HOCHSCHULE DER MEDIEN

INTERNET 1

Stand: 23.06.2016

Prof. Dr. Wolf-Fritz Riekert
Hochschule der Medien (HdM) Stuttgart
Stuttgart Media University

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

INHALT

Einführung, Allgemeines zu Netzen

Das Subnetz nach Schichten (Ebenen)
- Teil 1: Bitübertragungsschicht (Physical Layer)
- Teil 2: Sicherungsschicht (Data Link Layer)

Das eigentliche Internet nach Schichten (Ebenen)
- Teil 3: Vermittlungsschicht (Network Layer)
- Teil 4: Transportschicht (Transport Layer)
- Teil 5: Anwendungsschicht (Application Layer)

Spezielle Themen
- Teil 6: Sicherheit im Internet durch Kryptographie
- Teil 7: Aufbau von Websites

LERNZIELE

- Verstehen, wie das Internet funktioniert
  - ⇨ Hardware- und Softwarekomponenten, Subnetze
  - ⇨ Architektur (Schichten, Dienste, Protokolle)
  - ⇨ Anwendungen (z.B. Web, mobile Apps)
- Verstehen, wie das Internet durch Verschlüsselung und Signierung von Daten sicherer gemacht wird
- Grundlagen der Web-Entwicklung kennen lernen
- Praktische Anwendung des Kenntnisse durch die Gestaltung einer Website mit HTML und CSS

NETZE

Definition Netze (im Sinne von Computernetze, Rechnernetze):

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

Zweck:

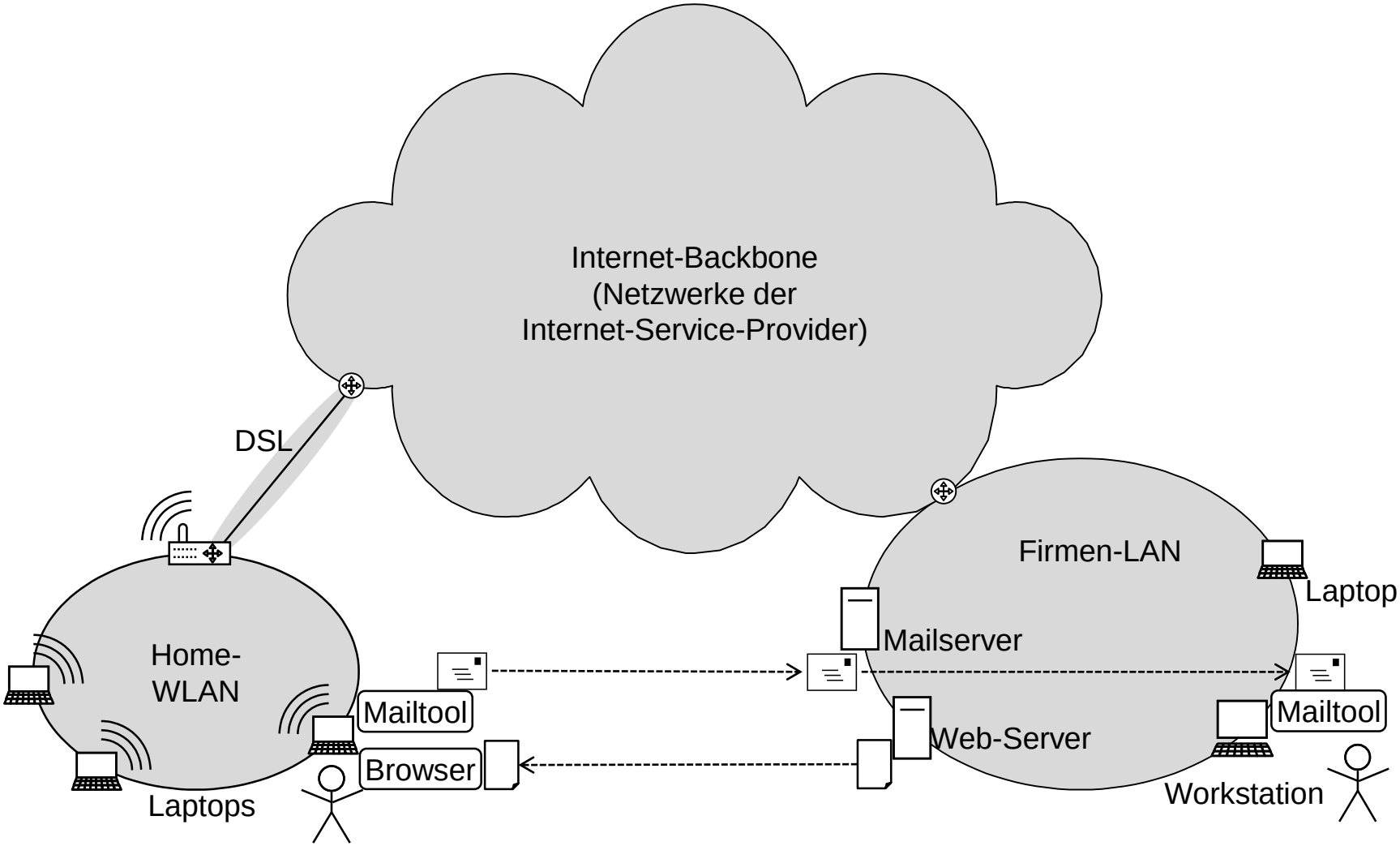
- Gemeinsame Nutzung von Ressourcen (Geräte, Programme, Daten)
- Fernbedienung, Überwindung räumlicher Distanzen
- Kommunikation zwischen Menschen, Zusammenarbeit
- Elektronischer Handel (E-Commerce)
- Informationsbeschaffung, -bereitstellung
- Unterhaltung (Multimedia)

DAS INTERNET: EIN VERBUNDNETZ AUS SUBNETZEN

Das Internet ist ein Verbundnetz, das sich aus unterschiedlichen „Subnetzen“ zusammensetzt:

- Lokale Netze:
  - ⇨ kabelgebunden: (Ethernet-)LAN
  - ⇨ drahtlos: WLAN
- Internetzugangsnetze:
  - ⇨ DSL
  - ⇨ Breitbandnetze (Kabelnetze, ursprünglich nur Fernsehen)
  - ⇨ Mobilfunknetze (3G/4G)
  - ⇨ Telefonnetz (mittels Modem, ISDN)
- Internet-Backbone (Netzwerke der Internet Service Provider), oft als „eigentliches“ Internet betrachtet
- Intranets (firmeninterne Netze)

BEISPIELSZENARIO
SUBNETZE DES INTERNET



BEDEUTUNG DER SOFTWARE FÜR NETZE

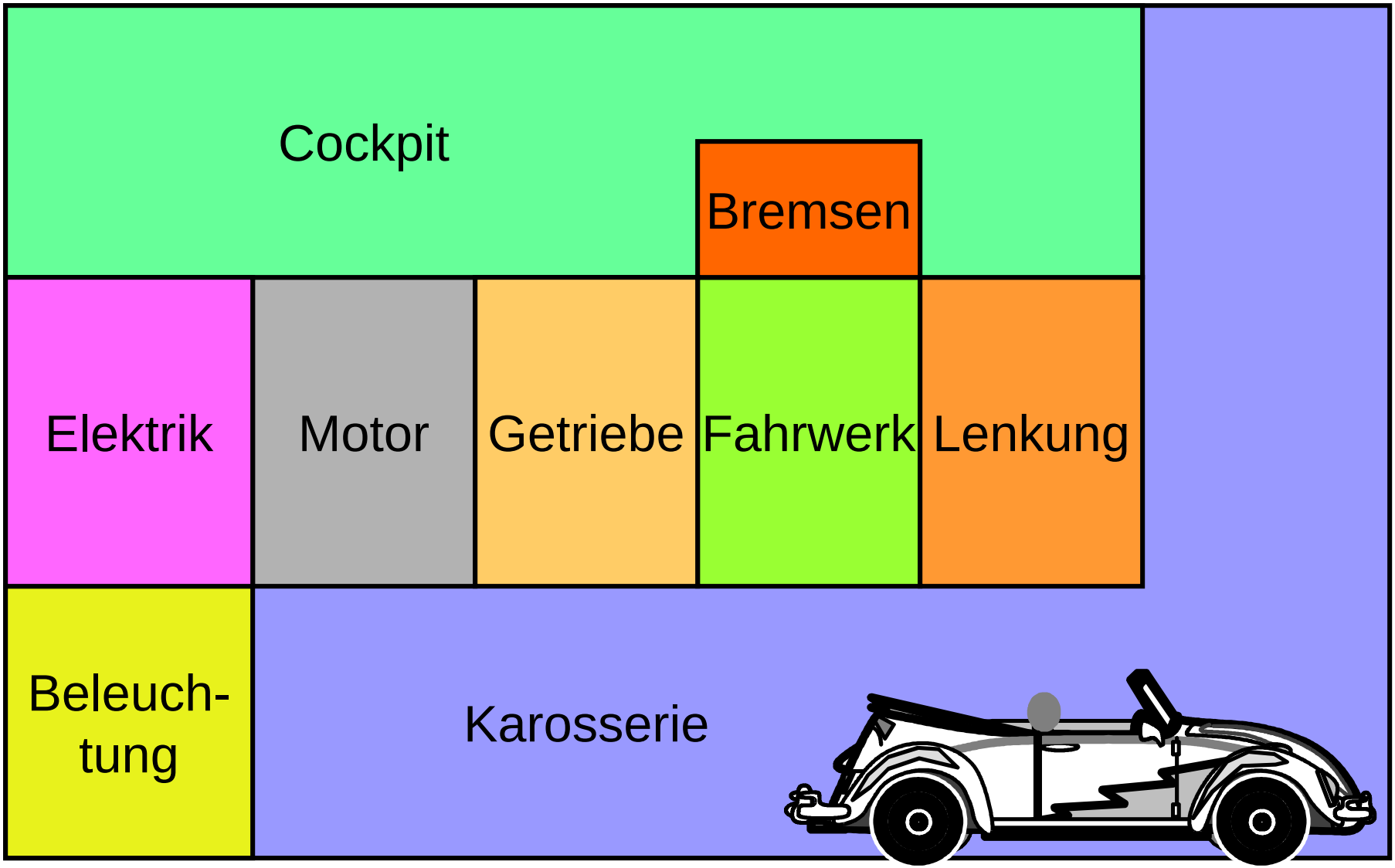
- Software ist inzwischen die entscheidende Komponente zur Bereitstellung von Netzwerkdiensten geworden
- Der überwiegende Teil dieser Vorlesung ist mit Netzwerksoftware befasst.
- Netzwerksoftware: ein komplexes Feld, das einer besonderen Strukturierungstechnik bedarf
  - ⇨ Strukturierung in Form von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

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).

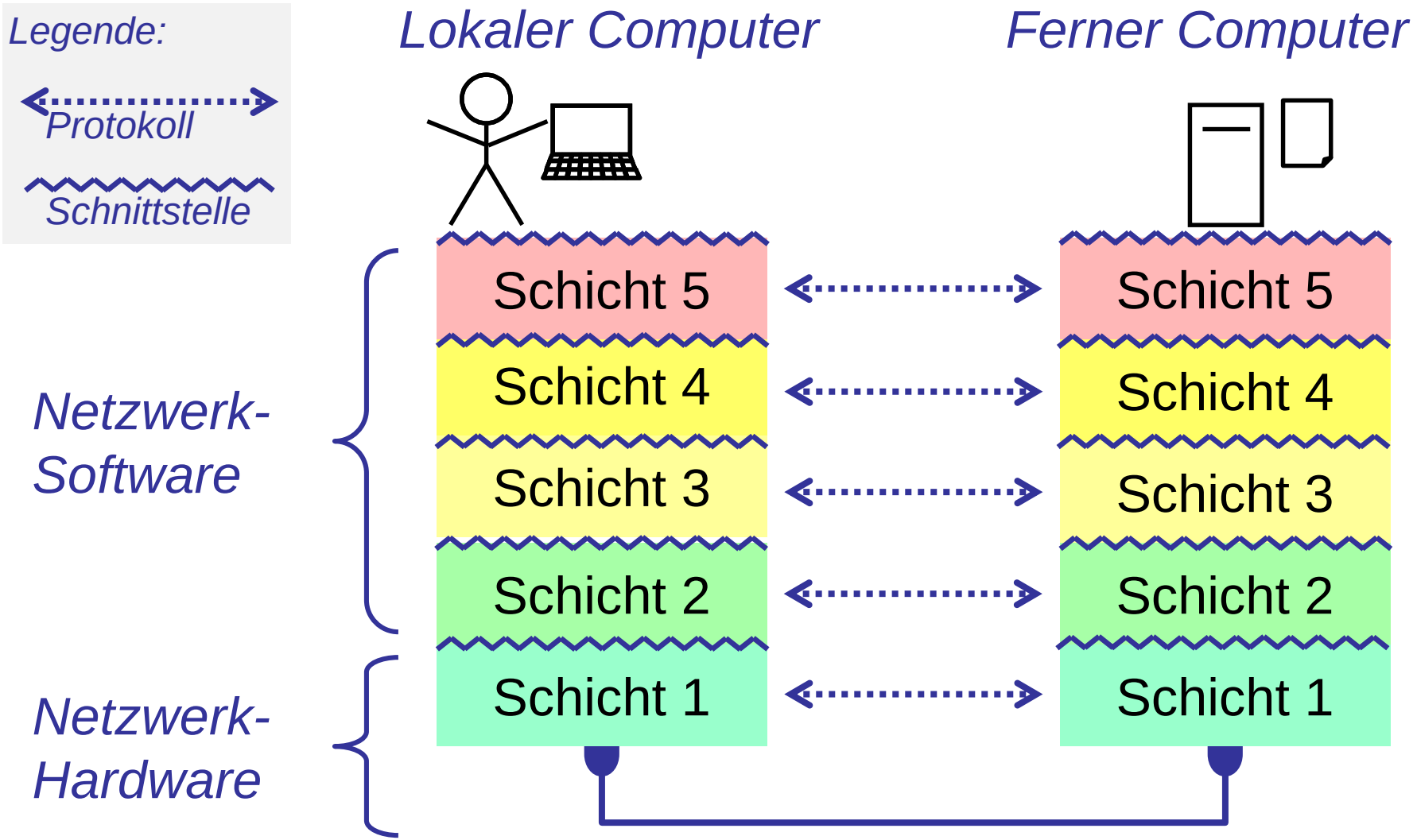
BEISPIEL FÜR MODULARISIERUNG: AUTOMOBIL

HOCHSCHULE DER MEDIEN



SCHICHTEN GLIEDERN
NETZWERKSOFT- UND HARDWARE

HOCHSCHULE DER MEDIEN



SCHICHTEN, DIENSTE, PROTOKOLLE, SCHNITTSTELLEN

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.

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)

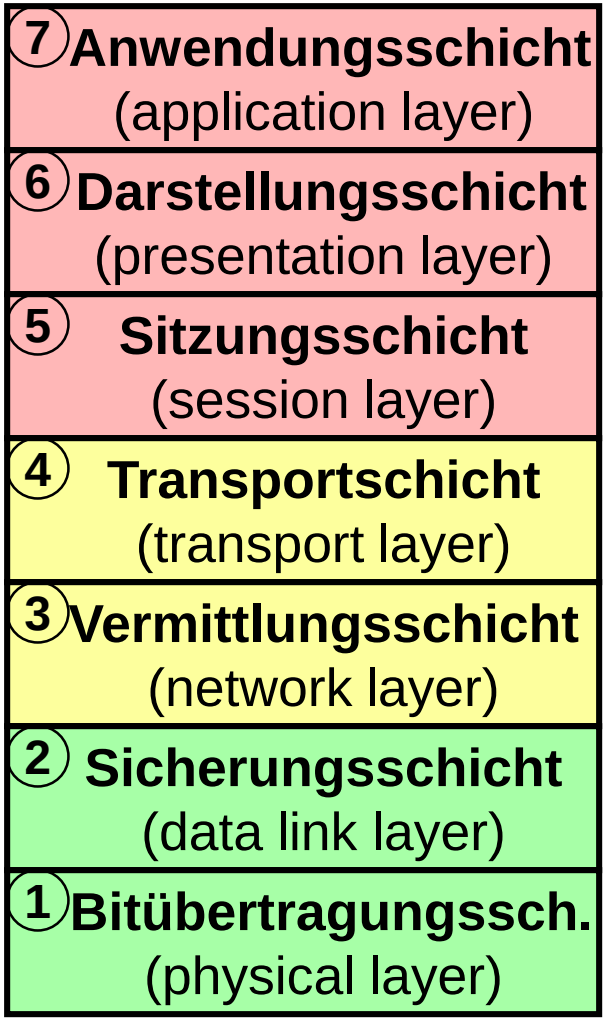
VERBINDUNGSORIENTIERTE DIENSTE

- 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,)

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 die **ISO** (International Organization for Standardization) 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

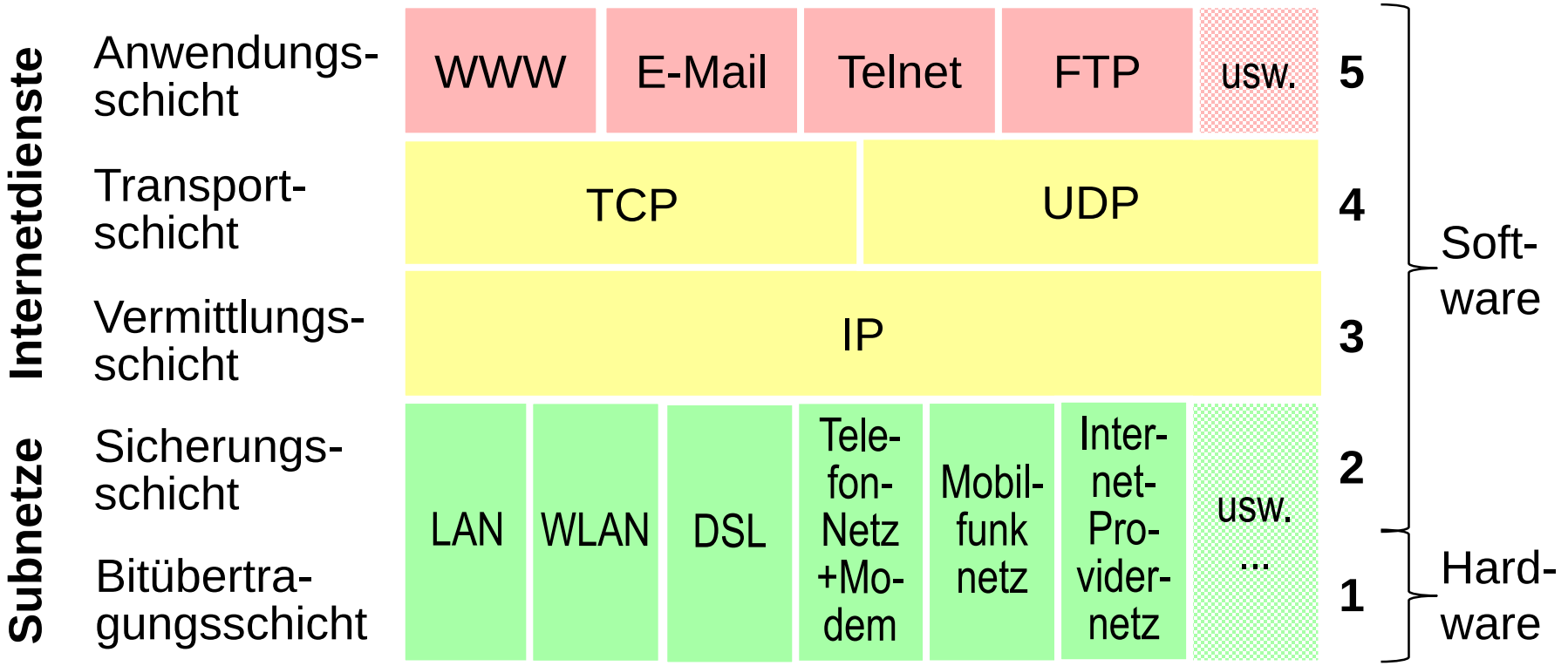
Das **Internet** ist ein offenes Verbundnetz, das verschiedene existierende Netze als „Subnetze“ miteinander verbindet.

- Entstanden 1969 als **ARPANET** (gefördert durch US-amerikanische Militärforschungsinstitution „**A**dvanced **R**esearch **P**roject **A**gency“)
- Anfangs entwickelt durch verschiedene Universitäten und Forschungsinstitute
- Betrieb und Weiterentwicklung heute weitgehend durch kommerzielle Einrichtungen (z.B. Internet-Provider)

Pragmatische Entwicklungsphilosophie, folgt nicht dem OSI-Modell. Zur Strukturierung ist das Fünf-Schichten-Modell nach Tanenbaum & Wetherall (2012) geeignet. Dies sieht vor:

- 3 Schichten innerhalb des Internets
- 2 Subnetzschichten unterhalb des Internets

SCHICHTEN DER INTERNETARCHITEKTUR



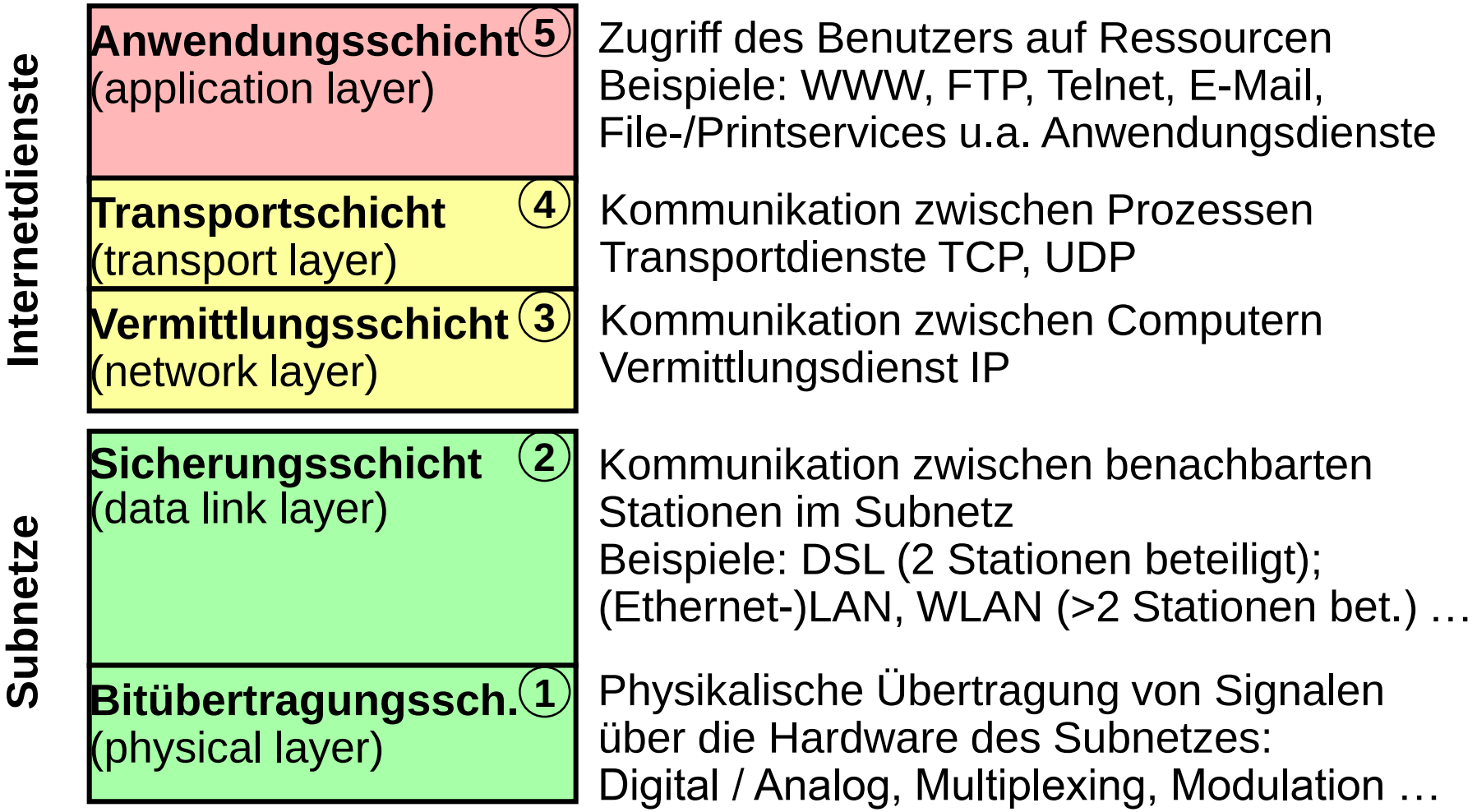
Die unteren zwei Netzwerkschichten (1+2) sind gegeben durch beliebige Übertragungseinrichtungen, die so genannten Subnetze.
Diese werden durch die die oberen drei Netzwerk-Schichten (3-5) zum „Internet“ als globalem Verbundnetz zusammengeschlossen.
So entsteht ein Fünf-Schichten-Modell (Tanenbaum & Wetherall, 2012).

