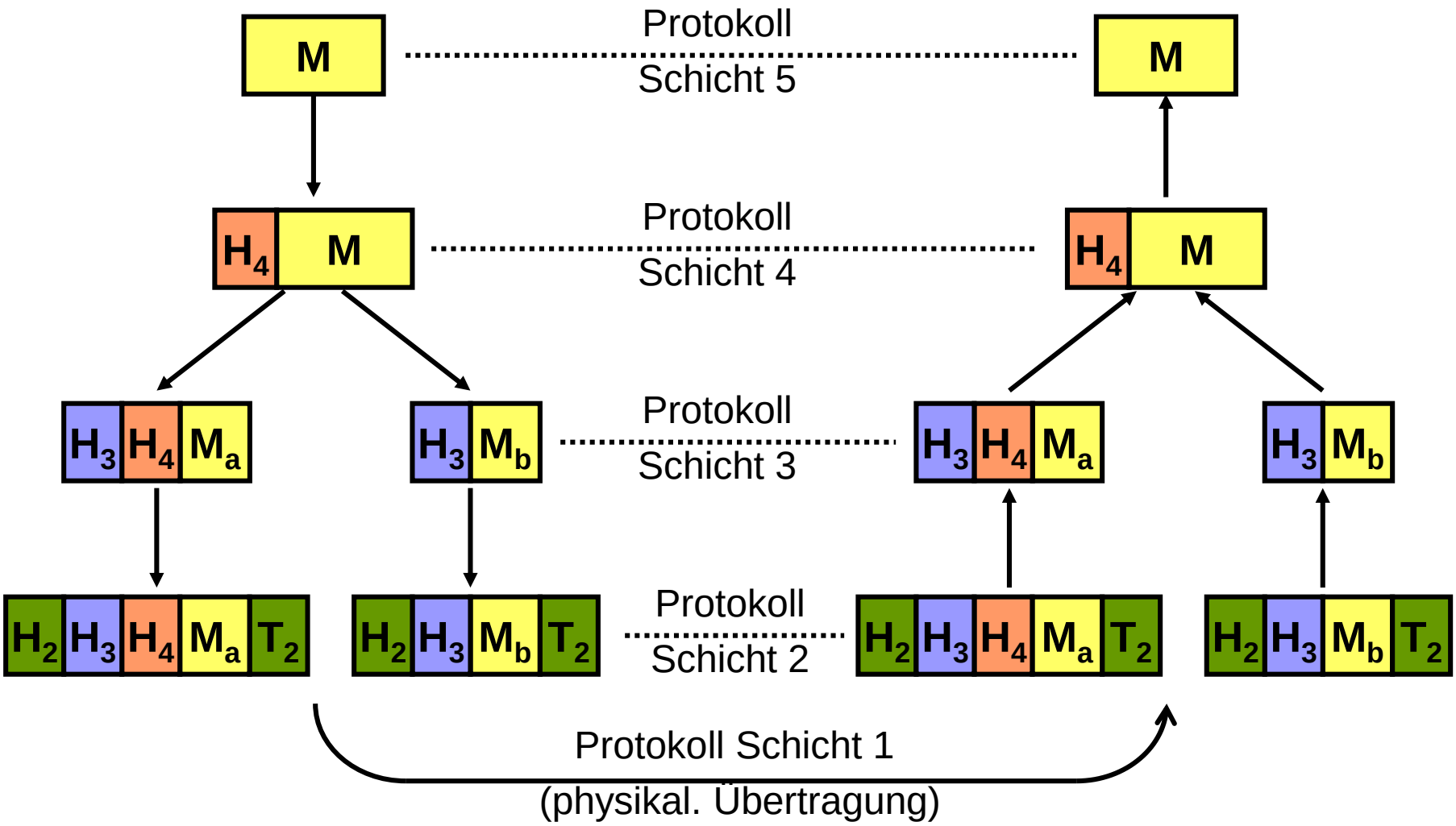
TECHNISCHE REALISIERUNG VON NETZWERKDIENSTEN

Netzwerkdienste werden in Form von Software realisiert. Hierzu stehen verschiedene Techniken zur Verfügung:

- „**Anwendungsprogramme**“ auf der obersten Schicht. Beispiel: Mailtool, Web-Browser
- „Unterprogramme“ in „**Unterprogrammbibliotheken**“ (klassisch) bzw. „Methoden“ in „**Klassenbibliotheken**“ (objektorientiert). Diese werden von der höheren Schicht aus durch Aufrufe aktiviert
- Als Hintergrundprozesse gestartete „**Serverprogramme**“, die periodisch oder ereignisgesteuert die nächsttiefere Schicht über Aufrufe abfragen und z.B. ankommende Nachrichten übernehmen und weiterverarbeiten.
- „**Treiberprogramme**“ zur Ansteuerung der Netzwerk-Hardware (Netzwerkinterfaces, Interrupt Controller)

KOMMUNIKATION IN COMPUTERNETZEN (1)

HOCHSCHULE DER MEDIEN



Lokaler Computer

Ferner Computer

KOMMUNIKATION IN COMPUTERNETZEN (2)

- Abgehende Nachrichten M werden fortgesetzt an tiefere Schichten übergeben, bis die unterste Schicht erreicht ist, die die physikalische Übertragung übernimmt. Jede Schicht kann einen Nachrichtenkopf H („Header“) und ggf. auch einen Nachspann T („Trailer“) hinzufügen.
- Manche Schichten zerlegen größere Nachrichten in kleinere Teile. Umgekehrt können Schichten auch mehrere kleinere Nachrichten zu einer langen Nachricht zusammenfassen.
- Ankommende Nachrichten werden ausgehend von der untersten Schicht fortgesetzt an höhere Schichten übergeben. Dabei werden die der jeweiligen Schicht zugeordneten Header und Trailer entfernt.
- Beim Versand erfolgte Zerlegungen bzw. Zusammenfassungen von Nachrichten können beim Empfang von der jeweils zuständigen Schicht wieder rückgängig gemacht werden.

DESIGNASPEKTE DER SCHICHTEN

- Art der Dienstleistung: Anwendungsdienst, Datenübertragungsdienst, Hardwareansteuerung
- logische Kommunikationskanäle
  - ⇨ Richtung: Simplex, Halbduplex, Vollduplex
  - ⇨ mehrere logische Kanäle gleichzeitig: Multiplexing
- Fehlerüberwachung, -behebung
- Zerlegung von Nachrichten in Teile, Zusammenfassung
- Geschwindigkeitsanpassung (z.B. langsamer Empfänger)
- Adressierung
- Routing (Vermittlung von Datenpaketen durch das Netz)
- Einhaltung der Reihenfolge der übertragenen Daten
- Aufbau einer Verbindung (oder nicht)

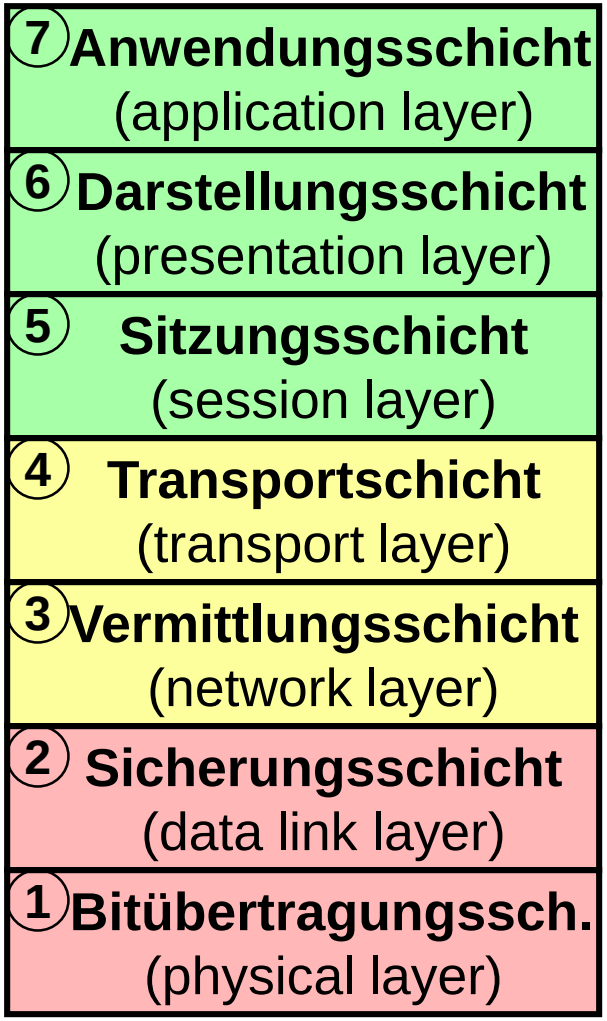
VERBINDUNGSORIENTIERTE DIENSTE

- 3 Phasen: Verbindungsaufbau, Datenübertragung, Verbindungsabbau
- Analogie: Telefonsystem
- Adressierung des Kommunikationspartners nur beim Verbindungsaufbau erforderlich
- Empfang der Daten in ursprünglicher Reihenfolge garantiert
- In der Regel hohe Dienstqualität:
  - ⇨ Hohe Zuverlässigkeit: Automatische Erkennung und Korrektur von Übertragungsfehlern durch Bestätigungsnachrichten und wiederholte Übertragungen möglich.
  - ⇨ Garantierte Datenübertragungsrate
  - ⇨ Garantierte Begrenzung von Übertragungsverzögerungen

VERBINDUNGSLOSE DIENSTE

- Es findet kein Verbindungsaufbau statt, die Nachrichten (sog. Datengramme) können sofort gesendet werden
- Analogie: Postsystem („gelbe Post“)
- Jedes Datengramm trägt volle Zieladresse
- Nachrichten werden nicht notwendig in ursprünglicher Reihenfolge empfangen
- Dienstqualität i.d.R. gering (keine Garantie hinsichtlich Übertragungsgeschwindigkeit u. –verzögerung, kaum Fehlererkennung u. -korrektur,)
- Varianten
  - ⇨ unzuverlässiges Datengramm (analog: Postkarte)
  - ⇨ bestätigtes Datengramm („Einschreiben mit Rückschein“)
  - ⇨ Anfrage/Antwort (z.B.: Datenbankabfrage, WWW)

DAS OSI-REFERENZMODELL DER ISO

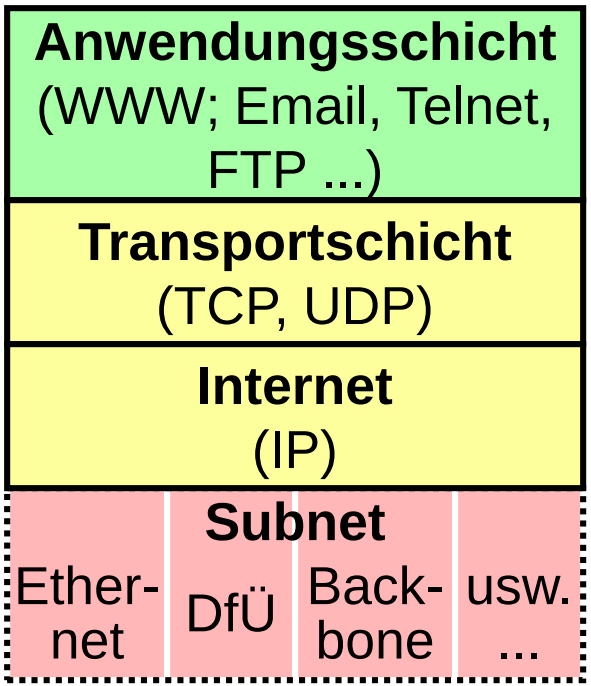


OSI (Open Systems Interconnection)

- Modell zur Verbindung offener Systeme (d.h. offen zur Kommunikation mit Systemen unterschiedlicher Hersteller)
- Festgelegt durch **ISO** (International Standards Organization) Ende 70er bis Anfang 80er-Jahre
- OSI sieht 7 Schichten vor und legt fest, was diese Schichten bewirken sollen
- OSI definiert keine Dienste und Operationen, ist daher keine Netzarchitektur
- In der Folge wurden aber auf der Basis von OSI Dienste und Operationen genormt und implementiert.

DAS INTERNET

Das **Internet** ist ein offenes Verbundnetz, das verschiedene existierende Netze als „Subnetze“ miteinander verbindet



- Entstanden 1969 als **ARPANET** (gefördert durch US-amerikanische Militärforschungsinstitution „Advanced Research Project Agency“)
- Anfangs entwickelt durch verschiedene Universitäten und Forschungsinstitute
- Betrieb und Weiterentwicklung heute weitgehend auch durch kommerzielle Einrichtungen.

Pragmatische Entwicklungsphilosophie, folgt nicht dem OSI-Schichtenmodell. Dienste lassen sich grob in 3 Schichten innerhalb des Internet sowie 1 Subnetzschicht strukturieren.

INTERNET: HISTORIE

- Ab 1969: **ARPANET**, durch amerikanisches Militär gefördert, von Wissenschaftlern genutzt und betrieben
  - ⇨ Erste Dienste: E-Mail, FTP (File Transfer), Telnet (Login auf fernen Computern)
- 1982: Umbenennung in **Internet**
  - ⇨ Einführung der Übertragungsprotokollfamilie TCP/IP
  - ⇨ Internetworking: Zusammenschluss verschiedener Netzwerke zum „Internet“ als globalem Verbundnetz
- 1990: Beginn der Kommerzialisierung des Internet
- 1993: Web-Browser Mosaic (Vorläufer von Internet Explorer u. Firefox, entwickelt von Marc Andreessen, NCSA), macht den **WWW-Dienst** (Tim Berners-Lee, CERN, ab 1989) und damit das Internet vielen, auch privaten Nutzern verfügbar

DAS HYBRIDE FÜNFSCHICHTEN-MODELL VON TANENBAUM

Im Lehrbuch „Computernetzwerke“ (Tanenbaum & Wetherall 2012) wird ein „hybrides“, d.h. aus OSI- und Internet-Modell abgeleitetes Fünfschichtenmodell vorgestellt.

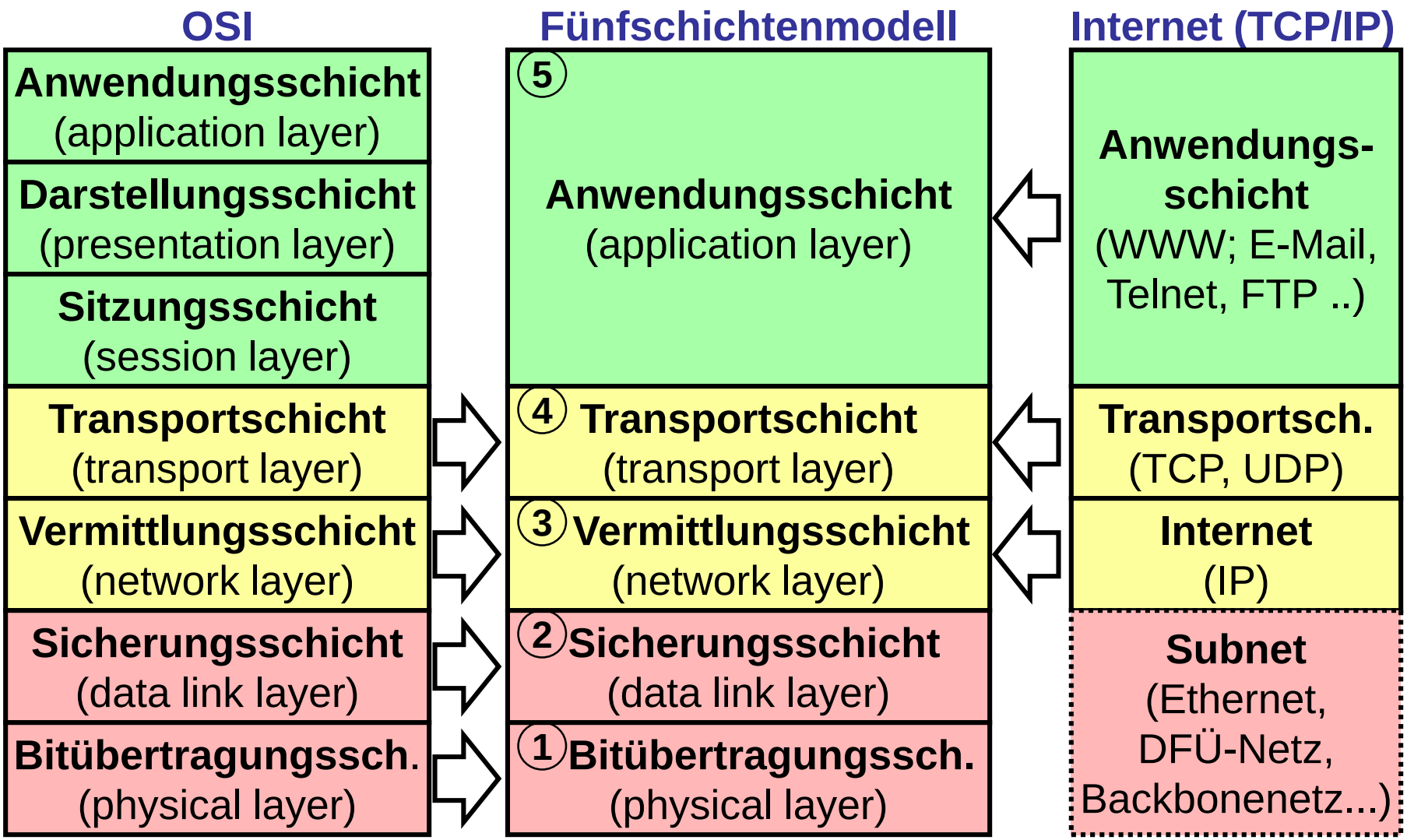
5	**Anwendungsschicht** (application layer) umfasst auch Darstel-lungs- u. Sitzungsschicht
4	**Transportschicht** (transport layer)
3	**Vermittlungsschicht** (network layer)
2	**Sicherungsschicht** (data link layer)
1	**Bitübertragungssch.** (physical layer)

- Vergröberung des OSI-Modells: Die Schichten 5 bis 7 werden zu einer Schicht zusammengefasst.
- Übereinstimmung in Schicht 3 u. 4
- Verfeinerung des Internet-Modells: Die Subnet-Schicht des Internet wird in die zwei entsprechenden OSI-Schichten 1 u. 2 aufgespaltet.

Nach diesem Modell wird im Folgenden vorgegangen.

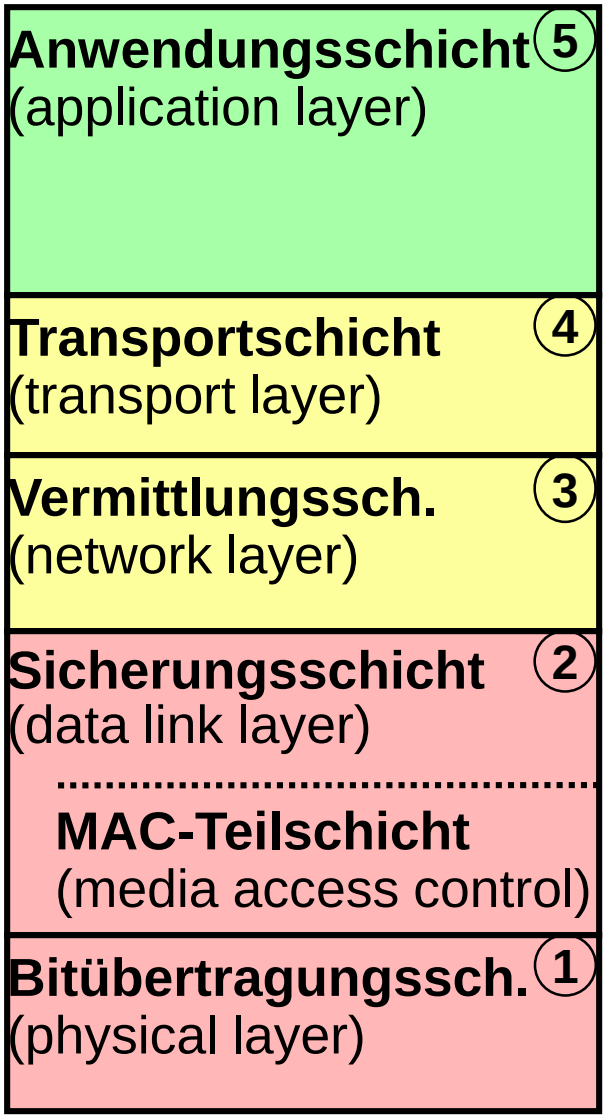
FÜNFSCHICHTENMODELL, OSI UND INTERNET IM VERGLEICH

HOCHSCHULE DER MEDIEN



GLIEDERUNG DES STOFFS NACH DEM HYBRIDEN MODELL

HOCHSCHULE DER MEDIEN



Zugriff des Benutzers auf Ressourcen

Beispiele: WWW, FTP, Telnet, E-Mail, File-/Printservices u.a. Anwendungsdienste

Kommunikation zwischen Prozessen
Beispiele: TCP, UDP

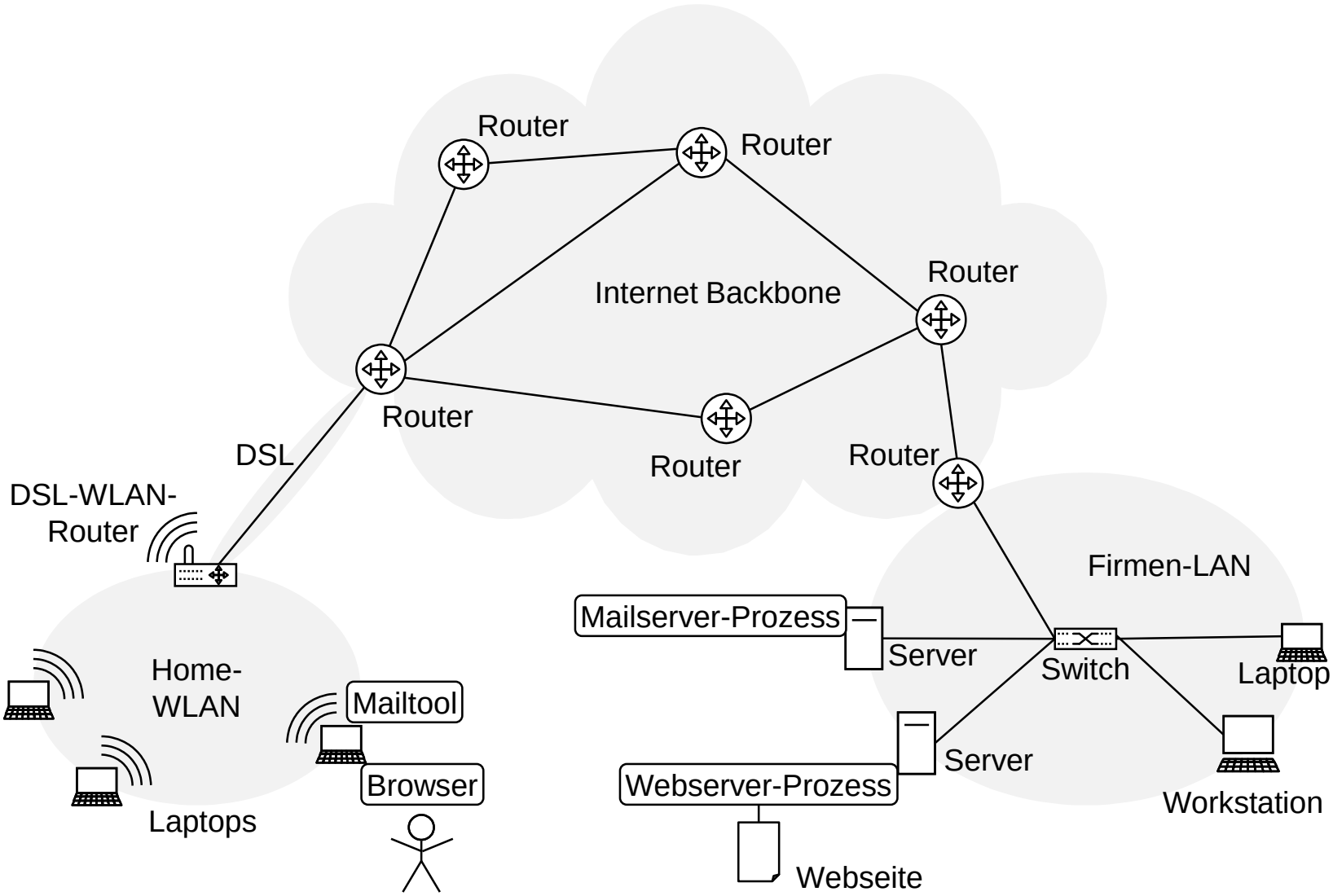
Kommunikation zwischen Computern
Beispiel: IP

Kommunikation zwischen benachbarten Stationen
Beispiel: Punkt-zu-Punkt-Protokoll (PPP)

Spezialfall Broadcastnetze: Mehrere Stationen benutzen denselben Übertragungskanal
Beispiele: (Ethernet-)LAN, WLAN