INTERNET: HISTORIE

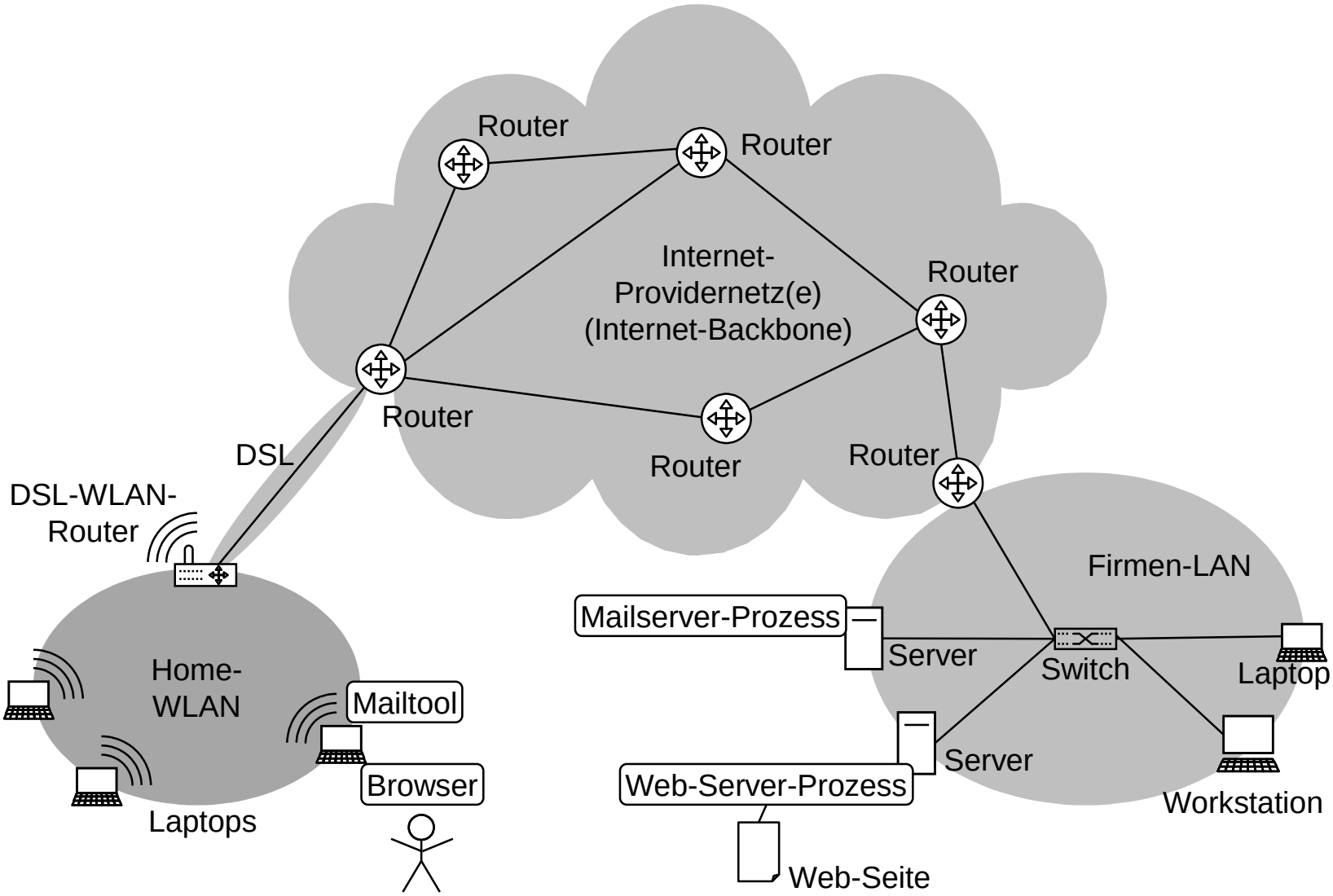
- Ab 1969: **ARPANET**, durch amerikanisches Militär gefördert, von Wissenschaftlern genutzt und betrieben
  - ⇨ Erste Dienste: E-Mail, FTP (File Transfer), Telnet (Login auf fernen Computern)
- 1982: Umbenennung in **Internet**
  - ⇨ Einführung der Übertragungsprotokollfamilie TCP/IP
  - ⇨ Internetworking: 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.

FÜNF-SCHICHTEN-MODELL

Der Vorlesungsstoff ist nach dem Fünf-Schichten-Modell von Tanenbaum & Wetherall (2012) gegliedert.



BEISPIELSZENARIO



BEISPIELSZENARIO

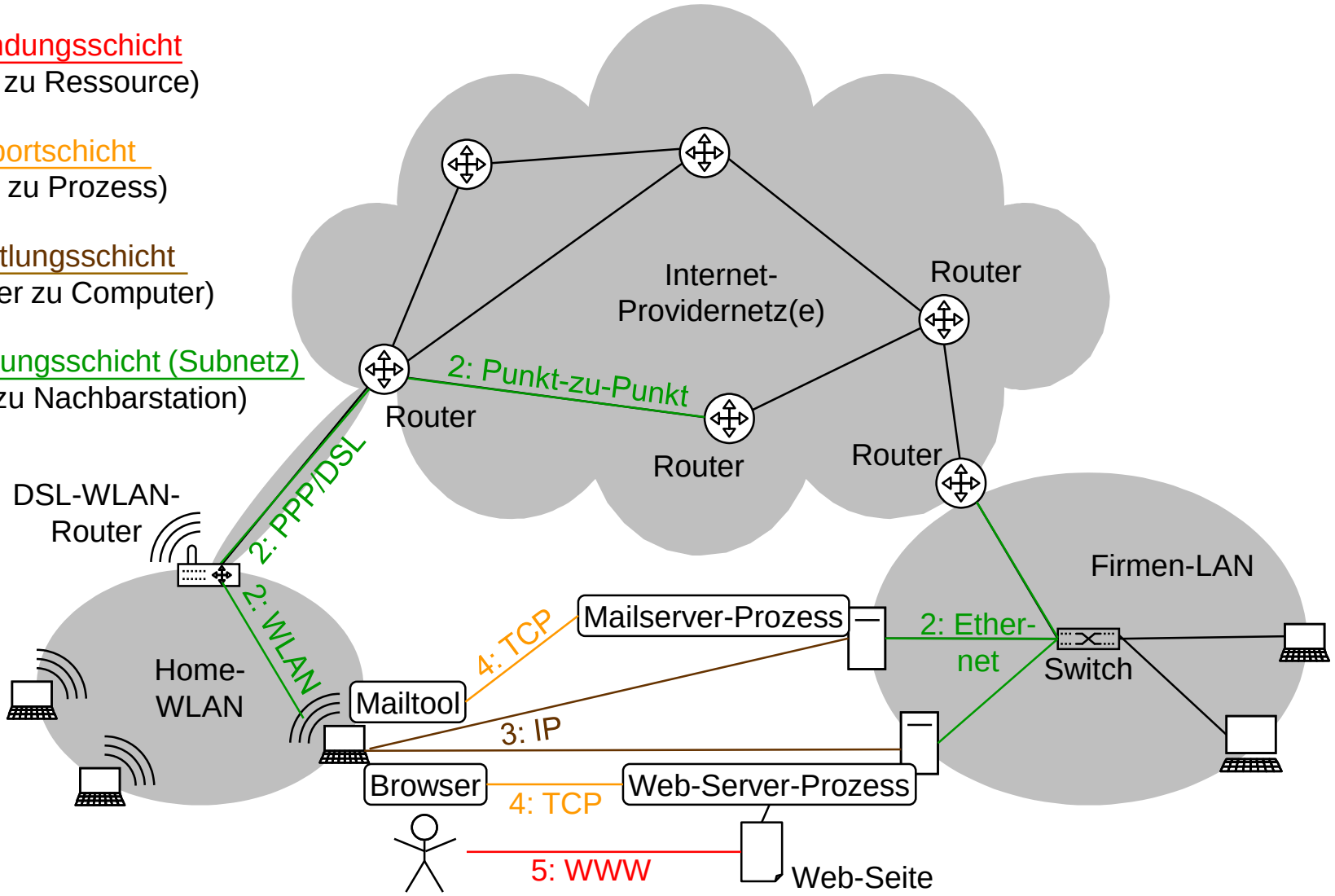
HOCHSCHULE DER MEDIEN

5: Anwendungsschicht
(Mensch zu Ressource)

4: Transportschicht
(Prozess zu Prozess)

3: Vermittlungsschicht
(Computer zu Computer)

2: Sicherungsschicht (Subnetz)
(Station zu Nachbarstation)



LITERATUR

Andrew S. Tanenbaum & David J. Wetherall : Computernetzwerke. 5., aktualisierte Auflage. München [u.a.] : Pearson, 2012. 1040 Seiten, ISBN 978-3-8689-4137-1 (*Standardwerk, geeignet zum Nachschlagen, geht weit über den Vorlesungsstoff hinaus*)

TEIL 1: BITÜBERTRAGUNGSSCHICHT IM SUBNETZ (PHYSICAL LAYER)

Übertragung von rohen Bits über einen Übertragungskanal:

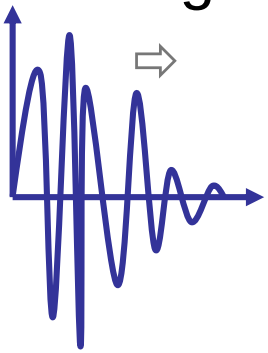
- Festlegung des physischen Übertragungsmediums
- mechanische, elektrische und prozedurale Festlegungen

Typische Festlegungen der Bitübertragungsschicht:

- Wie ist der Stecker für den Netzanschluss mechanisch aufgebaut?
- Wie viel Volt entsprechen einer logischen 1 bzw. 0
- Wie viele 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

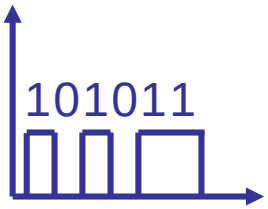
- **Analoge Signale**: Kontinuierliche Veränderungen physikalischer Größen (z.B. elektrische Spannung, magnetische Feldstärke) mit der Zeit



⇨ 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



BANDBREITE UND DATENRATE

- Jeder **analoge Übertragungskanal** besitzt eine Grenzfrequenz, d.h. Schwingungen mit höheren Frequenzen werden nicht mehr übertragen. Diese Frequenz heißt auch die **Bandbreite**.
  - ⇨ Frequenz und damit auch die Bandbreite wird 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.
  - ⇨ Die Bandbreite eines Rundfunksenders ist maßgeblich für die höchste durch den Sender übertragene Frequenz und damit für die effektive Klangqualität.
- Die Leistungsfähigkeit eines **digitalen Übertragungskanals** wird in **Bit/s** (Anzahl übertragener binärer Zustände pro Sekunde) gemessen und als **Datenrate** bezeichnet.

MEDIEN ZUR ÜBERTRAGUNG VON SIGNALEN

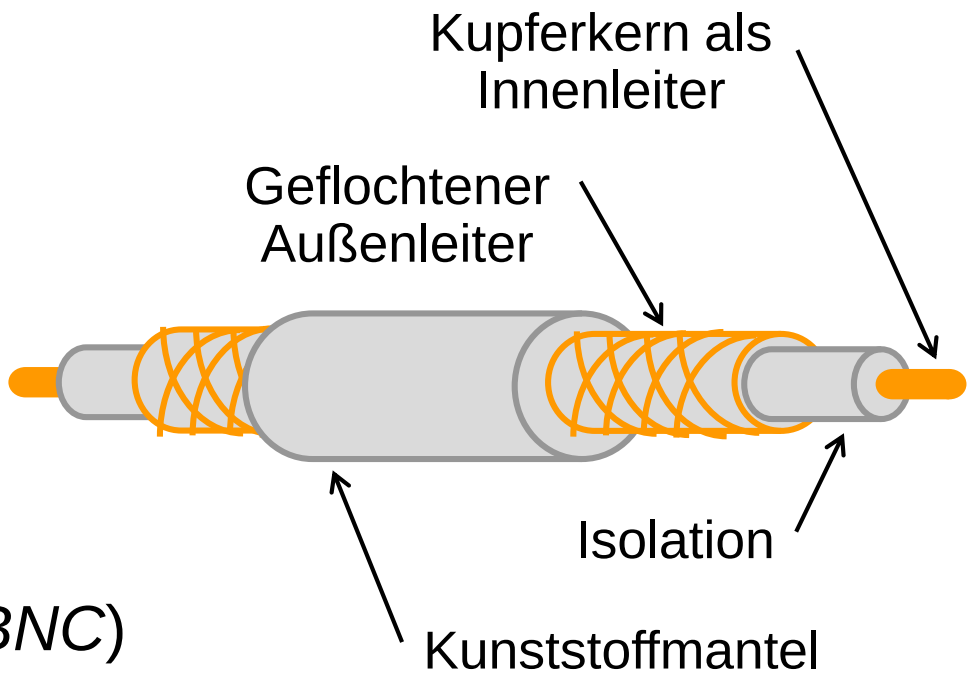
Verschiedene Medien sind zur Übertragung von Signalen geeignet:

- **Elektrische Übertragungsmedien** (Kabel)
  - ⇨ Gut geeignet für analoge Signale
  - ⇨ Mit Einschränkungen (geringe Reichweite bzw. niedrige Datenrate) 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)

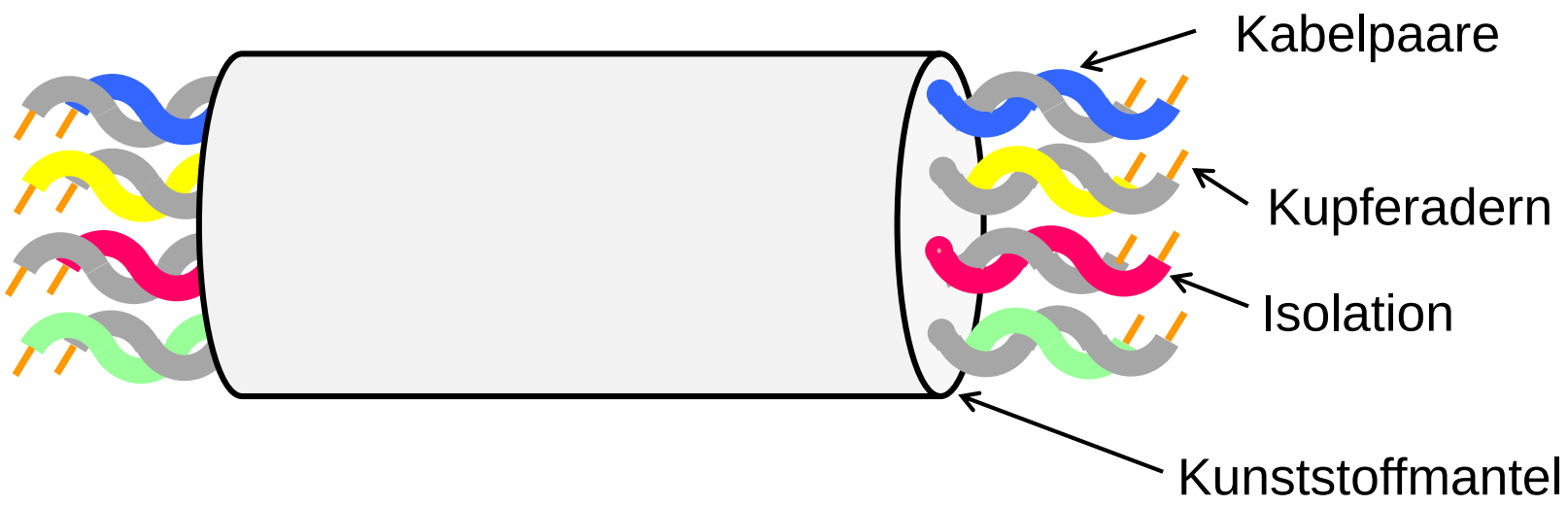
KOAXIALKABEL (BROADBAND NETWORK CABLE = BNC)



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

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

VERDRILLTE KABELPAARE (TWISTED PAIRS, TP-KABEL)



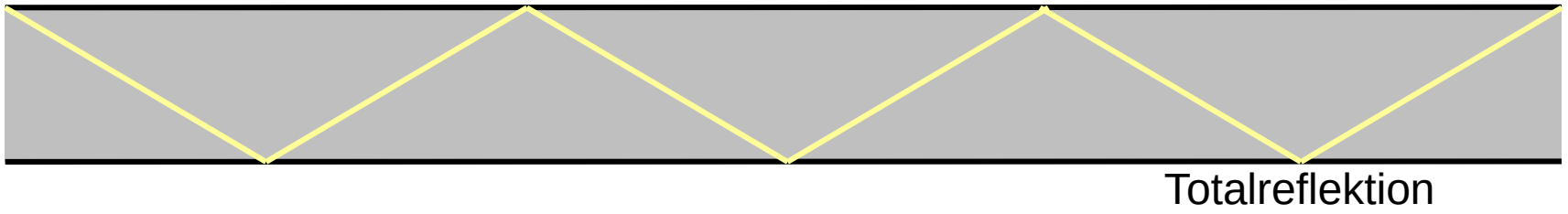
Verdrillte Kabelpaare (engl.: *twisted pair, kurz TP*)

- Verdrillung verringert Störungen durch Einstrahlungen
- Vergleichsweise preiswert
- max. Datenrate 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

LICHTWELLENLEITER (GLASFASERKABEL)



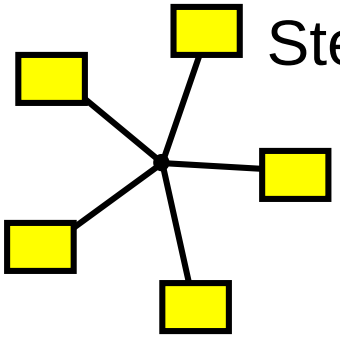
Lichtwellenleiter (Glasfaserkabel):

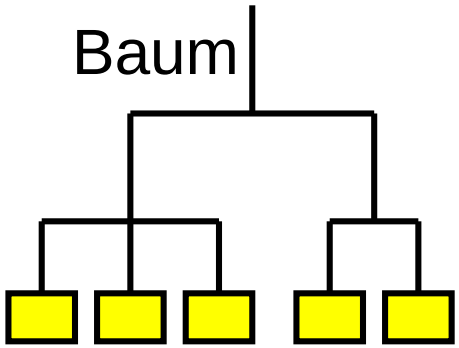
- Gut geeignet für digitale Signale (Ein-Ausschalten von Licht)
- Übertragungsrate ähnlich Koaxialkabel
  (im Gigabit-Bereich, potenziell noch besser)
- verwendet für Hochgeschwindigkeitsnetze und Fernnetze
- Totalreflektion
  von Lichtwellen verringert Verluste
- erfordert LED (*Light Emitting Diode* = Lichtdiode) oder Laser als Sender, Fotodiode als Empfänger

NACHBARSCHAFTSBEZIEHUNGEN (TOPOLOGIEN) IN NETZEN

Punkt-zu-Punkt-Verbindung

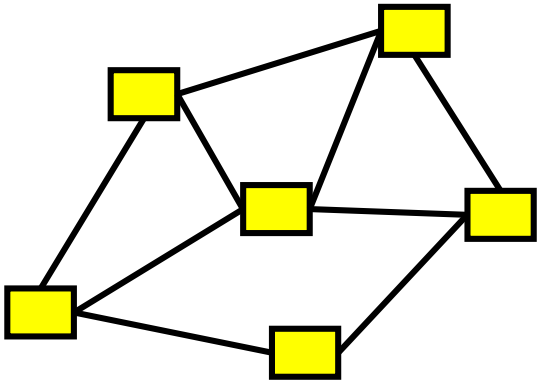
Beispiel: DSL



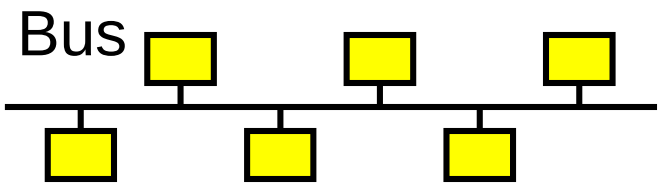


Beispiel: Heutiges LAN

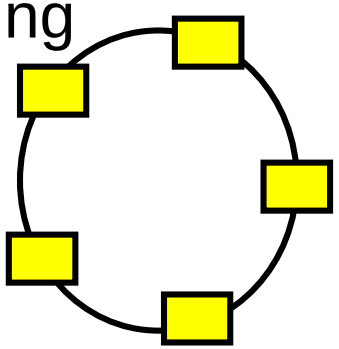
Vermaschtes Netz aus Punkt-zu-Punkt-Verbindungen



Beispiel: Internet-Backbone



Beispiel: Klassisches Ethernet-LAN



Netze lassen sich anhand ihrer Nachbarschaftsbeziehungen (Topologien) klassifizieren

STERN- UND BAUMVERKABELUNG MIT HUB ODER SWITCH

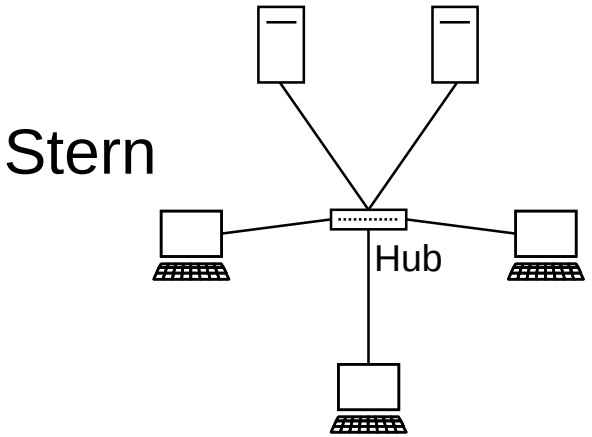
HOCHSCHULE DER MEDIEN

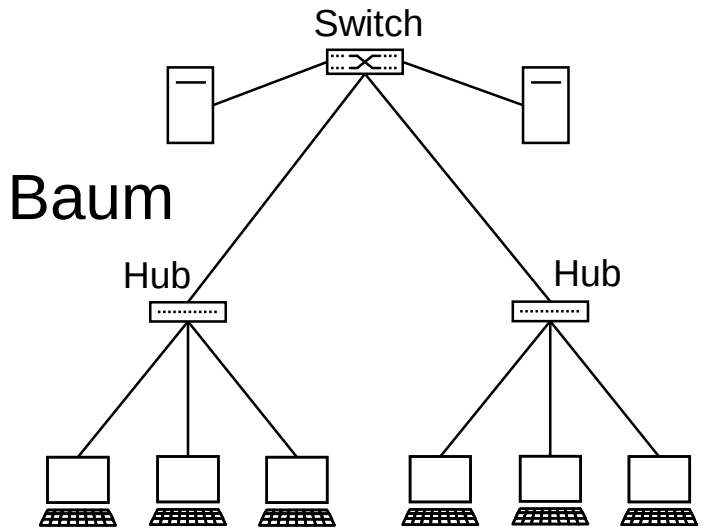
In LANs heute übliche Arten der Verkabelung:

- Stern: Im Zentrum steht ein Verteiler (Hub oder Switch)
- Baum: Unterverteilung über weitere Hubs oder Switches

Kabeltypen:

- Twisted-Pair-Kabel (max. Entfernung zum Verteiler 100m)
- Oder: Lichtwellenleiter (Glasfaserkabel, engl. “fiber”, max. Entfernung 2000m)

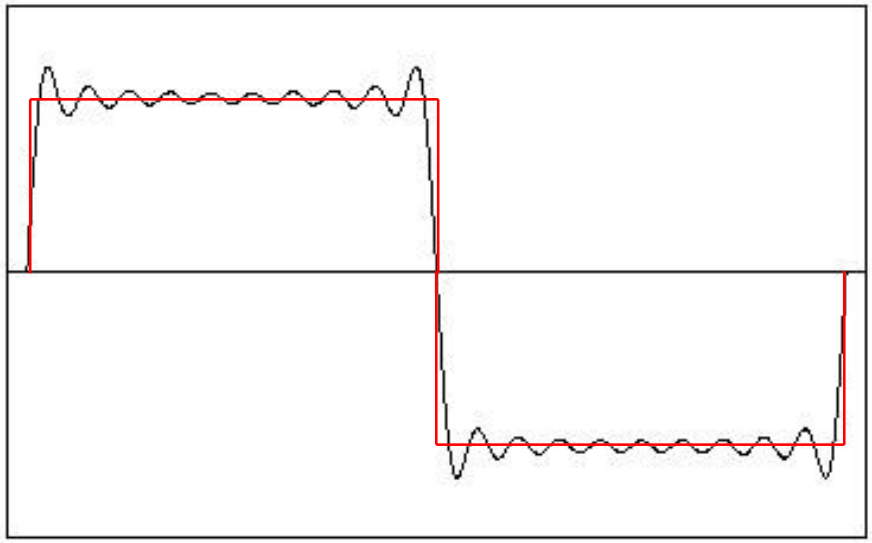


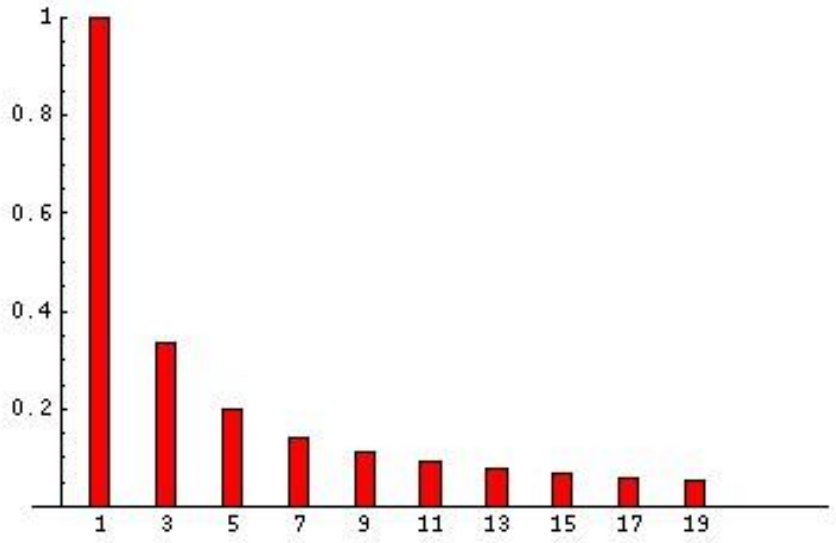


WANDLUNG DIGITALER SIGNALE IN ANALOGE SIGNALE

- Die direkte Übertragung digitaler Signale über elektrische Kabel hat Grenzen: Eine hohe Datenrate ist nur möglich bei geringer Kabellänge, längere Kabel funktionieren nur mit niedrigerer Datenrate. Gänzlich unmöglich ist die direkte Übertragung digitaler Signale über Funk.
  - ⇨ Ursache: Rechteckig geformte Signale enthalten hohe Frequenzanteile, d.h. zur originalgetreuen Übertragung ist eine hohe Bandbreite erforderlich.
- Deshalb wurden verschiedene Verfahren entwickelt, um digitale Signale ohne Informationsverlust in analoge Schwingungen mit möglichst geringer Bandbreite umzusetzen.
- Diese Verfahren werden als **Modulations**verfahren bezeichnet. Sie werden mit Hilfe elektronischer Geräte, so genannter **Modems** realisiert.