Physikalische Übertragung von Signalen
Digital / Analog, Kodierung, Modulation

BEISPIELSZENARIO



BEISPIELSZENARIO

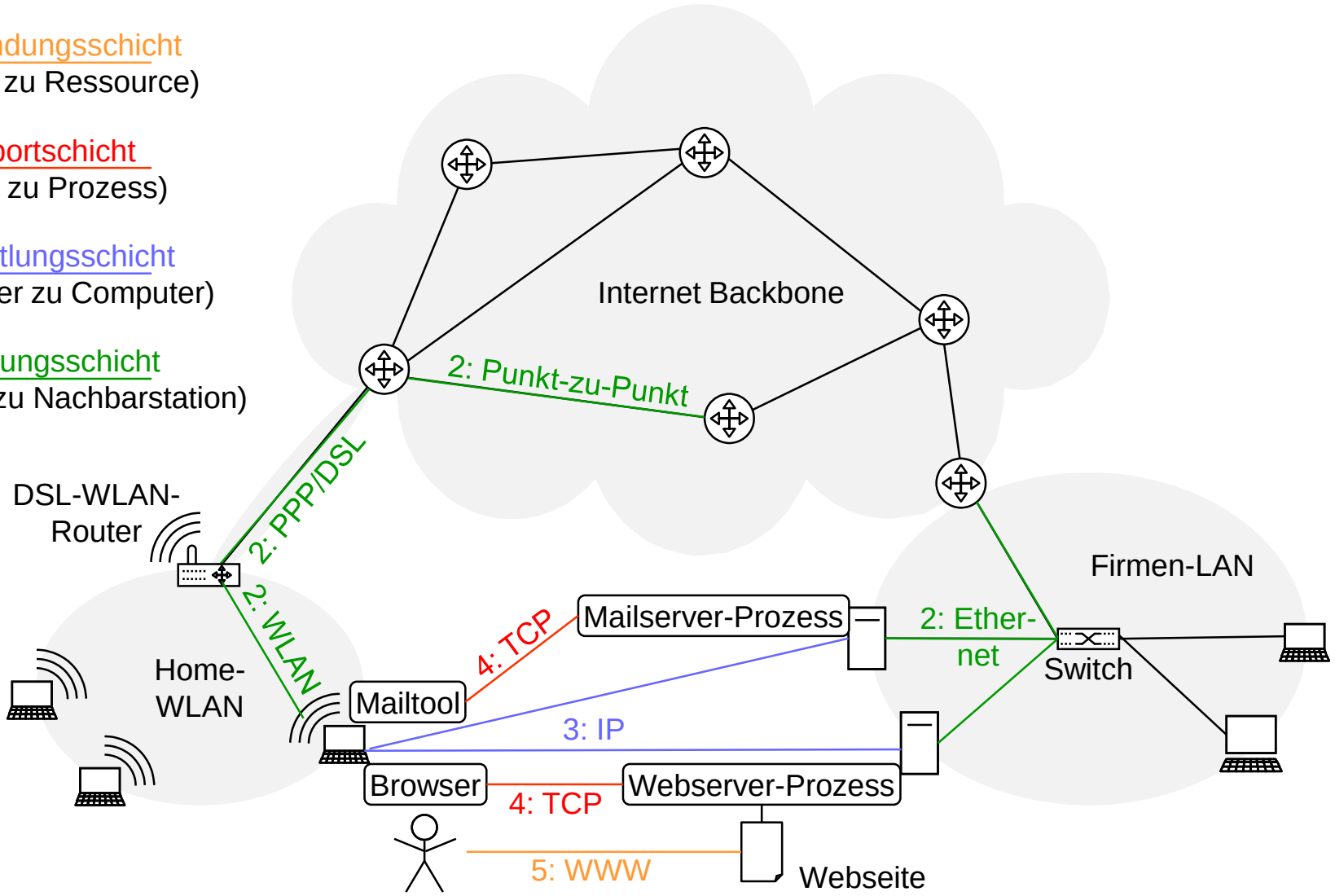
HOCHSCHULE DER MEDIEN

5: Anwendungsschicht
(Mensch zu Ressource)

4: Transportschicht
(Prozess zu Prozess)

3: Vermittlungsschicht
(Computer zu Computer)

2: Sicherungsschicht
(Station zu Nachbarstation)



TEIL 1: BITÜBERTRAGUNGSSCHICHT (PHYSICAL LAYER)

Übertragung von rohen Bits über einen Übertragungskanal:

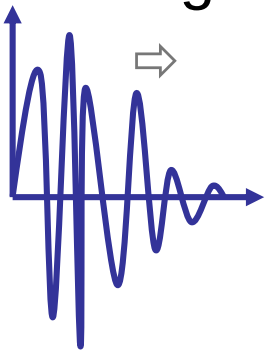
- Festlegung des physischen Übertragungsmediums
- mechanische, elektrische und prozedurale Festlegungen

Typische Festlegungen der Bitübertragungsschicht:

- Wie ist der Stecker für den Netzanschluss mechanisch aufgebaut?
- Wieviel Volt entsprechen einer logischen 1 bzw. 0
- Wieviel Millisekunden dauert ein Bit
- Gleichzeitige Übertragung in beide Richtungen oder nicht?
- Wie kommt die erste Verbindung zustande und wie wird sie wieder gelöst

ANALOGE UND DIGITALE SIGNALE

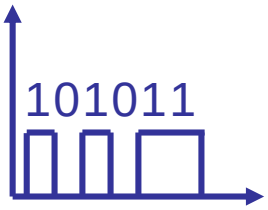
- **Analoge Signale**: Kontinuierliche Veränderungen physikalischer Größen (z.B. elektrische Spannung, magnetische Feldstärke) mit der Zeit



⇨ Mikrophone, Lautsprecher, Rundfunk, Fernsehen, klassische Telephonie, Compact-Kassetten oder Schallplattenspieler beruhen alle auf der Verarbeitung analoger Signale

- **Digitale Signale**: Abrupter Wechsel zwischen diskreten physikalischen Zuständen (z.B. stromführend / nicht stromführend) mit der Zeit

⇨ Moderne Computertechnik, Compact Disks sowie die modernen digitalen Varianten der Telephonie, digitale Video- und Audiotechnik beruhen alle auf der Verarbeitung digitaler Signale



MEDIEN ZUR ÜBERTRAGUNG VON SIGNALEN

Verschiedene Medien sind zur Übertragung von Signalen geeignet:

- **Elektrische Übertragungsmedien** (Kabel)
  - ⇨ Gut geeignet für analoge Signale
  - ⇨ Mit Einschränkungen (geringe Reichweite) für digitale Signale

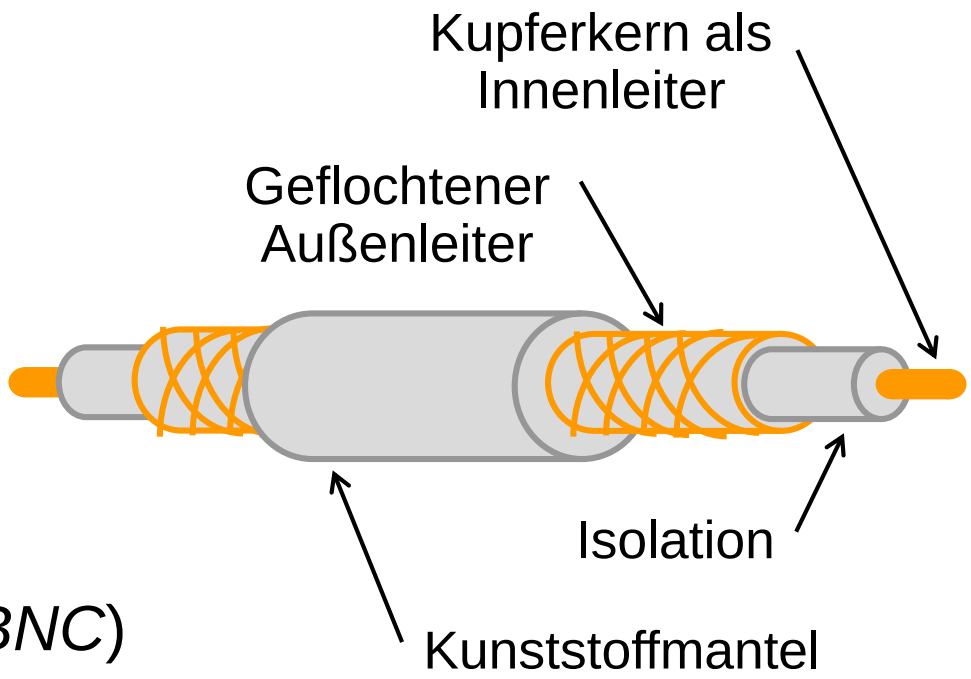
- **Elektromagnetische Wellen** (Funk)
  - ⇨ Für analoge Signale („Wellen“)

- **Optische Übertragungsmedien**
  - ⇨ Für digitale Signale („Ein-/Ausschalten von Licht“)
  - ⇨ **Lichtwellenleiter** (Glasfaserkabel)
  - ⇨ Übertragung ohne Leiter (Infrarot, Laserstrecken)

ELEKTRISCHE ÜBERTRAGUNGSMEDIEN

- Kabel dienen als elektrisches Übertragungsmedium
- Kabel sind gut geeignet für analoge Signale
- Empfindlich für Verluste, Störungen bei digitalen Signalen
  - ⇨ Besondere Bauweisen von Kabeln erforderlich
  - ⇨ Besondere Kodierung der digitalen Signale
- Besondere Bauweisen von Kabeln vermindern Abstrahlungen und Einstrahlungen
  - ⇨ Koaxialkabel: Außenleiter dient zur Abschirmung
  - ⇨ verdrillte Kabelpaare: minimieren Störungen

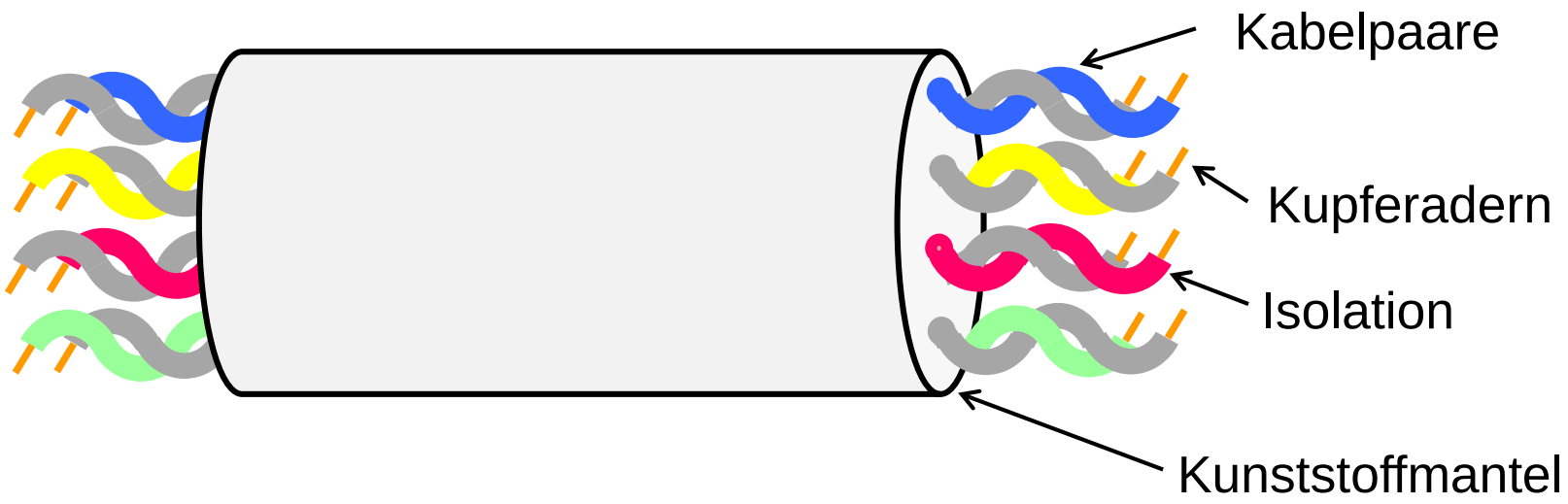
KOAXIALKABEL (BROADBAND NETWORK CABLE = BNC)



Koaxialkabel
für „Breitbandnetze“ (engl.: *broadband network cable = BNC*)

- Außenleiter dient zur Abschirmung gegen Abstrahlungen und Einstrahlungen
- Übertragungsrate z.B. 2 Gbit/s auf 2 km
- Beispiel: Fernsehantenne, Kabelfernsehen, breitbandige Computernetze, frühe lokale Netze (LAN)

VERDRILLTE KABELPAARE (TWISTED PAIRS, TP-KABEL)



Verdrillte Kabelpaare (engl.: *twisted pair, kurz TP*)

- Vergleichsweise preiswert
- max. Übertragungsrate ca. 100 Mbit/s auf 100m, mit zusätzlicher Abschirmung sogar bis zu 10 Gbit/s
- Beispiel: Telefonleitungen, lokale Computernetze (LAN)

TWISTED-PAIR-KABEL (TP-KABEL) MIT STECKER NACH RJ45

HOCHSCHULE DER MEDIEN

REPEATER

- Bei der Übertragung von Signalen über elektrische Leitungen (verdrillte Kabelpaare, Koaxialkabel) treten bei zunehmender Leitungslänge Abschwächungen der Signale und Einstrahlungen von Störungen auf.
  - ⇨ Dies verringert den Rauschabstand, d.h. das Verhältnis zwischen Signalstärke und Störungen. Im Extremfall sind die Störungen stärker als die Signale.
  - ⇨ Abhängig vom Kabeltyp und von der maximal verwendeten Datenrate gibt es eine maximale nutzbare Leitungslänge.
- Abhilfe: Durch Verwendung von elektronischen Geräten, so genannten **Repeatern**, können in regelmäßigen Abständen die Signale verstärkt und aufgefrischt werden.

HUBS

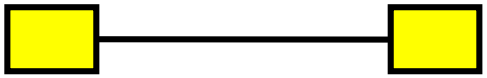
- Die typische Ausprägung eines Repeaters ist ein **Hub**.
- Ein Hub besitzt mehrere Anschlüsse (auch Ports genannt).
- Elektrische Signale die am Eingang eines Ports ankommen, werden verstärkt und an die Ausgänge aller anderen Ports weitergeleitet.
- Ein **Hub** arbeitet rein elektrisch und gehört deshalb im Schichtenmodell zur **Bitübertragungsschicht 1**:
  Die übertragenen Daten werden nicht interpretiert.
- Alternativ zu den Hubs können auch so genannte **Switches** eingesetzt werden. Switches interpretieren die übertragenen Daten und arbeiten daher auf der Sicherungsschicht 2 oder gar auf der Vermittlungsschicht 3. Switches werden daher in Kapitel 2 behandelt.

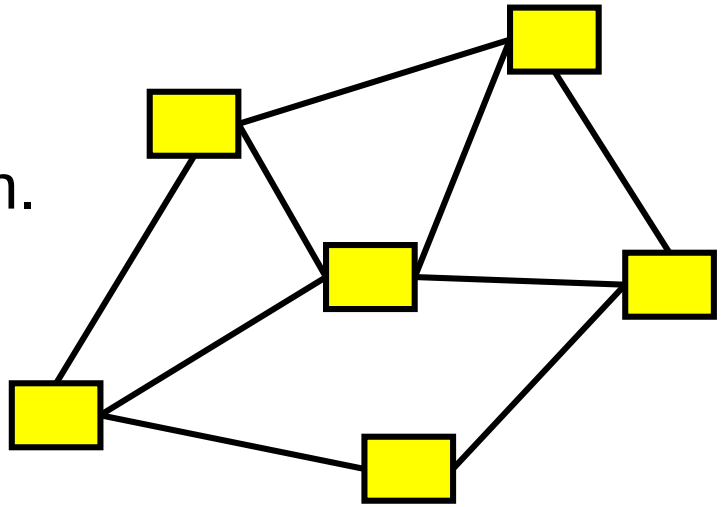
EINFACHSTE TOPOLOGIE: PUNKT-ZU-PUNKT-VERBINDUNG

Netze lassen sich anhand ihrer Topologien (Nachbarschaftsbeziehungen) klassifizieren.

Einfachste Topologie:
Die Punkt-zu-Punkt-Verbindung:

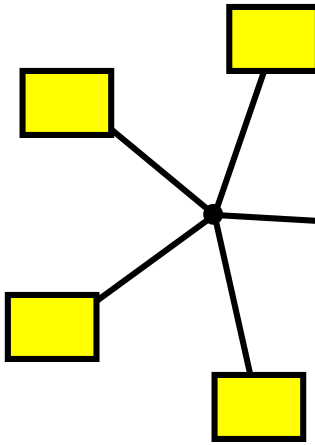
- Genau zwei Stationen kommunizieren über ein Verbindungskabel
- Mit Punkt-zu-Punkt-Verbindungen lassen sich ganze Netze aufbauen. Beispiel: Das aus so genannten Routern gebildete Internet-Backbone-Netz.



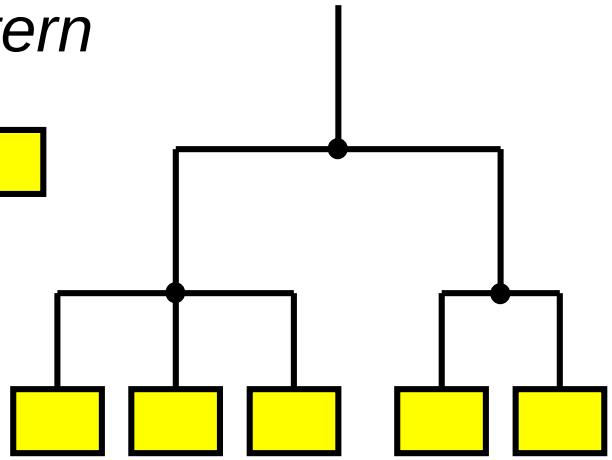


TOPOLOGIEN FÜR LOKALE NETZE (LANS)

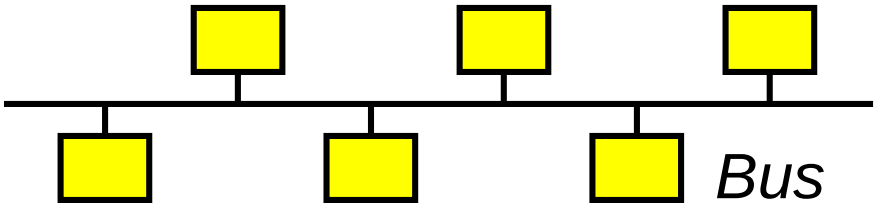
- Schleifenfreie LANs (Diffusionsnetze)
  - ⇨ Stern-Topologie
  - ⇨ Baum-Topologie
  - ⇨ Bus-Topologie



Stern

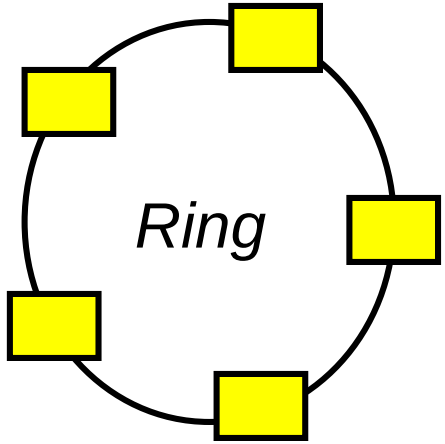


Baum



Bus

- Schleifenhaltige LANs
  - ⇨ Ring-Topologie



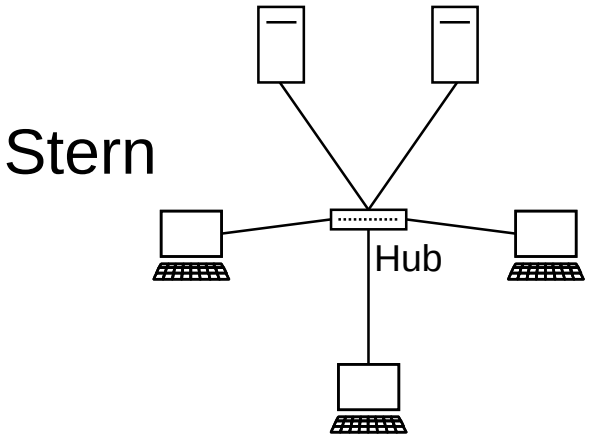
Ring

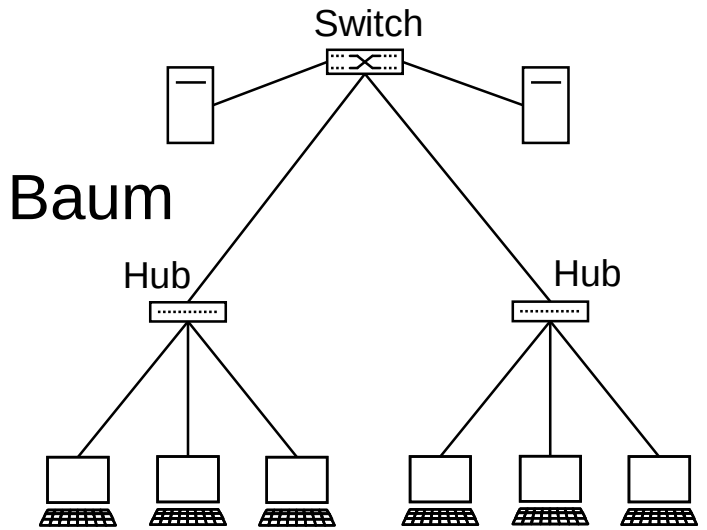
STERN- UND BAUMVERKABELUNG MIT HUB ODER SWITCH

HOCHSCHULE DER MEDIEN

In LANs heute übliche Topologien: Stern- und Baumverkabelung

- Stern: Im Zentrum steht ein Verteiler (Hub oder Switch)
- Baum: Unterverteilung über weitere Hubs oder Switches
- Twisted-Pair-Verkabelung (max. Länge zwischen Verteiler und Computer 100m)
- Oder Lichtwellenleiter (Glasfaserkabel, engl. “fibre”, max. Länge zwischen Verteiler und Computer 2000m)





ETHERNET: WICHTIGE SYSTEMLINIEN

HOCHSCHULE DER MEDIEN

Übertragungsgeschwindigkeit 10MBit/s (veraltet)

10Base5: Basis-Ethernet, dickes Koax. („Yellow Cable"), max. 500m Länge

10Base2: „Cheapernet", dünnes Koax., max. 200m

10BaseT: **Standard-Ethernet**, Hub oder Switch, verdrilltes Paar, max. 100m

Übertragungsgeschwindigkeit 100MBit/s

100BaseT: **Fast-Ethernet**, Hub oder Switch, verdrilltes Paar, max. 100m

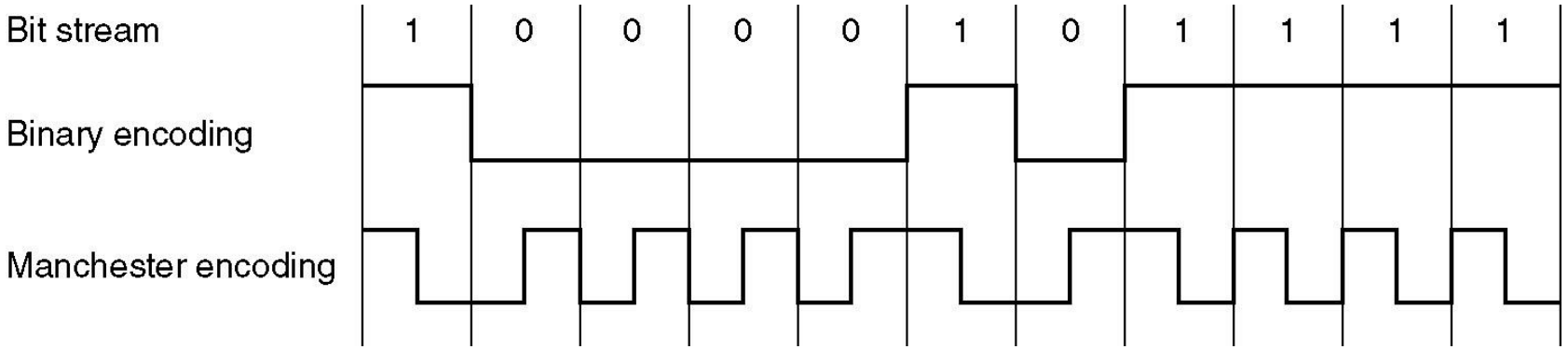
100BaseF: dto. aber mit Glasfaserkabel, max. 2000m

Übertragungsgeschwindigkeit 1000MBit/s

1000BaseT und 1000BaseF: **Gigabit-Ethernet**

Nächste Generation: 10 Gigabit-Ethernet (noch sehr teuer)

BITÜBERTRAGUNG IM ETHERNET



- Binary Encoding ist das naheliegendste Verfahren zur Kodierung eines Bitstroms. Eine 1 entspricht hoher Spannung, eine 0 niedriger Spannung
- Allerdings ist Binary Encoding aufgrund des großen Gleichstromanteils störanfällig.
- Manchester Encoding kodiert den Bitstrom durch Spannungsveränderung (weniger störanfällig): eine fallende Flanke bedeutet 1, eine steigende Flanke bedeutet 0.
- Manchester Encoding wird im 10Mbit-Ethernet verwendet, ab 100Mbit werden noch ausgefeiltere Verfahren genutzt.

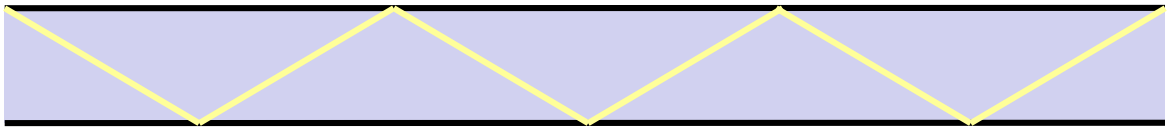
ELEKTROMAGNETISCHE WELLEN ALS ÜBERTRAGUNGSMEDIUM

Verschiedene Bereiche des elektromagnetischen Spektrums geeignet:

- **Radiowellen** (10kHz-1GHz):
  - ⇨ Lang-, Mittel-, Kurzwelle, Amateurfunk, UKW (FM),
  - ⇨ Fernsehen,
  - ⇨ Mobilfunk (D-Netz)
  - ⇨ rundstrahlend (omnidirektional), geradlinige Ausbreitung bei höheren Frequenzen (UKW, Fernsehen, Mobilfunk)
- **Mikrowellen** (1GHz-100GHz):
  - ⇨ Satellitenkommunikation
  - ⇨ Mobilfunk (E-Netz, UMTS, LTE)
  - ⇨ Richtfunkstrecken (z.B. Telefonübertragung)
  - ⇨ Strahlung lässt sich bündeln mit Parabolantennen (quasioptische Ausbreitung)

OPTISCHE ÜBERTRAGUNGSMEDIEN

- **Lichtwellenleiter**(Glasfaserkabel):
  - ⇨ Übertragungsrate ähnlich Koaxialkabel (im Gigabit-Bereich, potenziell noch besser)
  - ⇨ verwendet für Hochgeschwindigkeitsnetze und Fernnetze
  - ⇨ Totalreflektion von Lichtwellen verringert Verluste



Totalreflektion

  - ⇨ erfordert LED (*Light Emitting Diode* = Lichtdiode) oder Laser als Sender, Fotodiode als Empfänger
- Lichtwellenübertragung ohne Leiter:
  - ⇨ **Infrarot** (z.B. zur Verbindung von PCs, Notebooks, Palmtops und Druckern in einem einzelnen Raum)
  - ⇨ **Laserstrecken** zur Informationsübertragung

Sichtbares Licht, Infrarot und Ultraviolett zählen eigentlich auch zu den elektromagnetischen Wellen.