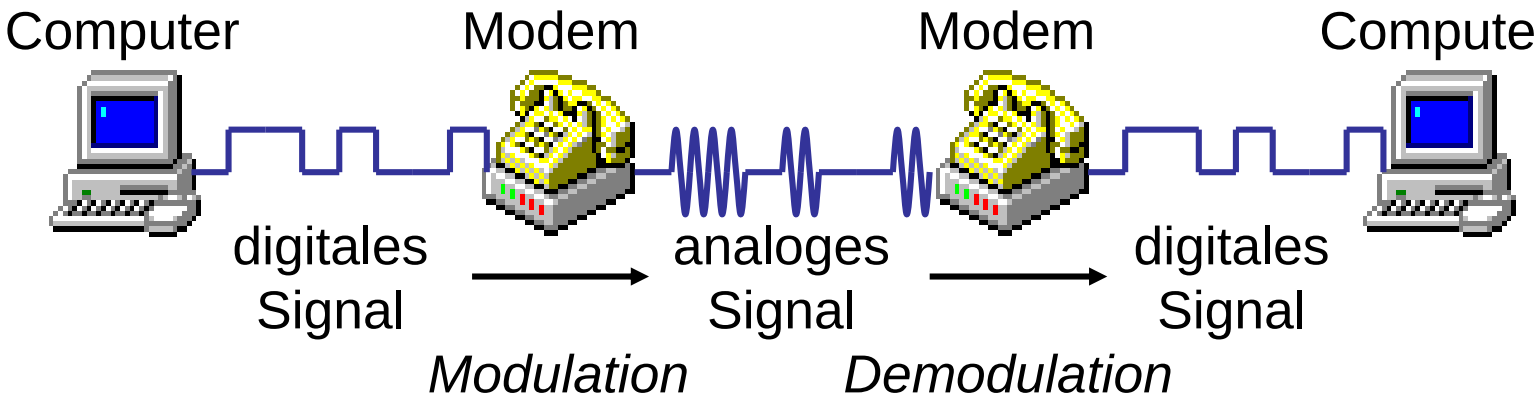
APPROXIMATION EINES RECHT-ECKSIGNALS DURCH SINUSKURVEN





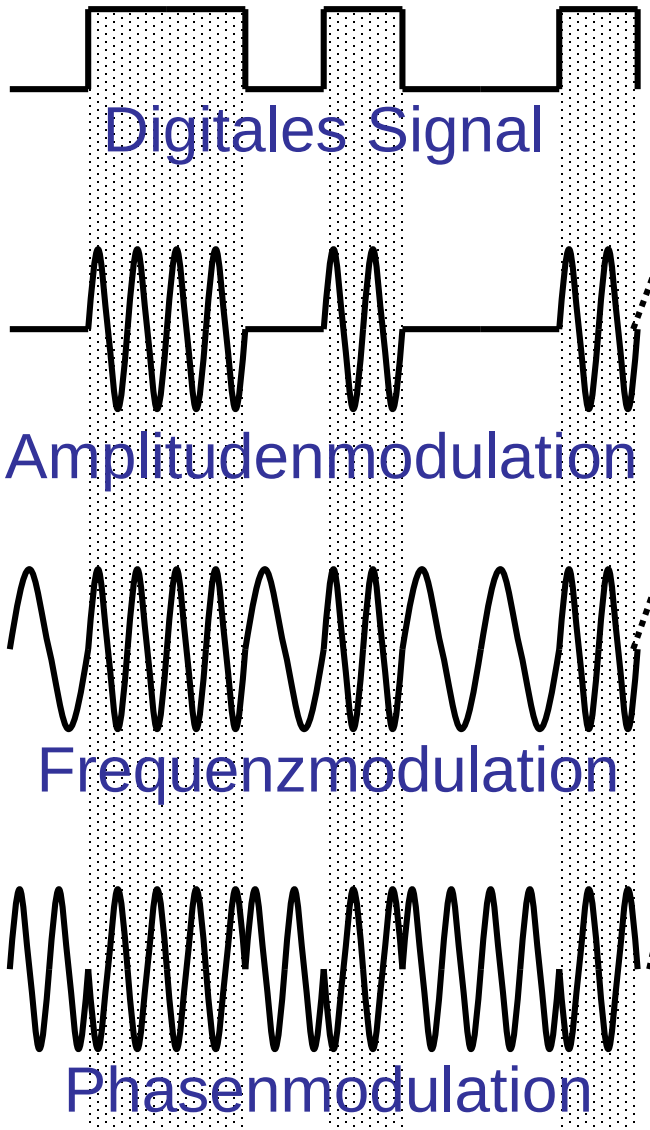
- Digitale Signale haben Rechteckform.
- Versucht man sie durch analoge Signale zu approximieren, werden Sinuskurven mit sehr hohen Frequenzen benötigt und die Rechteckform wird nur angenähert. (Im Beispiel oben werden Frequenzen bis zur 19. Oberschwingung genutzt.)
- D.h. die originalgetreue Übertragung digitaler Signale über analoge Kanäle benötigt sehr hohe Bandbreiten.

MODEMS



- **Modems** setzen digitale Signale in analoge mit demselben Informationsgehalt um (***Mo****dulation*) und wandeln diese wieder in die originalen digitalen Signale zurück (***Dem****odulation*).
- Modems ermöglichen dadurch die Übertragung von digitalen Signalen über längere analoge Leitungen:
  - ⇨ Klassisches Telefonmodem: bis zu 56 kbit/sec über das globale Telefonnetz
  - ⇨ DSL-Modem: bis zu 100MBit/sec über die „letzte Meile“ zur nächsten Vermittlungsstelle

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.

SHANNONS THEOREM

- Es besteht ein linearer Zusammenhang zwischen der Bandbreite eines analogen Kanals und der durch Modulation maximal erzielbaren Datenrate. Außerdem wird die Datenrate beeinflusst durch den Rauschabstand (= Signalstärke / Stärke des Rauschens).
- **Claude Shannon** fasste diesen Zusammenhang 1948 in folgendem Lehrsatz (**Shannons Theorem**) zusammen:
  Max. Datenrate = Bandbreite × $log_2(1 + Rauschabstand)$
- Moderne Modems nutzen Modulationsverfahren, die der maximalen Datenrate nach Shannons Theorem möglichst nahe kommen.

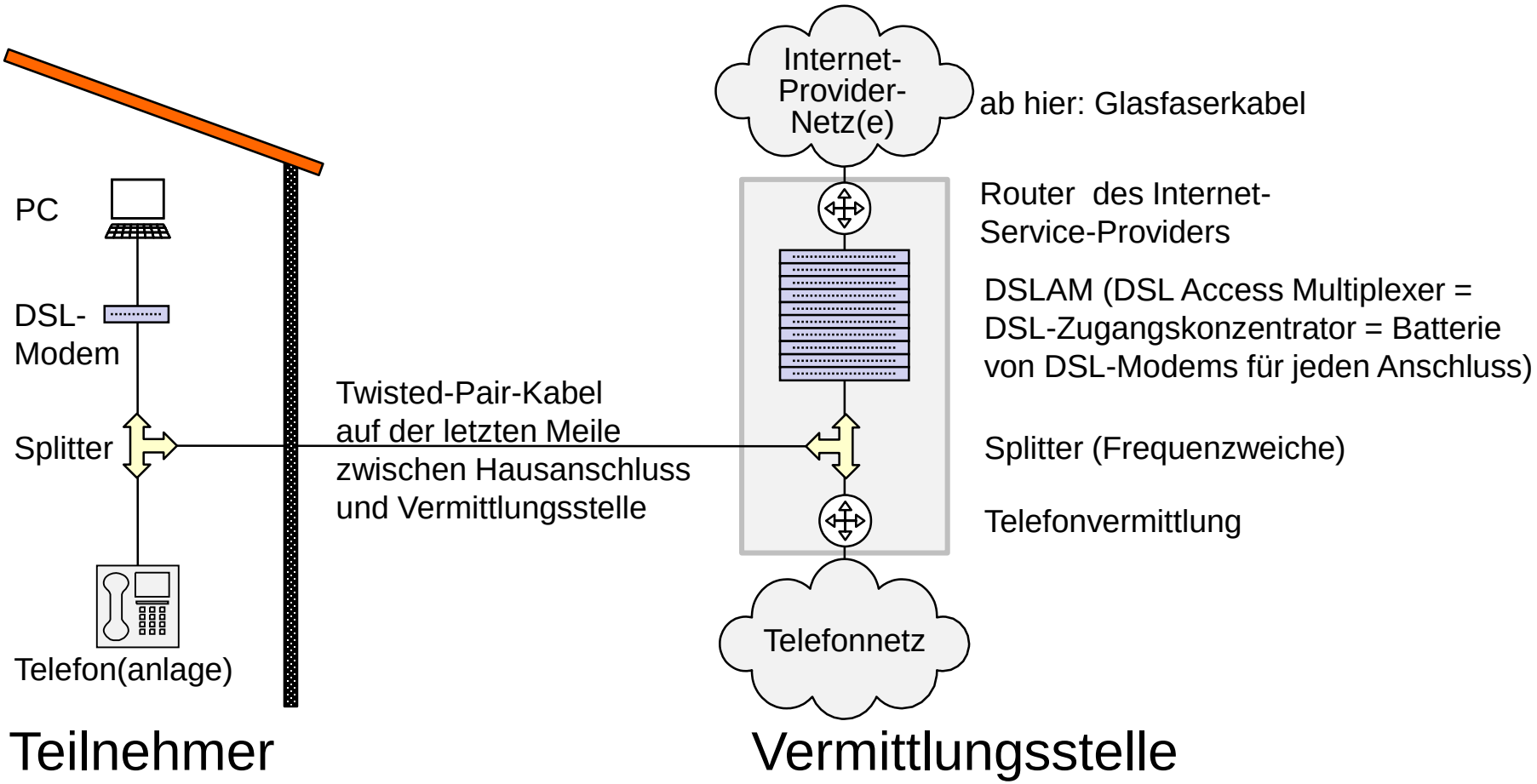
DIGITAL SUBSCRIBER LINE (DSL)

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

- Durch fortschrittliche Modulationstechniken kann die Zweidrahtverkabelung (Twisted Pair) eines bestehenden Telefonanschlusses auf der „letzten Meile“ zwischen Vermittlungsstelle und Hausanschluss verwendet werden.
- DSL kombiniert auf einem einzigen Kabelpaar
  - ⇨ einen Telefonkanal (analog oder digital = ISDN)
  - ⇨ einen digitalen Downstream-Kanal (typische Datenrate 2, 6, 16, 50, 100 Mbit/sec je nach Verfahren)
  - ⇨ einen digitalen Upstream-Kanal (typische Datenrate Faktor 2 bis Faktor 10 geringer als Downstream)
- Ein Splitter (Frequenzweiche) trennt die hochfrequenten Datenkanäle (Down- und Upstream) vom niederfrequenten Telefonkanal.

KLASSISCHES DSL-ANSCHLUSS-SCHEMA

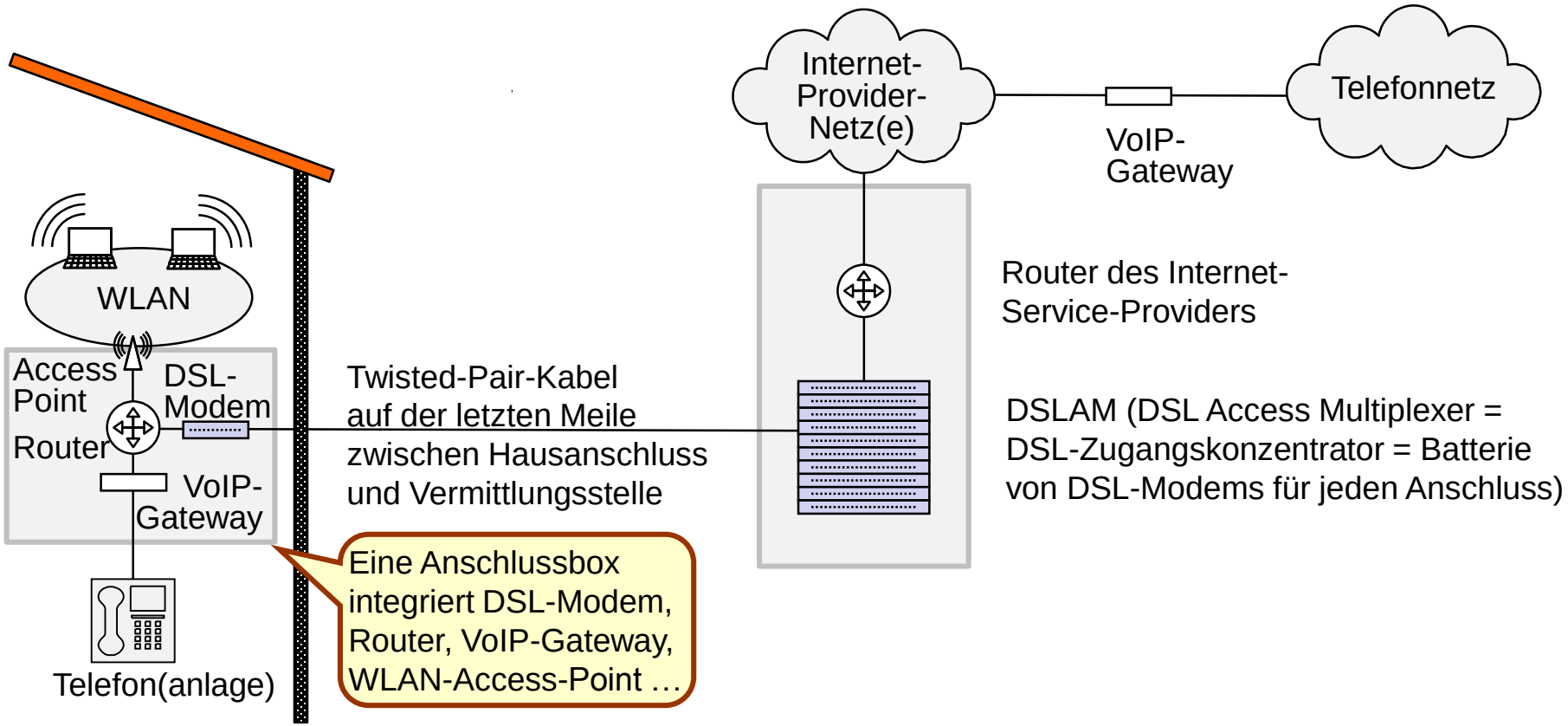
HOCHSCHULE DER MEDIEN



Klassisches Anschluss-Schema: Das Internet nutzt die Telefoninfrastruktur. Die hohen, unhörbaren Frequenzen werden durch den Splitter abgezweigt und für das DSL-Signal genutzt.

DSL-ANSCHLUSS-SCHEMA FÜR NGN-TELEFONIE

HOCHSCHULE DER MEDIEN



Modernes Anschluss-Schema für Next-Generation-Network(NGN)-Telefonie:
Das Telefon nutzt die Internet-Infrastruktur mittels Voice over IP (VoIP).
Kein physisches Telefonsignal auf der Leitung, kein Splitter mehr erforderlich.

ADSL UND VDSL

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

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

In jüngster Zeit werden sehr schnelle DSL-Varianten eingerichtet:

- **Very high speed Digital Subscriber Line (VDSL)**
- Typische Downstreamraten: 16, 50 oder gar 100 Mbit/sec
- Upstreamraten bis zu 40 Mbit/sec
- Nur möglich, falls die Kupferleitung des Hausanschlusses sehr kurz ist (wenige hundert Meter)
  - ⇨ Erfordert den Bau von neuen Vermittlungsstellen (Verteilerkästen) in der Nähe der Hausanschlüsse, ab dort geht es weiter über Glasfaser.

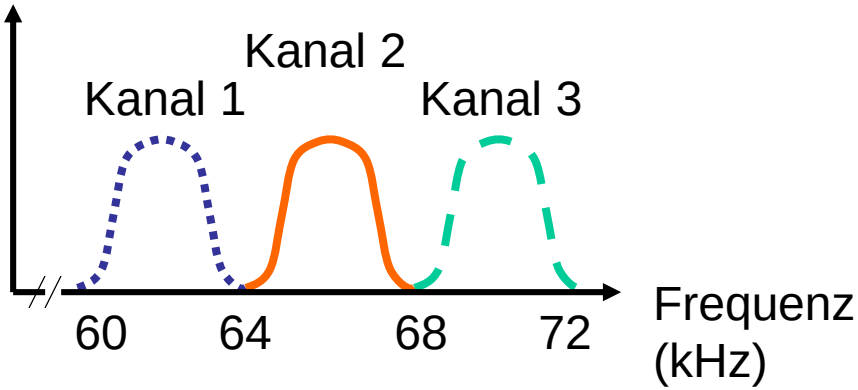
DSL VERSUS TELEFONMODEM

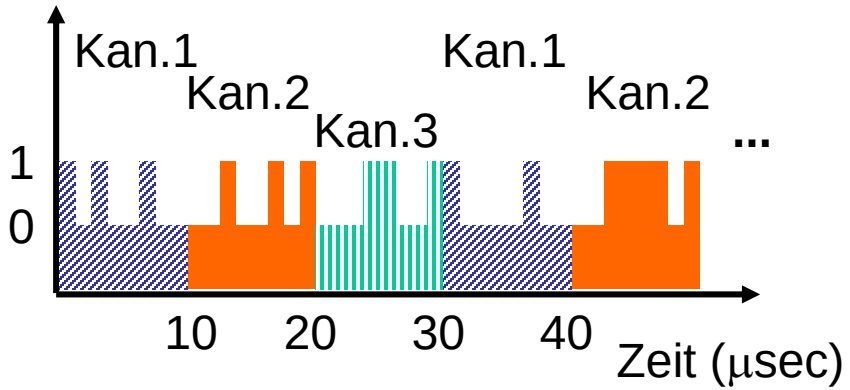
DSL und die Einwahl über ein klassisches Telefonmodem sind beides Modemübertragungen über den Telefonanschluss. Es gibt aber wesentliche Unterschiede:

- **DSL** nutzt von der Telefoninfrastruktur nur die „letzte Meile“ vom Hausanschluss bis zu einer Vermittlungsstelle; ab dort wird ein schnelles Glasfasernetz des Internet-Service-Providers benutzt.
  - ⇨ Durch fortschrittliche Modulationsverfahren lassen sich sehr hohe Datenraten (bis 100MBit/sec) erreichen.
- Ein klassisches **Telefonmodem** nutzt eine normale Telefon-Sprachverbindung zwischen dem privaten Telefonanschluss und dem Telefonanschluss eines Internet-Providers.
  - ⇨ Die Übertragung über das Telefonnetz ist aber analog auf 4000Hz und digital auf 56 (im Einzelfall 64) kBit/sec beschränkt, daher lassen sich keine höheren Datenraten als 56 kBit/sec erreichen.

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

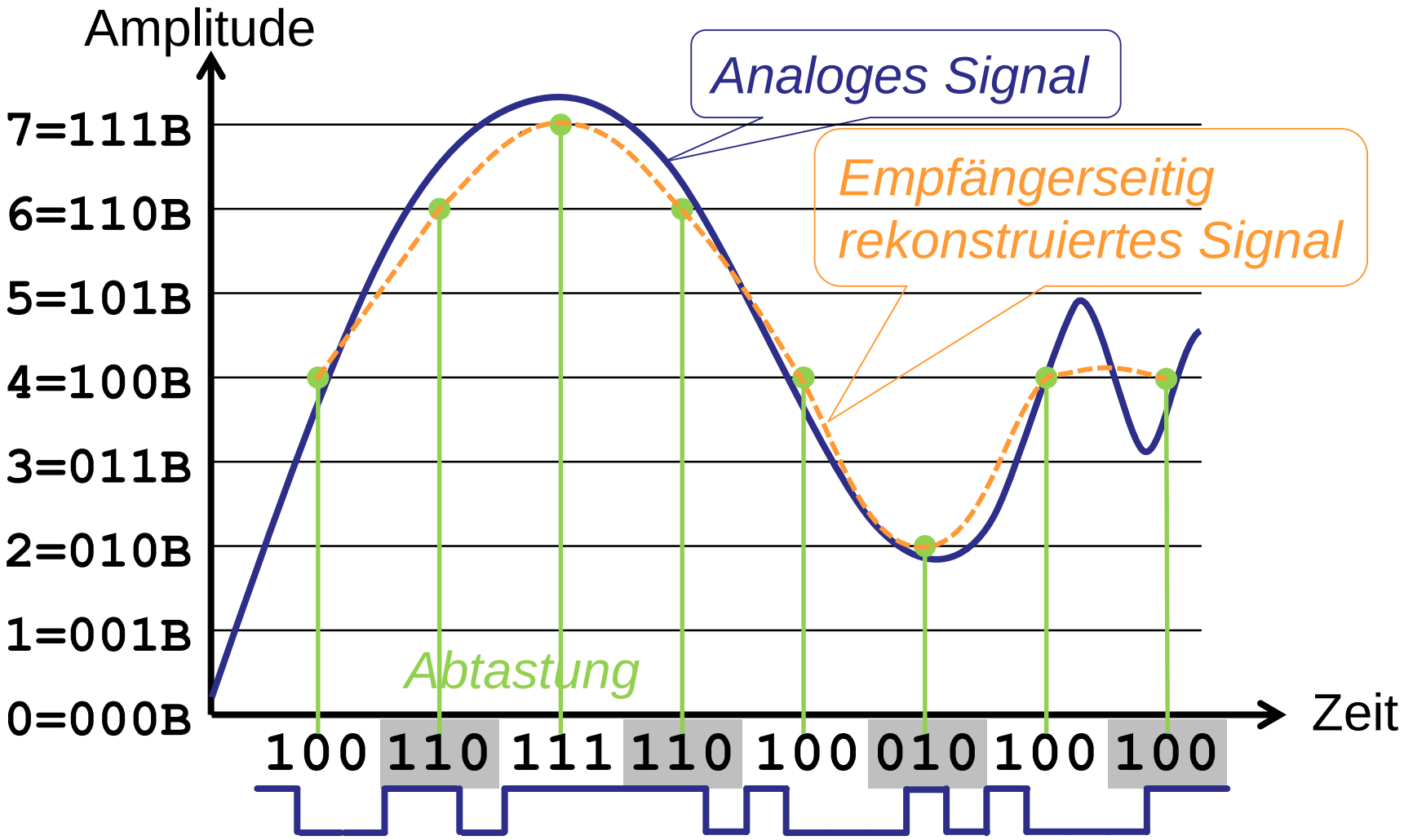
(Abk.: TDM=time division multiplexing): Die logischen Kanäle erhalten abwechselnd nacheinander Zugriff auf den physikalischen Kommunikationskanal. Geeignet für **digitale** Kanäle.

ZEITMULTIPLEXVERFAHREN IN DER TELEFONIE

- Das Zeitmultiplexverfahren wird gerne verwendet, um in der klassischen Telefonie viele Gespräche gleichzeitig auf einer einzigen Glasfaserleitung zu übertragen.
- Dies 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)

HOCHSCHULE DER MEDIEN



Im 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.

TEIL 2: SICHERUNGSSCHICHT IM SUBNETZ (DATA LINK LAYER)

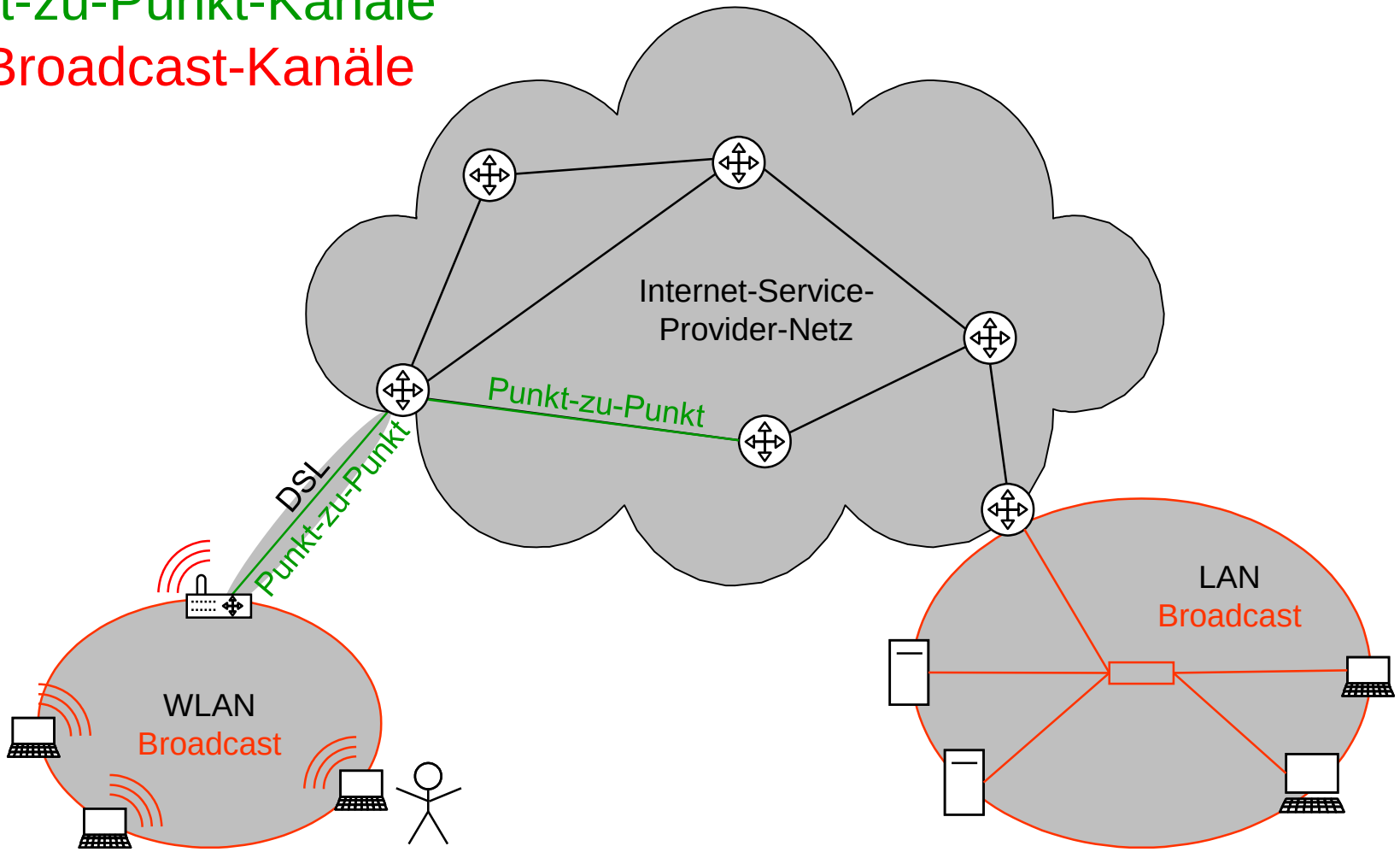
Die Sicherungsschicht ist eine Software, die regelt, wie zwei **benachbarte** Computer miteinander kommunizieren. Es lassen sich zwei Arten von Übertragungskanälen unterscheiden:

- **Punkt-zu-Punkt-Kanäle** verbinden genau **zwei Stationen** im Netz miteinander. Beispiele:
  - ⇨ Langstreckenverbindung zwischen zwei benachbarten Routern im Netz eines Internet Service Providers
  - ⇨ Einwahlverbindung zwischen einem Computer und dem Einwahlknoten (Router) eines Internet-Service-Providers über Analogmodem oder DSL.
- **Broadcast-Kanäle** (engl. *broadcast* = Rundfunk) verbinden **eine Gruppe von Stationen** im Netz miteinander. Ein solches Netz nennt man auch **Broadcastnetz**. Beispiele:
  - ⇨ LAN (Local Area Network) auf Basis Ethernet
  - ⇨ WLAN (Wireless LAN)

ÜBERTRAGUNGSDIENSTE DER SICHERUNGSSCHICHT (EBENE 2)

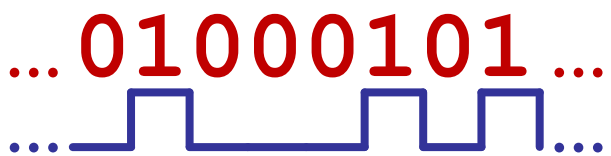
HOCHSCHULE DER MEDIEN

Punkt-zu-Punkt-Kanäle
und Broadcast-Kanäle



RAHMEN (FRAMES)

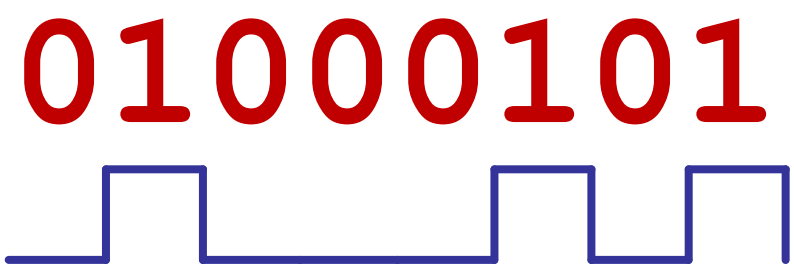
- Auf der Sicherungsschicht werden Daten in Form von so genannten Rahmen (engl. „Frames“) übertragen.
- Rahmen = Folgen von Bits
- Die Bits werden in der Regel seriell, d.h. nacheinander als Bitstrom über eine einzige Leitung übertragen.