BANDBREITE ANALOGER ÜBERTRAGUNGSKANÄLE

- Jeder analoge Übertragungskanal besitzt eine Grenzfrequenz, d.h. Schwingungen mit höheren Frequenzen werden nicht mehr übertragen. Diese Frequenz heißt auch die **Bandbreite**.
- Frequenzen werden gemessen in Hz (Hertz): **1 Hz = 1/sec**
- Der Begriff Bandbreite stammt aus der Rundfunktechnik: Die Bandbreite entspricht der „Breite“ eines Senders auf der Rundfunkskala.
  - ⇨ Beispiel: Wenn ein Sender auf der Frequenz ***f*** Signale mit einer Bandbreite ***b*** überträgt, kann der nächste Sender (theoretisch) erst wieder auf der Frequenz ***f+b*** bzw. ***f-b*** senden, ohne dass es zu Störungen kommt.
  - ⇨ Die Bandbreite eines Senders ist maßgeblich für die höchste durch den Sender übertragene Frequenz und damit für die effektive Klangqualität.

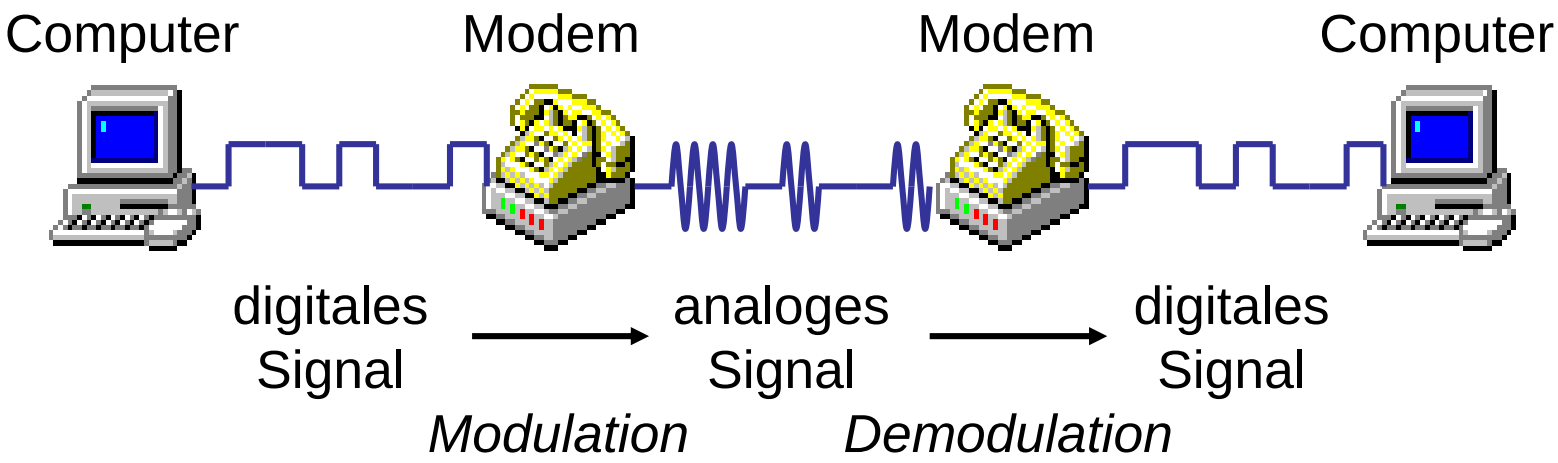
DATENRATE DIGITALER ÜBERTRAGUNGSKANÄLE

- Die Leistungsfähigkeit eines digitalen Übertragungskanals wird in **Bit/s** (Anzahl übertragener binärer Zustände pro Sekunde) gemessen und als **Datenrate** bezeichnet.
- Oft müssen digitale Signale zur Übertragung oder Aufzeichnung in analoge Signale gewandelt werden
  - ⇨ Es besteht ein linearer Zusammenhang zwischen der Bandbreite eines analogen Kanals und der maximal erzielbaren Datenrate. Darüber hinaus wird die Datenrate durch den Rauschabstand (= Signalstärke / Stärke des Rauschens) beeinflusst.
  - ⇨ **Shannons Theorem** (1948):
    Max. Datenrate = Bandbreite $\log_2(1 + \text{Rauschabstand})$

WANDLUNG DIGITALER SIGNALE IN ANALOGE SIGNALE

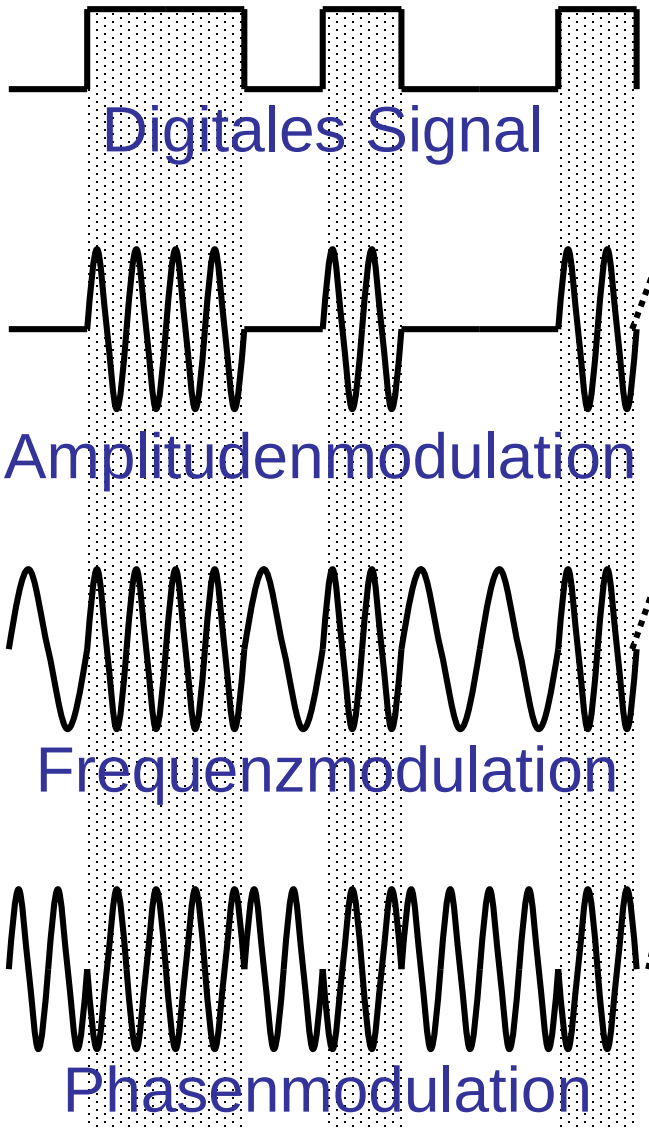
- Die direkte Übertragung digitaler Signale über elektrische Kabel oder Funk stößt auf Schwierigkeiten, da rechteckig geformte Signale hohe Frequenzanteile enthalten, d.h. zur korrekten Übertragung ist eine hohe Bandbreite erforderlich.
- Deshalb wurden verschiedene Modulationsverfahren entwickelt, um digitale Signale in analoge Schwingungen mit möglichst geringer Bandbreite umzusetzen.
- Ziel ist es, bei gegebener Bandbreite die maximale Datenrate (entsprechend Shannons Theorem) zu erreichen
- Wandlung zwischen Digital- und Analogsignale durch **Modems** (Modulator/Demodulator)

MODEMS



- Modems setzen digitale Signale in analoge um (***Mo****dulation*) und umgekehrt (***Dem****odulation*).
- Modems ermöglichen dadurch die Übertragung von digitalen Signalen über analoge Leitungen, z.B. im Telefonnetz:
  - ⇨ Über das klassische, analoge Telefonnetz (mit einer einer nutzbaren Bandbreite von max. 4000 Hz analog) sind Datenübertragungsraten von bis zu 56 kbit/sec möglich.

MODULATIONSVERFAHREN



Amplitudenmodulation:
Entsprechend dem digitalen Signal wird die Amplitude (Stärke) einer analogen Schwingung verändert.

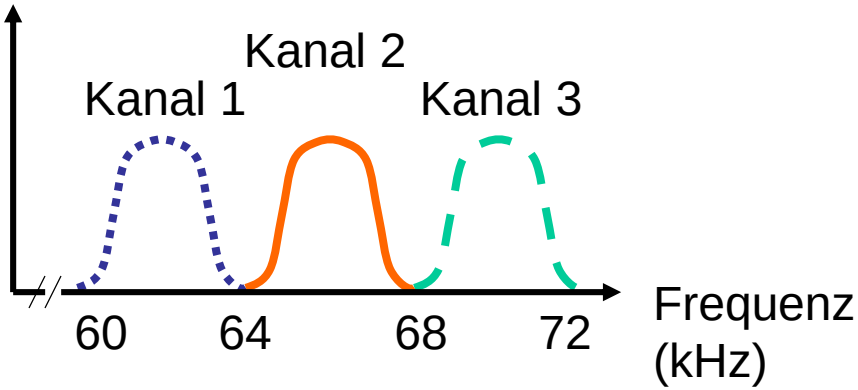
Frequenzmodulation: Hierbei wird die Frequenz einer analogen Schwingung verändert.

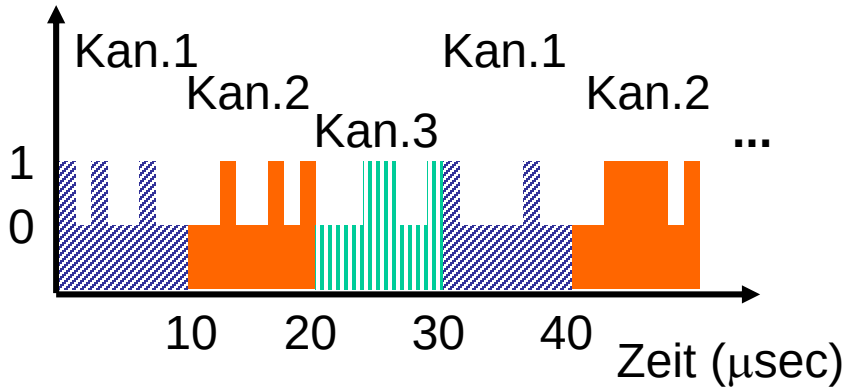
Phasenmodulation: Der zeitliche Ablauf einer analogen Schwingung wird um einen bestimmten Anteil ihrer Schwingungsperiode verschoben.

Für Modems werden in der Regel **Kombinationen** aus Amplituden- und Phasenmodulation benutzt.

MULTIPLEXVERFAHREN

Multiplexverfahren dienen dazu, um über einen (meist: physischen) Kommunikationskanal mehrere logische Kommunikationskanäle zu realisieren:





Frequenzmultiplexverfahren

(Abk.: FDM= frequency division multiplexing): Das verfügbare Frequenzspektrum wird auf verschiedene logische Kanäle aufgeteilt, ähnlich wie auf einer Rundfunkskala. Geeignet für **analoge** Kanäle.

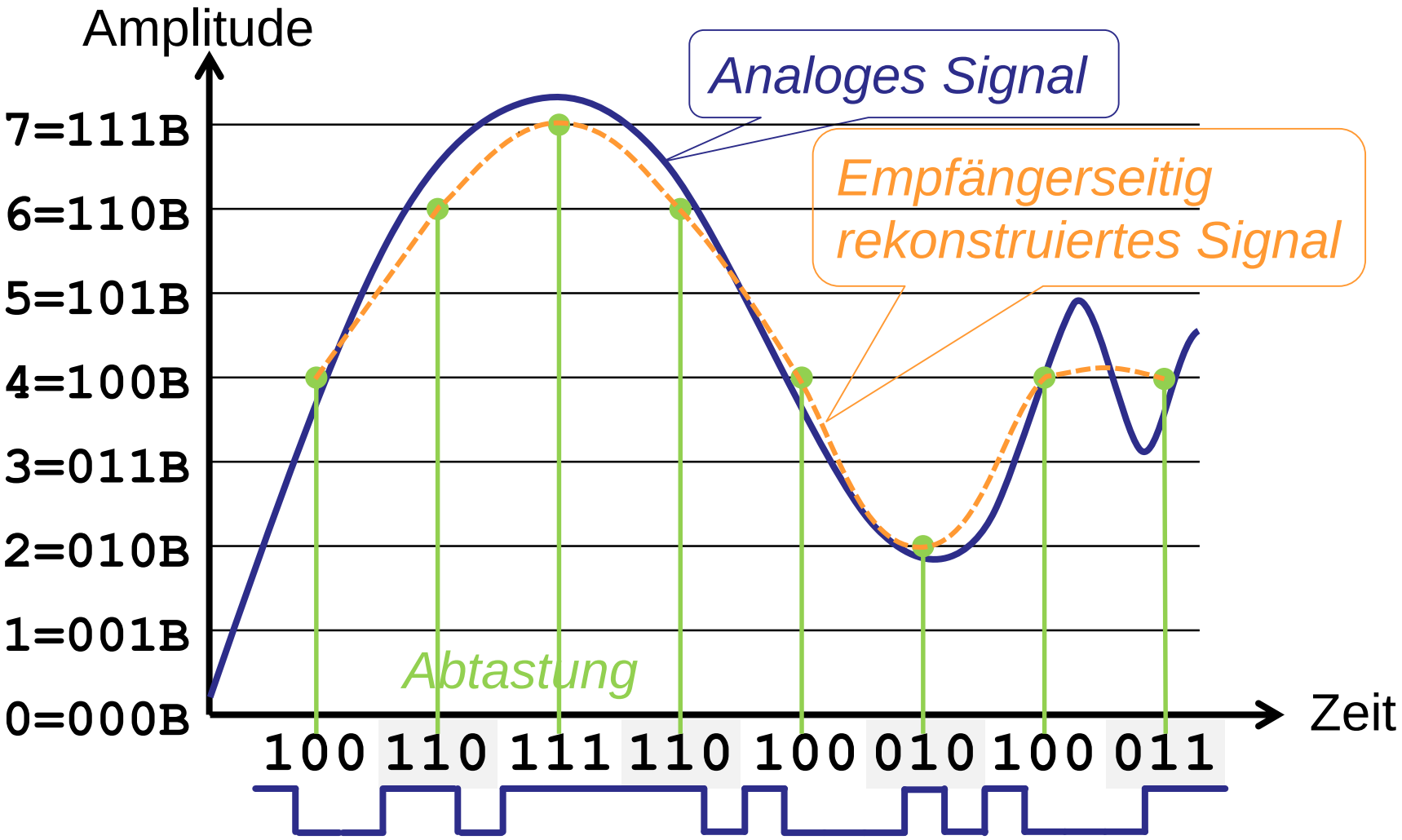
Zeitmultiplexverfahren

(Abk.: TDM=time division multiplexing): Die logischen Kanäle erhalten abwechselnd nacheinander Zugriff auf den physikalischen Kommunikationskanal. Geeignet für **digitale** Kanäle.

ZEITMULTIPLEXVERFAHREN IN DER TELEFONIE

- Das Zeitmultiplexverfahren wird gerne verwendet, um in der klassischen Telefonie viele Gespräche gleichzeitig auf einer einzigen Glasfaserleitung zu übertragen.
- Das Zeitmultiplexverfahren funktioniert aber nur mit digitalen Signalen zufriedenstellend.
- Deshalb müssen analoge Telefongespräche vor der Übertragung über lange Strecken in der Regel in digitale Form gewandelt werden und nach der Übertragung wieder zurückgewandelt werden.
- Die hierfür verwendeten Wandler heißen Codec (**Co**der/**Dec**oder)

ANALOG-DIGITALWANDLUNG MIT EINEM CODEC (BEISPIEL)



Mit 3 Bit Genauigkeit kodiertes digitales Signal

CODECS: FUNKTIONSWEISE

Ein Codec umfasst eine **Co**der- und eine **Dec**oderfunktion

- **Coderfunktion** am Startpunkt der Übertragung
  - ⇨ Messung der Stärke eines Analogsignals in regelmäßigen zeitlichen Abständen (Abtastrate für Telefonate 8000/sec, für CDs 44100/sec). Werte dazwischen werden ignoriert (zeitliche Quantisierung). Theorem von Nyquist (1924): Die Abtastrate muss mindestens doppelt so hoch sein wie die höchste zu übertragende Frequenz.
  - ⇨ Kodierung der gemessenen Werte als Binärzahlen mit einer bestimmten Genauigkeit (z.B. 7- oder 8-Bit für Telefonate, 16 Bit für CD-Kanal). Es wird auf den nächsten Wert gerundet (wertmäßige Quantisierung). Die Folge der Binärzahlen wird digital übertragen.
- **Decoderfunktion**: Am Zielpunkt werden die übertragenen digitalen Werte in elektrische Spannungsstufen gewandelt.

VERWENDUNG VON CODECS IN DER TELEFONIE

- Die Digitalisierung von analogen Telefonaten wird auch **Pulscodemodulation (PCM)** genannt:
  - ⇨ Abtastrate: **8000/sec** (d.h. alle 125µsec), also Grenzfrequenz nach Nyquist 4000Hz
  - ⇨ Wertmäßige Quantisierung: 8 Bit (256 diskrete Werte), in USA oft: 7 Bit (128 Werte).
  - ⇨ Übertragung: über so genannte **PCM-Kanäle** mit der Datenrate 8×8000 = **64000 Bit/sec** (in USA meist 7×8000 = **56000 Bit/sec**).
- Anwendung
  - ⇨ Zeitmultiplexing und Übertragung von PCM-Kanälen über Glasfaserleitungen
  - ⇨ Die voll-digitale ISDN-Telefonie (Integrated Services Digital Network)

MODEMS UND CODECS: WAS IST DER UNTERSCHIED?

- **Modems** ermöglichen
  die Übertragung digitaler Signale
  über analoge Übertragungsstrecken.
  - ⇨ Senderseite: Digital-Analog-Wandlung durch Modem
  - ⇨ Analoge Übertragung (z.B. über Zweidraht-Telefonleitung)
  - ⇨ Empfangsseite: Analog-Digital-Wandlung durch Modem
- **Codecs** ermöglichen
  die Übertragung analoger Signale
  über digitale Übertragungsstrecken.
  - ⇨ Senderseite: Analog-Digital-Wandlung durch Codec
    (Ergebnis: Reihe von digitalen Messwerten)
  - ⇨ Digitale Übertragung (z.B. über Glasfaser)
  - ⇨ Empfangsseite: Rekonstruktion des ursprünglichen analogen Signals durch Codec

ISDN

Integrated Services Digital Network (ISDN):

- voll digitales Telefonsystem (Gegensatz zur alten analogen Telefoniedienst, dem „*plain old telephone service*“ - POTS), integriert Sprach- und Datendienste
- ISDN ist leitungsvermittelt wie „POTS“, für jede Verbindung (Gespräch, Datenübertragung) wird ein logischer (PCM-) Kanal mit 64000 Bit/sec (USA: 56000) reserviert.
- Digitale Übertragung von der Vermittlungsstelle zum Kunden über die vorhandene Zweidrahtleitung („letzte Meile“). Keine neuen Anschlussleitungen nötig.
- konzipiert im Jahr 1984 durch CCITT (Comité Consultatif International Télégraphique et Téléphonique), heute ITU (International Telecommunication Union)

DIE ISDN-SCHNITTSTELLE

Ein ISDN-Anschluss unterstützt mehrere Kanäle, die durch das Zeitmultiplexverfahren aufgeteilt werden, darunter als wichtigste:

- B: digitaler Kanal für Sprache oder Nutzdaten (PCM-Kanal mit 64000 Bit/sec bzw. in USA 56000 Bit/sec)
  - ⇨ Telefongespräche werden bereits im ISDN-Endgerät digitalisiert, jeder Telefonapparat enthält einen Codec.
- D: digitaler Kanal (16000 Bit/sec) für Steuerdaten

Wichtigste Anschlusstypen sind:

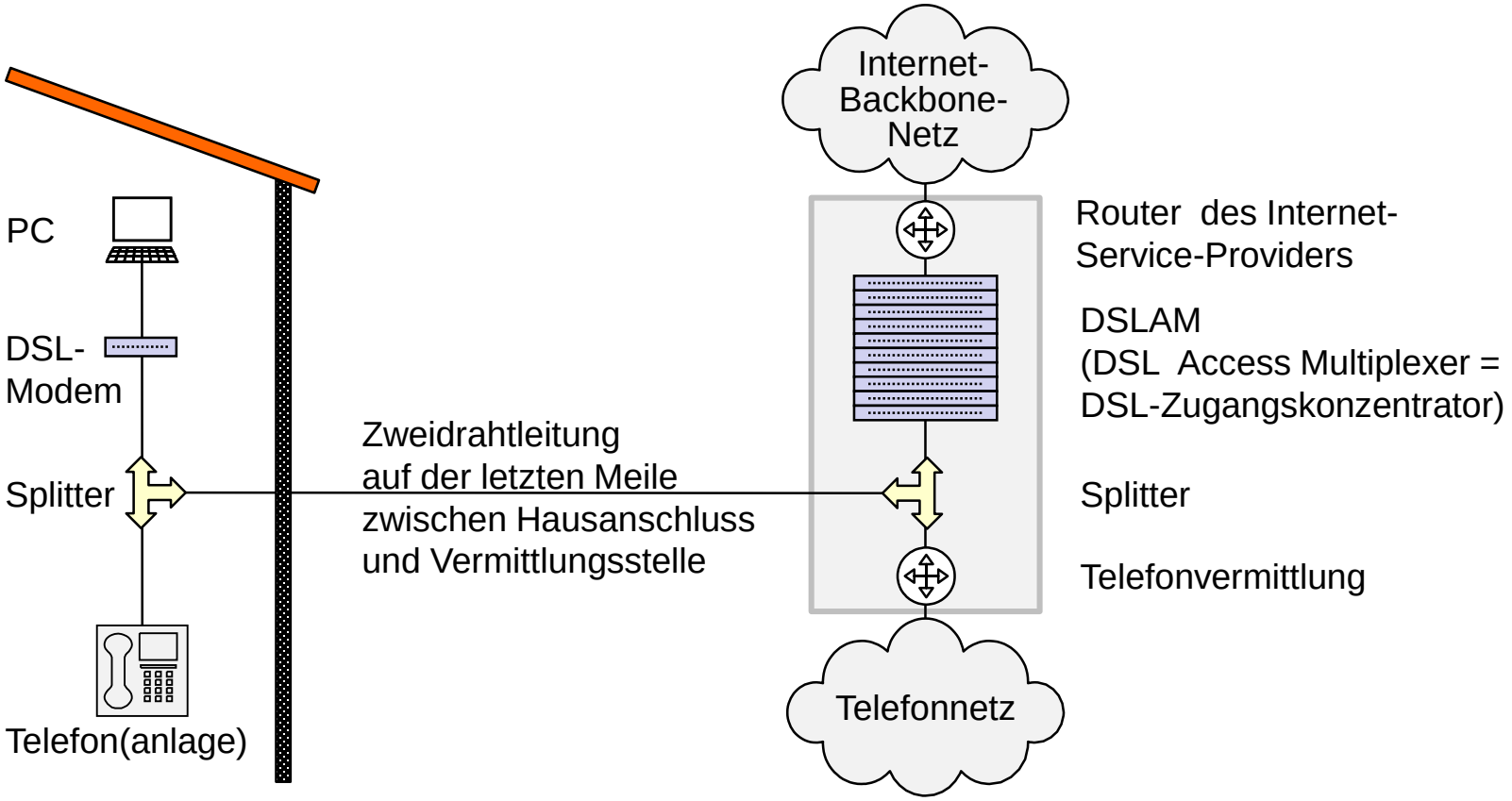
- Basisanschluss z.B. für Privatkunden: 2B + 1D
- Primärmultiplexanschluss z.B. für Firmen: 30B + 1D, in USA: 23B + 1D

DIGITAL SUBSCRIBER LINE (DSL)

Digital Subscriber Line (DSL): Digitaler Übertragungsdienst (Internetanschluss) für Telefon-Teilnehmer („***Subscriber***“)

- Durch fortschrittliche Modulations- und Multiplexingtechniken kann auf der „letzten Meile“ zwischen Vermittlungsstelle und Hausanschluss die bestehende Zweidrahtverkabelung des Telefonanschlusses verwendet werden.
- DSL kombiniert auf einem einzigen Kabelpaar
  - ⇨ einen Telefonkanal (analog oder ISDN-Basisanschluss mit 2 PCM-Kanälen)
  - ⇨ einen digitalen Downstream-Kanal (typische Übertragungsraten 2, 6, 16, 50 Mbit/sec je nach Verfahren)
  - ⇨ einen digitalen Upstream-Kanal (typische Übertragungsraten 128, 196, 256 oder 640 Kbit/sec)
- Ein Splitter (Frequenzweiche) trennt die hochfrequenten Datenkanäle (Down- und Upstream) vom niederfrequenten Telefonkanal.

DSL-ANSCHLUSSSCHEMA



ADSL UND VDSL

Meist sind die Datenraten von Uplink und Downlink „asymmetrisch“ (d.h. der Downlink ist deutlich schneller)

- **Asymmetric Digital Subscriber Line (ADSL)**
- **Anwendung**: Video on Demand, Surfen im Web (beides erfordert hohe Datenraten für Downlink, geringe für Uplink)

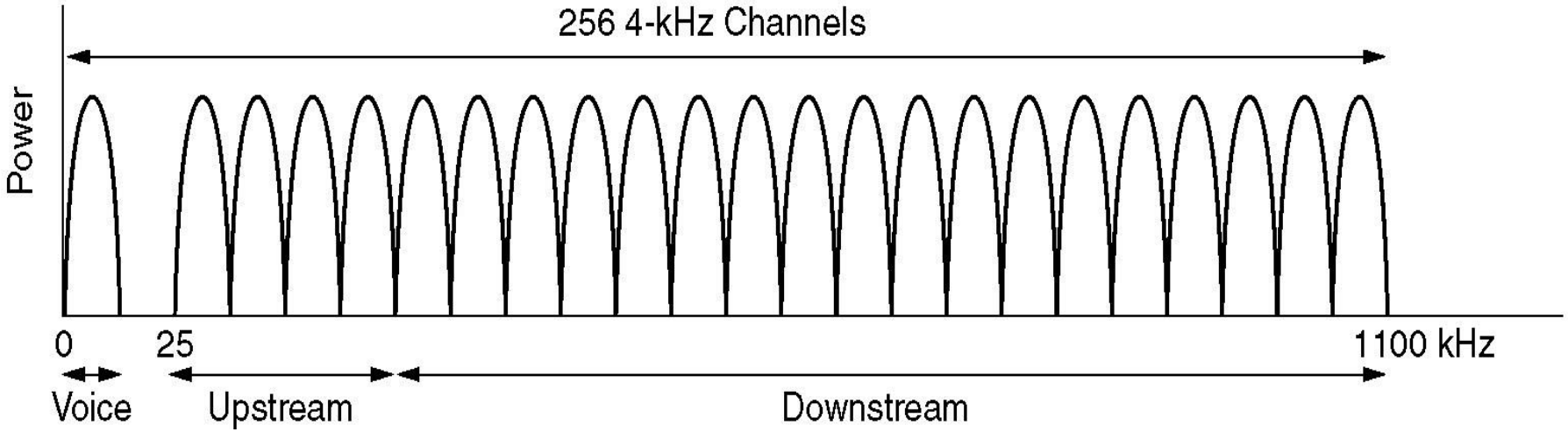
In jüngster Zeit werden sehr schnelle DSL-Varianten eingerichtet:

- **Very high speed Digital Subscriber Line (VDSL)**
- Typische Downstreamraten: 16 oder gar 50 Mbit/sec
- Upstreamraten bis zu 6 Mbit/sec
- Nur möglich, falls die Kupferleitung des Hausanschlusses sehr kurz ist (z.B. 300m)
  - ⇨ Erfordert den Bau von neuen Vermittlungsstellen (Verteilerkästen) in der Nähe der Hausanschlüsse, ab dort geht es weiter über Glasfaser.