- Die Bits werden durch Spannungsstufen kodiert, z.B. 0 = niedrige Spannung, 1 = hohe Spannung.
- Rahmen bestehen aus
  - ⇨ Steuerungsdaten (z.B. Anfangskennung, Endekennung, Adressen, Bezeichnung des angeforderten Dienstes …)
  - ⇨ sowie Nutzdaten (eigentlich zu übertragende Daten).

DIGITALE ÜBERTRAGUNG VON DATEN IN RAHMEN

- Zahlen und Texte werden binär (im Zweier-System) dargestellt (als Folge von Bits = Nullen und Einsen)



  - ⇨ Beispiel:

69 (dezimal)

= 64 +4 +1

= 0*2⁷ + 1*2⁶ + 0*2⁵ + 0*2⁴ + 0*2³ + 1*2² + 0*2¹ + 1*2⁰

= 01000101B (binär)

- Die Bits, d.h. die Nullen und Einsen werden als Spannungsniveaus kodiert, z.B. so: 
- Buchstaben lassen sich als Zahlen (und damit auch als Bits) darstellen, z.B. in den Codes ASCII oder UTF-8:

… **+ = 53, , = 54, - = 55, . = 56** …

… **A = 65, B = 66, C = 67, D = 68, E = 69,** … **Z = 90** …

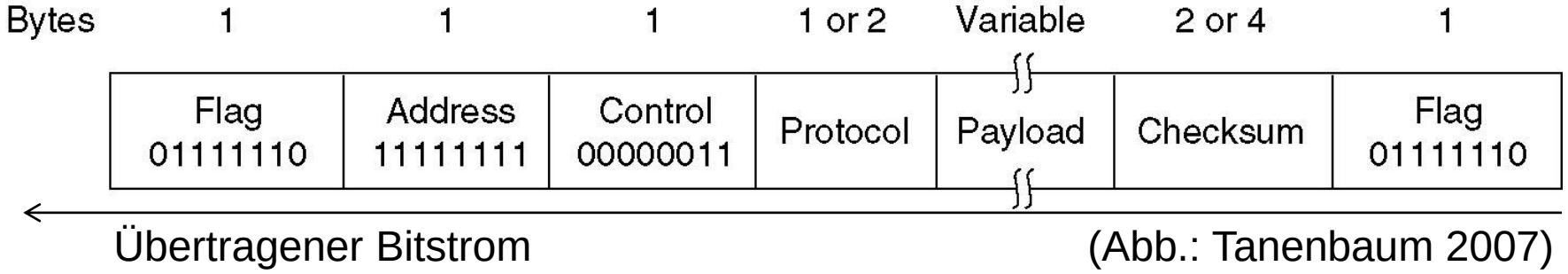
PUNKT-ZU-PUNKT-KANÄLE: BEISPIEL: PPP

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
- Strukturierung der zu übertragenden Daten in Form von „Rahmen“.
- 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

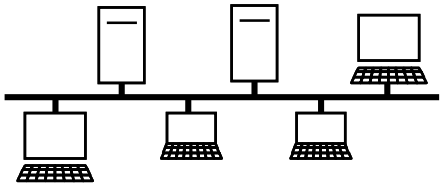


(Abb.: Tanenbaum 2007)

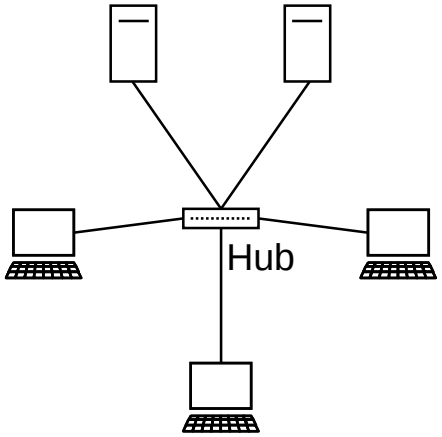
BROADCAST-KANÄLE: BEISPIEL ETHERNET-LAN

Das Ethernet (heute gängige LAN-Technik) ist ein Beispiel für ein Broadcastnetz: Mehrere (alle) Stationen nutzen dasselbe Übertragungsmedium als so genannten Broadcast-Kanal.

- 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, genannt Media Access Control (MAC) ist erforderlich.

CSMA/CD: MEDIA ACCESS CONTROL FÜR ETHERNET-LANS

Das Protokoll **CSMA/CD** (Carrier Sense Multiple Access Collision Detect) dient zur Media Access Control für Ethernet-LANs:

- **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.

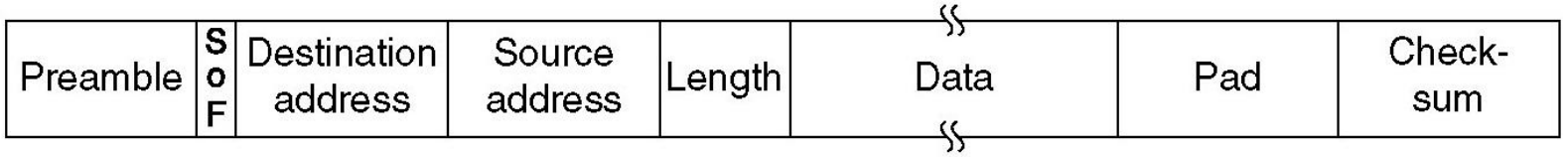
Verfahren genormt durch IEEE 802.3 / ISO 8802.3

IEEE: Institute of Electrical and Electronics Engineers
ISO: International Organization for Standardization

MAC-ADRESSEN

- Bei der Übertragung von Daten in Broadcastnetzen muss die Zielstation spezifiziert werden.
- In LANs, WLANs geschieht das i.d.R. mit Hilfe so genannter MAC-Adressen. Jedes Netzwerkinterface hat eine weltweit eindeutige **MAC-Adresse**.
- MAC-Adressen bestehen aus 6 Bytes. Beispiel für eine MAC-Adresse: **`00-1d-19-59-5c-9b`**
- Die Bytes der MAC-Adressen werde typischerweise im Hexadezimalsystem angegeben, mit Hilfe der 16 Hexziffern **`0`**, **`1`**, **`2`**, **`3`**, **`4`**, **`5`**, **`6`**, **`7`**, **`8`**, **`9`**, **`a`** (=**`10`**), **`b`** (=**`11`**), **`c`**, **`d`**, **`e`**, **`f`** (=**`15`**)
  - ⇨ Beispiel:
    `9b H` (hexadezimal) =
    $9*16^1 + 11*16^0 = 144 + 11 = 155$ **(dezimal)**

FORMAT VON ETHERNET-RAHMEN („FRAMES“) 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 MAC-Adressen der Netzwerkkarten von Ziel- und Ausgangsstation

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

Data: zu übertragende Nutzdaten

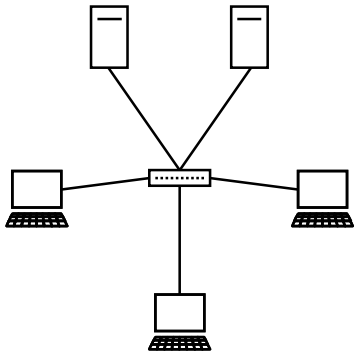
Pad: ggf. Füllzeichen auf die minimale Frame-Länge

Checksum: Prüfcode zur Fehlererkennung (4 Bytes)

ARTEN VON VERTEILERN: HUBS UND SWITCHES

Es gibt zwei Arten von Verteilern in Ethernets:

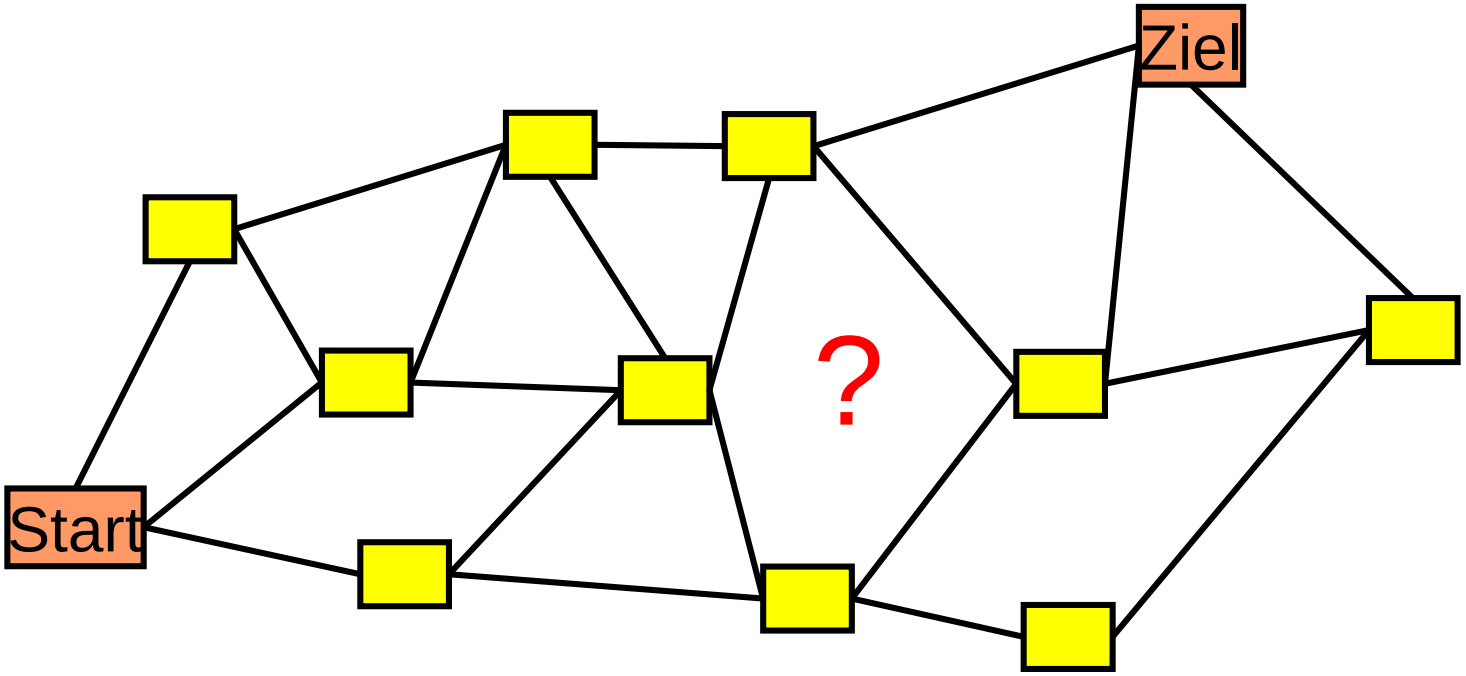
- **Hubs** („Naben“) sind im einfachsten Fall elektrische Verstärker (Repeater) für die Signale und unterstützen nur eine Datenübertragung zu einem Zeitpunkt. Die Geschwindigkeit des Netzes teilt sich auf die Teilnehmer auf. Hubs arbeiten auf der Ebene 1 (Bitübertragungsschicht).



- **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 interpretieren die Ethernet-Frames (lesen z.B. die Zieladresse) und arbeiten daher auf der Ebene 2 (Sicherungsschicht).

TEIL 3: VERMITTLUNGSSCHICHT DES INTERNET (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)
- Im Internet übernimmt diese Aufgabe der Dienst IP (= Internet Protocol nach dem zugrundeliegenden Protokoll),

ZIELE DER DIENSTE DER VERMITTLUNGSSCHICHT

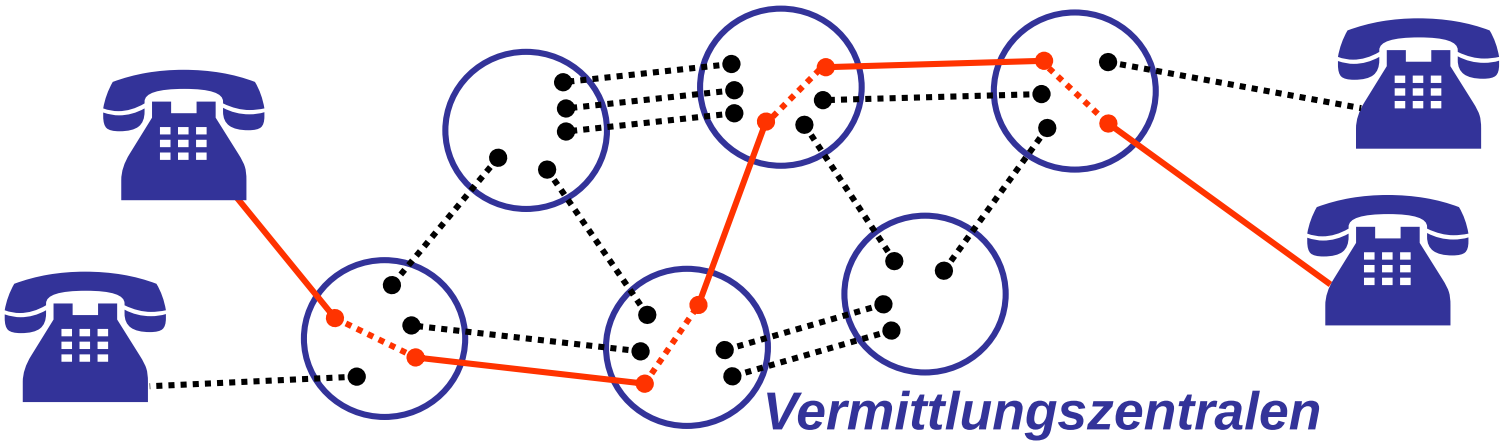
- Die Dienste sollen unabhängig von der Topologie des Subnetzes sein
- Die nächsthöhere Schicht, die Transportschicht, muss von der Anzahl, der Art, und der Topologie der vorhandenen Subnetze abgeschirmt werden
- Die für die Transportschicht vorgesehenen Netzadressen müssen ein einheitliches Nummerierungsschema 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.

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)
- **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.

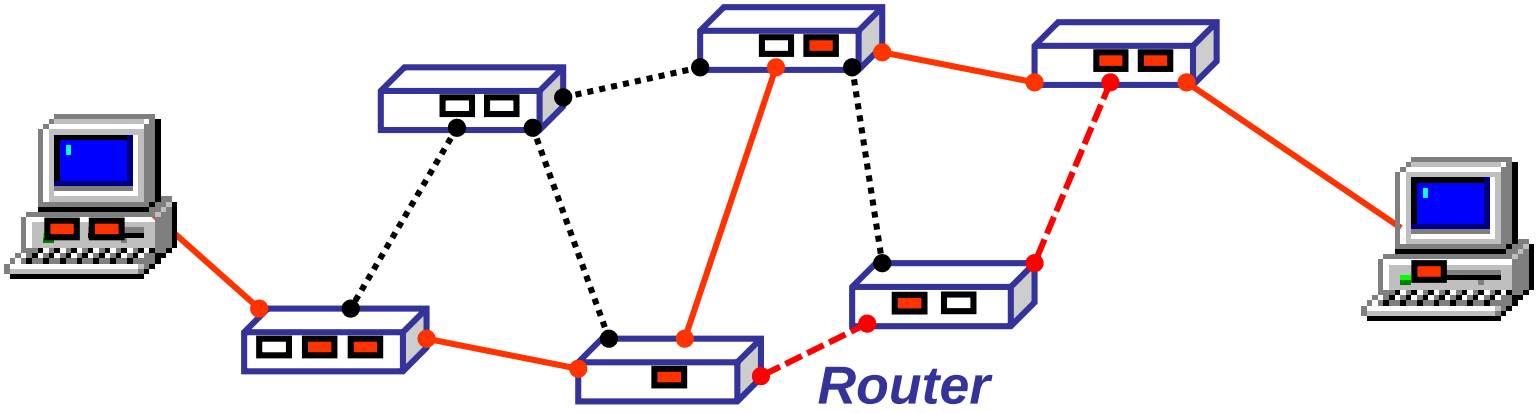
KLASSISCHE TELEFON-VERMITTLUNGSZENTRALE

Telefonvermittlungszentrale Montreal / Montreal telephone exchange (c. 1895)
Various photographers for Cassell & Co. - The Queen's Empire. Volume 3. Cassell & Co. London
Zugriff am 20.10.2015 unter https://en.wikipedia.org/wiki/File:Telephone_exchange_Montreal_QE3_33.jpg

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
Zeitpunkt möglicher Überlastungen	Beim Verbin-dungsaufbau	Bei jedem Paket
Gebührenberechnung	Pro Minute	Pro Paket

(nach Tanenbaum/Wetherall, 2012, Abb. 2.44)

ROUTING UND ROUTER

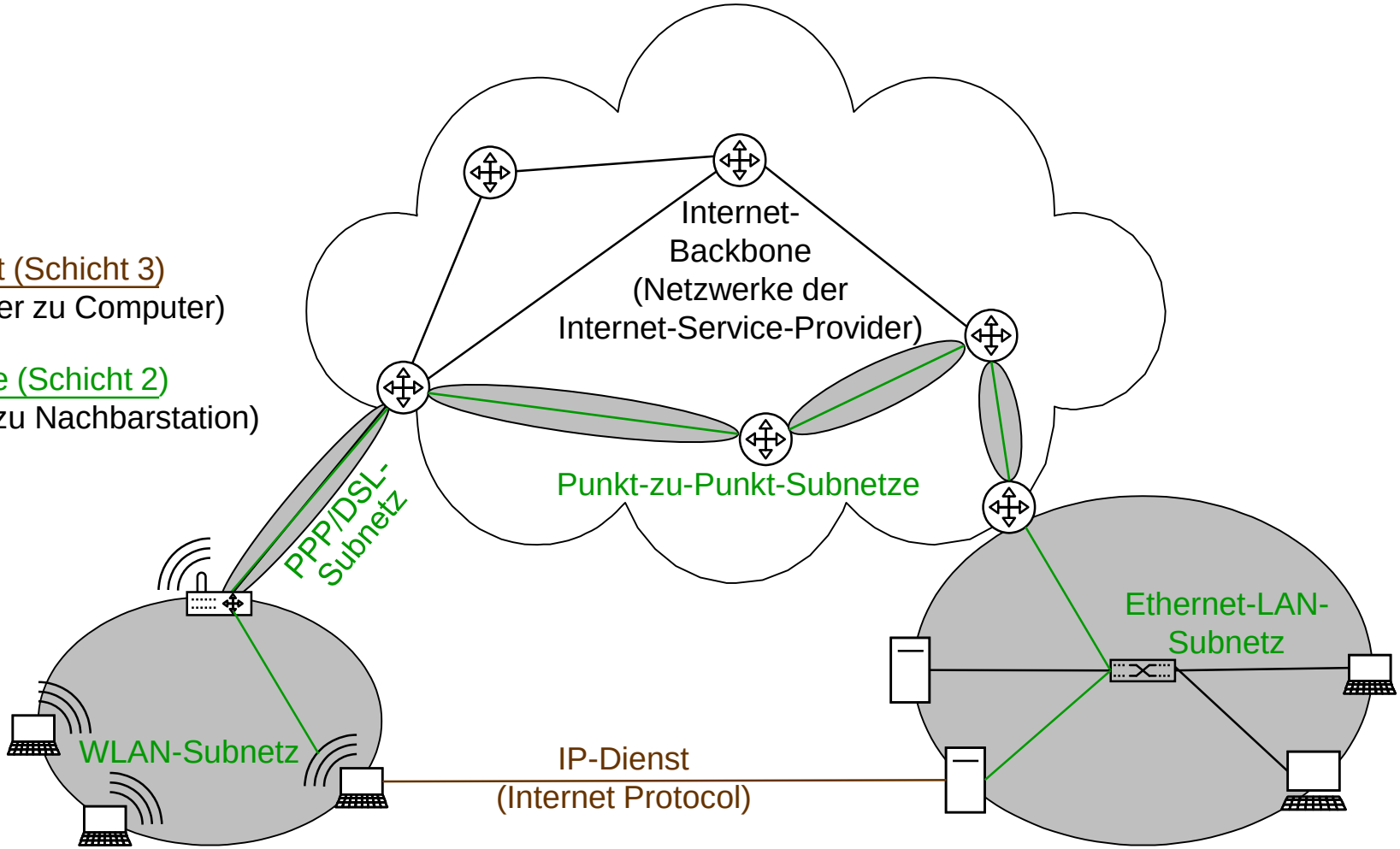
- **Routing**: Weitervermitteln von Daten in einem Netz auf der möglichst günstigsten Route auf eine möglichst günstige Weise. Hierzu gibt es sog. **Routingalgorithmen**.
- Das Routing wird im Wesentlichen von sogenannten **Routern** übernommen, speziellen Vermittlungscomputern, auf denen die Routingalgorithmen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

DAS INTERNET ALS VERBUNDNETZ HETEROGENER SUBNETZE

HOCHSCHULE DER MEDIEN

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

Subnetze (Schicht 2)
(Station zu Nachbarstation)

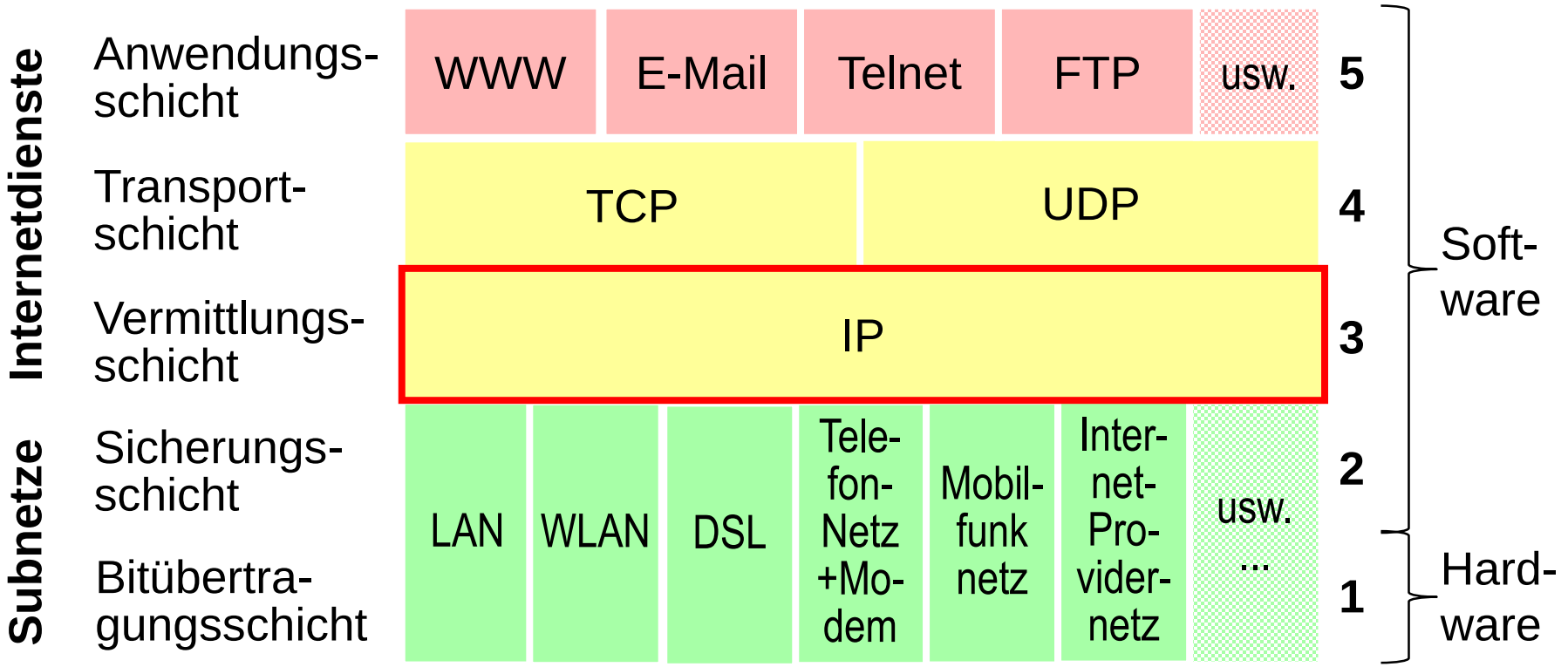


DIE VERMITTLUNGSSCHICHT IM INTERNET

- Das Internet ist ein Verbundnetz, das sich aus unterschiedlichen „Subnetzen“ zusammensetzt, z.B.:
  - ⇨ Lokale Netze: z.B. vom Typ Ethernet oder WLAN
  - ⇨ Internet-Zugangsnetze (z.B. DSL, Kabelnetze, 3G/4G)
  - ⇨ Backbone-Netze (Netze der Internetprovider)
  - ⇨ Intranets (firmeninterne Netze)
- Jede Art von Subnetz hat eigene Vorgaben für die Gestaltung von Schicht 2 (Bitübertragungsschicht) und 1 (Sicherungsschicht). Das Internet schränkt diese nicht ein.
- Die Vermittlungsschicht (Schicht 3) des Internet (d.h. der Dienst IP) verknüpft diese Subnetze und stellt für die Schicht 4 (Transportschicht) eine einheitliche Schnittstelle bereit.
- So funktionieren die Internetdienste der Schichten 3-5 nach oben hin global einheitlich, unabhängig vom zugrundeliegenden Subnetz.