MEHR ZU DSL

- DSL ist eine besondere Art von Modem-Übertragung.
- Im Gegensatz zur klassischen Modem-Übertragung muss DSL nur die „letzte Meile“ (die letzten hundert Meter bei VDSL) bis zu einer Vermittlungsstelle überbrücken.
- Die DSL-Übertragung läuft nicht über das öffentliche Telefonnetz. Dadurch fällt die Beschränkung auf die max. Bandbreite 4000Hz (Analogtelefonie) bzw. auf die Datenrate 64000 oder 56000 Bit/sec (PCM/ISDN bei einer 8- bzw 7-Bit-Abtastung von 8000/sec) weg. Die DSL-Übertragung endet bei der Vermittlungsstelle, ab dort wird ein schnelles Internet-Backbone-Netz benutzt.
- Dennoch erfordert DSL sehr fortschrittliche Modulationsverfahren, damit die bestehende Kupferverkabelung zwischen Hausanschluss und Vermittlungsstelle genutzt werden kann.

DSL: DISCRETE MULTITONE MODULATION



Quelle: Tanenbaum & Wetherall (2012) Abb. 2.34

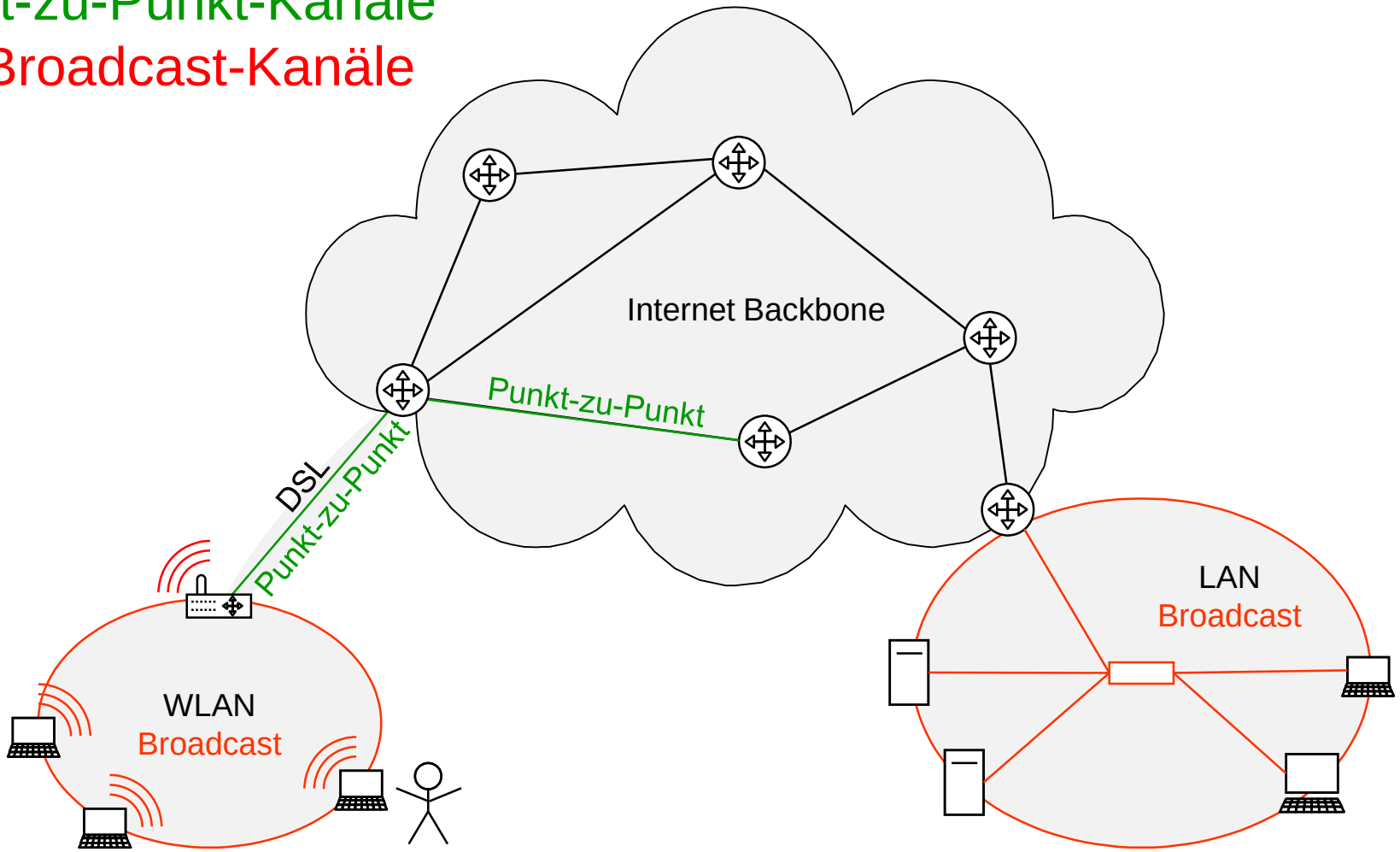
TEIL 2: SICHERUNGSSCHICHT (DATA LINK LAYER)

Übertragung von Daten zwischen zwei benachbarten (d.h. direkt durch ein Übertragungsmedium verbundenen) Computern

- Fehlerfreie Übertragung von Daten mit Hilfe von **Rahmen** (engl. Frames = voneinander abgrenzbare Bitfolgen)
  - ⇨ besondere Bitmuster als Rahmengrenzen, die innerhalb des Rahmens nicht auftreten dürfen
  - ⇨ „Datenrahmen“ und „Bestätigungsrahmen“
  - ⇨ Wiederholung der Übertragung im Fehlerfall, Erkennung und Eliminierung von Duplikaten
  - ⇨ Geschwindigkeitsanpassung
- **MAC-Teilschicht** (Media Access Control): Regelung des Zugriffs auf das Übertragungsmedium in einem sog. **Broadcast-Netz**, in dem alle Stationen denselben Kanal benutzen

ÜBERTRAGUNGSDIENSTE DER SICHERUNGSSCHICHT (EBENE 2)

Punkt-zu-Punkt-Kanäle
und Broadcast-Kanäle



PUNKT-ZU-PUNKT-KANÄLE UND BROADCAST-KANÄLE

Die Sicherungsschicht beschreibt, wie zwei **benachbarte** Computer miteinander kommunizieren. Die Kommunikation kann dabei über zwei Arten von Kanälen laufen:

- **Punkt-zu-Punkt-Kanäle** verbinden genau **zwei Stationen** im Netz miteinander. Beispiele:
  - ⇨ Langstreckenverbindung zwischen zwei benachbarten Routern in einem Internet-Backbone-Netz
  - ⇨ Einwahlverbindung zwischen einem Computer und einem Internetprovider: Punkt-zu-Punkt-Verbindung über Analogmodem, ISDN oder DSL.
- **Broadcast-Kanäle** (engl. *broadcast* = Rundfunk) verbinden **eine Gruppe von Stationen** im Netz miteinander. Dies wird im Rahmen der MAC-Teilschicht behandelt. Beispiele:
  - ⇨ LAN (Local Area Network) auf Basis Ethernet
  - ⇨ WLAN (Wireless LAN)

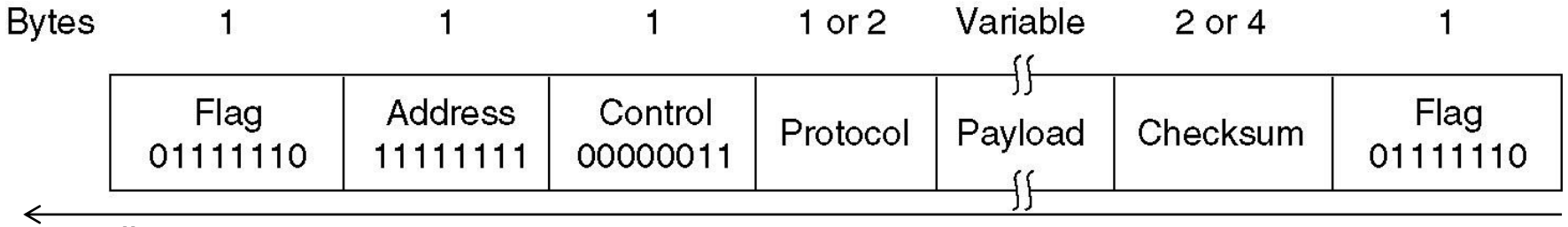
PUNKT-ZU-PUNKT-KANÄLE: BEISPIEL: PPP

PPP (Point to Point Protocol):

- Protokoll und gleichnamiger Dienst für die Einwahl-Verbindung zwischen dem Computer eines Internet-Benutzers und dem Einwahlknoten (Router) eines Internet-Service-Providers.
- Serielle Übertragung über Analogmodem, ISDN oder DSL (seriell: Daten werden nacheinander als Bitstrom über eine eine einzelne Leitung übertragen).
- Übertragung der Nachrichten in Form von „Rahmen“ mit Anfangs- und Endekennung sowie Fehlererkennung.
- Automatische Übertragung von Internet-Konfigurationsdaten (Internetadresse für den Computer, weitere Einstellungen für Routing und Domain-Name-System)
  - ⇨ Dadurch voller Internet-Zugang ohne besonderen lokalen Netzwerkkonfigurationsaufwand möglich

RAHMEN FÜR DIE SERIELLE ÜBERTRAGUNG AM BEISPIEL PPP

- **Flag:** Anfangskennung
- **Address:** Zieladresse, bei PPP normalerweise nicht relevant
- **Control:** zur Steuerung, z.B. Bestätigung, Nummerierung
- **Protocol:** Bezeichnung des übergeordneten Dienstes bzw. Protokolls, z.B. IP (Internet Protocol) oder IPCP (IP Control Protocol, für Übertragung der Internet-Konfigurationsdaten)
- **Payload:** Nutzlast = zu übertragende Daten
- **Checksum:** Prüfsumme zur Fehlererkennung
- **Flag:** Endekennung

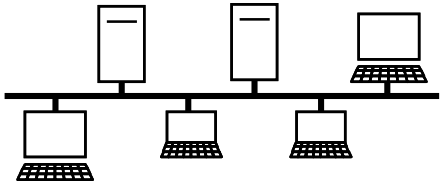


(Abb.: Tanenbaum 2007)

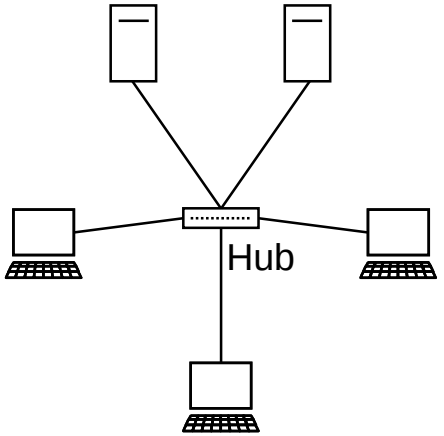
BROADCAST-KANÄLE: BEISPIEL ETHERNET-LAN

Das Ethernet: Beispiel für ein Broadcastnetz
Alle Stationen nutzen dasselbe Übertragungsmedium

- Klassisch: Bustopologie
  Ein Koaxialkabel verbindet
  alle Stationen miteinander



- Heute: Sterntopologie
  Ein Hub überträgt die gesendeten
  Daten über Twisted-Pair-Kabel
  oder Glasfaserkabel
  an **alle** anderen Stationen



Ein Steuerungsverfahren für den Zugriff auf das Übertragungsmedium (Media Access Control – MAC) ist erforderlich.

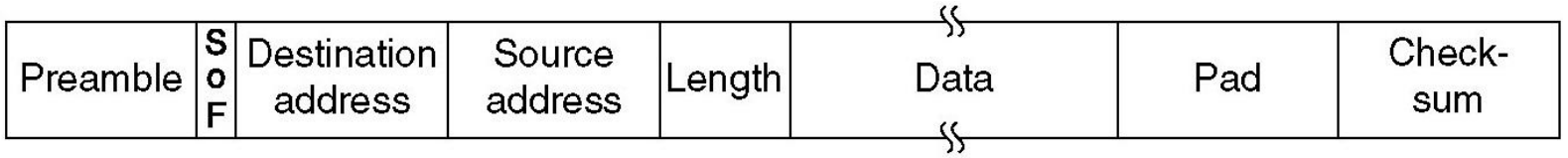
CSMA/CD: MEDIA ACCESS CONTROL FÜR ETHERNET-LANS

Media Access Control für Ethernet-LANs:
CSMA/CD (Carrier Sense Multiple Access Collision Detect)

- **Multiple Access**: Mehrere Stationen haben Zugang zum Übertragungskanal (aber nicht gleichzeitig)
- **Carrier Sense**: Abhören des Kanals vor und bei dem Senden.
  - ⇨ Es wird nur gesendet, wenn keine andere Station sendet.
- **Collision Detect**: Gleichzeitiger Zugriff („Kollision“) auf das Medium wird erkannt.
  - ⇨ Wenn zwei Stationen gleichzeitig lossenden, bemerken sie dies, stoppen beide die Übertragung und versuchen nach zufallsgesteuerter Zeit wieder zu senden.

Verfahren genormt durch IEEE 802.3 / ISO 8802.3
IEEE: Institute of Electrical and Electronics Engineers
ISO: International Standards Organisation)

ETHERNET FRAME-FORMAT NACH IEEE 802.3



Preamble: 7 Bytes der Form 10101010 binär (abwechselnd 1 und 0) zur Synchronisation

SOF: 1 Byte “Start of Frame” 10101011 binär

Destination & Source Address: jeweils 6 Bytes Adressen der Netzwerkkarten von Sender und Empfänger, so genannte MAC-Adressen oder physikal. Adressen

Length: Codierung von Länge/Typ der Daten (2 Bytes)

Data: zu übertragende Nutzdaten

Pad: ggf. Leerzeichen zum Auffüllen auf die minimale Frame-Länge (48 Bytes bei 100Mbit/s-Ethernet)

Checksum: Prüfcode zur Erkennung von Übertragungsfehlern (4 Bytes)

ARTEN VON VERTEILERN: HUBS UND SWITCHES

Es gibt zwei Arten von Verteilern:

- **Hubs** („Naben“) sind im einfachsten Fall elektrische Verstärker (Repeater) für die Signale und unterstützen nur eine Datenübertragung zu einem Zeitpunkt. Die Geschwindigkeit des Netzes teilt sich auf die Teilnehmer auf. Hubs arbeiten auf der Ebene 1 (Bitübertragungsschicht).
- **Switches** (Analogie: Switchboards der ersten Telefongeneration) unterstützen mehrere gleichzeitige Datenübertragungen durch das „Durchschalten“ von Verbindungen, so dass mehrere Teilnehmerpaare mit voller Geschwindigkeit des Netzes kommunizieren können. Switches arbeiten auf der Ebene 2 (Sicherungsschicht) bzw. auf der Ebene 3 (Vermittlungsschicht).

TOPOLOGIEN UND KOLLISIONSDOMÄNEN

Das klassische Ethernet nutzt eine Bustopologie

- Der Bus stellt eine „Kollisionsdomäne“ dar: Kollisionen können zwischen allen Stationen stattfinden.

Die Verwendung eines Hub ändert daran nichts

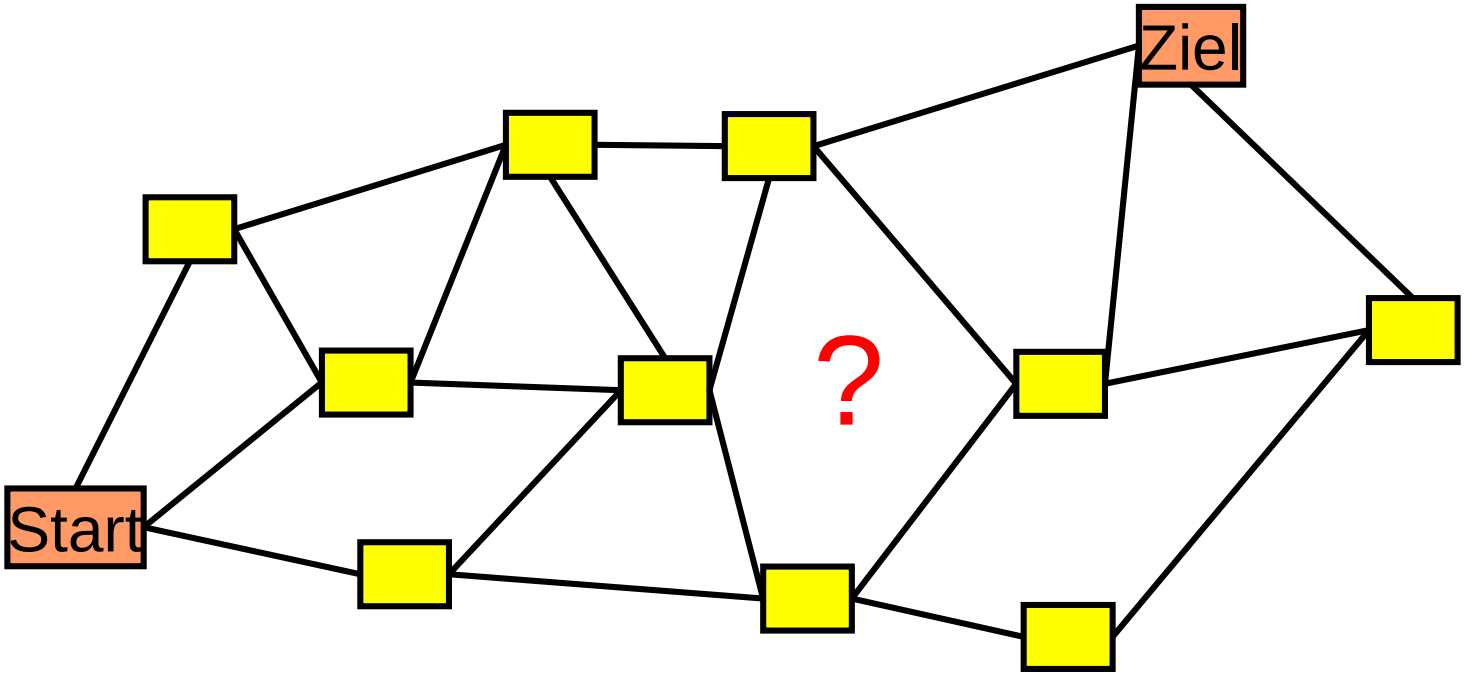
- Äußerlich wird zwar eine Sterntopologie verwandt
- Eine logische Bus-Topologie steckt jedoch im Hub
- Alle am Hub angeschlossenen Stationen bilden zusammen eine Kollisionsdomäne.

Anders beim Switch:

- Die Stationen sind separiert, jeder Anschluss des Switch ist eine eigene Kollisionsdomäne
- Kollisionen kommen praktisch nicht mehr vor.

TEIL 3: VERMITTLUNGSSCHICHT (NETWORK LAYER)

Vermittlung: Herstellen eines Übertragungswegs durch ein komplexes Netzwerk bestehend aus Knoten und Kanten („Routenmanagement“ im Netzwerk)



AUFGABEN DER VERMITTLUNGSSCHICHT

Steuerung des Betriebs des Subnetzes (der Subnetze):

- Eigentliche Vermittlungsaufgabe
- Vermeidung von Staus bei hoher Netzbelastung
- Abrechnungsfunktion
- Verbindung heterogener Subnetze (z.B. mit unterschiedlichen Protokollen und Adressierungsarten)
- Beispiele:
  - ⇨ IP (Internet Protocol), Dienst der Vermittlungsschicht des Internet
  - ⇨ Telefonnetz: klassische Analogtelefonie, ISDN (digital), ATM (Asynchronous Transfer Mode, digitales Übertragungsnetz der Telekoms, im Folgenden nicht weiter behandelt)

ZIELE DER DIENSTE DER VERMITTLUNGSSCHICHT

- Die Dienste sollen unabhängig von der Topologie des Subnetzes sein
- Die nächsthöhere Schicht, die Transportschicht, muß von der Anzahl, der Art, und der Topologie der vorhandenen Subnetze abgeschirmt werden
- Die für die Transportschicht vorgesehenen Netzadressen müssen ein einheitliches Nummerierungsschema darstellen
- **Konsequenz:**
  Die Schnittstellen der Vermittlungsschicht nach oben sind noch netzweit einheitlich und verstecken die Unterschiede der Subnetze. Auf den nächsttieferen Schichten (Sicherung, Bit-Übertragung) sind diese Unterschiede jedoch vorhanden.

DIENSTGÜTE (QUALITY OF SERVICE)

Übertragungsdienste, speziell auf Schicht 3, lassen sich anhand ihrer Dienstgüte charakterisieren:

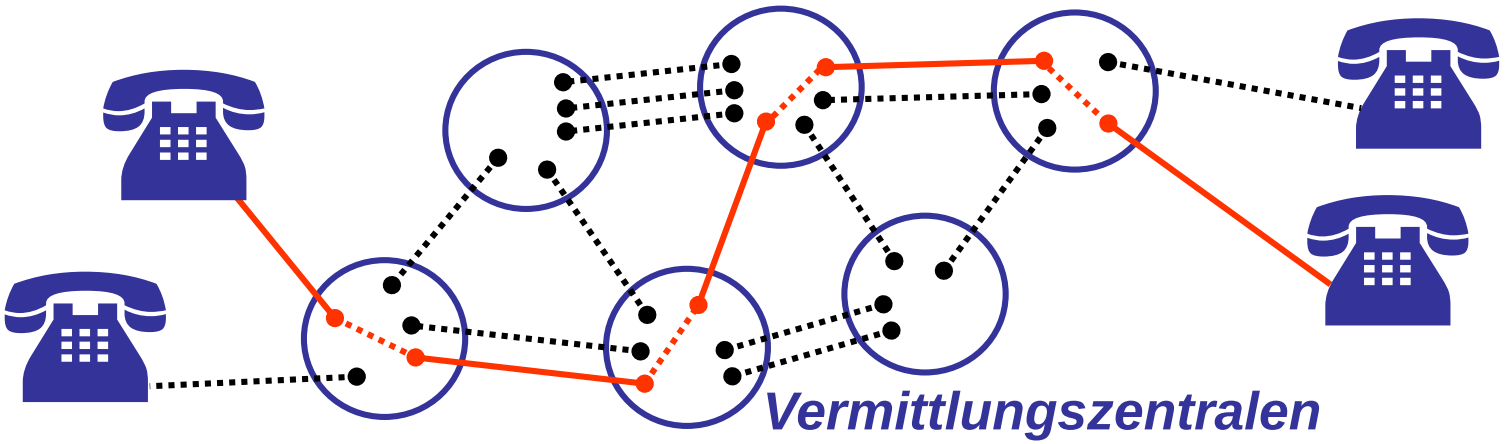
- Bandbreite (analog), Datenrate (digital): Übertragungsleistung des Übertragungsdienstes, sollte hoch und garantiert sein.
- Latenz (Übertragungsverzogerung) und Jitter (Schwankung der Latenz), sollten gering bzw. begrenzt sein.
- Zuverlässigkeit
  - ⇨ Überlaststeuerung (congestion control): Was passiert wenn das Netz überlastet ist.
  - ⇨ Datenflusssteuerung (flow control): Anpassung an die Verarbeitungsgeschwindiglkeit des Empfängers
  - ⇨ Fehlerüberwachung und -behebung

LEITUNGSVERMITTLUNG VS. PAKETVERMITTLUNG

Zwei grundsätzlich unterschiedliche Ansätze für die Vermittlung in Netzwerken:

- **Leitungsvermittlung**: Herstellen einer **Verbindung** („Leitung“) für die Dauer der Übertragung
  - ⇨ An so genannten Vermittlungszentralen werden die Leitungen zusammengeschaltet
  - ⇨ Beispiel: Klassische Telefonvermittlung (analog, ISDN, digitales ATM-Netzwerk der Telekoms)
- **Paketvermittlung**: **verbindungslose** Übertragung von Datenpaketen
  - ⇨ An jeder „Kreuzung“ des Netzwerks steht ein Router, der die Pakete in die richtige Richtung weiterleitet
  - ⇨ Beispiel: Internet

LEITUNGSVERMITTLUNG (CIRCUIT SWITCHING)

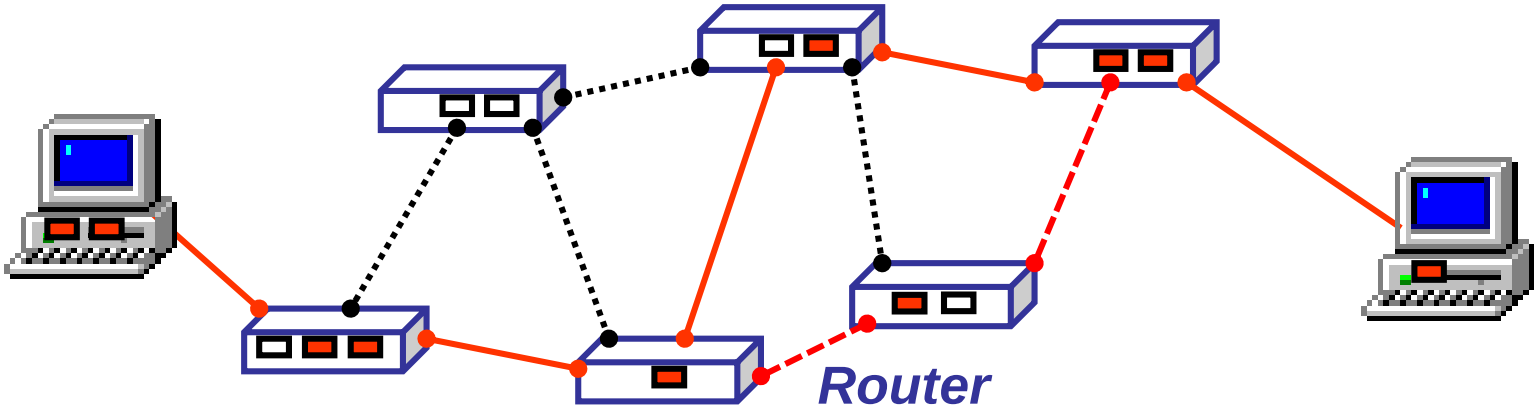


- angewendet in der klassischen Telefonie (Analog und ISDN)
- Leitungen verbinden Telefone mit Vermittlungszentralen und Vermittlungszentralen untereinander.
- Verbindungsorientiert: Vor der Kommunikation muss ein Ende-zu-Ende-Pfad aus miteinander verbundenen Leitungen eingerichtet werden. Danach wird der Pfad wieder abgebaut.
- In der Praxis ist alles etwas komplizierter, da Leitungen auch gemultiplext werden können.

ERFORDERNISSE BEI DER ÜBERTRAGUNG DIGITALER DATEN

- Leitungsvermittlung und verbindungsorientierte Vermittlung sind sehr stark verknüpft mit der Übertragung analoger Signale (Sprache) in der Telefonie
- Bei der Übertragung digitaler Daten ergeben sich neue Notwendigkeiten
- Daten müssen meist nicht ununterbrochen übertragen werden. Dadurch ergeben sich Pausen. Diese Pausen können für andere Übertragungen genutzt werden.
- Konsequenz: Daten werden in „Paketen“ portioniert versandt.
- Wenn gerade keine Leitung frei ist, können Datenpakete zwischengespeichert und verzögert versandt werden.
- Prinzip der „Paketvermittlung“

PAKETVERMITTLUNG (PACKET SWITCHING)



- Es wird für die Dauer der Kommunikation keine Verbindung hergestellt.
- Nachrichten werden in einzelne Datenpakete zerlegt (erfordert Digitalisierung)
- Statt Vermittlungszentralen werden sogenannte Router genutzt. Datenpakete werden in den Routern zwischengespeichert und weitergeleitet, sobald eine Leitung in Richtung des Ziels frei ist („store and forward“).

VERGLEICH VON LEITUNGS- UND PAKETVERMITTELTEN NETZEN

HOCHSCHULE DER MEDIEN

Merkmal	Leitungs-vermittlung	Paket-vermittlung
Durchgehender „Kupferpfad“	Ja	Nein
Verfügbare Bandbreite bzw. Datenrate	Fest	Dynamisch
Übertragungsverzögerung (Latenz)	Begrenzt	Unbegrenzt
Potenzielle Verschwendung von Bandbreite bzw. Datenrate	Ja	Nein
Übertragung mit Zwischenspeicherung	Nein	Ja
Durchgängig selbe Route benutzt	Ja	Nein
Verbindungsaufbau notwendig	Ja	Nein
Punkt möglicher Überlastungen	Beim Verbin-dungsaufbau	Bei jedem Paket
Gebührenberechnung	Pro Minute	Pro Paket

(nach Tanenbaum 2007, Abb. 2.36)

ROUTING UND ROUTER

- **Routing**: Weitervermitteln von Daten in einem Netz auf der möglichst günstigsten Route auf eine möglichst günstige Weise. Hierzu gibt es sog. **Routingalgorithmen**.
- Das Routing wird im Wesentlichen von sogenannten **Routern** übernommen, speziellen Vermittlungscomputern, auf denen die Routingalgorithmen implementiert sind und die über eine Datenbasis verschiedener Übertragungsrouten verfügen.
- Ein normaler Computer, der eine Daten über eine ihm unbekannte Route übertragen muss, schickt diese einfach an den nächstgelegenen Router.

VERBINDUNGSORIENTIERUNG AUF EBENE 3: ARGUMENTE DAFÜR

Zur Frage der Verbindungsorientierung der Vermittlungsschicht gibt es zwei gegensätzliche Lager:

Die **Netzbetreiber** (z.B. Telekoms) sind dafür:

- Vor jeder Übertragung muss eine Verbindung hergestellt werden (siehe Telefonsystem). Diese Verbindung erhält eine spezielle Kennung und wird so lange benutzt, bis die Verbindung abgebaut wird.
- Dienstgütekriterien wie Datenrate, Übertragungsverzögerung (Latenz), Fehlerüberwachung und Flusssteuerung sind beim Verbindungsaufbau verhandelbar.

VERBINDUNGSORIENTIERUNG AUF EBENE 3: ARGUMENTE DAGEGEN

Zur Frage der Verbindungsorientierung der Vermittlungsschicht gibt es zwei gegensätzliche Lager:

Das „**Internet-Lager**“ ist dagegen:

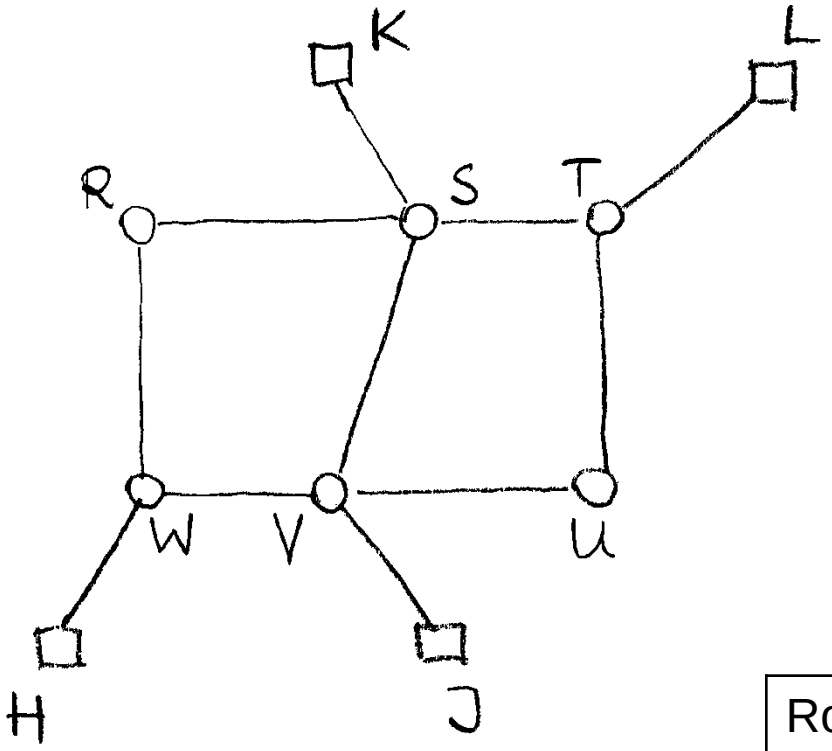
- Das Subnetz ist prinzipiell unzuverlässig.
- Die Vermittlungsschicht hat genug zu tun, um die Subnetze zu integrieren. Fehlerüberwachung und Flusssteuerung sind Aufgabe der Transportschicht.
- Daher: **verbindungslose Dienste** auf der Vermittlungsschicht. Versenden einzelner Datenpakete, die alle mit der vollständigen Empfängeradresse „beschriftet“ sind.

VERBINDUNGSLOSE VERMITTLUNGSDIENSTE

Verbindungslose Vermittlungsdienste lassen sich mit Datengrammen („Daten-Telegrammen“) realisieren:

- Verbindungslose Vermittlungsdienste übertragen die Daten in Form voneinander unabhängiger Datengramme.
- Routen werden nicht im voraus festgelegt, nachfolgende Pakete können auch andere Routen nehmen
- Jedes Datengramm muss die volle Zieladresse enthalten (z.B. ein Dutzend Byte oder mehr)
- Nachteil: Volle Zieladressierung bei kleinen Datenpaketen großer Overhead (Mehr „Aufschrift“ als Inhalt)
- Vorteil: Verfahren sehr robust. Falls ein Router ausfällt, wird andere Route gewählt.
- Vorteil: Schnell, vor allem bei kleinen Datenmengen, da auf Verbindungsauf- und abbau verzichtet wird.
- Beispiel: Internet-Vermittlungsdienst IP (Internet Protocol)

VERBINDUNGSLOSE VERMITTLUNG: IMPLEMENTATION



Router: R, S, T, U, V, W

Hosts: H, J, K, L

Routing-Tabelle von H	
Ziel	Route
H	-
*	W

Routing-Tabelle von V	
Ziel	Route
H	W
J	J
K	S
L	S
R	W
S	S
T	S
U	U
W	W
V	-

DAS INTERNET

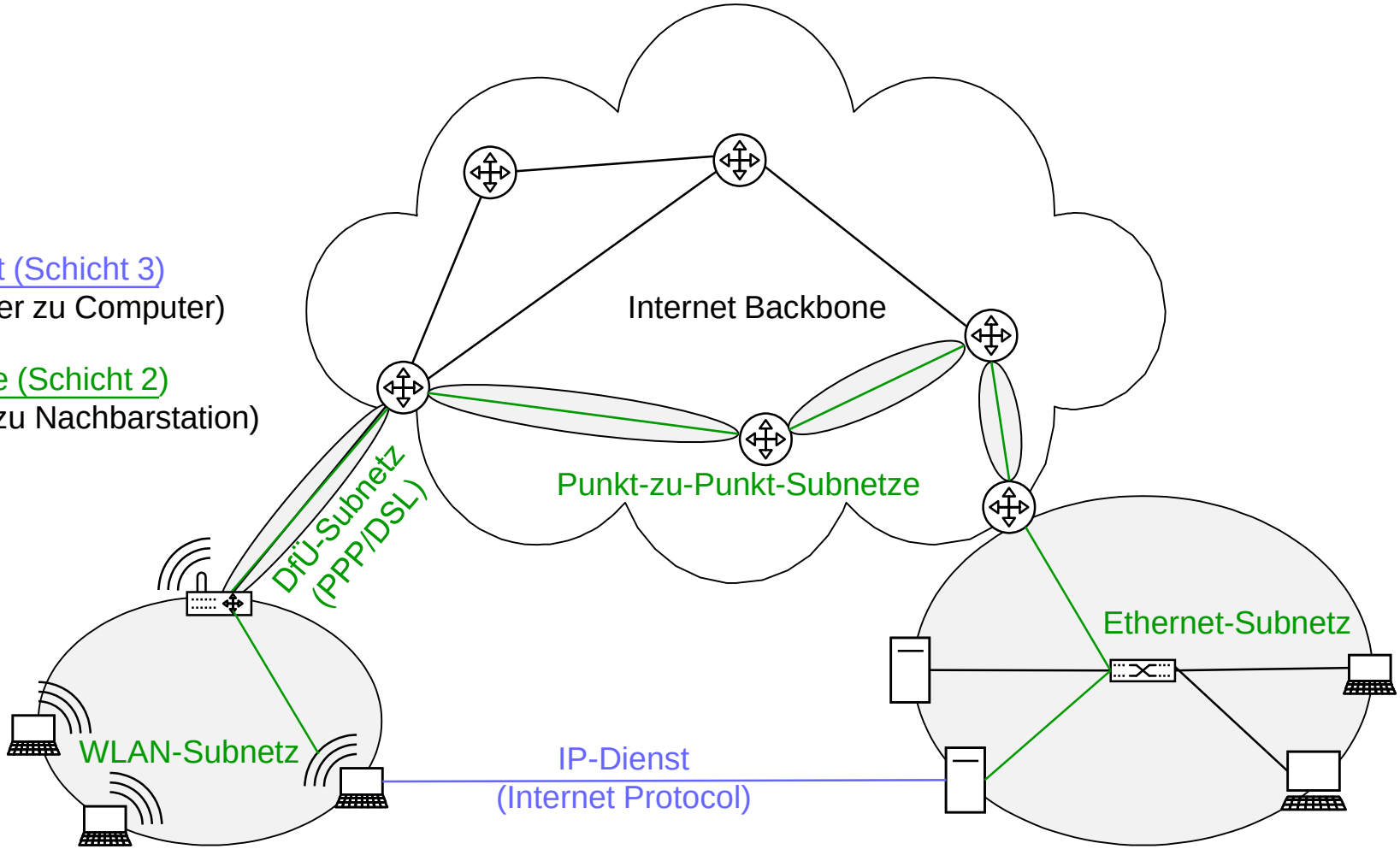
- Das Internet ist ein Verbundnetz, das unterschiedliche „Subnetze“ verbindet, z.B.:
  - ⇨ DFÜ-Netz (d.h. Datenfernübertragungsnetz): dient u.a. zur Verbindung von Internet-Benutzern und Internet-Providern über Telephonleitungen.
  - ⇨ Backbone-Netze: Netz aus schnellen Übertragungsstrecken zwischen sogenannten Routern
  - ⇨ Lokale Netze: z.B. vom Typ Ethernet oder WLAN
- Jede Art von Subnetz hat eigene Vorgaben für die Gestaltung von Bitübertragungsschicht und Sicherungsschicht. Das Internet schränkt diese nicht ein.
- Die Protokolle der Schichten 3-5 im Internet sind jedoch genormt und funktionieren global einheitlich, unabhängig vom zugrundeliegenden Subnetz.

DAS INTERNET ALS VERBUNDNETZ HETEROGENER SUBNETZE

HOCHSCHULE DER MEDIEN

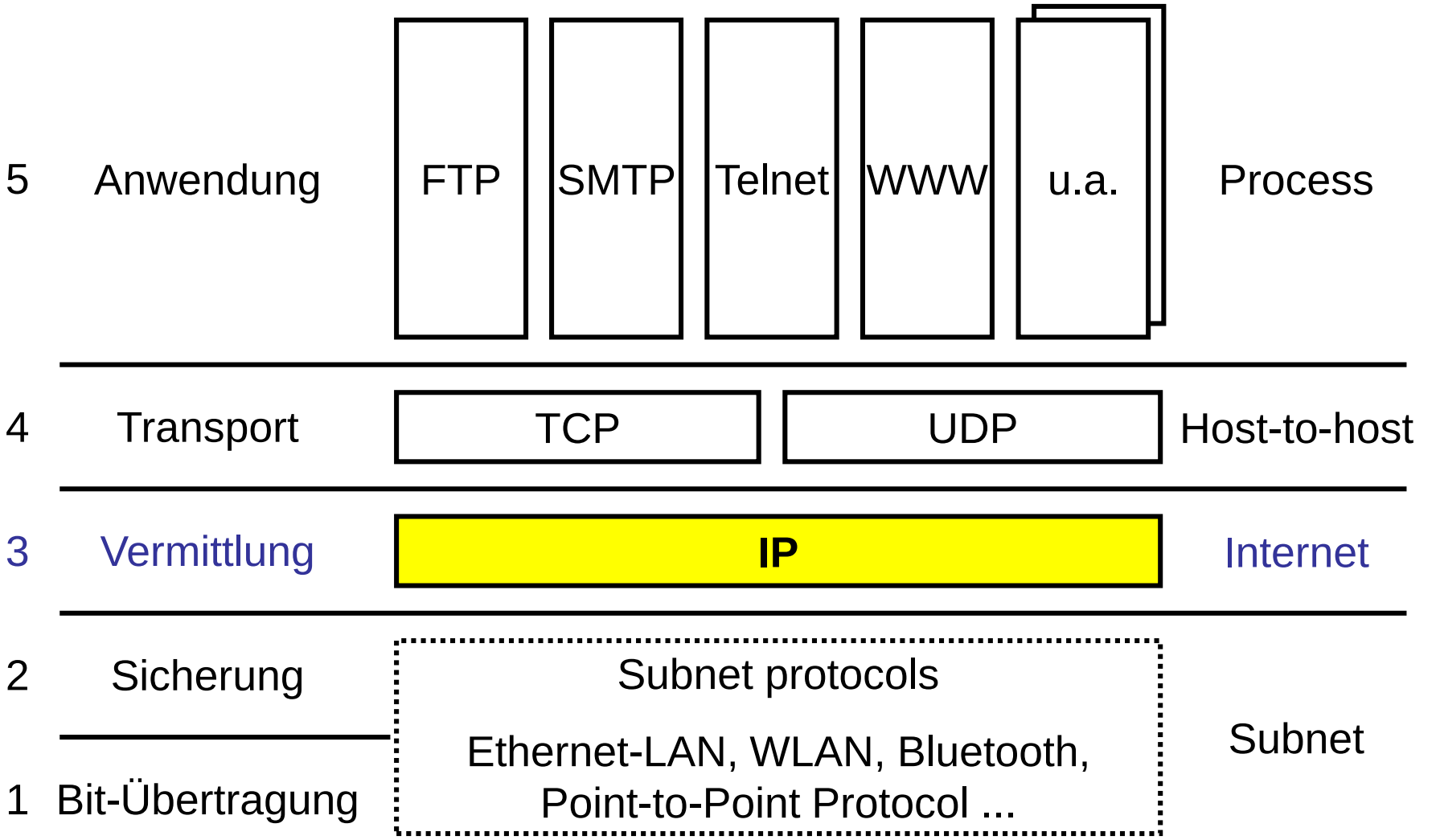
IP-Dienst (Schicht 3)
(Computer zu Computer)

Subnetze (Schicht 2)
(Station zu Nachbarstation)



IP (INTERNET PROTOCOL): DIE BASIS DES „TCP/IP-STACKS“

HOCHSCHULE DER MEDIEN



IP: EIN VERBINDUNGSLOSER VERMITTLUNGSDIENST

- IP (Internet-Protocol) ist der Vermittlungsdienst des Internet
- IP ist verbindungslos, versandt werden Datengramme, auch Pakete genannt.
- Es wird über IP-Adresse ein Rechner in einem Netzwerk („Subnet“) adressiert.
- Zuverlässigkeit nicht garantiert („Best Effort“). Zuverlässigkeit ist die Aufgabe von Diensten höherer Schichten (TCP)
- Unterhalb von IP sind beliebige (auch relativ unzuverlässige Subnetze möglich)
- Oberhalb von IP auf Schicht 4 existieren 2 Transportdienste
  - ⇨ TCP: verbindungsorientierter Transportdienst
  - ⇨ UDP: verbindungsloser Transportdienst
- Vielfalt von Anwendungsdiensten auf Schicht 5

DER IP-HEADER: DER KOPFTEIL VON IP-DATENGRAMMEN (PAKETEN)

HOCHSCHULE DER MEDIEN

IP-Datengramme (Pakete) bestehen aus Kopfteil (Header) und Textteil. Wichtige Datenelemente des Headers sind:

Version: z.Zt.=4, Im künftigen IPV6 = 6

Total Length: Länge von Header+Text

Source Address: IP-Adresse des Senders

Destination Address: IP-Adresse des Empfängers

Time to Live: Ein Zähler, der bei jeder Teilstrecke, d.h. bei jedem Router heruntergezählt wird, dient zur Begrenzung der „Lebensdauer“ eines Pakets

Protocol: Bezeichnung des Transportprozesses, i.d.R. TCP oder UDP

ADDRESSIERUNG IM INTERNET

Die Adressierung im Internet erfolgt über Internet-Adressen (auch „IP-Adressen“ genannt)

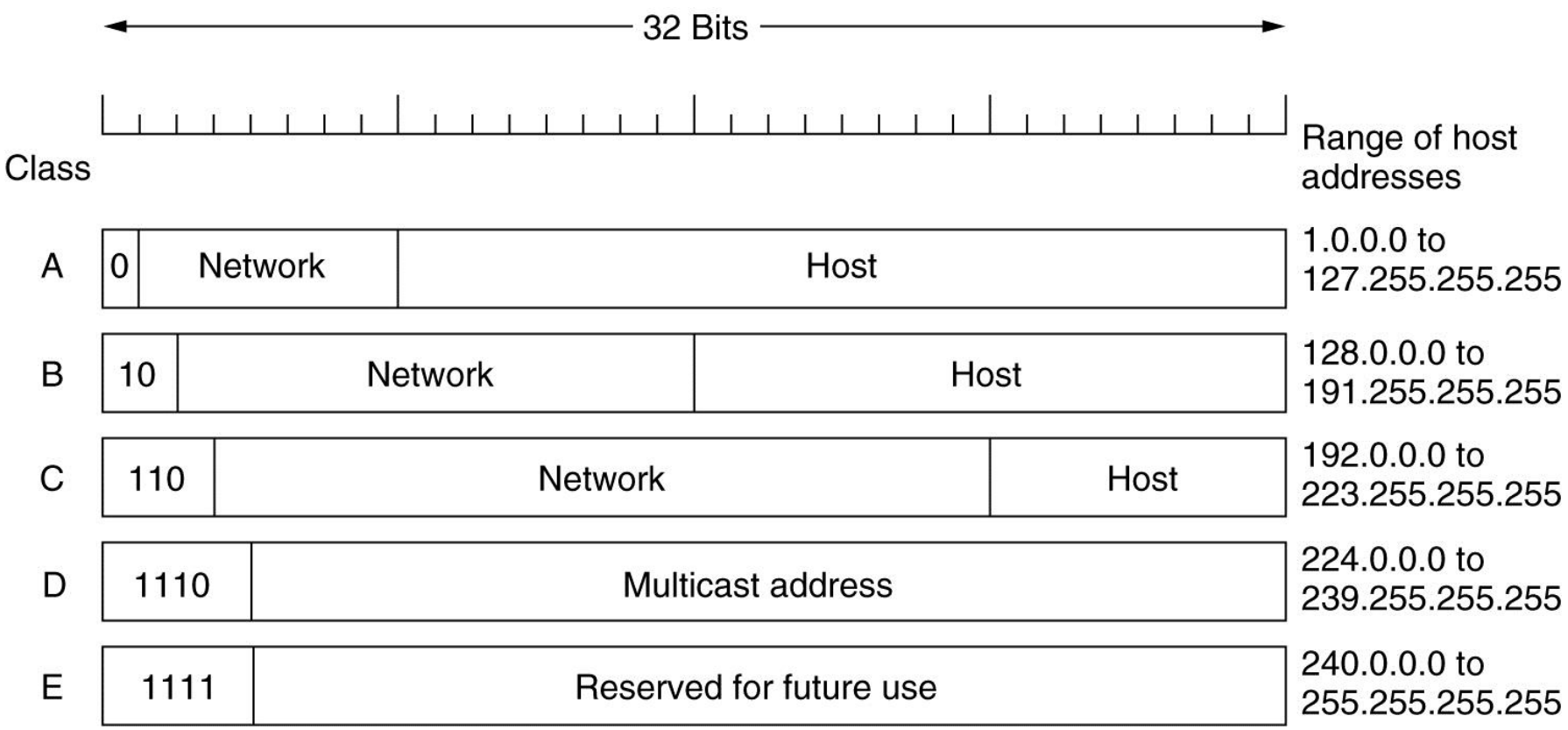
- IP-Adressen bestehen aus vier durch Punkte getrennten Zahlengruppen, z.B. 193.196.176.30
- In der derzeit gebräuchlichen Internet-Version IPv4 ist jede Zahlengruppe durch 8 Bit dargestellt und kann die Werte 0 bis 255 annehmen. Dadurch sind 2^{32} = rund 4 Milliarden Internetadressen möglich.
- In der künftigen Internet-Version IPv6 werden 16 Bit (statt 8) für 8 (statt 4) Zahlengruppen verwendet, die hexadezimal notiert werden. Beispiel für eine IPv6-Adresse: 2001:0db8:85a3:08d3:1319:8a2e:0370:7344. Dadurch sind künftig 2^{128} = ca. $3{,}4*10^{38}$ unterschiedliche Internetadressen möglich.

LOGISCHER AUFBAU VON IP-ADRESSEN

- IP-Adressen sind aufgeteilt in Network ID und Host ID
- In IPV4 gab es ursprünglich nur drei Arten (Klassen) von Aufteilungen:
  - ⇨ Class A: 7 Bit Network ID, 24 Bit Host ID
  - ⇨ Class B: 14 Bit Network ID, 16 Bit Host ID
  - ⇨ Class C: 21 Bit Network ID, 8 bit Host ID
- An den führenden Bits der Adresse erkennt man, zu welcher Klasse sie gehört.
- Um den Adressraum besser auszunutzen, verwendet man in IPV4 heute klassenlose Adressformate.
  - ⇨ Hier erfolgt die Aufteilung in Subnet ID und Host ID mit Hilfe einer so genannten Subnet-Maske

KLASSEN VON IP-ADRESSFORMATEN

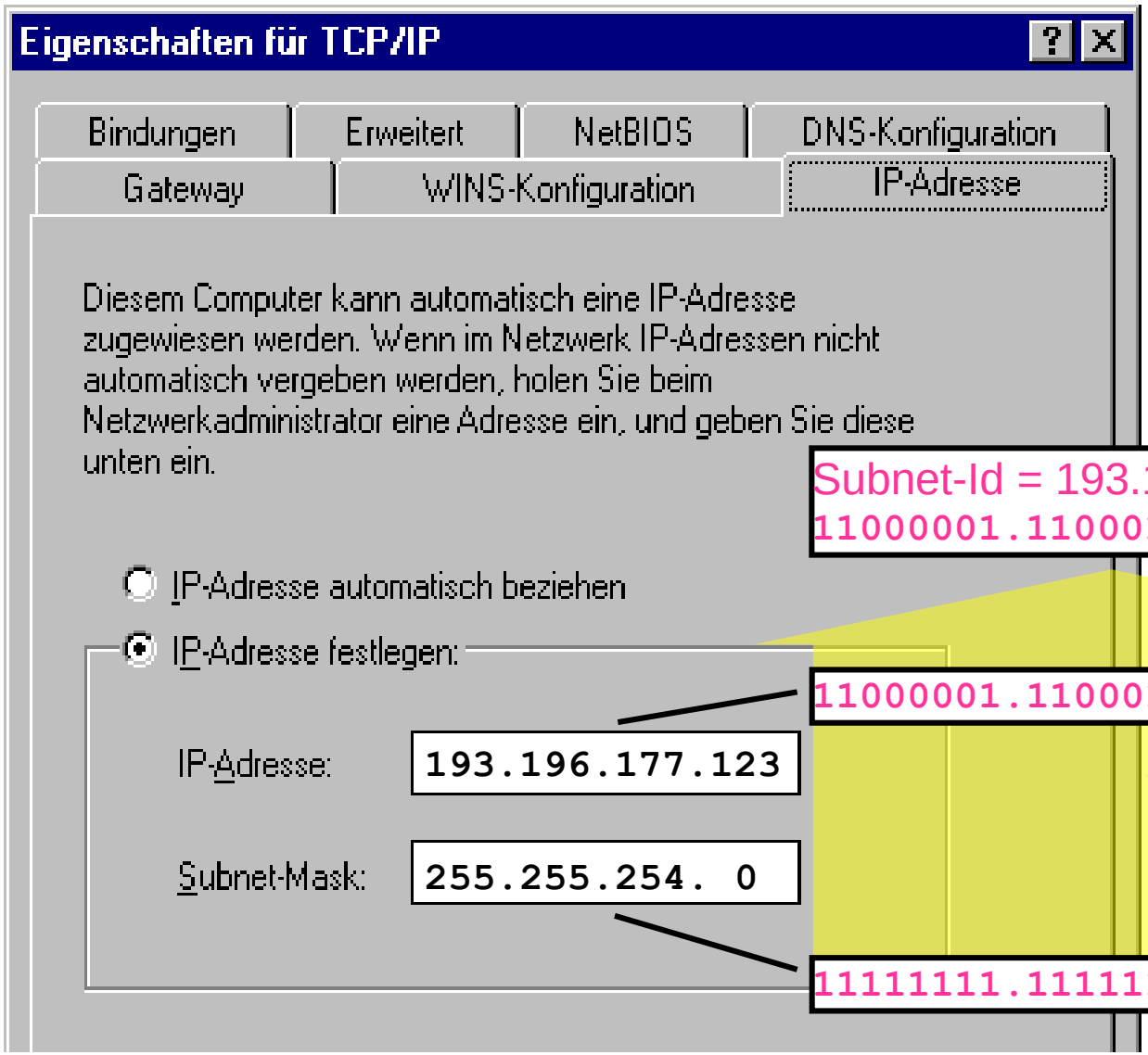
HOCHSCHULE DER MEDIEN



Quelle: Tanenbaum

KLASSENLOSE ADRESSFORMATE
AUFTEILUNG MIT SUBNETZMASKE

HOCHSCHULE DER MEDIEN



Host-Id = 379
= 1.01111011

Subnet-Id = 193.196.176.0 =
11000001.11000100.10110000.00000000

11000001.11000100.10110001.01111011

Network *Host*

11111111.11111111.11111110.00000000

PRIVATE IP-VERGABE

Folgende IP-Adressblöcke sind für private Zwecke reserviert:

Adressbereich:	Subnet-Id:	Subnet-Maske:
10.0.0.0 - 10.255.255.255	10.0.0.0	255.0.0.0
172.16.0.0 - 172.31.255.255	172.16.0.0 8	255.240.0.0
192.168.0.0 - 192.168.255.255	192.168.0.0	255.255.0.0

Diese Adressen können für ein privates Netz innerhalb einer Firma verwendet werden, außerhalb sind diese nicht sichtbar.