IP: DER INTERNET-VERMITTLUNGSDIENST

HOCHSCHULE DER MEDIEN



Die unteren zwei Netzwerkschichten (1+2) sind gegeben durch beliebige Übertragungseinrichtungen, die so genannten Subnetze.
Der Dienst IP verknüpft diese Subnetze und stellt nach oben hin für die Transportschicht eine einheitliche Schnittstelle bereit.

IP: EIN VERBINDUNGSLOSER VERMITTLUNGSDIENST

- IP (Internet-Protocol) ist der Vermittlungsdienst des Internet.
- IP ist verbindungslos.
- IP ist paketvermittelt, versandt werden Datengramme, auch Pakete genannt.
- Es wird über eine 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).
- Versionen
  - ⇨ Zurzeit noch weitgehend verwendet: IPV4 (= Version 4)
  - ⇨ Künftig (zurzeit in Einführung): IPV6 (= Version 6)

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

HOCHSCHULE DER MEDIEN

IP-Datengramme (Pakete) bestehen aus Kopfteil (Header) und Textteil (Nutzdaten). 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.

HIERARCHISCHES ROUTING

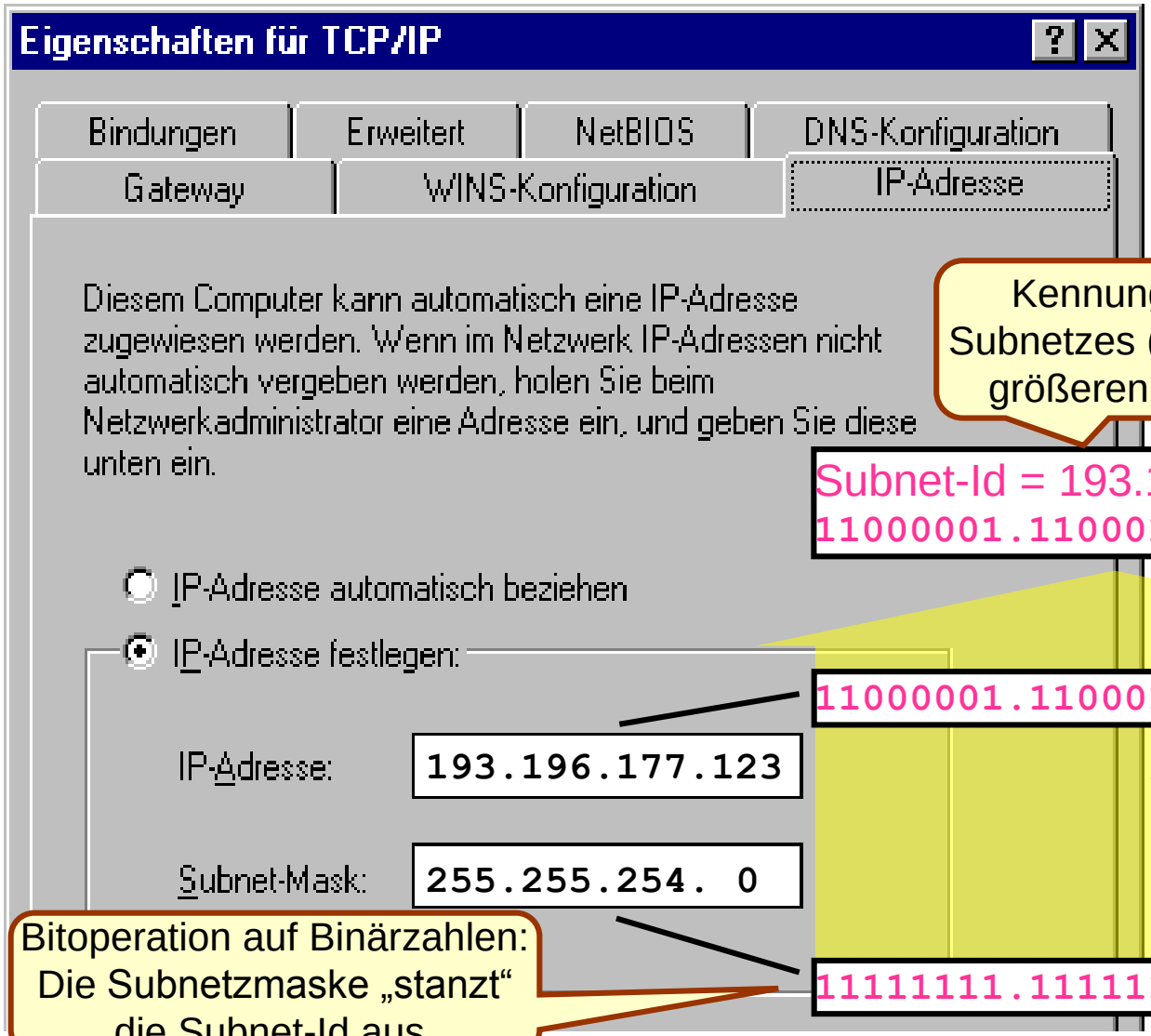
- Die Datenbasis der Router würde sehr groß, wenn darin alle möglichen Zielstationen aufgeführt würden.
- Abhilfe: Hierarchisches Routing
  - ⇨ Nahe beieinander liegende Stationen werden in „Regionen“ zusammengefasst.
  - ⇨ In den Routing-Tabellen stehen im Wesentlichen nur noch diese Regionen und die 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 (oder Zusammenfassungen von Subnetzen) verwendet.

HIERARCHISCHES ROUTING IM INTERNET ÜBER DIE SUBNET-ID

- IP-Adressen bestehen aus zwei Teilen, der Subnet-Id (die „Vorwahl“, identifiziert das Subnetz) und der Host-Id („Rufnummer“, 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 Subnetze (oder größere Regionen) zerlegen (jeweils 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.

AUFTEILUNG VON INTERNET-ADRESSEN MIT SUBNETZMASKE

HOCHSCHULE DER MEDIEN



Kennung eines Computers im Subnetz bzw. in der Region

Host-Id = 379 = 1.01111011

Kennung eines Subnetzes (oder einer größeren Region)

Subnet-Id = 193.196.176.0 = 11000001.11000100.10110000.00000000

11000001.11000100.10110001.01111011

Network *Host*

11111111.11111111.11111110.00000000

Bitoperation auf Binärzahlen: Die Subnetzmaske „stanzt“ die Subnet-Id aus.

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	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.

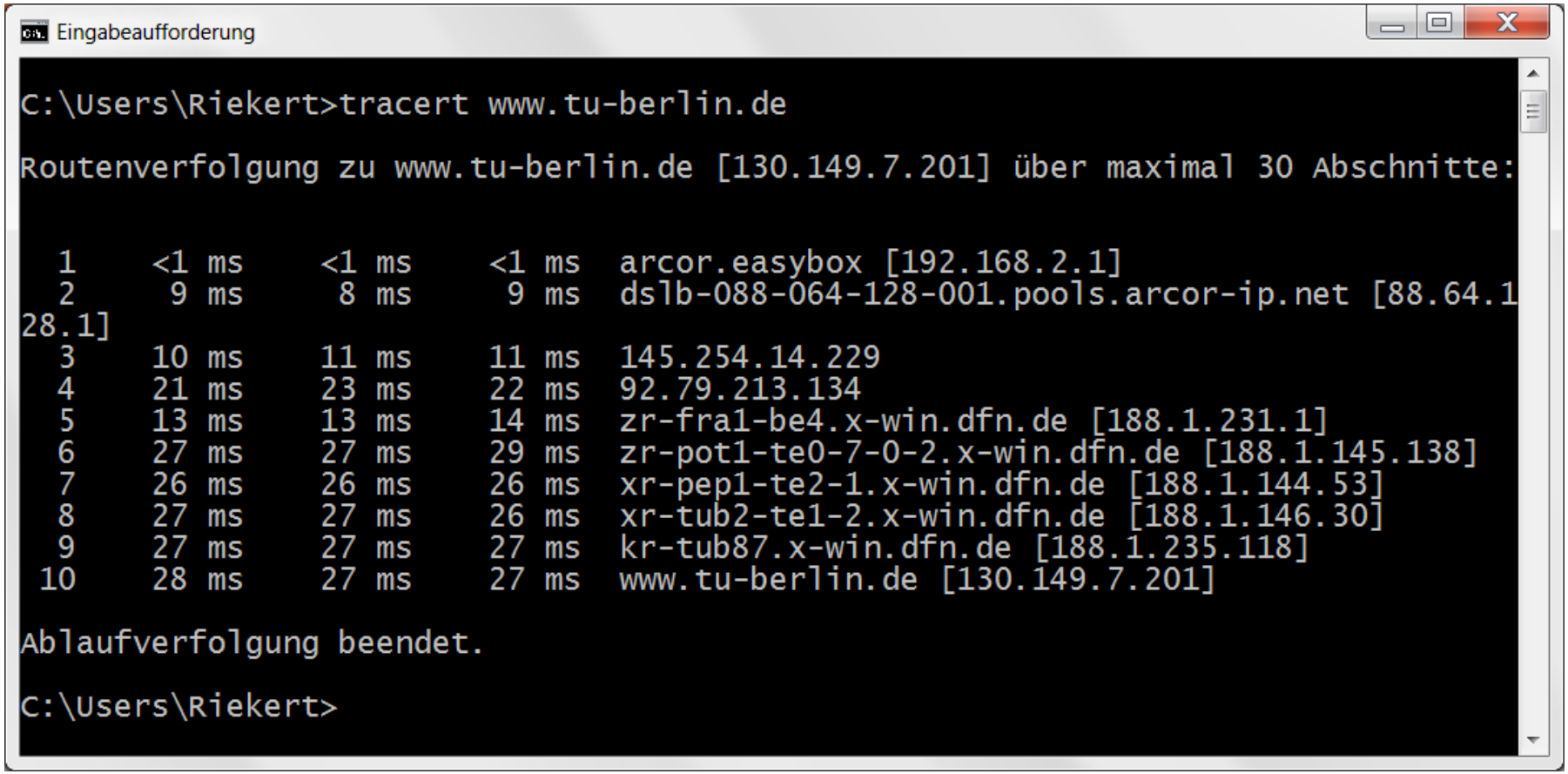
Automatische private IP-Adressen-Vergabe:

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

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

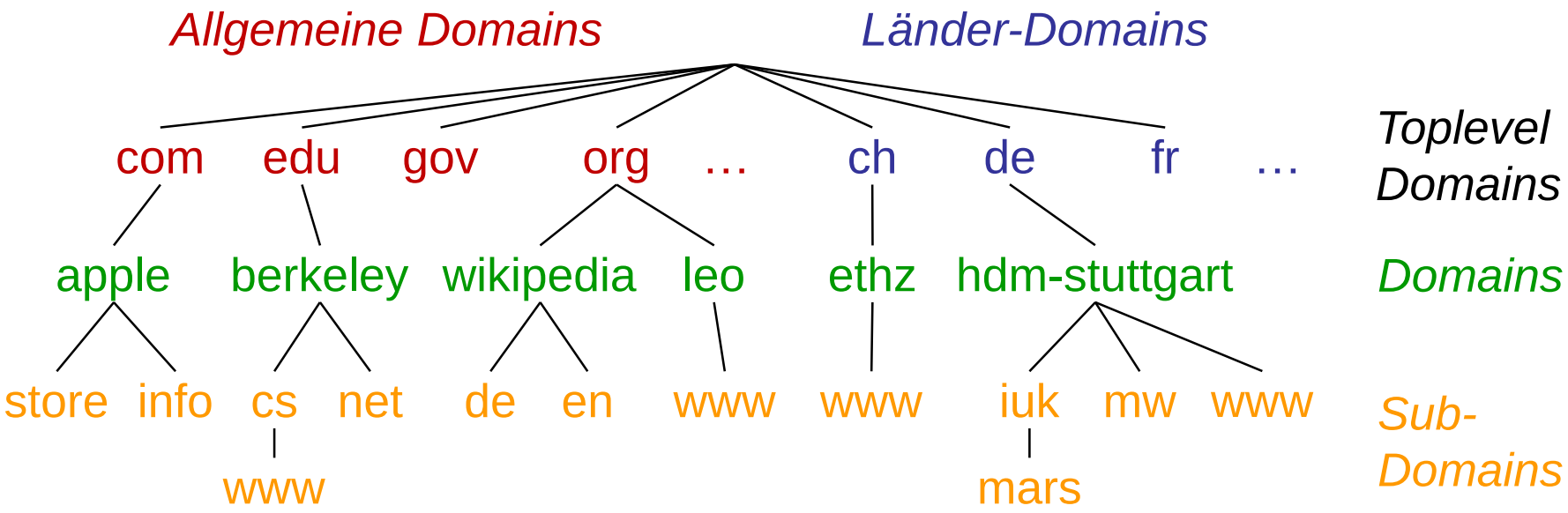
HOCHSCHULE DER MEDIEN

- **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.

DNS (DOMAIN NAME SYSTEM)

- Jeder Host (Computer im Internet) ist eindeutig identifiziert durch eine IP-Adresse, d.h. eine Reihe von Zahlen.
- Das DNS (Domain Name System) gibt es, weil Menschen sich Namen leichter merken können als Zahlen.
  - ⇨ hdm-stuttgart.de ist leichter zu merken als die IP-Nummer 141.62.1.25.
- Domänenname (Domain Name): Der alphanumerische, für die menschliche Benutzung bestimmte Name, der einen Computer im Internet eindeutig identifiziert
- Technisch gesehen stehen Domain Names für IP-Adressen.
- Das DNS ist ein System aus Servern im Internet, die mithilfe von Datenbanken die Domänennamen in die zugehörigen IP-Adressen übersetzen und umgekehrt.

DNS (DOMAIN NAME SYSTEM)



- Domain Name System: Hierarchisches System zur Benennung von Computern (sog. „Hosts“) im Internet
- Notation der Namen „von unten nach oben“, z.B. www.cs.berkeley.edu, mars.iuk.hdm-stuttgart.de usw.

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
    - Stets 64 Bit: Keine Subnetzmaske erforderlich
    - Kann allen Kunden 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)

BESTIMMUNG VON MAC-ADRESSEN AUS DER IP-ADRESSE

Für die Kommunikation mit anderen Hosts oder dem Gateway in einem Broadcastnetz muss die IP-Schicht IP-Adressen in Adressen der Sicherungsschicht konvertieren, das sind meist MAC-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)**

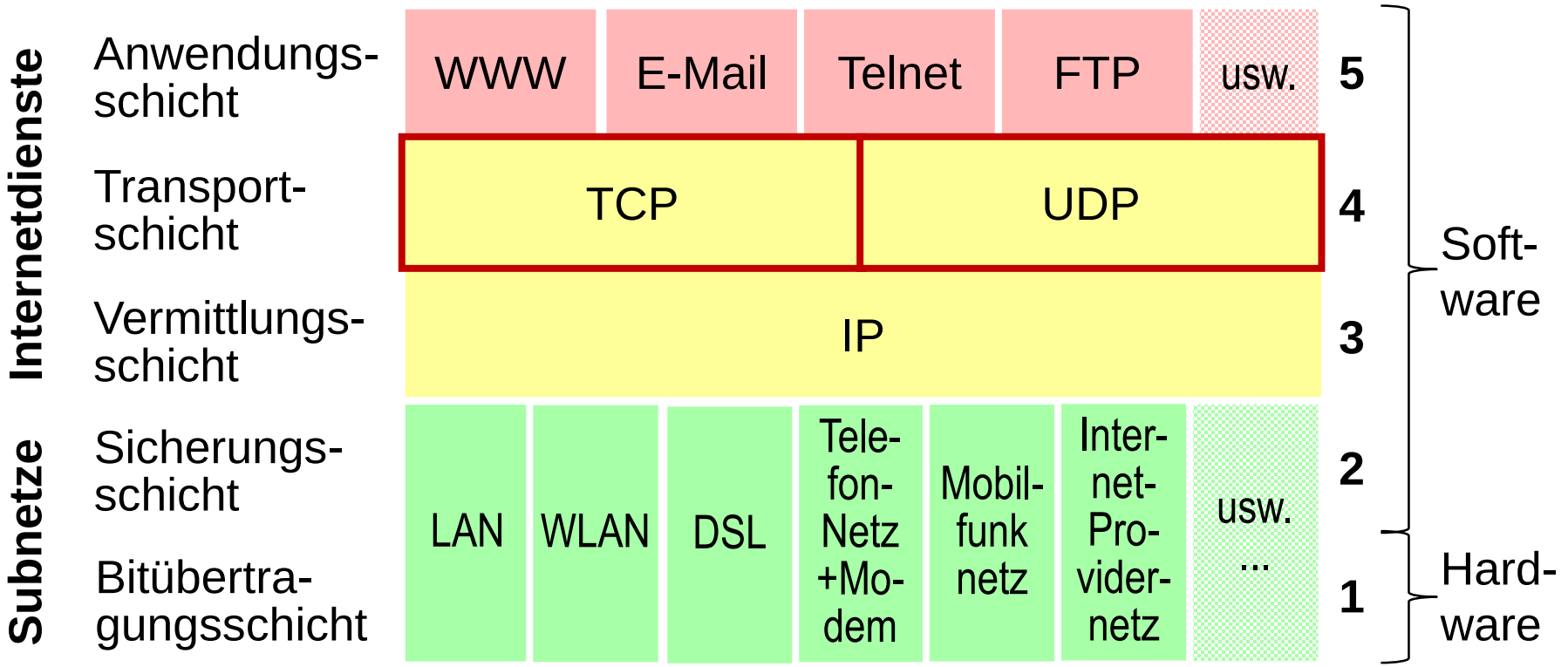
TEIL 4: TRANSPORTSCHICHT IM INTERNET (TRANSPORT LAYER)

HOCHSCHULE DER MEDIEN

- 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

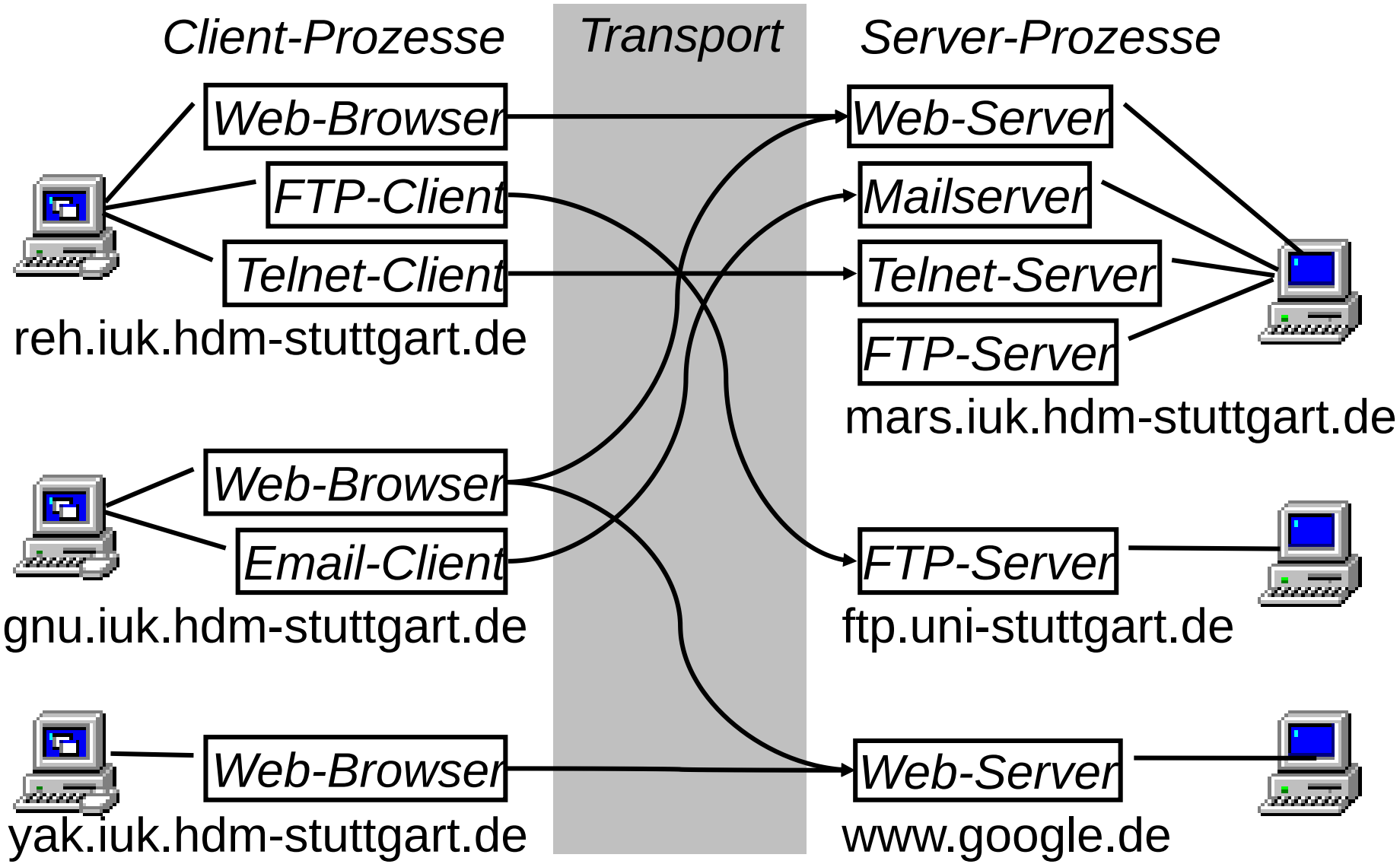
INTERNET-TRANSPORTDIENSTE
TCP UND UDP

HOCHSCHULE DER MEDIEN



Die Transportschicht überträgt Daten zwischen den Prozessen der Internet-Anwendungsschicht. Sie nutzt IP, den Übertragungsdienst der Vermittlungsschicht, über eine hardwareunabhängige, global einheitliche Schnittstelle.

TRANSPORTSCHICHT: KOMMUNI-KATION ZWISCHEN PROZESSEN

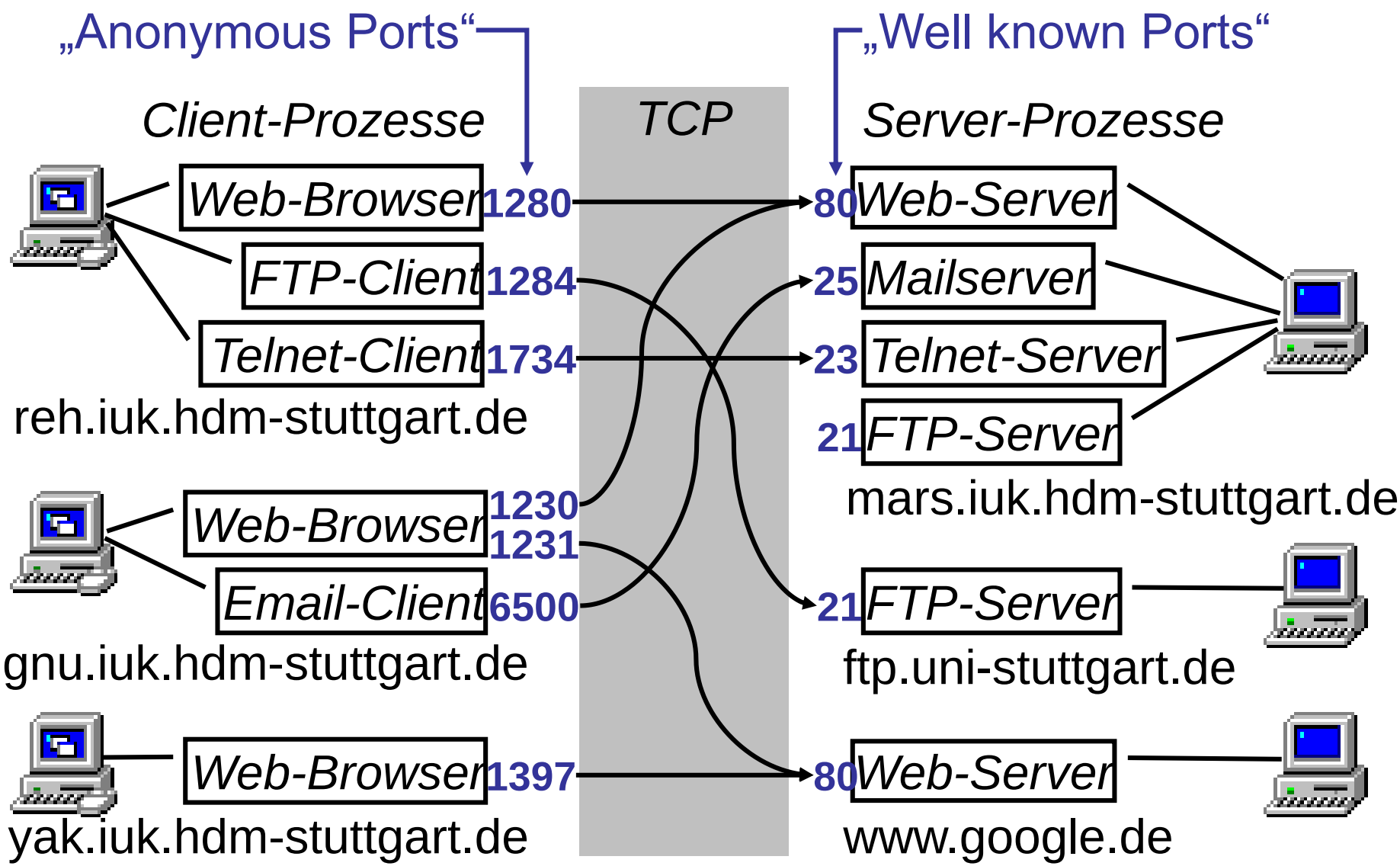


TRANSMISSION CONTROL PROTOCOL (TCP)

- Internet-Dienst der Transportschicht
- Verbindungsorientiert (Phasen verlässlicher Verbindungsaufbau, zuverlässige Datenübertragung, geregelter Verbindungsabbau)
- Zuverlässigkeit: verlustfreie, fehlerfreie Datenübertragung; richtige Reihenfolge der Nachrichten
- Verlustfreiheit durch Versand von Bestätigungsnachrichten: Falls Bestätigung ausbleibt, wird nochmals gesendet.
- 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, mit 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	Web-Server
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://urts55.uni-trier.de:8080/Projekte/DWB
(Datum des letzten Zugriffs 04.11.2015)

Der Web-Server auf dem Computer mit dem Domainname urts55.uni-trier.de akzeptiert Verbindungen auf dem Port 8080.