Automatische private IP-Adressen-Vergabe:

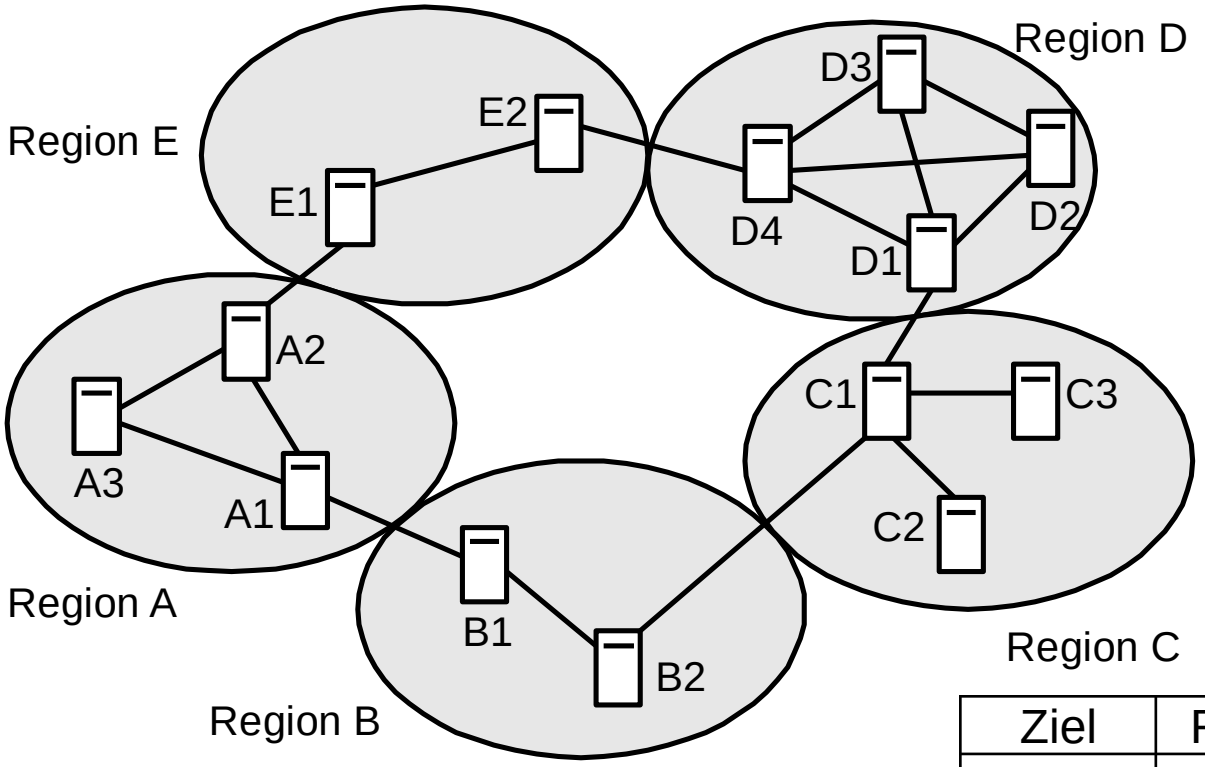
Adressbereich:	Subnet-Id:	Subnet-Maske:
169.254.0.0 - 169.254.255.255	169.254.0.0	255.255.0.0

Falls automatische Adressvergabe gewählt ist und kein spezielles Protokoll (wie z.B. PPP oder DHCP) zur automatischen Vergabe von IP-Adressen aktiv ist, wählt sich der Computer zufallsgesteuert eine dieser Adressen

HIERARCHISCHES ROUTING

- Wenn in Routing-Tabellen alle Zielstationen (Hosts, Router) aufgeführt sind, werden die Tabellen sehr groß
- Abhilfe: Hierarchisches Routing
  - ⇨ Nahe beieinander liegende Stationen werden in „Regionen“ zusammengefasst.
  - ⇨ In den Routing-Tabellen stehen im Wesentlichen nur noch diese Regionen und die zugehörigen Routen.
  - ⇨ Nur sehr nahe Stationen, z.B. die aus der eigenen Region, werden noch einzeln in den Routing-Tabellen geführt.
  - ⇨ Dadurch werden die Routing-Tabellen kleiner und leichter handhabbar.
- Anwendung im Internet: Als Regionen werden Subnetze verwendet (definiert über Subnet-ID und Subnet-Mask).

HIERARCHISCHES ROUTING: BEISPIEL



Ziel	Route
A1	-
A2	A2
A3	A3
B1	B1
B2	B1
C1	B1
C2	B1
C3	B1
D1	B1
D2	B1
D3	A2
D4	A2
E1	A2
E2	A2

Routing-Tabellen für Station A1

Normales Routing

Hierarchisches Routing

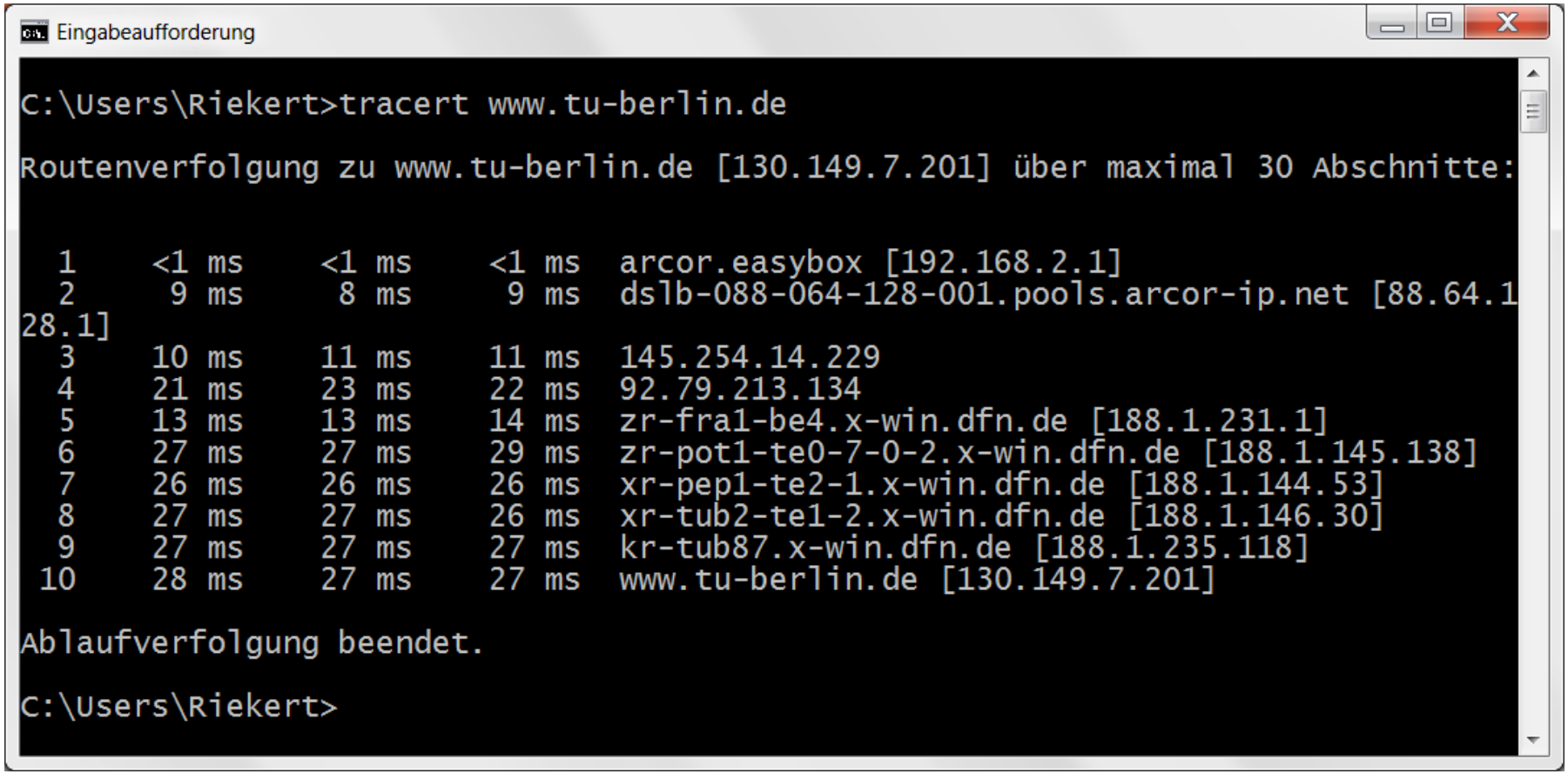
Ziel	Route
A1	-
A2	A2
A3	A3
B	B1
C	B1
D	A2
E	A2

HIERARCHISCHES ROUTING IM INTERNET ÜBER DIE SUBNET-ID

- IP-Adressen bestehen aus zwei Teilen, der Subnet-Id (identifiziert das Subnetz) und der Host-Id (identifiziert den Computer im Subnetz).
- Mit Hilfe der Subnet-Mask, die für jedes Subnetz festgelegt ist, lässt sich die Host-Id von der Subnet-Id trennen.
- Jeder Router hat Tabellen, die die Menge aller IP-Adressen in verschiedene, u.U. auch sehr große Subnetze zerlegen (dargestellt durch Subnet-Id und Subnet-Mask).
- Diese Tabellen beschreiben, welche Subnetze der Router über eine Netzwerkkarte direkt erreicht und welche nur über einen benachbarten Router erreicht werden.
- Auf diese Weise kann ein Router stets entscheiden,
  - ⇨ ob er ein IP-Paket selbst direkt zustellen kann
  - ⇨ oder ob er es an den nächsten zuständigen Router weiterleiten muss und welcher Router das ist.

IP-ROUTEN ANZEIGEN MITTELS TRACERT

HOCHSCHULE DER MEDIEN



Das Kommando tracert („*Trace Route*“) macht die Route eines mit IP versandten Datenpakets sichtbar. Aufruf über Eingabeaufforderung ([Start] – Ausführen… – cmd – OK.)

ARTEN VON ADRESSEN IN EINEM LAN MIT INTERNET-PROTOKOLLEN

HOCHSCHULE DER MEDIEN

- **MAC-Adresse** oder **Physikalische Adresse** (meist eine Ethernet-Adresse), z.B.: 00-A0-24-DF-F6-98, verwendet in MAC-Teilschicht der Sicherungsschicht (Nr. 2). Liegt bereits hardwaremäßig in der Netzwerkkarte fest. Nicht routingfähig, erreicht nur Computer im lokalen Netz
- **Internet-Adresse** (IP-Adresse), z.B.: 193.196.176.114 verwendet in Vermittlungsschicht (Ebene Nr. 3) des Internet, muss nach Absprache mit dem Netzwerkadministrator oder Internetprovider eingestellt werden
- **Domain-Name**, z.B.: mars.iuk.hdm-stuttgart.de verwendet in Transport- und Anwendungsschicht (Ebenen Nr. 4 und 5) des Internet, kann nach Absprache mit dem Netzwerkadministrator oder Internetprovider vergeben werden. Domain-Namen werden durch sog. Domain-Name-Server in IP-Adressen umgewandelt.

MANUELLE KONFIGURATION DES INTERNETZUGANGS

Um einen Computer (z.B. Server) in einem lokalen Netz manuell für die Nutzung des Internets einzurichten, müssen verschiedene Einstellungen vorgenommen werden:

- Festlegung der **eigenen IP-Adresse** und der **Subnet-Mask** des lokalen Netzes (erhältlich vom Netzwerkadministrator bzw. Internetprovider),
- Festlegung der IP-Adresse eines **Gateways**, d.h. des Routers, der den Zugang zum Rest des Internets herstellt und alle IP-Pakete erhält, die nicht im LAN bleiben sollen.
- Einrichtung des Domain Name Systems (DNS):
  - ⇨ Festlegung des **eigenen Domain-Namens** (in Absprache mit Netzwerkadministrator/Internetprovider)
  - ⇨ Festlegung der IP-Adresse des **Domain Name Servers**

AUTOMATISCHE KONFIGURATION DES INTERNETZUGANGS

Möglichkeiten der automatischen Bestimmung von Internetkonfigurationsdaten (z.B. für Client-Computer):

- Das PPP-Protokoll (verwendet in Einwahlverbindungen über Telefon oder DSL) kann Konfigurationsdaten (siehe vorige Folie) übertragen
- Das DHCP-Protokoll (verwendet in Broadcastnetzen). Ein DHCP-Server überträgt Konfigurationsdaten
- Automatische Selbstkonfiguration: Der Computer wählt selbständig eine zufällig generierte IP-Adresse im Bereich 169.254.0.0 - 169.254.255.255. Resultat: „Eingeschränkte Konnektivität“, d.h. meist können so konfigurierte Systeme nur untereinander kommunizieren, ein Internetzugang ist i.d.R. nicht möglich.

IPV6 (INTERNET PROTOCOL VERSION 6)

Neue Features:

- 128-Bit-Adressen: Ausreichende Zahl von IP-Adressen
  - ⇨ 64 Bit Prefix: identifiziert Subnetz, z.B. Heimnetz
    - Kann dauerhaft vergeben werden
    - aber: Privatsphäre! Deshalb wechselnde Prefixes möglich
  - ⇨ 64 Bit Interface-Identifier: Identifiziert Station im Subnetz
    - Kann aus MAC-Adresse abgeleitet werden, DHCP überflüssig
    - aber: Privatsphäre! Abhilfe: Privacy Extensions)
- Mobiles IP
  - ⇨ insbesondere keine wechselnden IP-Adressen für Mobilgeräte
- IPsec (Verschlüsselung und Authentizität für IP)
- Unterstützung von Quality of Service

BESTIMMUNG VON MAC-ADRESSEN AUS DER IP-ADRESSE

Für die Kommunikation mit anderen Hosts oder dem Gateway in einem LAN muss die IP-Schicht IP-Adressen in Adressen der Sicherungsschicht (MAC-Adressen) konvertieren, das sind meist Ethernet-Adressen (48-Bit lang, weltweit eindeutig):

Mögliche Lösungen:

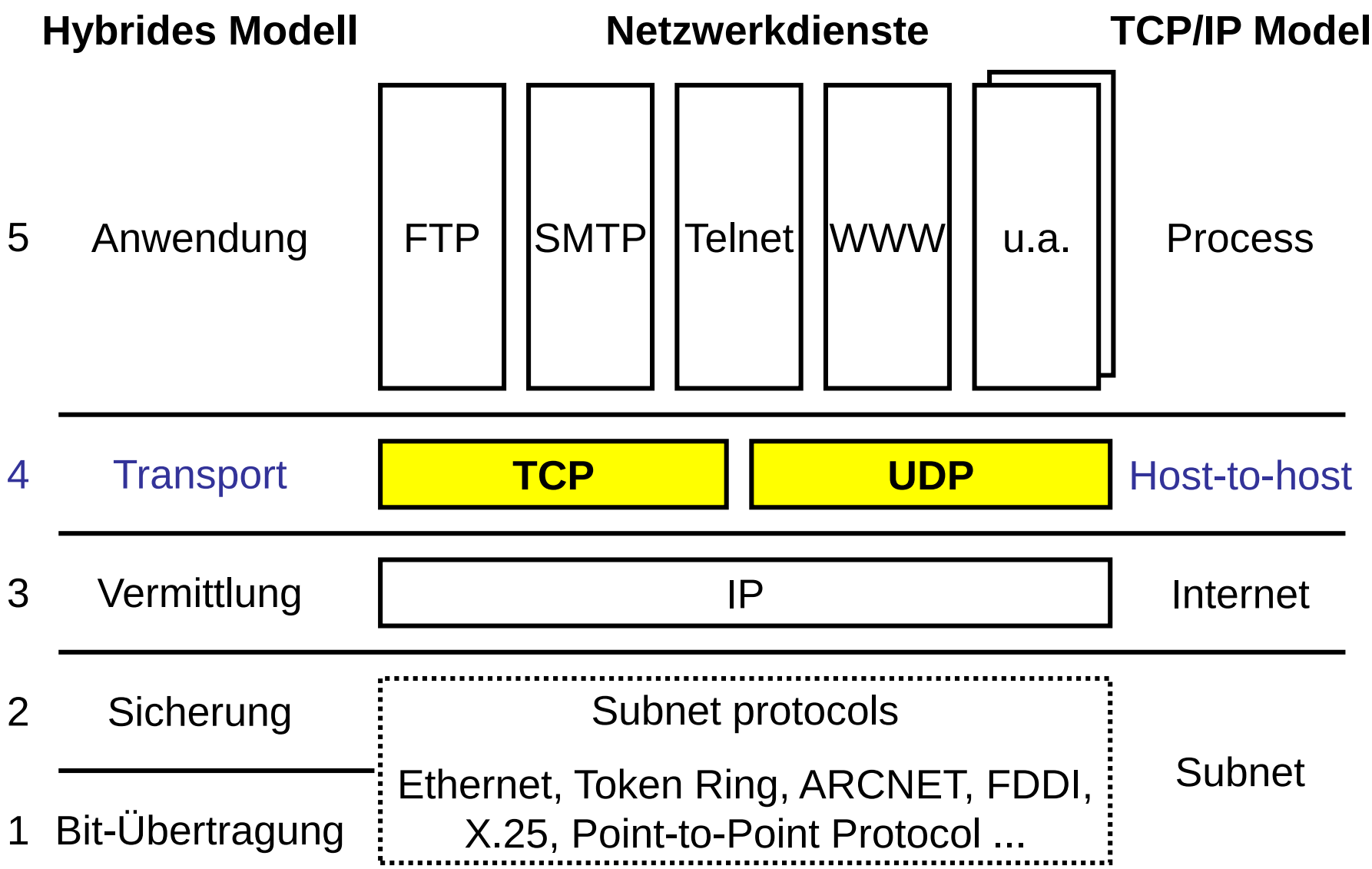
- Tabellen mit Zuordnung IP-Adresse - MAC-Adresse auf jeder Maschine
  - ⇨ pflegeaufwendig, fehleranfällig
- Vor dem Senden einer Nachricht zuerst ein Broadcast (Rundruf): „Wem gehört diese Internet-Adresse“ und lokales Abspeichern der Antwort (mit Verfallsdatum)
  - ⇨ Dies wird so realisiert im **ARP (Address Resolution Protocol)**

TEIL 4: TRANSPORTSCHICHT (TRANSPORT LAYER)

- Echte Ende-zu-Ende-Schicht: ermöglicht die Kommunikation zwischen zwei Prozessen auf unterschiedlichen Rechnern
- Verschiedene Arten von Transportdiensten möglich, z.B. verbindungsorientierter Transport (z.B. TCP) oder verbindungsloser Transport über Datengramme (z.B. UDP) oder als Broadcast an viele Empfänger
- Benennungsmechanismus für die Endpunkte einer Kommunikationsbeziehung zwischen zwei Prozessen
- Ggf. Zerlegung der Nachrichten in kleinere Einheiten und Zusammensetzen in richtiger Reihenfolge beim Empfänger
- Multiplexen von Kanälen der Vermittlungsschicht, damit mehrere Prozesse über dieselbe Übertragungsroute quasi gleichzeitig kommunizieren können
- Flusssteuerung zur Geschwindigkeitsanpassung

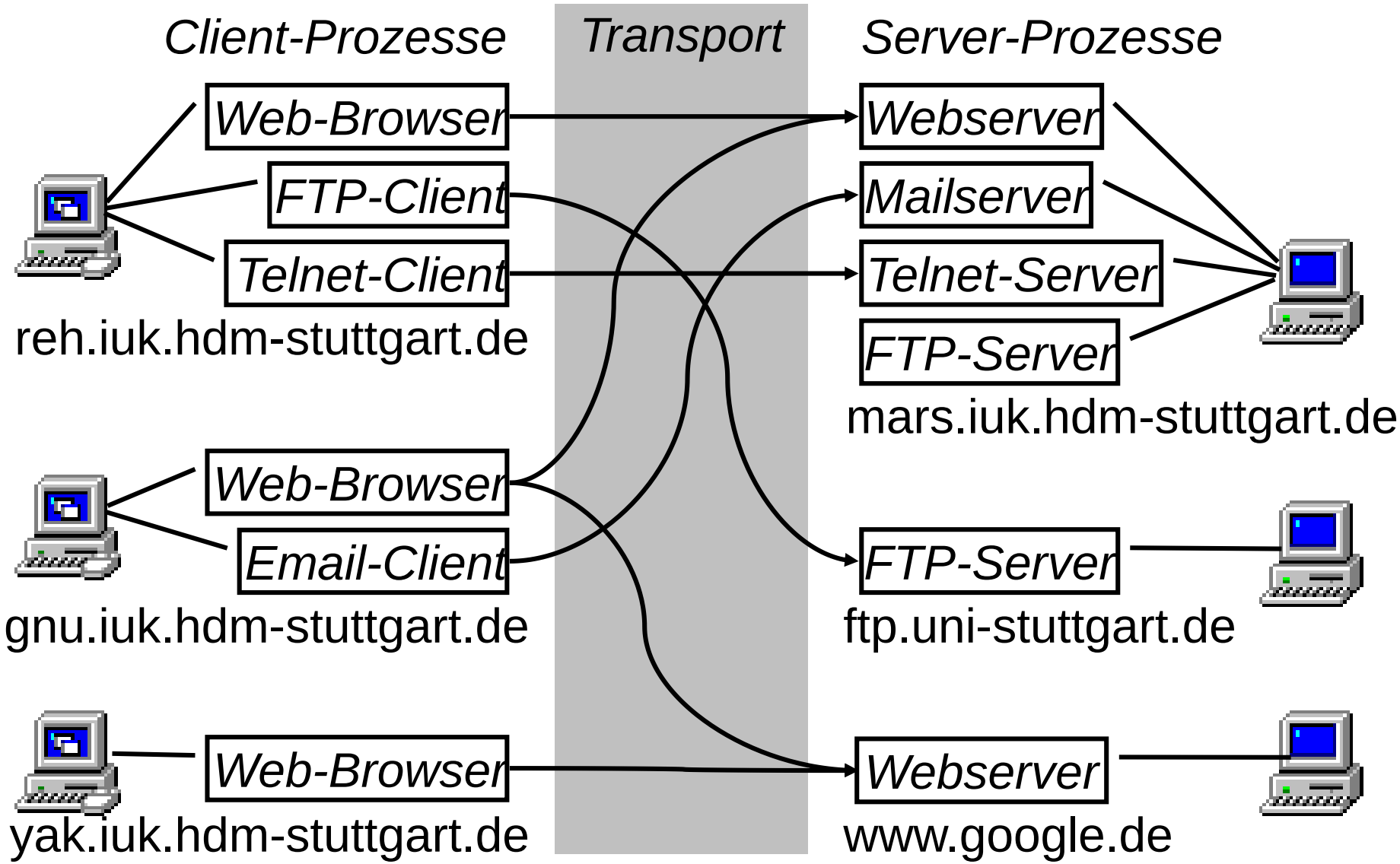
INTERNET-TRANSPORTDIENSTE: TCP UND UDP

HOCHSCHULE DER MEDIEN



TRANSPORTSCHICHT: KOMMUNIKATION ZWISCHEN PROZESSEN

HOCHSCHULE DER MEDIEN

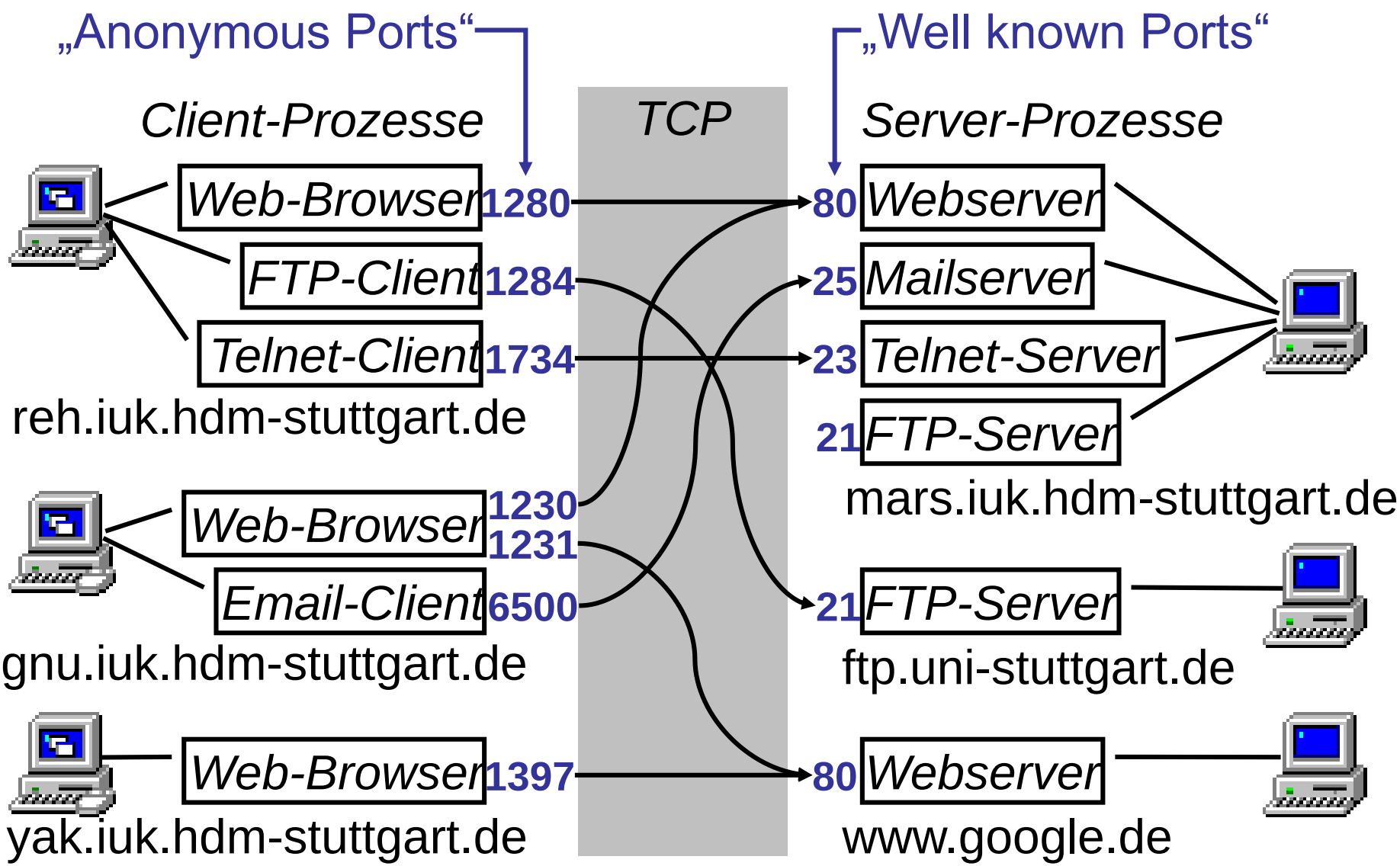


TRANSMISSION CONTROL PROTOCOL (TCP)

- Internet-Dienst der Transportschicht
- Verbindungsorientiert (Phasen Verbindungsaufbau, Datenübertragung, Verbindungsabbau)
- Verlässlicher Verbindungsaufbau, geregelter Verbindungsabbau
- Zuverlässigkeit: verlustfreie, fehlerfreie Datenübertragung; richtige Reihenfolge der Nachrichten
- Zerlegung der Nachrichten in kleinere Einheiten und Zusammensetzen in richtiger Reihenfolge beim Empfänger
- Vollduplex: Beide Seiten können jederzeit senden und empfangen
- Datenstromartige Schnittstelle, Nachrichtengrenzen bleiben nicht erhalten

PORTS ALS SERVICE ACCESS POINTS FÜR DEN TCP-DIENST

HOCHSCHULE DER MEDIEN



PORTS ALS ENDPUNKTE VON TCP-VERBINDUNGEN

- Ports bilden die **Endpunkte** (Service Access Points) von TCP-Verbindungen. Intern sind die Ports Tabelleneinträge, in denen die TCP-Software über die vorhandenen Verbindungen Buch führt.
- Ports werden mit **Nummern** bezeichnet. Diese Nummern sind innerhalb eines Computers eindeutig.
- An bestimmten, per Konvention bekannten Ports (*well-known ports*, Portnummer in der Regel kleiner als 1024) warten **Serverprozesse**, bis ein Clientprozess mit ihnen Verbindung aufnimmt.
- **Clientprozesse** benutzen untereinander unterschiedliche, ansonsten weitgehend beliebige Ports (*anonymous ports*, Portnummer i.d.R. größer als 1023), um eine Verbindung zu den Ports von Serverprozessen aufzunehmen.
- **Verbindungen** sind eindeutig definiert durch Angabe von IP-Adresse (oder Computernamen) und Portnummer auf Client- und auf Serverseite.

WELL-KNOWN PORTS

Kleine Portnummern bis ca. 1023 sind entsprechend einer Übereinkunft aller Internet-Serverbetreiber für bestimmte Serverprozesse (sog. Demons) vorgesehen. Beispiele:

Port	Transportdienst	Serverprozess	Zweck
21	TCP	FTP Demon	File Transfer
22	TCP	SSH Demon	Secure Shell
23	TCP	Telnet Demon	Virtuelles Terminal
25	TCP	SMTP Demon	Versenden von Email
37	UDP	Time Demon	Uhrzeit-Server
79	TCP	Finger Demon	Info über Benutzer
80	TCP	HTTP Demon	Webserver
139	TCP	NETBIOS	File-/Printservices

Eine vollständige Liste aller well-known Ports befindet sich auf jedem Unix- bzw. Linux-Rechner in der Datei /etc/services

BEISPIEL EINES PORTS

Portnummern sind oft sichtbar in WWW-Adressen (URLs).

Beispiel:

http://www.parlament-berlin.de:8080/

(Datum des letzten Zugriffs 16.06.2012)

Der Webserver auf dem Computer mit dem Domainname www.parlament-berlin.de akzeptiert Verbindungen auf dem Port 8080.

Normalerweise verwenden Webserver den Port mit der Nummer 80. Deshalb dient die 80 als Voreinstellung („Default“), wenn in der URL keine Portnummer angegeben ist.

USER DATAGRAM PROTOCOL (UDP)

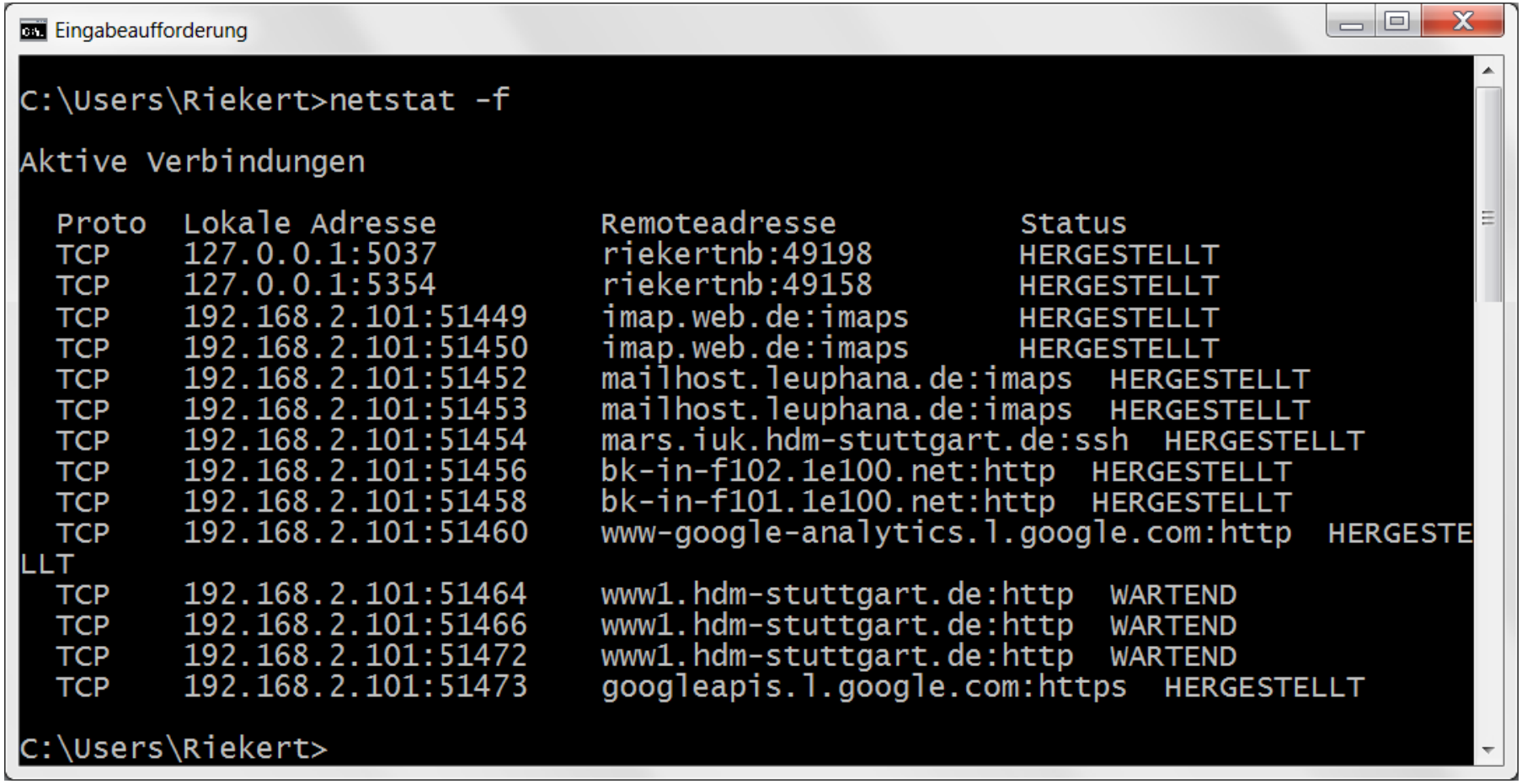
- ein Internet-Dienst der Transportschicht (Host-to-host), ebenso wie TCP
- Verbindungsloser Dienst
- Schnittstellen zu UDP sind ähnlich gestaltet wie die zu TCP, zur Adressierung werden ebenfalls Ports verwendet
- UDP-Ports unterscheiden sich von TCP-Ports; ein UDP-Port kann dieselbe Nummer haben wie ein TCP-Port,ohne dass die beiden Ports etwas miteinander zu tun haben
- Es werden Datengramme übertragen
- Nachrichtengrenzen bleiben erhalten
- Erhaltung der Reihenfolge der Datengramme nicht garantiert
- Zuverlässigkeit nicht garantiert („Best Effort“)
- Schneller als TCP

ÜBUNG ZU TCP

- Öffnen Sie verschiedene TCP-Verbindungen, indem Sie z.B. via Filezilla oder Putty SSH-Sessions mit dem Rechner mars öffnen oder indem Sie ein Mailtool oder einen Web-Browser nutzen.
- Starten Sie in der Eingabeaufforderung das Programm Netstat mit **netstat -f** bzw. **netstat -n**. Es zeigt die aktiven TCP-Verbindungen. (Die Eingabeaufforderung öffnen Sie z.B. über  [Start] – Ausführen… – **cmd** – OK.)
- Hilfe und weitere Netstat-Optionen erhalten Sie mit **netstat -h** .
- Netstat funktioniert auch unter Unix bzw. Linux.
  Loggen Sie sich mit Putty auf einem Server ein (z.B. mars.iuk.hdm-stuttgart.de) und rufen Sie dort Netstat auf.

NETSTAT-KOMMANDO AUF EINEM PC (CLIENTCOMPUTER)

HOCHSCHULE DER MEDIEN



netstat -f zeigt Remoteadresse textuell (Domain:Portname)
netstat -n zeigt Remoteadresse numerisch (IP-Adresse:Portnr.)

NETSTAT-KOMMANDO AUF EINEM SERVERCOMPUTER (Z.B. MARS)

HOCHSCHULE DER MEDIEN

```
netstat
tcp 0    0 mars.iuk.hdm-stuttgar:www host-47.subnet-74.:4831 ESTABLISHED
tcp 0    0 mars.iuk.hdm-stuttgar:www surprise.mchh.sie:62050 TIME_WAIT
tcp 0 3998 mars.iuk.hdm-stuttgar:www ABD1481A.ipt.aol.c:1294 ESTABLISHED
tcp 0    0 mars.iuk.hdm-stuttgar:www kuen103.kuen.fh-he:1832 TIME_WAIT
tcp 0 1313 mars.iuk.hdm-stuttgar:www ABD1481A.ipt.aol.c:1293 ESTABLISHED
tcp 0    0 mars.iuk.hdm-stuttga:4898 mars.iuk.hdm-stutt:domain TIME_WAIT
tcp 0    0 mars.iuk.hdm-stuttga:4897 auth02.ns.de.uu.:domain TIME_WAIT
tcp 0    0 mars.iuk.hdm-stuttgar:www bw11olt.bluewin.c:62980 TIME_WAIT
tcp 0    0 mars.iuk.hdm-stuttgar:www stu1ir7-101-170.ra:1131 TIME_WAIT
tcp 0    0 mars.iuk.hdm-stutt:telnet ripc.hbi-stuttgart:1268 ESTABLISHED
tcp 0    0 mars.iuk.hdm-stuttgar:www stu1ir7-101-170.ra:1126 FIN_WAIT2
tcp 0    1 mars.iuk.hdm-stuttga:4875 ierrs1.ier.uni-stu:smtp SYN_SENT
tcp 0    0 mars.iuk.hdm-stutt:telnet A8b2b.pppool.de:1113    ESTABLISHED
tcp 0    0 mars.iuk.hdm-stutt:telnet a02-18.dialin.msh.:1091 ESTABLISHED
tcp 0    0 mars.iuk.hdm-stutt:telnet astapc2.hbi-stuttg:2154 ESTABLISHED
tcp 0    0 mars.iuk.hdm-stuttgar:ssh steinbock.hbi-stut:1299 ESTABLISHED
tcp 0    0 mars.iuk.hdm-stuttgart:20 r-44.stuttgart.ipd:1051 ESTABLISHED
tcp 0    0 mars.iuk.hdm-stuttgar:ftp r-44.stuttgart.ipd:1044 ESTABLISHED
```

NETSTAT MIT NUMERISCHER AUSGABE AUF SERVERCOMPUTER

HOCHSCHULE DER MEDIEN

```
netstat -n
tcp 0   0 141.62.122.233:80   62.158.165.55:2068   TIME_WAIT
tcp 0   0 141.62.122.233:80   151.189.0.129:45520  TIME_WAIT
tcp 0   0 141.62.122.233:23   62.155.181.56:1117   ESTABLISHED
tcp 0   0 141.62.122.233:80   195.186.27.6:4695    TIME_WAIT
tcp 0   0 141.62.122.233:80   195.186.27.6:4694    TIME_WAIT
tcp 0   0 141.62.122.233:80   195.186.27.6:4693    TIME_WAIT
tcp 0   0 141.62.122.233:80   195.186.27.6:4692    TIME_WAIT
tcp 0   0 141.62.122.233:80   195.186.27.6:4650    TIME_WAIT
tcp 0   0 141.62.122.233:80   195.186.27.6:4643    TIME_WAIT
tcp 0   0 141.62.122.233:80   213.200.1.41:1421    TIME_WAIT
tcp 0   0 141.62.122.233:80   142.231.43.247:1615  FIN_WAIT2
tcp 0   0 141.62.122.233:80   142.231.43.247:1612  TIME_WAIT
tcp 0   0 141.62.122.233:80   142.231.43.247:1611  TIME_WAIT
tcp 0   2 141.62.122.233:23   193.196.176.114:1268 ESTABLISHED
tcp 0   1 141.62.122.233:4875 129.69.80.12:25      SYN_SENT
tcp 0   0 141.62.122.233:23   213.6.139.43:1113    ESTABLISHED
tcp 0   0 141.62.122.233:23   212.4.224.82:1091    ESTABLISHED
tcp 0   0 141.62.122.233:23   193.196.176.132:2154 ESTABLISHED
tcp 0   0 141.62.122.233:22   193.196.176.91:1299  ESTABLISHED
tcp 0   0 141.62.122.233:20   62.180.41.44:1051    ESTABLISHED
tcp 0   0 141.62.122.233:21   62.180.41.44:1044    ESTABLISHED
```

TEIL 5: ANWENDUNGSSCHICHT (APPLICATION LAYER)

- Realisiert durch Prozesse (ablaufende Programme), die miteinander über die Transportschicht kommunizieren
  - ⇨ In der Regel Unterscheidung von **Clientprozess** (Dienstanforderer) und **Serverprozess** (Diensterbringer)
  - ⇨ Beispiele: Telnet-, FTP-, Email-, WWW-Server u. Clients
- Anwendungsschicht in unserem Hybridmodell entspricht der **Anwendungsschicht** im OSI-Modell, umfasst aber zusätzlich die Aufgaben der folgenden zwei OSI-Schichten
  - ⇨ **Sitzungsschicht** (session layer): Verwaltung von sog. Sitzungen, z.B. Login Sessions oder Filetransfers
  - ⇨ **Darstellungsschicht** (presentation layer): Kodierung von Daten auf standardisierte Weise, z.B. Buchstaben, Zahlen, Geldbeträge, Rechnungen usw.

NETZWERKDIENSTE DER ANWENDUNGSSCHICHT

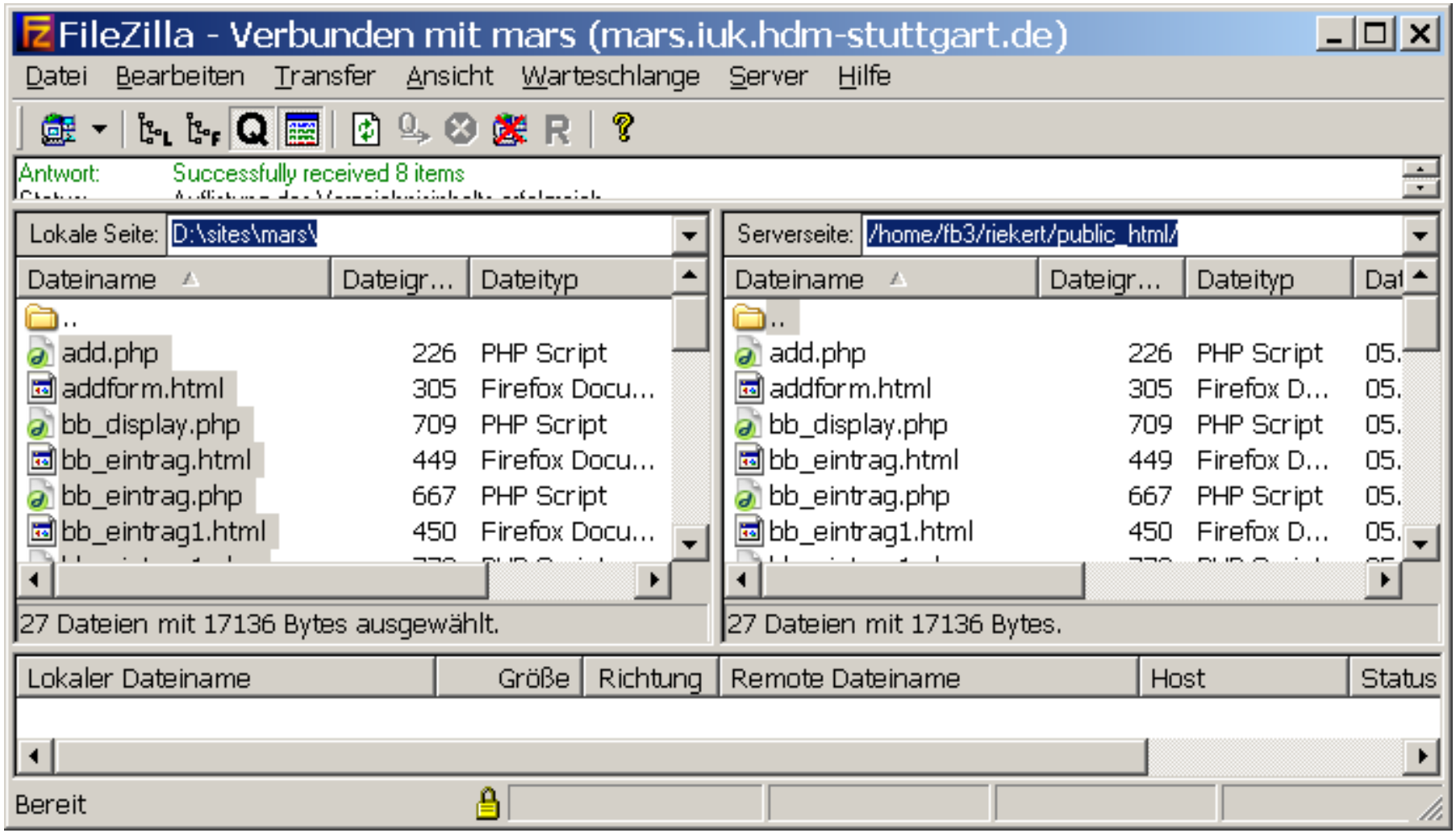
- Dateitransfer (FTP, SFTP via SSH)
- Terminalemulation (TELNET, RLOGIN, SSH)
- Elektronische Post (SMTP, POP3, IMAP, MIME)
- WWW (HTTP) - umfasst auch die vorgenannten Dienste
- Datei- und Druckerfreigabe (CIFS, SMB, Samba)
- Verzeichnisdienste (LDAP, ADS, DNS)
- netzbasiertes Fenstersystem (X Window System, Remote Desktop)
- Nutzung von fernen Programmen (RSH, RPC, RMI, CORBA, Web Services)
- Nutzung von fernen Datenbanken (z.B. ODBC, JDBC)
- Synchrone Kommunikation (sog. Messenger, z.B. ICQ)
- Voice over IP (SIP, H.323, Skype)
- Netzwerkmanagement (SNMP)
- usw.

DER FTP-DIENST

- FTP = File Transfer Protocol
  (Der Dienst heißt wie das Protokoll)
- Dienst zur Übertragung von Dateien zwischen Computern
- Verschiedene FTP-Clients (klassischer kommandobasierter Client, Windows-basierter Client, z.B. Filezilla)
- FTP ist verbindungsorientiert, nutzt TCP
  - ⇨ Verwendeter well-known Port = 21
- Verschiedene Dienstoperationen: PUT, GET usw.
- Nachteil des klassischen FTP: Übertragung von Daten und Passwörtern unverschlüsselt.
  - ⇨ Übergang zu SFTP (Secure FTP) über SSH
  - ⇨ SSH (Secure Shell) ermöglicht verschlüsselte Übertragung nach einem Public-Private-Key-Verfahren
  - ⇨ SSH verwendet well-known Port 22

FILEZILLA:
BEISPIEL EINES FTP-CLIENTS

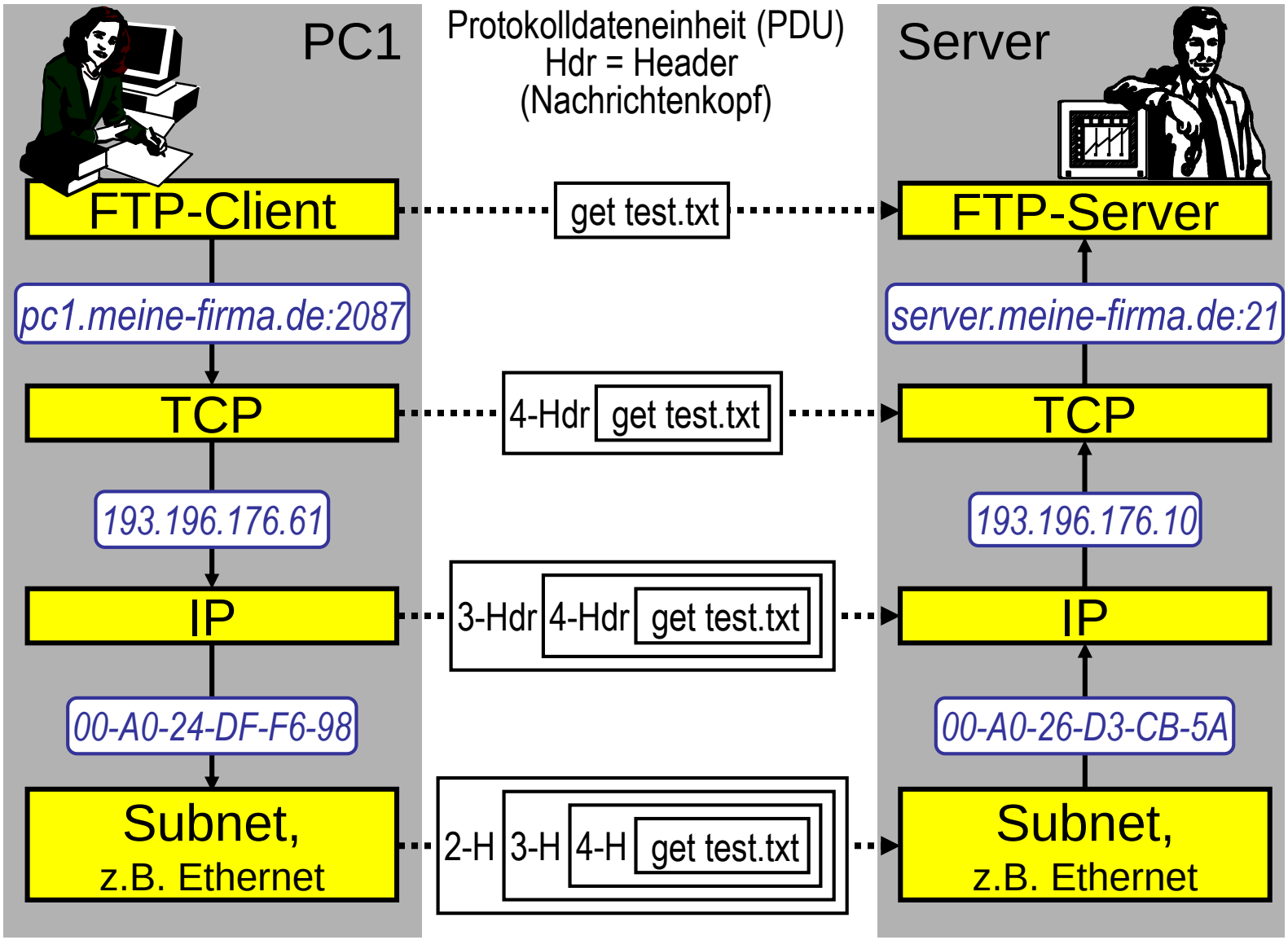
HOCHSCHULE DER MEDIEN



Dateien können durch Ziehen hin und her kopiert werden.