Normalerweise verwenden Web-Server 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)

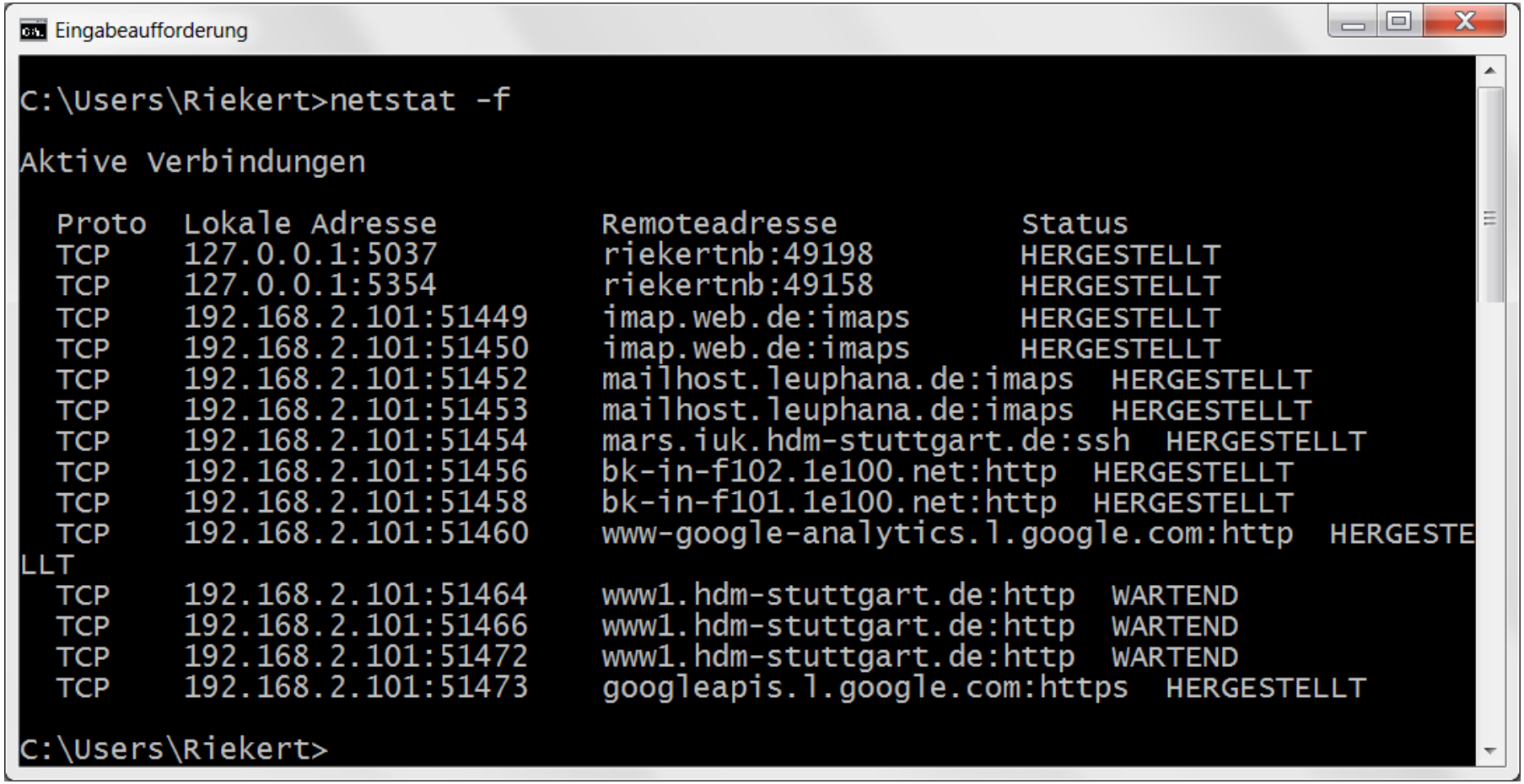
- ein Internet-Dienst der Transportschicht (Host-to-host), ebenso wie TCP
- Verbindungsloser Dienst
- Schnittstellen zu UDP sind ähnlich gestaltet wie die zu TCP, zur Adressierung werden ebenfalls Ports verwendet
- UDP-Ports unterscheiden sich von TCP-Ports; ein UDP-Port kann dieselbe Nummer haben wie 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.iuk.hdm-stuttgart.de 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-KOMMANDO AUF EINEM PC (CLIENTCOMPUTER)

HOCHSCHULE DER MEDIEN



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

TEIL 5: ANWENDUNGSSCHICHT IM INTERNET (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
- Die Anwendungsschicht im Fünf-Schichten-Modell entspricht der **Anwendungsschicht** im siebenschichtigen 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

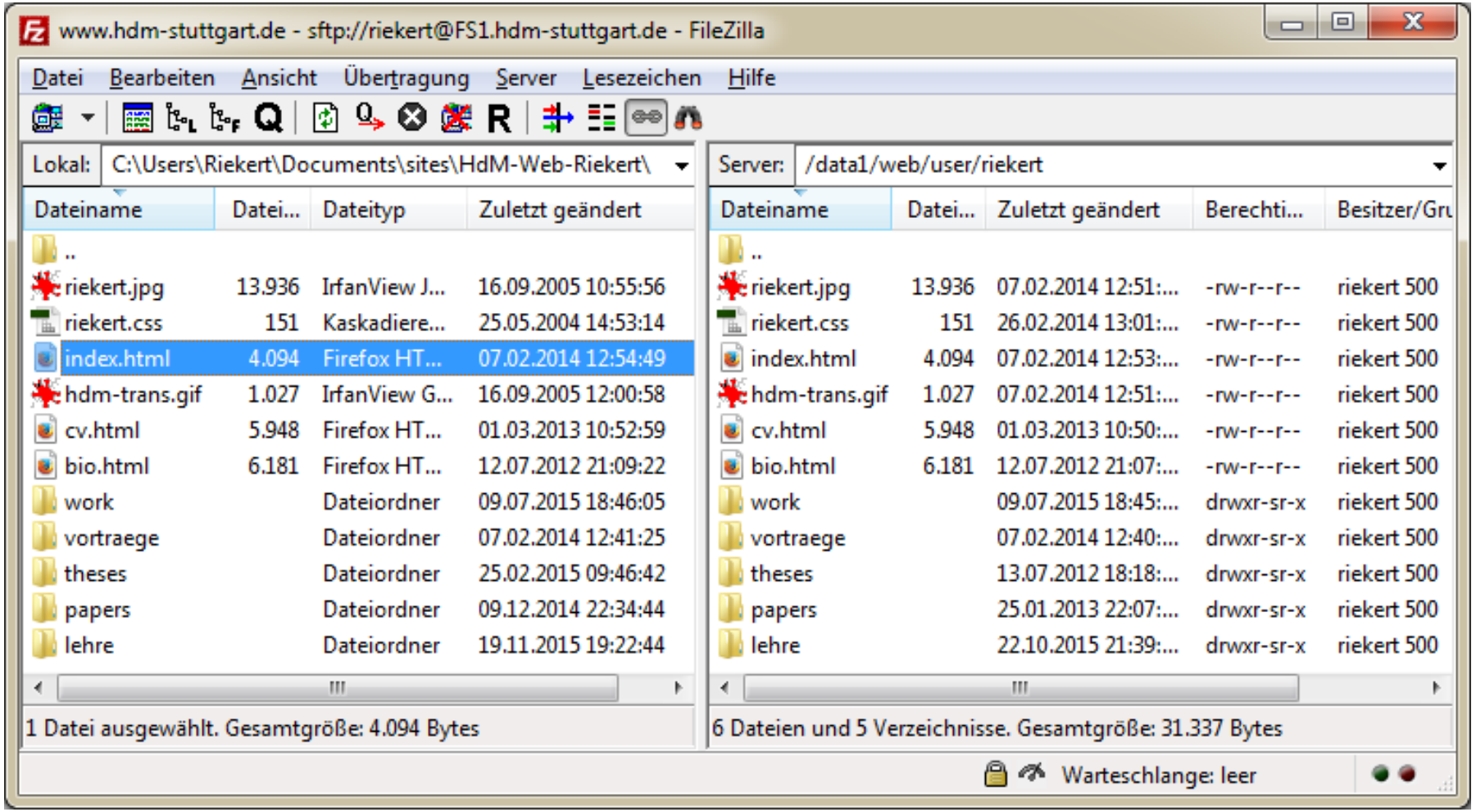
- Dateitransfer (FTP, SFTP)
- Terminalemulation (TELNET, RLOGIN, SSH)
- Elektronische Post (SMTP, POP3, IMAP, MIME)
- WWW (HTTP) - umfasst auch die vorgenannten Dienste
- Datei- und Druckerfreigabe (CIFS, SMB, Samba)
- Verzeichnisdienste (LDAP, ADS, DNS)
- netzbasiertes Fenstersystem (X Window, Remote 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)
- Dynamische Konfigurierung (DHCP)
- 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



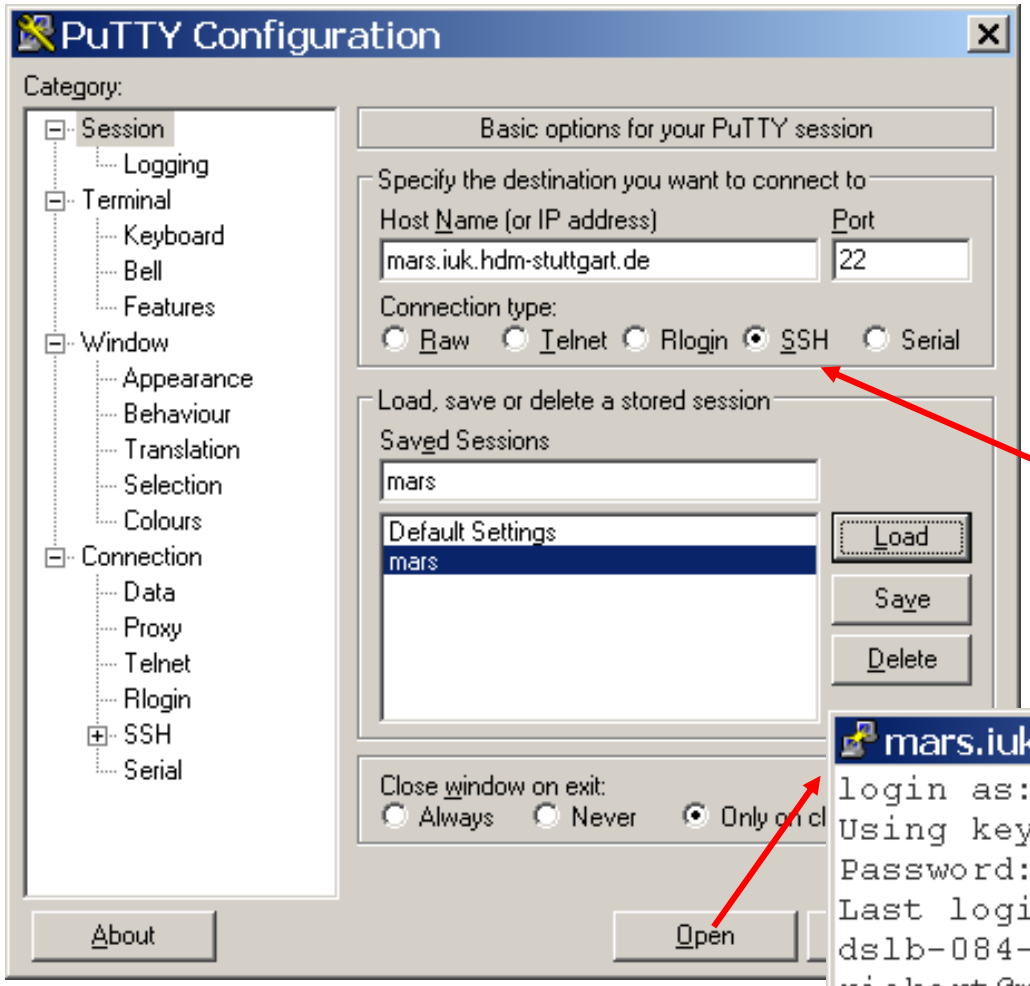
Dateien können durch Ziehen zwischen den Dateisystemen von lokalem Computer (links) und Server (rechts) kopiert werden.

DER TELNET-DIENST

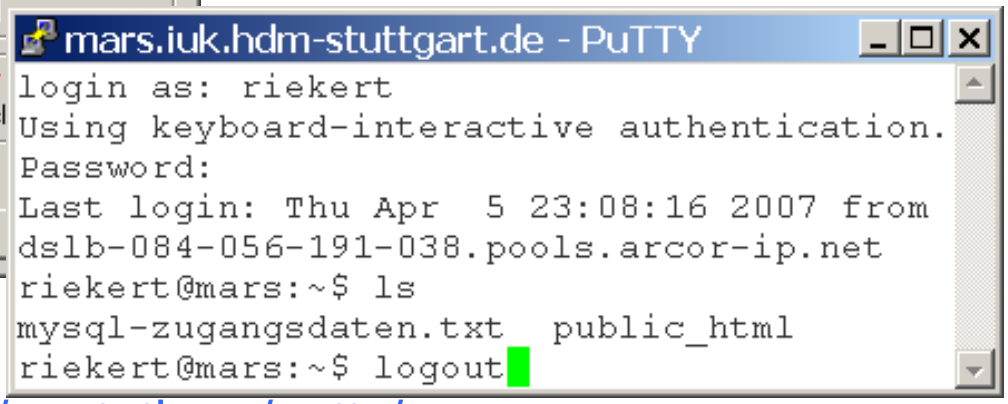
- Telnet ermöglicht die Fernsteuerung eines Computers über zeilenweise eingegebene textuelle Kommandos
- Telnet-Client: Ein „virtuelles Terminal“ ersetzt das klassische Bildschirmgerät eines Großrechners („Mainframe“)
  - ⇨ Funktionsweise zeilenorientiert, nicht seitenorientiert
  - ⇨ Aufruf unter DOS oder Unix Shell: Kommando telnet
  - ⇨ Aufruf unter Windows: Anwendung PuTTY
  - ⇨ Aufruf unter Mac OS über Terminalfenster / neue entfernte Verbindung
- Telnet-Server verbunden mit zeilenorientiertem Kommandointerpreter (z.B. Unix Shell)
- Telnet ist verbindungsorientiert, nutzt TCP, Port = 23
- Auf vielen Servern ist der Telnet-Dienst deaktiviert und durch den verschlüsselten Dienst SSH ersetzt (Port = 22).

PUTTY: VIRTUELLES TERMINAL AUF BASIS TELNET UND SSH

HOCHSCHULE DER MEDIEN



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



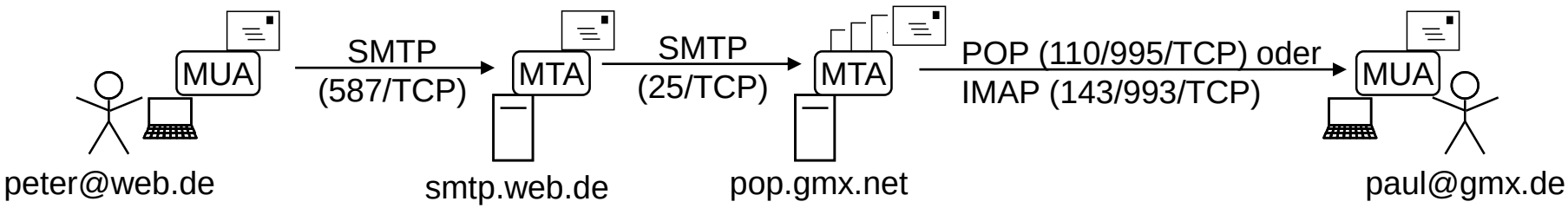
Download:
http://www.chiark.greenend.org.uk/~sgtatham/putty/

INTERNET MAIL

- Mailclient und Mailserver 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**:
  - ⇨ **Formatierte Nachrichten** (Schrifttypen, -größen usw.)
  - ⇨ **Typisierte Nachrichten** (mit sog. 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)

INTERNET-MAIL
ALLGEMEINE FUNKTIONSWEISE

HOCHSCHULE DER MEDIEN



MUA: Mail User Agent = Mailclient (z.B. Outlook, Thunderbird): Erstellen, Versenden und Empfangen von E-Mails durch Endbenutzer

MTA: Mail Transfer Agent = Mailserver: E-Mails vom MUA des Absenders entgegennehmen, weiterleiten und bereitstellen für MUA des Empfängers

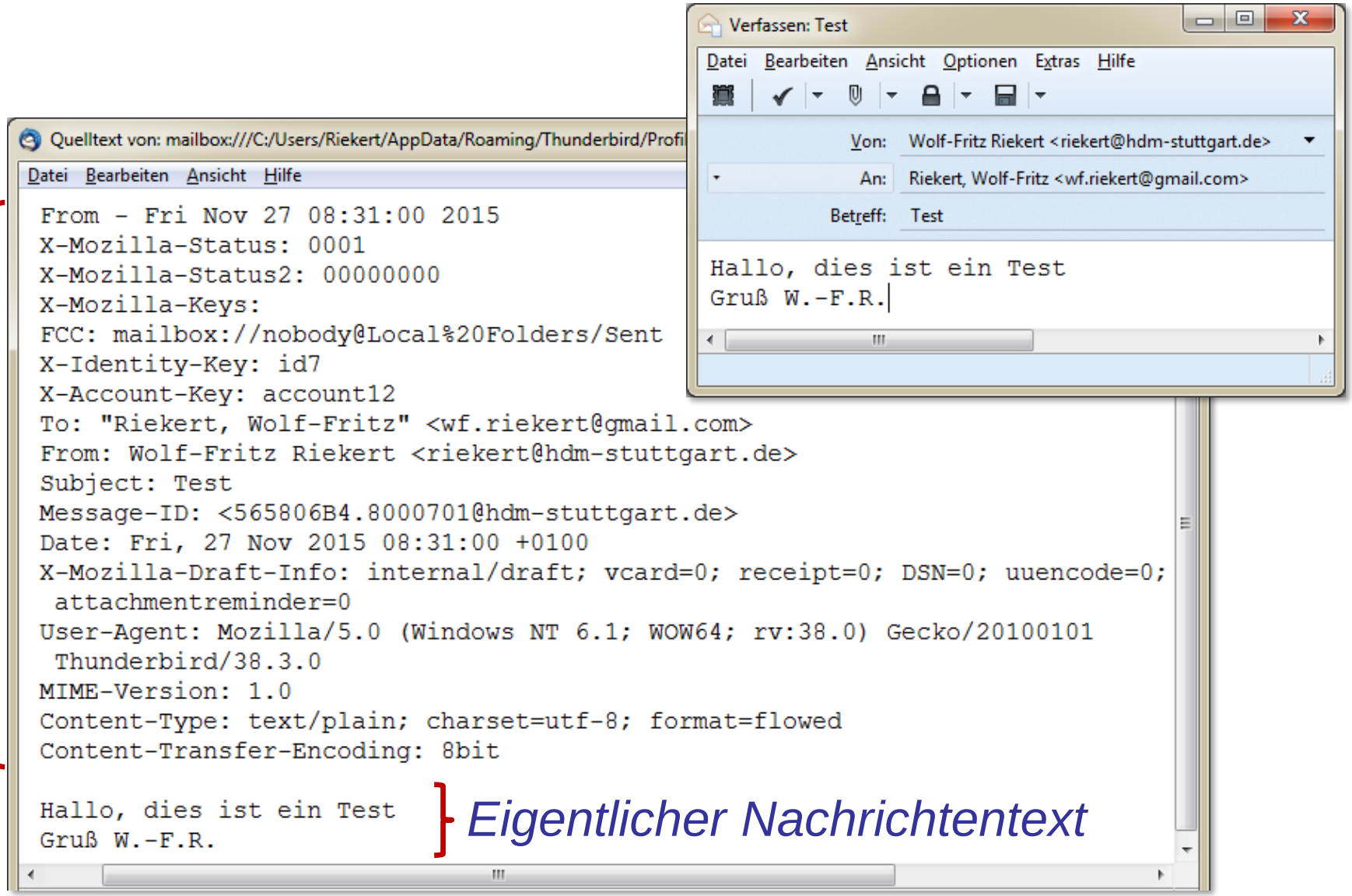
SMTP (Simple Mail Transfer Protocol): Übertragung vom MUA zum MTA über TCP-Port 587 und Weiterleitung zwischen MTAs über TCP-Port 25

POP (Post Office Protocol): Abholen von E-Mails vom MTA (Mailserver) über TCP-Port 110 bzw. 995 (verschlüsselt).

IMAP (Internet Message Access Protocol): Bereitstellung von E-Mails in Ordnern auf dem MTA (Mailserver) und Synchronisieren mit MUA (Mailtool) über TCP-Port 143 oder 993 (verschlüsselt)

AUFBAU EINER E-MAIL: HEADER UND EIGENTLICHER NACHRICHTENTEXT

HOCHSCHULE DER MEDIEN



ÜBERTRAGUNG VON ANHÄNGEN MIT MIME

HOCHSCHULE DER MEDIEN

Quelltext von: mailbox:///C:/Users/Riekert/AppData/Roaming/Thunderbird/Profiles/cjwc7nl0.default/Mail/Local%20Folders/...

Datei Bearbeiten Ansicht Hilfe

```
 Thunderbird/38.3.0
MIME-Version: 1.0
Content-Type: multipart/mixed;
 boundary="------------090501040306030200000000"

This is a multi-part message in MIME format.
--------------090501040306030200000000
Content-Type: text/plain; charset=utf-8; format=flowed
Content-Transfer-Encoding: 8bit

Hallo, dies ist ein Test
Gruß W.-F.R.

--------------090501040306030200000000
Content-Type: image/jpeg;
 name="ri-q-web-bw.jpg"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
 filename="ri-q-web-bw.jpg"

/9j/4AAQSkZJRgABAgEASABIAAD/7Q5UUGhvdG9zaG9wIDMuMAA4QklNA+0AAAAAABAASAAA
AAEAAgBIAAAAAQACOEJJTQQNAAAAAAAEAAAAHjhCSU0EGQAAAAAABAAAAB44QklNA/MAAAAA
AAkAAAAAAAAAAAEAOEJJTQQKAAAAAAABAAA4QklNJxAAAAAAAAoAAQAAAAAAAAACOEJJTQP0
```

Verfassen: Test

Datei Bearbeiten Ansicht Optionen Extras Hilfe

Von: Wolf-Fritz ...

An: Riekert, Wolf-Fritz

Betreff: Test

1 Anhang 13,6 KB

ri-q-web-bw.jpg 13,6 KB

Hallo, dies ist ein Test
Gruß W.-F.R.

DAS WORLD WIDE WEB (WWW)

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

Server: Web-Server (z.B. Apache HTTP Server, Microsoft Internet Information Services)

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

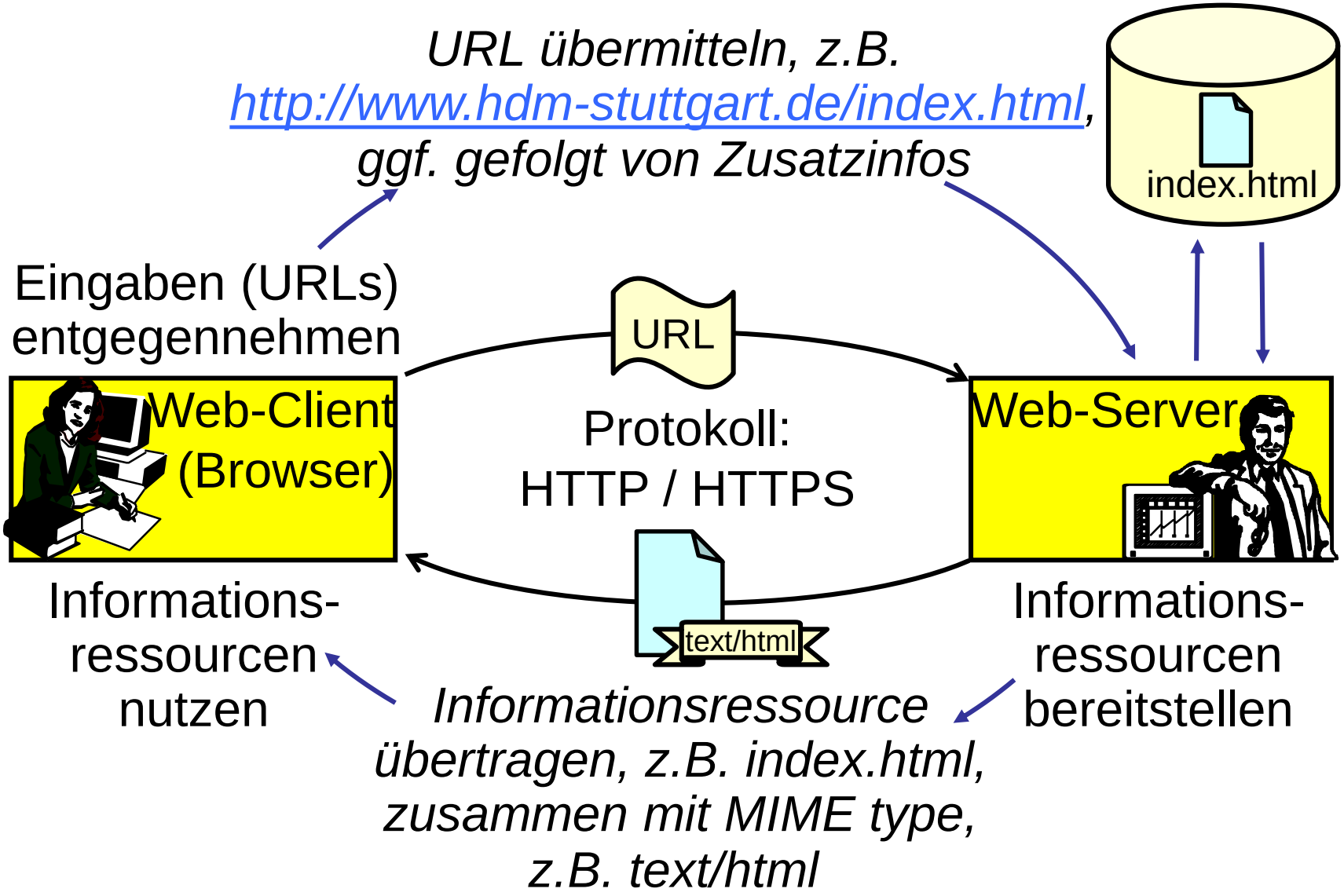
Art des Dienstes: Verbindungsloser Anfrage-/Antwort-Dienst

Protokolle: Hypertext Transfer Protocol (HTTP), sichere Protokollvariante HTTPS über SSL (verschlüsselt, signiert)

Transportprotokoll: TCP (verbindungsorientiert!) über Port 80 (HTTP) bzw. Port 443 (HTTPS)

WEB-CLIENT (BROWSER) UND WEB-SERVER

HOCHSCHULE DER MEDIEN



WEB-SERVER

- 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, CSS-Formatvorlagen, GIF-, JPEG- und PNG-Grafiken
  - ⇨ direkte Ausführung: JavaScript
  - ⇨ Anzeige/Ausführung über Plug-In (nachladbare Browser-Erweiterung): z.B. Acrobat Reader, Java Plugin, Adobe Flash
  - ⇨ Anzeige/Ausführung durch sog. Helper Application: z.B. Winword für Doc-Files usw.
- nimmt Eingaben von URLs an und leitet diese weiter an den Web-Server
  - ⇨ Direkteingabe über Tastatur
  - ⇨ Anklicken von Hyperlinks (mit URL hinterlegte Bereiche)
  - ⇨ Ausfüllen und Abschicken von Web-Formularen

UNIFORM RESOURCE LOCATOR (URL)

HOCHSCHULE DER MEDIEN

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)

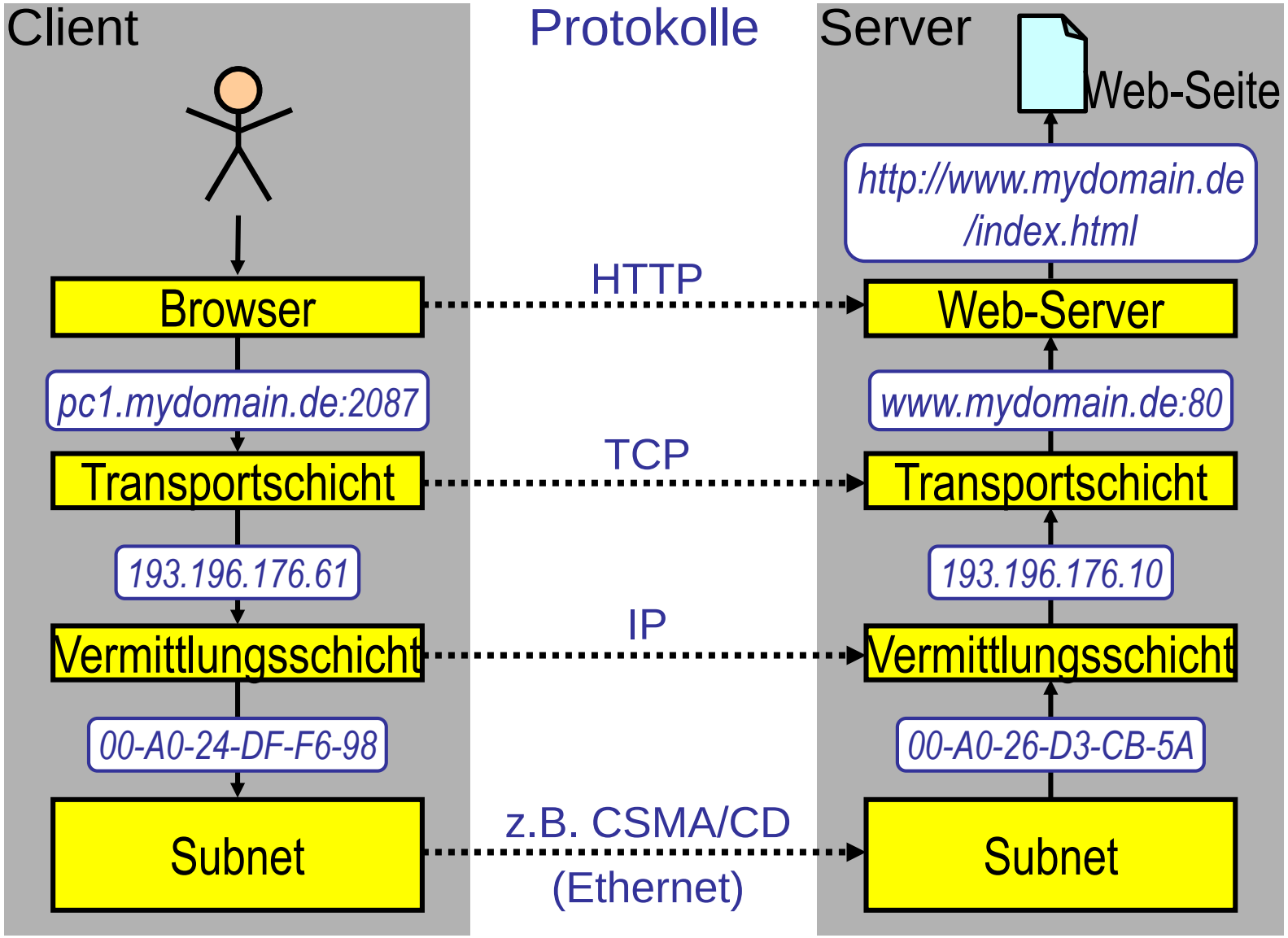
Protokoll: = Übertragungsprotokoll, z.B. **http:** bzw **https:** für Hypertext Transfer Protocol (Secure)

//Domain = Bezeichnung des Servercomputers im Internet

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

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

ROLLE DER SCHICHTEN AM BEISPIEL DES WWW



TEIL 6: SICHERHEIT IM INTERNET DURCH KRYPTOGRAPHIE

Die Sicherheit im Internet kann durch so genannte Kryptographietechniken (Verschlüsselungstechniken) erhöht werden.

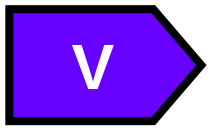
Dabei geht es um folgende **Schutzgüter** für die Übertragung von Informationen im Internet

- Vertraulichkeit von Informationen (Schutz von Betriebsgeheimnissen und von Privatsphäre)
- Authentizität von Informationen (Echtheit der Herkunft)
- Verbindlichkeit von Informationen (Unabstreitbarkeit)
- Integrität von Informationen (Unverfälschtheit)

BEGRIFFE

Chiffre	Verschlüsselungsverfahren für Nachrichten (einschließlich zugehörigem Entschlüsselungsverfahren)
Kryptographie	Entwerfen von Chiffren
Kryptoanalyse	Aufbrechen („Knacken“) von Chiffren
Klartext	(engl. plain text) zu verschlüsselnde Nachricht
Chiffretext	(engl. cypher text) verschlüsselte Nachricht
Verschlüsselung	(engl. encryption) Umsetzung von Klartext in Chiffretext
Entschlüsselung	(engl. decryption) umgekehrter Vorgang

DIE „CAESAR“-CHIFFRE – EIN EINFACHES BEISPIEL:



Verschlüsselungsverfahren:
„Gehe in alphabetischer Reihenfolge um **k** Buchstabenpositionen weiter!“

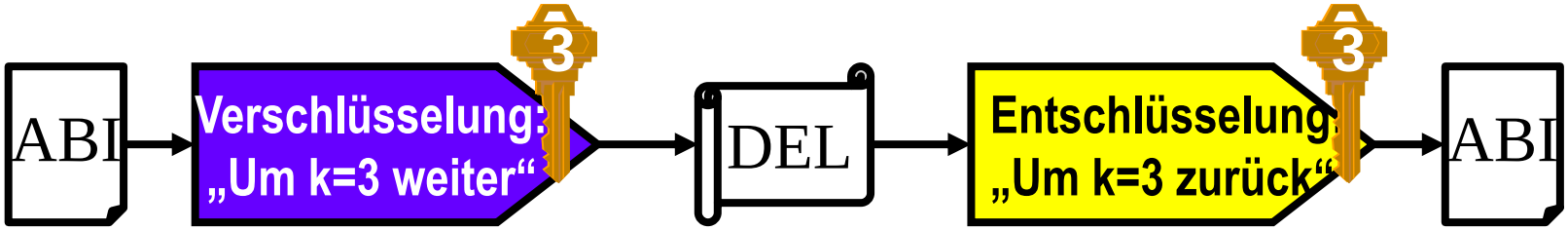
Schlüssel k (= 3 im Beispiel)

Entschlüsselungsverfahren:
„Gehe in alphabetischer Reihenfolge um **k** Buchstabenpositionen zurück!“

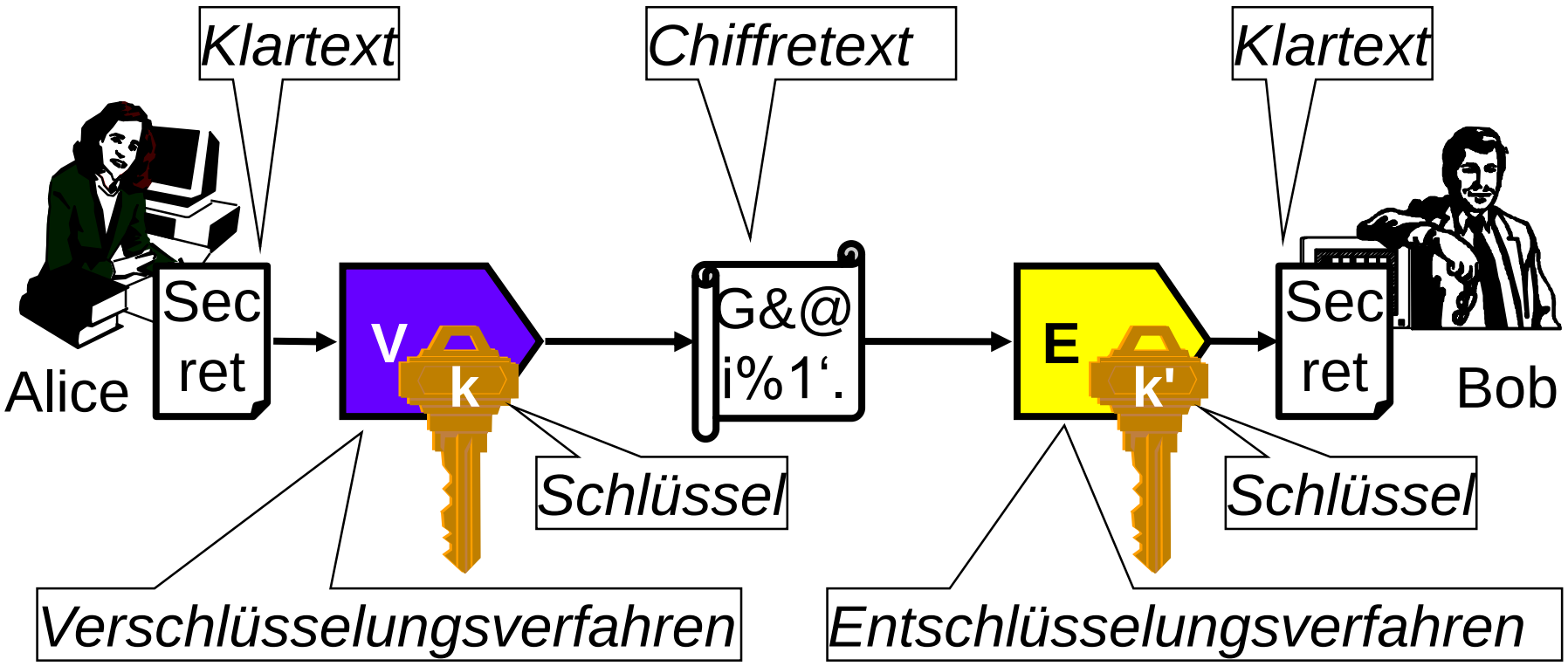
A	→	D
B	→	E
C	→	F
...		
I	→	L
…		
W	→	Z
X	→	A
Y	→	B
Z	→	C

Für Verschlüsselung und Entschlüsselung wird hier derselbe Schlüssel **k** verwendet.

⇒ **Symmetrisches Verschlüsselungsverfahren.**



VERSCHLÜSSELUNG (1)

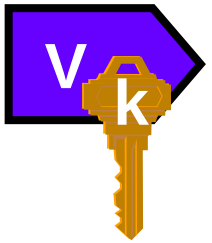


Senderin Übertragung Empfänger

VERSCHLÜSSELUNG (2)

Eine **Verschlüsselung** $\mathbf{V_k}$ ist festgelegt durch zwei Vorgaben:

- ein allgemeines **Verschlüsselungsverfahren V** (auch Verschlüsselungsalgorithmus genannt, realisiert durch ein Programm),
- einen **Schlüssel** (Key) **k** (ein Zahlencode oder eine Zeichenkette), der das Verfahren einstellt (parametrisiert).



Für die **Entschlüsselung** $\mathbf{E_{k'}}$ gilt Entsprechendes, diese ist festgelegt durch:

- ein allgemeines **Entschlüsselungsverfahren E,**
- einen **Schlüssel k'**, der das Verfahren einstellt (parametrisiert).

WORIN BESTEHT DAS GEHEIMNIS?

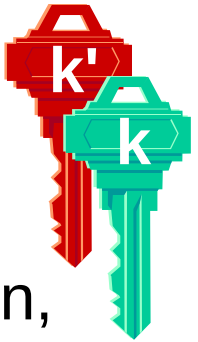
Was muss geheim gehalten werden, damit kein Unberechtigter an die verschlüsselten Informationen kommt?

- Der Verschlüsselungsalgorithmus?
  - ⇨ „Security by obscurity“ (Niemand weiß, wie die Verschlüsselung funktioniert
  - ⇨ Nicht empfehlenswert: Der Algorithmus kann Schwächen haben und niemand kann diese aufdecken.
- Der Schlüssel?
  - ⇨ Ja, das entspricht dem heutigen Stand der Technik
  - ⇨ Der Algorithmus soll so leistungsfähig sein, dass er offengelegt werden kann

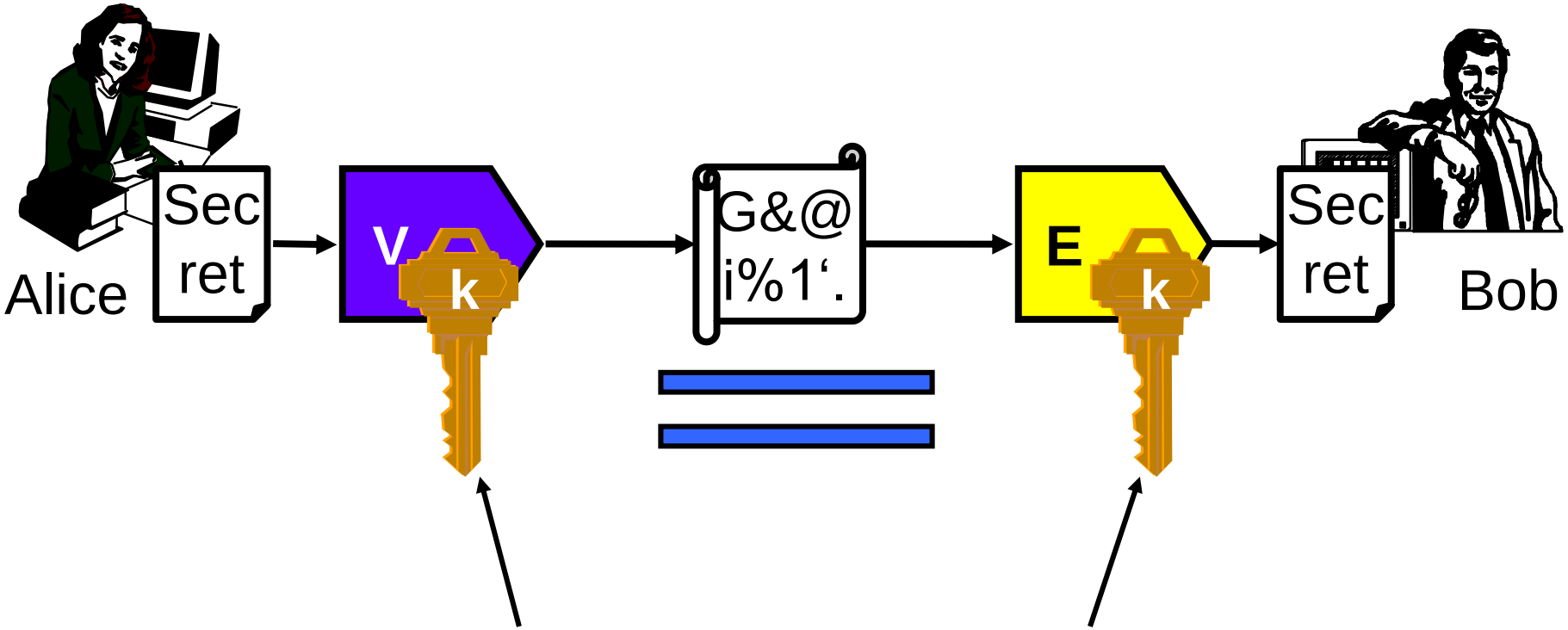
SYMMETRISCHE U. ASYMMETRISCHE VERSCHLÜSSELUNG

- **Symmetrische Verschlüsselung:**
  Für Entschlüsselung und Verschlüsselung wird derselbe Schlüssel k verwendet.
  - ⇨ Problem: Für jedes Paar von Kommunikationspartnern wird ein eigener Schlüssel benötigt.

- **Asymmetrische Verschlüsselung:**
  Für Entschlüsselung und Verschlüsselung werden unterschiedliche Schlüssel k und k' verwendet.
  - ⇨ Es gibt asymmetrische Verschlüsselungsmethoden, bei denen der Entschlüsselungsschlüssel k' mit heute verfügbarer Rechenleistung nicht aus dem Verschlüsselungsschlüssel k abgeleitet werden kann.
  - ⇨ Mögliche Verwendung: sogenannte öffentliche Verschlüsselungsverfahren.



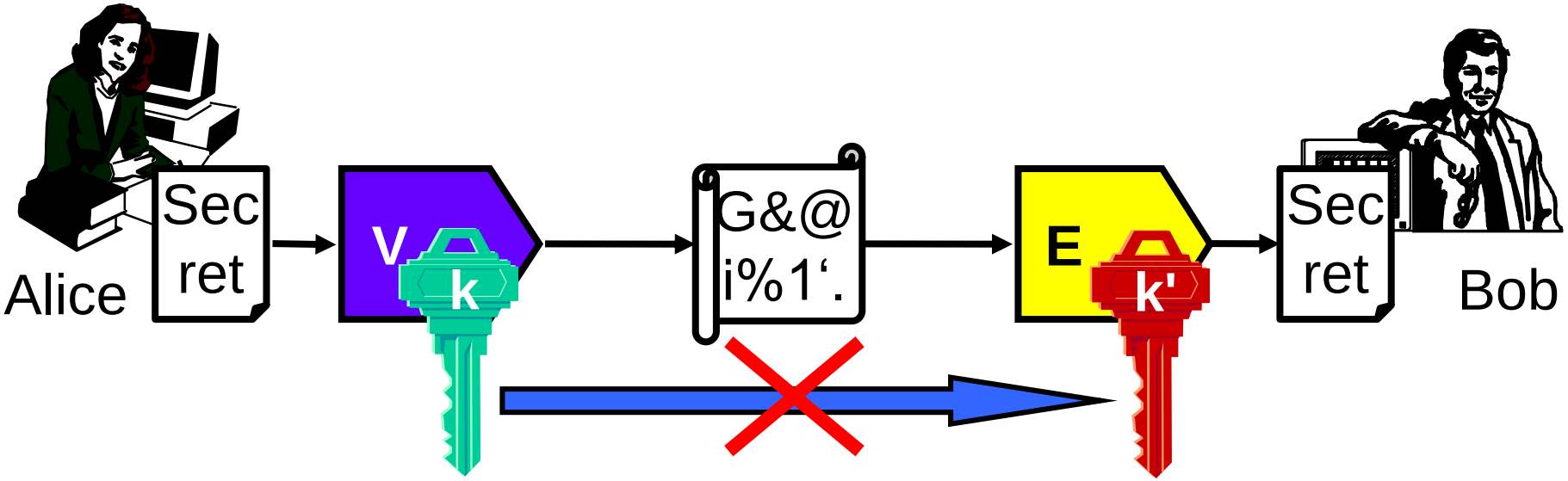
SYMMETRISCHE VERSCHLÜSSELUNG



Beide Schlüssel sind identisch:

Symmetrische Verschlüsselung

ASYMMETRISCHE VERSCHLÜSSELUNG



Der Entschlüsselungsschlüssel **k'** kann mit heute verfügbarer Rechenleistung nicht aus dem Verschlüsselungsschlüssel **k** abgeleitet werden:

Asymmetrische Verschlüsselung

ÖFFENTL. VERSCHLÜSSELUNGS-VERFAHREN (1)

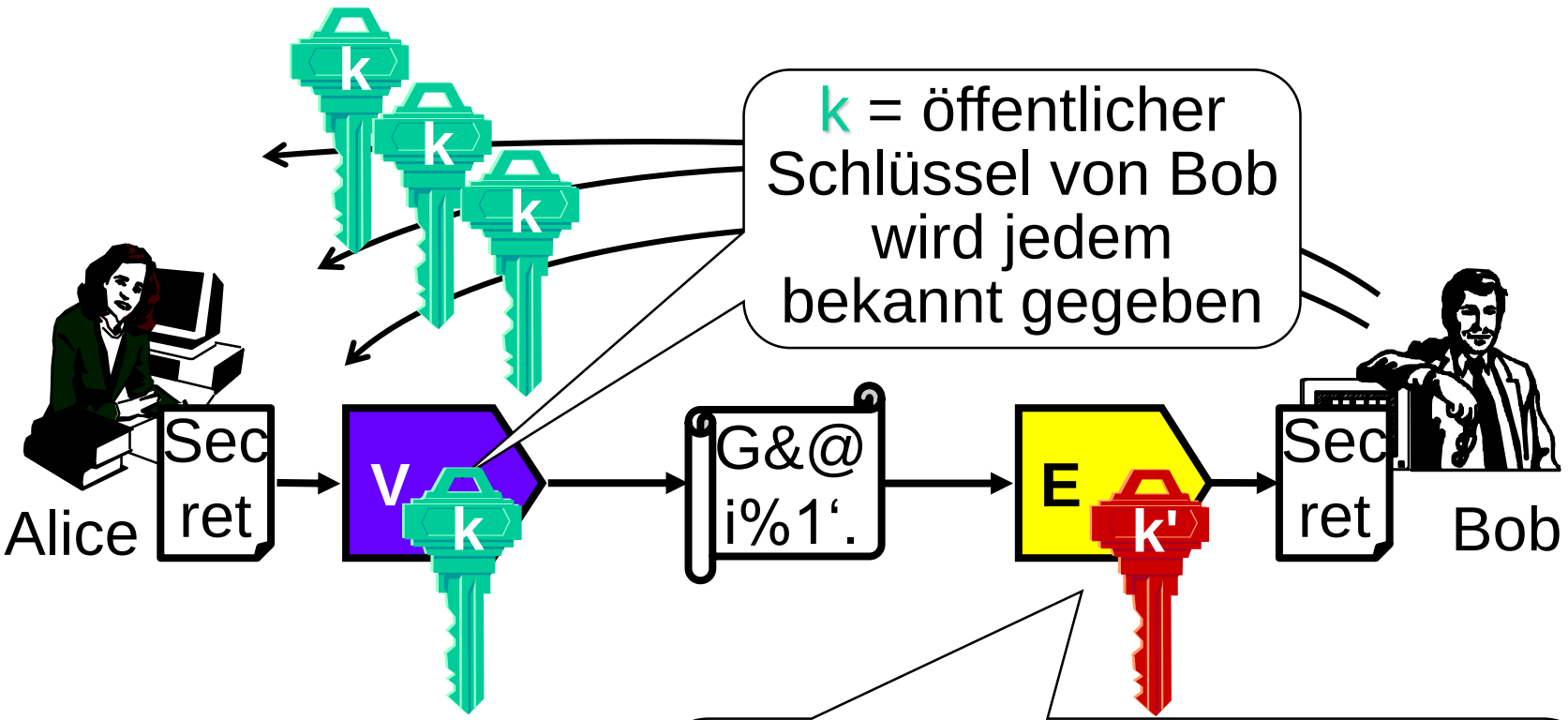
Asymmetrische Verschlüsselungsverfahren ermöglichen sogenannte öffentliche Verschlüsselungsverfahren:

- Die **Verschlüsselung** erfolgt mit einem öffentlich bekannten Schlüssel k (dem **öffentlichen Schlüssel**).