ROLLE DER SCHICHTEN AM BEISPIEL DES FTP-DIENSTES

HOCHSCHULE DER MEDIEN

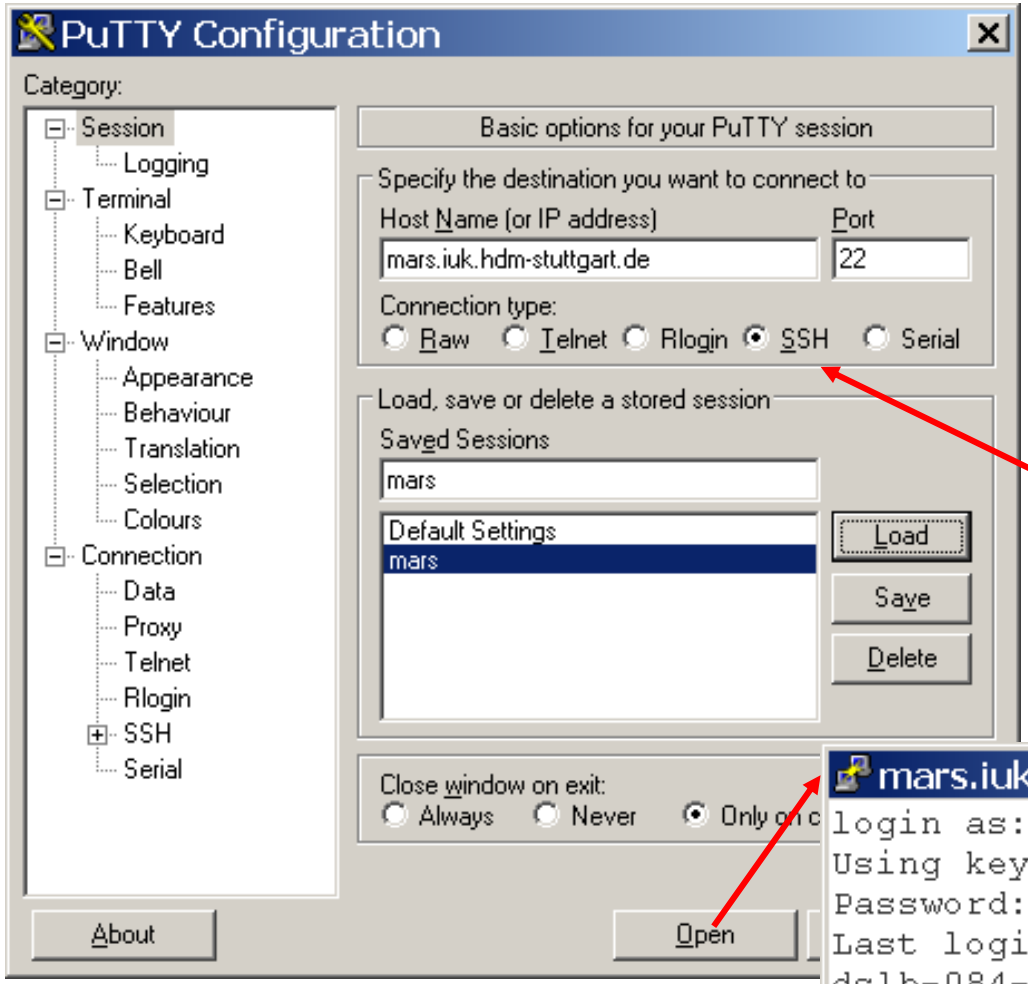


DER TELNET-DIENST

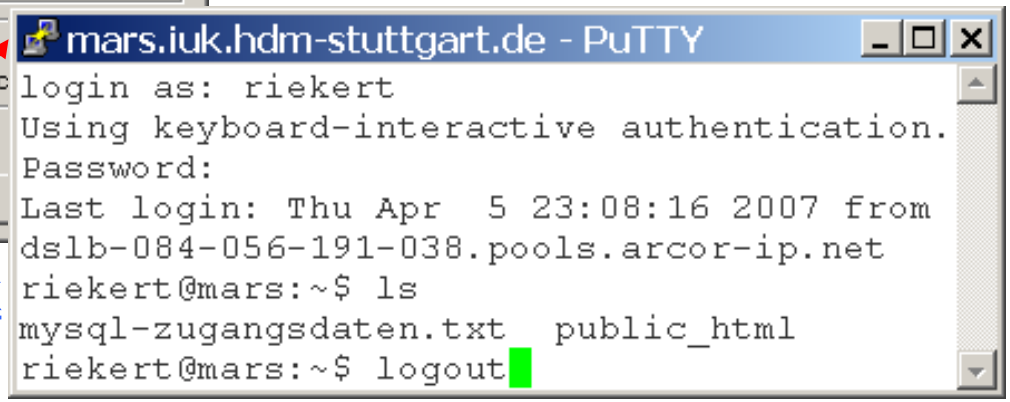
- virtuelles Terminal
  - ⇨ Das klassische Bildschirmterminal eines „Mainframe“-Computers (Großrechners) wird emuliert
- Telnet-Client zur Darstellung des Bildschirmterminals
  - ⇨ Klassisches Telnet-Kommando (unter DOS oder Unix Shell) oder Windows-basierter Client (z.B. PuTTY)
  - ⇨ Funktionsweise zeilenorientiert, nicht seitenorientiert
- Telnet-Server verbunden mit zeilenorientiertem Kommandointerpreter (z.B. UNIX Shell)
- Telnet ist verbindungsorientiert, nutzt TCP
  - ⇨ verwendeter well-known Port = 23
- Auf vielen Servern ist der Telnet-Dienst deaktiviert und durch SSH ersetzt (Vorteil: verschlüsselte Übertragung).

PUTTY: VIRTUELLES TERMINAL AUF BASIS TELNET UND SSH

HOCHSCHULE DER MEDIEN



Mit einem „virtuellen Terminal“, z.B. PuTTY, können Betriebssystem-Befehle auf einem Unix/Linux-Server ausgeführt werden. Möglich sind der unverschlüsselte Telnet-Dienst und der sichere SSH-Dienst.



http://www.chiark.greenend.org.uk/~sgtatham/putty/

DER „TELNET-CLIENT“ ALS CLIENT-SIMULATOR

Das Protokoll, mit dem Telnet-Client und Telnet-Server kommunizieren, ist praktisch identisch mit der TCP-Kommunikationsschnittstelle

- Alle Zeichen, die man in das Telnet-Fenster hineintippt, sendet der Telnet-Client unverändert mit TCP an den Server weiter
- Alle Zeichen, die der Server über TCP an den Client schickt, zeigt dieser unverändert im Telnet-Fenster an.

Da man den Telnet-Client mit einer beliebigen Portnummer als Aufrufparameter starten kann (statt der standardmäßigen Portnummer 23), kann Telnet beliebige Server ansprechen, die Verbindungen über TCP akzeptieren und deren Protokoll mit druckbaren Zeichen auskommt. Allerdings sollte man in Telnet das lokale Echo einschalten, sonst sieht man nicht, was man tippt. Auch darf man sich nicht vertippen!

INTERNET MAIL

- Mail-Client und Mail-Server kommunizieren über die Protokolle **SMTP** zum Senden sowie **POP3** oder **IMAP** zum Lesen von Email
- Email-Nachrichten sind gegliedert in Header und den eigentlichen Nachrichtentext. Aufbau des Headers im Internet genormt durch **RFC822**
- Erweiterung des Headers durch **MIME** (Multipurpose Internet Mail Extensions), genormt durch **RFC1521**
  - ⇨ **Typisierte Nachrichten** (mit MIME Types), dadurch können Dateien als Anhänge übertragen werden (Beispiele für MIME Types: text/plain, text/html, image/jpeg, image/gif, application/pdf, video/mpeg …)
  - ⇨ **Mehrteilige Nachrichten** (Multipart Messages)

EIN MIT TELNET SIMULIERTER EMAIL-CLIENT „SPRICHT“ SMTP (1)

HOCHSCHULE DER MEDIEN

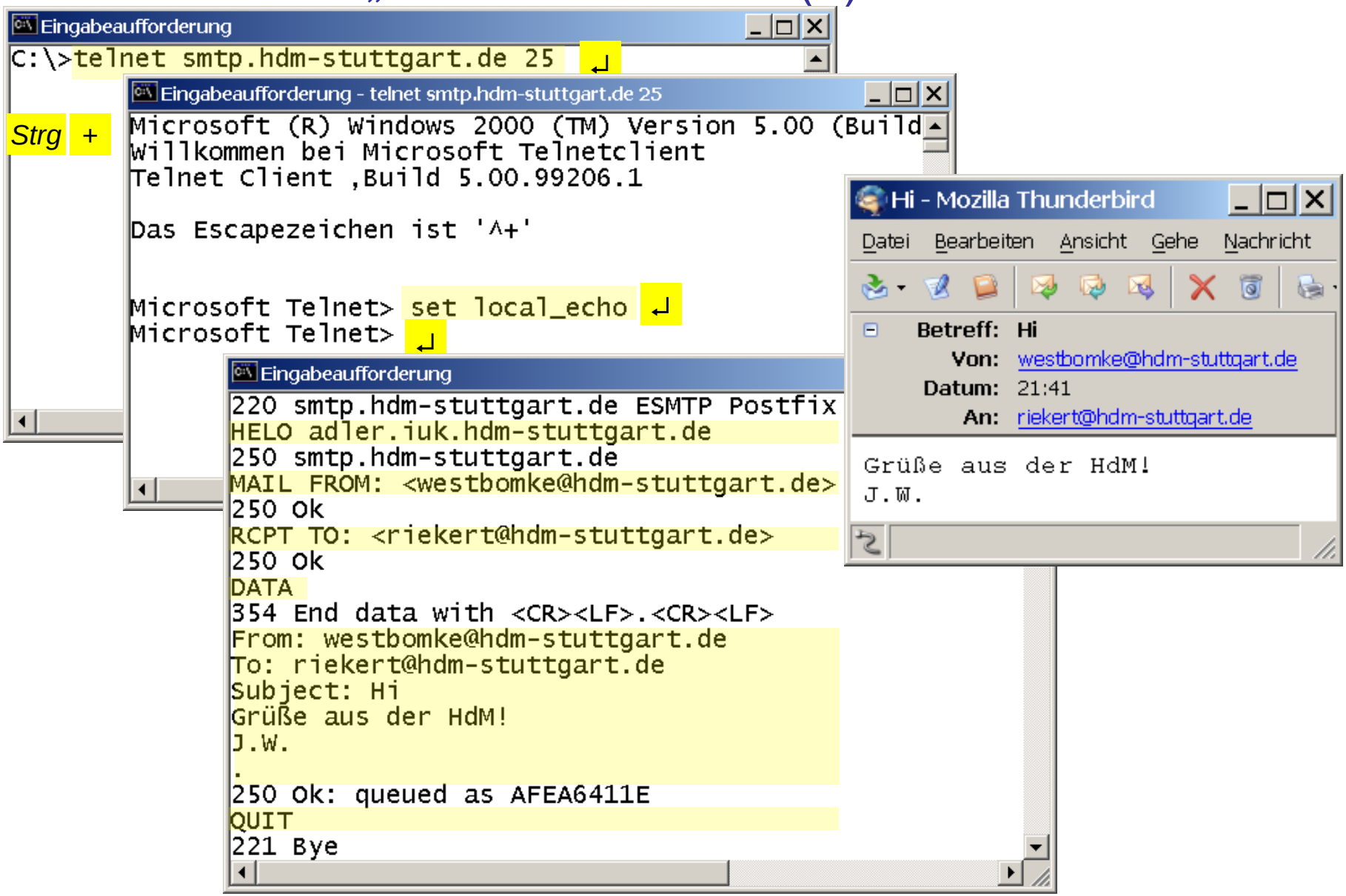
C: **telnet smtp.hdm-stuttgart.de 25**
S: 220 smtp.hdm-stuttgart.de SMTP service ready
C: **HELO adler.iuk.hdm-stuttgart.de**
S: 250 smtp.hdm-stuttgart.de says hello to adler.iuk.hdm-stuttgart.de
C: **MAIL FROM: <westbomke@hdm-stuttgart.de>**
S: 250 sender ok
C: **RCPT TO: <riekert@hdm-stuttgart.de>**
S: 250 recipient ok
C: **DATA**
S: 354 Send mail; end with "." on a line by itself
C: **From: westbomke@hdm-stuttgart.de**
C: **To: riekert@@hdm-stuttgart.de**
C: **Subject: Hi**
C: **Grüße aus der HdM!**
C: **J.W.**
C: **.**
S: 250 message accepted
C: **QUIT**
S: 221 smtp.hdm-stuttgart.de closing connection

Legende:

C = **Client**
S = Server

EIN MIT TELNET SIMULIERTER EMAIL-CLIENT „SPRICHT“ SMTP (2)

HOCHSCHULE DER MEDIEN



DAS WORLD WIDE WEB (WWW)

Client: Internet-Browser (z.B. Mozilla Firefox, Microsoft Internet Explorer)

Server: Webserver (z.B. Microsoft Internet Information Server, Apache)

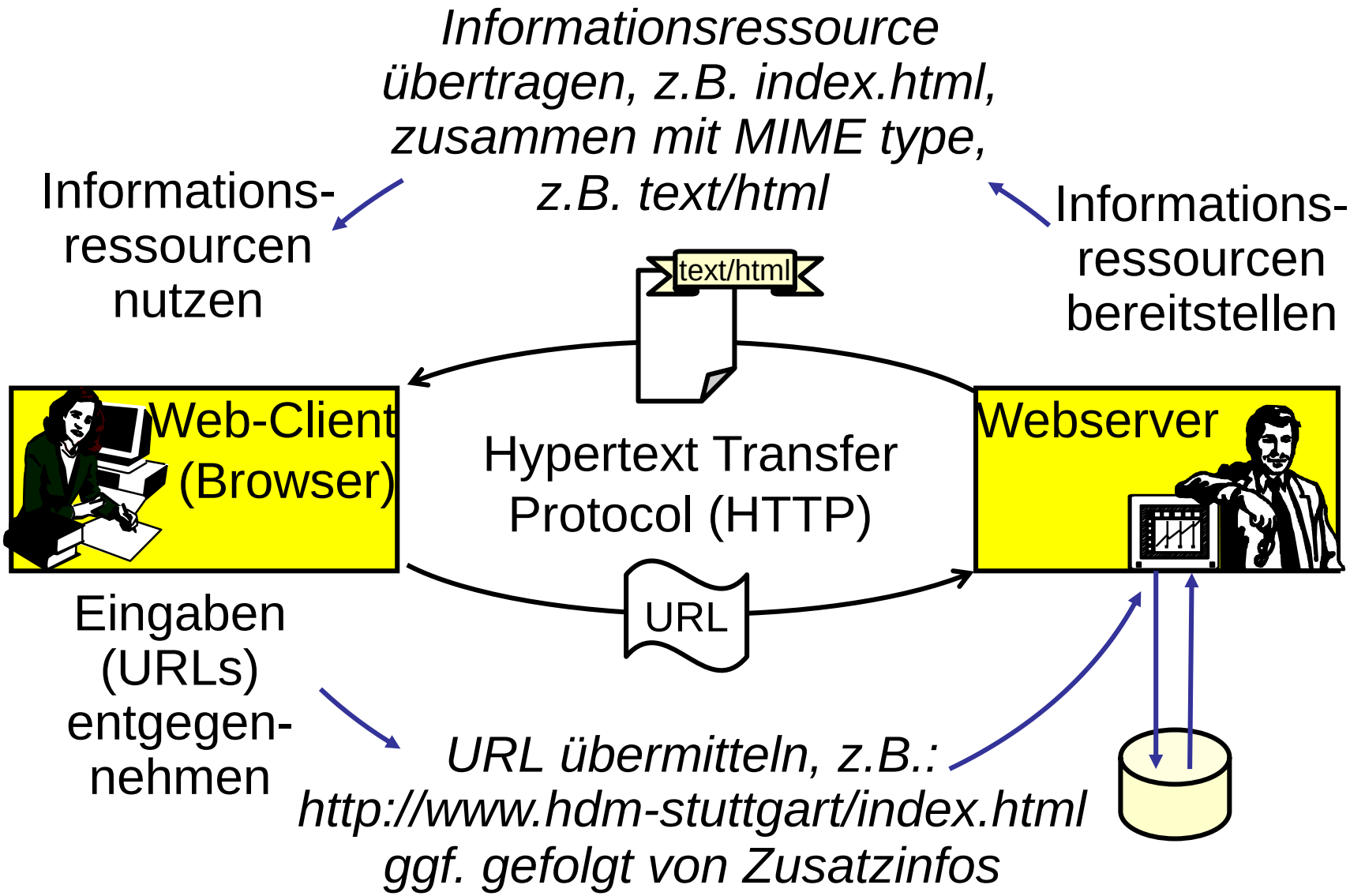
Dienst: Bereitstellen von Hypertextseiten und anderen Informationsressourcen (typisiert mit MIME Types) nach Angabe einer Adresse, der URL (Uniform Resource Locator)

Art des Dienstes: Verbindungsloser Anfrage/Antwort-Dienst

Protokoll: Hypertext Transfer Protokoll (HTTP).

Transportprotokoll: TCP (verbindungsorientiert!) über Port 80

WEB-CLIENT (BROWSER) UND WEBSERVER



WEBSERVER

- erhält eine Informationsressourcenanforderung, welche im Wesentlichen aus einer URL besteht,
- stellt die Informationsressource bereit,
  - ⇨ statisch: Informationsressource wird unverändert aus dem Dateisystem geholt
  - ⇨ oder dynamisch: Informationsressource ist das Ergebnis eines durch die URL adressierten Programms. Das Programm wird hierzu direkt durch die CPU oder durch einen Interpreter (z.B. PHP) ausgeführt.
- stellt den MIME-Type der bereitgestellten Informationsressource fest: z.B. text/html, image/gif, application/msword, application/pdf, ...
- und schickt die Informationsressource zusammen mit dem MIME-Type an den Client (Internet-Browser) zurück

WEB-CLIENT (INTERNET BROWSER)

- verarbeitet die vom Web-Server erhaltenen Informationsressourcen abhängig von deren Typ (MIME type)
  - ⇨ direkte Anzeige: HTML-Seiten, GIF- bzw. JPEG-Grafiken
  - ⇨ direkte Ausführung: JavaScript, ActiveX Controls (letzteres nur Microsoft Internet Explorer)
  - ⇨ Anzeige/Ausführung über Plug-In (nachladbare Browser-Erweiterung): z.B. Acrobat Reader, Java Plugin, Flash
  - ⇨ Anzeige/Ausführung durch sog. Helper Application: z.B. Winword für Doc-Files usw.
- nimmt Eingaben von URLs an und leitet diese weiter an Web-Server
  - ⇨ Direkteingabe über Tastatur
  - ⇨ Anklicken von Hyperlinks (mit URL hinterlegte Bereiche)
  - ⇨ Ausfüllen und Abschicken von Web-Formularen

UNIFORM RESOURCE LOCATOR (URL)

URLs adressieren weltweit eindeutig Informationsressourcen (d.h. Daten, Dienstprogramme und multimediale Dokumente):

Aufbau: *Protokoll://Domain:Port/Pfad*

Beispiel: **http:**//dvmail.zeppelin-nt.com:8080/lisa/index.html

(Die Zeichen //, :, / sind syntaktische Kennzeichnungen für die verschiedenen Elemente der URL)

Protokoll: = Übertragungsprotokoll
(http: = Hypertext Transfer Protocol)

//Domain = Bezeichnung des Servercomputers im Internet

:Port = Kommunikationsport des Webserver-Programms, i.d.R. nicht erforderlich, da Standardwert = 80

/Pfad = Ortsangabe im Dateisystem des Servers, bestehend aus Verzeichnis(pfad) und Dateiname

URLs: VARIANTEN

Relative URLs: Hypertextseiten enthalten oft relative Links. Das Protokoll, die Domain und der Schrägstrich vor dem Verzeichnispfad werden dann weggelassen. Beispiele:

- english.html (d.h. die Seite liegt im gleichen Verzeichnis wie aktuelle Hypertextseite)
- ../cgi-bin/test.cgi (liegt im Nachbarverzeichnis cgi-bin)

Andere Protokolle: Außer http: sind noch andere Protokolle möglich: **https:** (verschlüsselte Datenübertragung im Web, z.B. für Internet Banking etc.), **ftp:** (Verwendung des klassischen File Transfer Protocols).

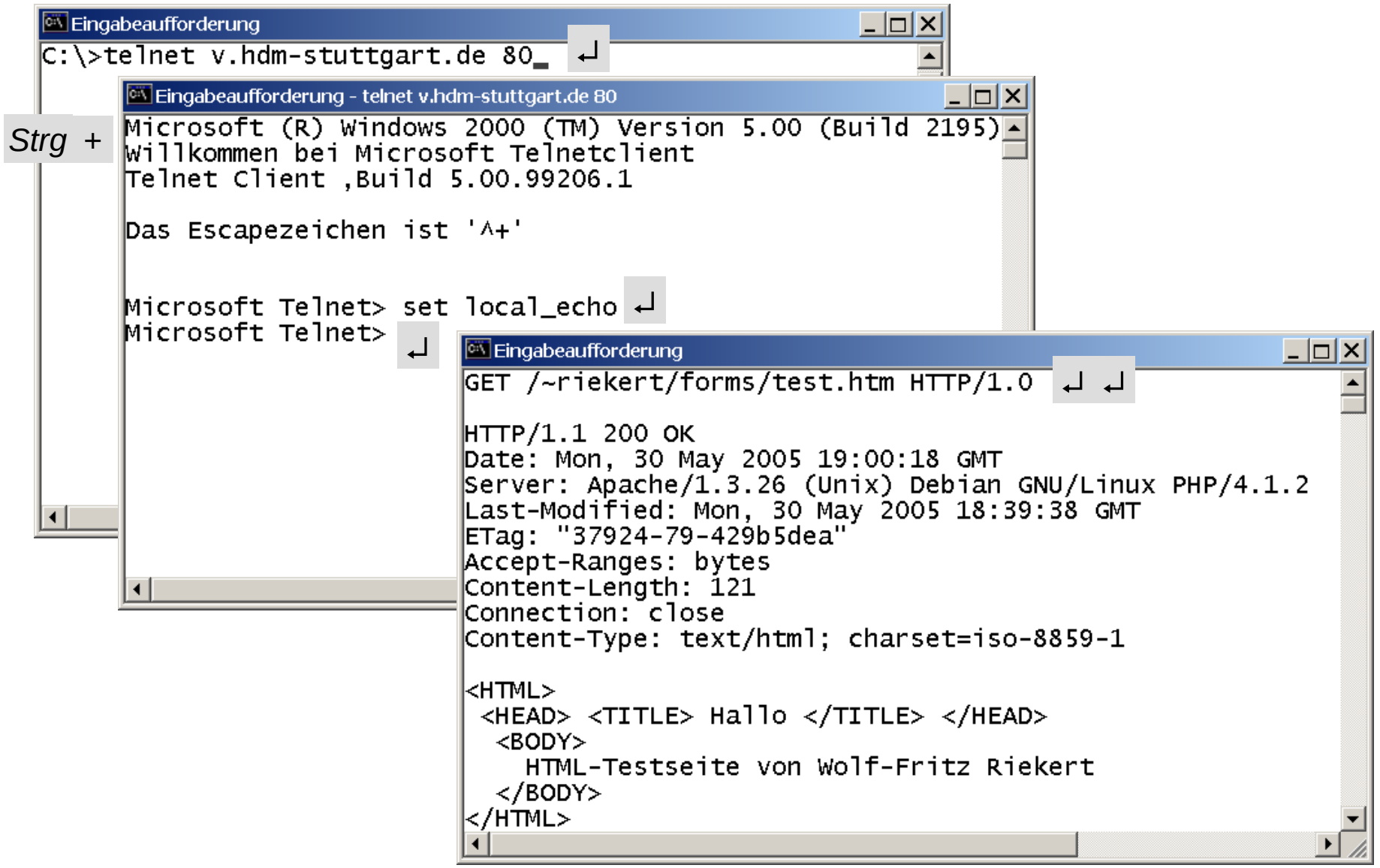
Wie ein Protokoll behandelt werden **mailto:** und **telnet:** (Aufruf des Mailsystems bzw. des Telnet-Clients für eine bestimmte Adresse**,** **file:** (lokaler Dateizugriff ohne Server).

EIN SIMULIERTER WEB-CLIENT (1)

- Starten Sie Telnet in einer DOS-Box mit folgendem Aufruf:
  `telnet v.hdm-stuttgart.de 80` ↵
- Stellen Sie das „Lokale Echo“ ein. Dazu zunächst mit Strg-+ in den Befehlsmodus gehen. Nach dem Befehl zweimal die Eingabetaste drücken, um in den Eingabemodus zu gehen:
  Strg + **`set local_echo`** ↵ ↵
- Geben Sie ein GET-Kommando ins Telnet-Fenster ein, gefolgt durch zweimaligen Druck der Eingabetaste:
  `GET /~riekert/forms/test.htm HTTP/1.0` ↵ ↵
- Der Webserver auf v.hdm-stuttgart.de schickt Ihnen dann den HTML-Code der Webseite zurück
- Probieren Sie dasselbe mit anderen URLs, eventuell auch mit URLs von CGI-Skripts.

EIN SIMULIERTER WEB-CLIENT (2)

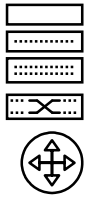
HOCHSCHULE DER MEDIEN



LITERATUR

Andrew S. Tanenbaum, David J. Wetherall : Computernetzwerke. 5., aktualisierte Auflage. München [u.a.] : Pearson, 2012. 1040 Seiten, ISBN 978-3-8689-4137-1
Abbildungen aus dem Buch im Web unter http://www.cs.vu.nl/~ast. (*Standardwerk, geeignet zum Nachschlagen, geht weit über den Vorlesungsstoff hinaus*)

LEGENDE DER NETZWERKSYMBOLE



Hub, diverse Verteiler

Switch

Router

WLAN-(DSL-)Router

WLAN-Access-Point

Laptop (mit WLAN-Interface)

Arbeitsplatz-PC

Servercomputer

Browser

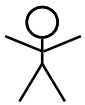
Prozess

Lokales Netzwerk
Broadcastnetz

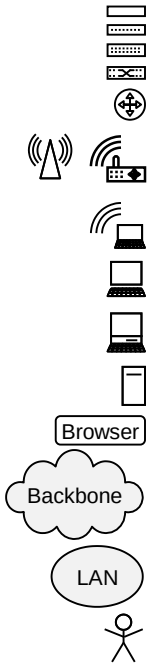
Lokales Netzwerk
(Hintergrund für
Komponenten)

Verbundnetz
(z.B. Internet)

Verbundnetz
(Hintergrund für
Komponenten)



Benutzer(in)



Kleine
Symbole