- Die **Entschlüsselung** erfolgt mit einem nur dem Besitzer bekannten **privaten Schlüssel** k'.

- Es ist in der Praxis **unmöglich, k' aus k abzuleiten**, selbst wenn man Beispiele von zueinander gehörigen Klar- und Chiffretexten kennt. Das heißt, ein solcher Versuch würde viele Jahre bis zum Erfolg benötigen, selbst wenn ein Supercomputer benutzt wird.

ÖFFENTL. VERSCHLÜSSELUNGS-VERFAHREN (2)



KOMBINATION ASYMMETR. UND SYMMETR. VERSCHLÜSSELUNG

- Um vertrauliche Nachrichten an Bob senden zu können, genügt ein öffentlicher Schlüssel für alle Absender.
- Nachteil: Asymmetrische Verschlüsselungsverfahren sind sehr aufwendig (erfordern viel Rechenleistung bzw. -zeit).
- Abhilfe: **Kombination mit symmetrischem Verschlüsselungsverfahren**. Alice erzeugt als erstes einen Schlüssel **s** für ein symmetrisches Verfahren, verschlüsselt diesen mit Bobs öffentlichen Schlüssel **k** und schickt ihn in dieser Form auf sichere Weise an Bob.
- Mit dem symmetrischen Schlüssel **s** können Bob und Alice vertrauliche Nachrichten in beide Richtungen austauschen! Mit dem öffentlichen Schlüssel **k** wäre das nur in Richtung Bob möglich gewesen!

GÄNGIGE VERSCHLÜSSELUNGSVERFAHREN

HOCHSCHULE DER MEDIEN

RSA = bedeutendste asymmetrische Chiffre, wird in den meisten Verfahren mit öffentlichen und privaten Schlüsseln verwendet. 1978 entwickelt von Ronald **R**ivest, Adi **S**hamir und Leonard **A**dleman, Wissenschaftler am MIT (Massachusetts Institute of Technology) und Gründer von **RSA Data Security**, Firma für Kryptographie-Technologie.

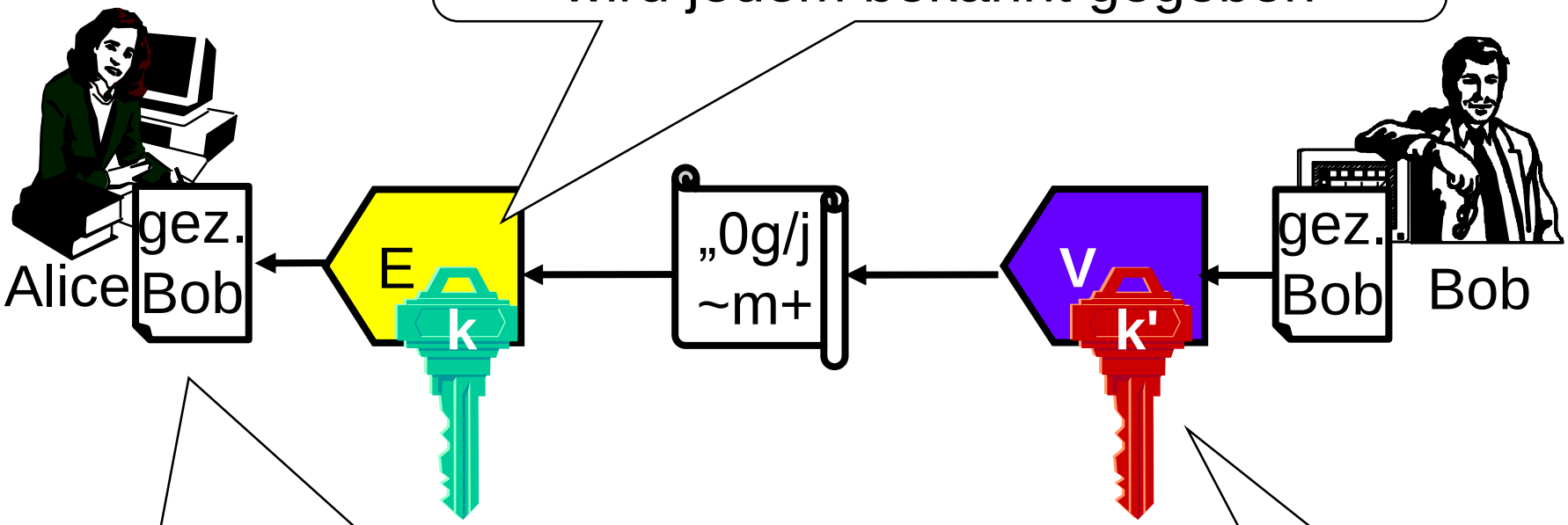
AES = heute wichtigste symmetrische Chiffre. Unter dem Namen **Rinjdael** von J. Daemen und V. Rijmen entwickelt, 2000 vom US-amerikanischen Normungsinstitut NIST zum Advanced Encryption Standard (AES) erklärt. Sehr schneller Algorithmus. Schlüssellängen 128, 192 und 256 Bits. (Ältere Verfahren: DES, Triple-DES, RC2, RC4, IDEA)

SIGNIERUNG: VERSCHLÜSSELUNG „IN UMGEKEHRTER RICHTUNG“

- Das asymmetrische Verschlüsselungsverfahren RSA (wie auch vergleichbare Verfahren) kann auch in umgekehrter Richtung betrieben werden.
- D.h., es wird eine Nachricht mit dem privaten Schlüssel verschlüsselt und mit dem öffentlichen Schlüssel entschlüsselt.
- Die Entschlüsselbarkeit mit dem öffentlichen Schlüssel ist der Beweis, dass die Nachricht vom betreffenden Absender stammt.
  - ⇨ Technische Grundlage für die **digitale Signierung** (**digitale Unterschrift**).

DIGITALE SIGNIERUNG

kB = öffentlicher Schlüssel von Bob, wird jedem bekannt gegeben



Alice kann die Nachricht mit dem öffentlichen Schlüssel k von Bob entschlüsseln, also stammt die Nachricht von ihm.

k' = privater Schlüssel, ist nur Besitzer Bob bekannt

VERSCHLÜSSELUNG UND SIGNIERUNG

- Verschlüsselung:
  - ⇨ Sender verwendet öffentlichen Schlüssel des Empfängers zur Verschlüsselung der Nachricht.
  - ⇨ Empfänger verwendet eigenen privaten Schlüssel zur Entschlüsselung der Nachricht.
- Digitale Unterschrift (Signierung):
  - ⇨ Die zu unterschreibende Nachricht wird mit dem privaten Schlüssel des Senders verschlüsselt. Das Ergebnis ist die unterschriebene Nachricht.
  - ⇨ Empfänger verwendet öffentlichen Schlüssel des Senders zur Entschlüsselung der Nachricht. Wenn diese Entschlüsselung gelingt, ist die „Unterschrift“ echt und die Nachricht stammt vom Besitzer der Unterschrift.

VERSCHLÜSSELUNG UND SIGNIERUNG: FOLGERUNGEN

Signierung und Verschlüsselung sind voneinander unabhängig möglich:

- Mit öffentlichen Schlüsseln verschlüsselte Nachrichten haben nicht notwendig eine Unterschrift. Sie können von jedermann stammen.
- Mit privaten Schlüsseln signierte Nachrichten sind nicht vertraulich. Sie können mit Hilfe des passenden öffentlichen Schlüssels von jedermann entschlüsselt werden.
- Verschlüsselung und Signierung können aber auch kombiniert werden. Hierzu verschlüsselt der Sender zunächst die Nachricht mit dem eigenen privaten Schlüssel (= Signierung) und dann mit dem öffentlichen Schlüssel des Empfängers (= Verschlüsselung).

INTEGRITÄT DURCH SIGNIERUNG VON MESSAGE DIGESTS

Signierung kann zur Gewährleistung der Integrität (Unverfälschtheit) von Nachrichten genutzt werden.

- Bob will Alice eine unverfälschbare Nachricht senden.
- Dazu bestimmt er aus der Nachricht einen Prüfcode, den sogenannten **Message Digest**.
- Bob signiert den Message Digest, d.h. er verschlüsselt ihn mit seinem privaten Schlüssel.
- Alice verifiziert Bobs Unterschrift, d.h. sie entschlüsselt den Message Digest mit Bobs öffentlichem Schlüssel.
- Alice berechnet den Message Digest aus der Nachricht und vergleicht ihn mit dem entschlüsselten Message Digest. Wenn beide gleich sind, ist die Integrität der Nachricht gesichert.

MESSAGE DIGESTS

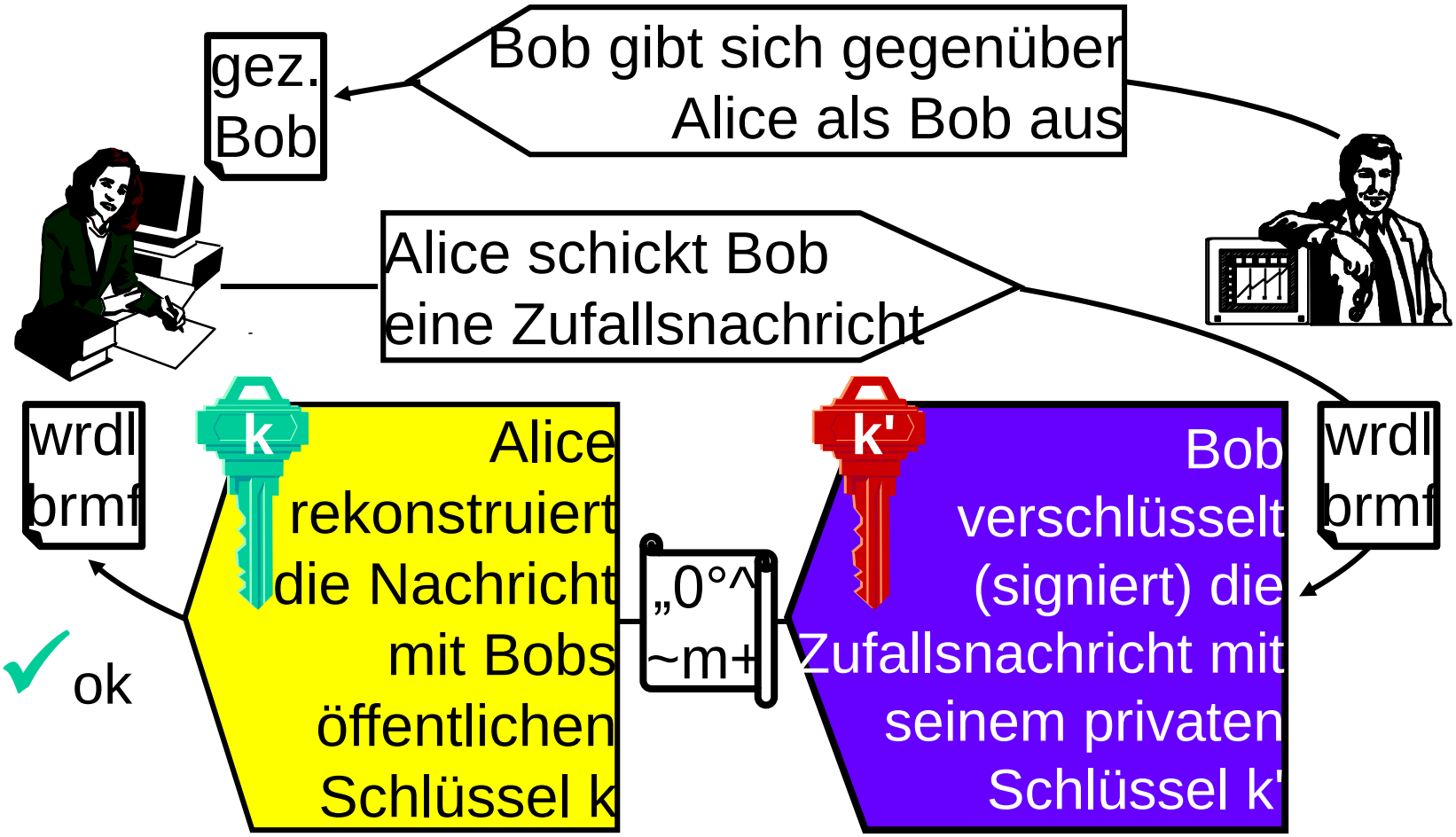
Eigenschaften guter Verfahren zur Berechnung von Message Digests:

- Jedes Bit des Message Digests wird von jedem Bit der Nachricht beeinflusst.
- Wenn irgendein Bit der Nachricht verändert wird, kann sich jedes Bit des Message Digest mit 50% Wahrscheinlichkeit ändern.
- Wenn eine Nachricht und ihr Message Digest vorgelegt wird, sollte es mit heutigen technischen Mitteln unmöglich sein, eine zweite Nachricht mit demselben Message Digest zu erzeugen.

In der Praxis werden meist nur die Message Digests signiert und nicht die eigentlichen Nachrichten.

AUTHENTIFIZIERUNG

Mit Hilfe der Technik der Signierung können sich Kommunikationspartner ausweisen (authentifizieren):



KRYPTOGRAPHIE-INFRASTRUKTUR

Problem:

- Wie erfährt Alice den öffentlichen Schlüssel ihres Gesprächspartners, wenn sie zu ihm keine persönliche Verbindung hat?
- Wenn Sie den öffentlichen Schlüssel kennt, welche Gewissheit hat sie über die Identität des Gesprächspartners?

Abhilfe:

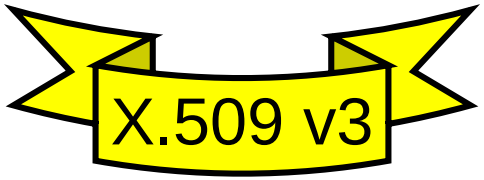
- Aufbau einer sog. „Kryptographie-Infrastruktur“.
- D.h.: Einrichtung von Zertifikatbehörden, sog. Certificate Authorities (CA) oder Trustcenters, die die Identität von Personen / Einrichtungen prüfen und deren öffentliche Schlüssel durch digitale Unterschrift beglaubigen.
- Diese Beglaubigung erfolgt mit sog. digitalen Zertifikaten.

DIGITALE ZERTIFIKATE

Zertifikate sind digitale Dokumente, die folgende Informationen enthalten:

- Angaben zur **Identität der Person/Institution** (Name, ggf. Adressangaben)
- **Öffentlicher Schlüssel** der Person/Institution
- **Ausgabedatum, Verfallsdatum**
- **Seriennummer**
- **Digitale Unterschrift des Trustcenters**
  - ⇨ kann mit öffentlichem Schlüssel des Trustcenters verifiziert werden.

Die derzeit gängige Norm für Zertifikate trägt die Bezeichnung **X.509 v3**



ARTEN VON ZERTIFIKATEN

Trustcenter unterscheiden **Zertifikate nach Einsatz**

- im Mailsystem: Verschlüsselung und Signierung (S/MIME)
- im Web-Server: Signierung von Web-Seiten, Initiierung einer sicheren Web-Verbindung (https)
- Signierung von Programmcode
- im Internet-Browser: Authentifizierung von Benutzern

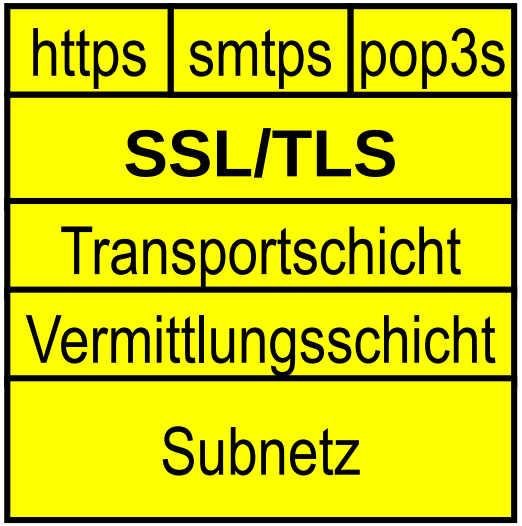
Es werden Zertifikate in verschiedenen **Klassen** ausgegeben.

- Im einfachsten Fall: Legitimierung durch gültige Email-Adresse (nur für Privatpersonen, Zertifikat wird umgehend per Email zugeschickt, Anbieter z.B. www.comodo.com).
- Für hohe Sicherheit: Legitimierung durch Personalausweis oder Reisepass und persönliches Erscheinen bei einer Behörde oder Agentur.

NORMEN UND PROTOKOLLE AUF BASIS VON X.509 V3

S/MIME: Erweiterung des MIME-Standards für Internet-Mail, erlaubt die Ende-zu-Ende-Verschlüsselung und -Signierung von E-Mails mit Hilfe von X.509v3-Zertifikaten

SSL v3 (Secure Socket Layer) oder der Nachfolgerstandard **TLS** (Transport Layer Secure): Zwischenschicht zwischen Verarbeitungsschicht und Transportschicht, realisiert eine sichere Transportverbindung zwischen Client und Server zur Verschlüsselung und Signierung basierend auf X.509v3-Zertifikaten



Auf SSL aufbauende Protokolle (Auswahl):

- **https** (HTTP secure)
- **smtps** (SMTP secure)
- **pop3s** (POP3 secure)

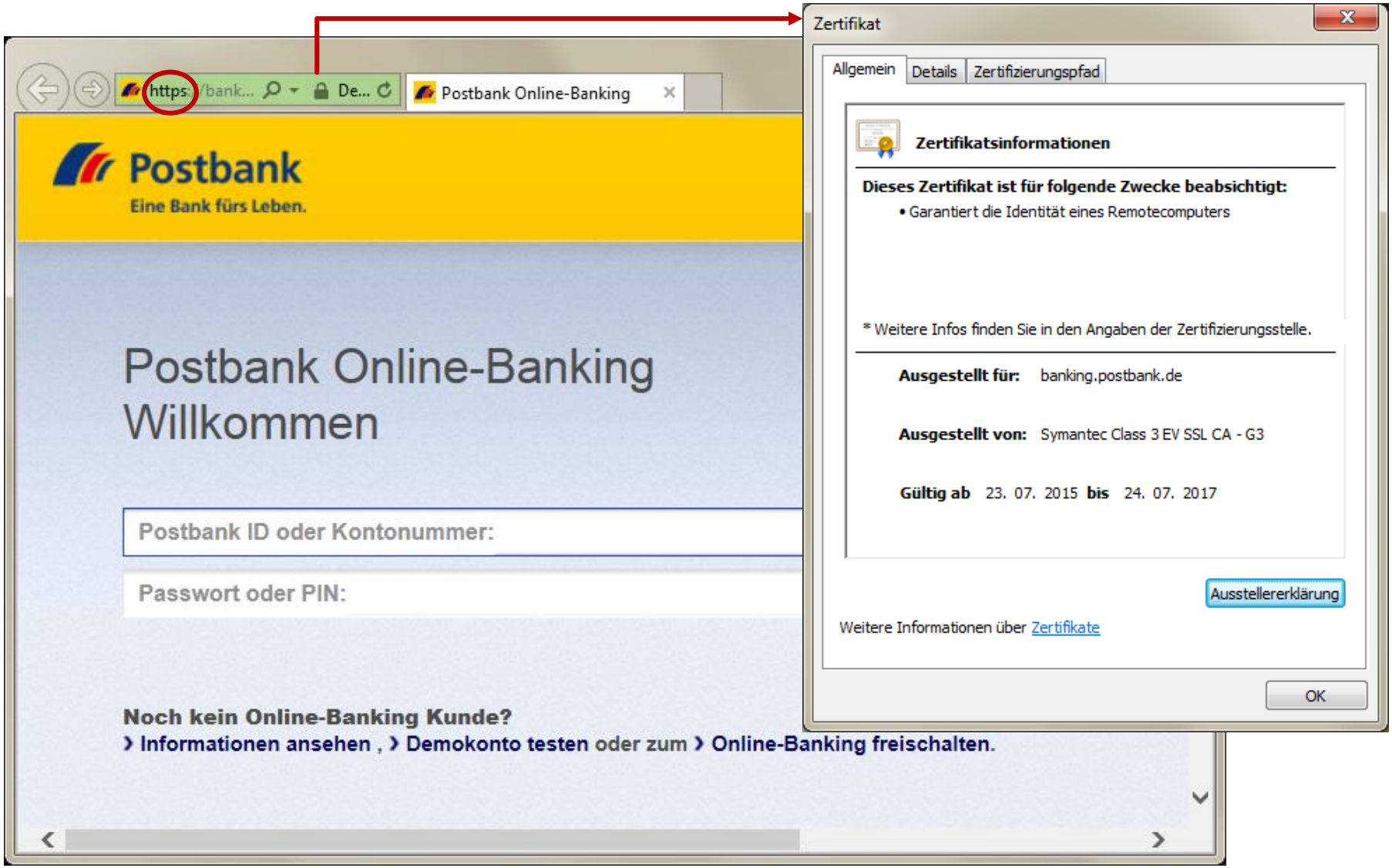
SICHERE ÜBERTRAGUNG MIT HILFE VON ZERTIFIKATEN NACH X.509 V3

Alle modernen **Internet-Browser** und **E-Mail-Clients** (Firefox, Google Chrome, Internet Explorer, Outlook, Thunderbird) sind für Zertifikate nach X.509 v3 vorbereitet:

- Sie verstehen die Protokolle SSL v3 / TLS bzw. S/MIME.
- Sie haben die öffentlichen Schlüssel der wichtigsten Trustcenter vorinstalliert.
- Dadurch ist eine sichere Kommunikation mit Teilnehmern möglich, deren öffentliche Schlüssel von einem dieser Trustcenter mit Zertifikaten beglaubigt (d.h. signiert) sind.
  - ⇨ Man kann ihnen verschlüsselte E-Mails schicken
  - ⇨ Man kann deren digitale Unterschrift verifizieren
  - ⇨ Man kann mit deren Websites verschlüsselt interagieren (z.B. im E-Business)

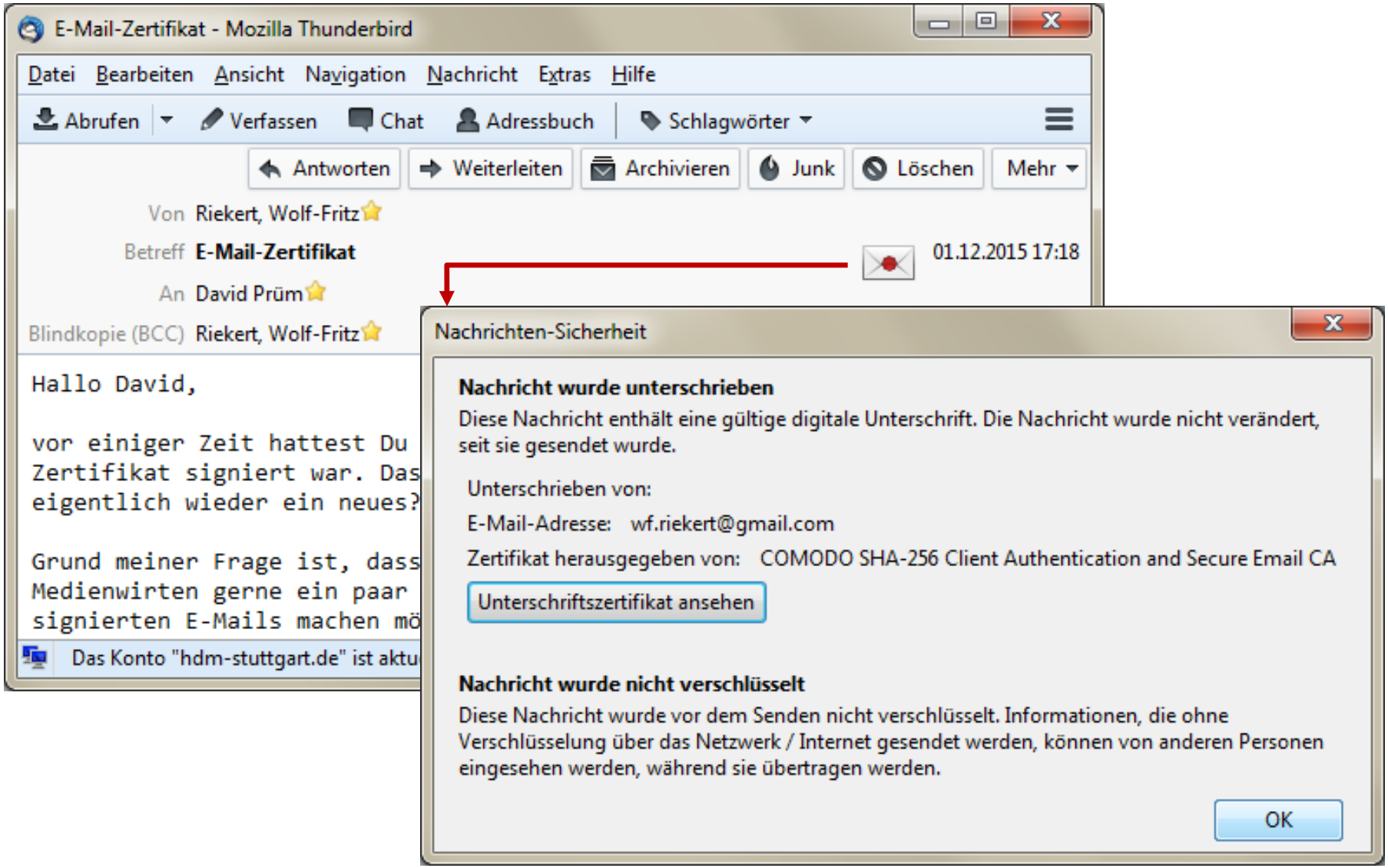
VERSCHLÜSSELTE KOMMUNIKATION MIT HTTPS UND SSL/TLS

HOCHSCHULE DER MEDIEN



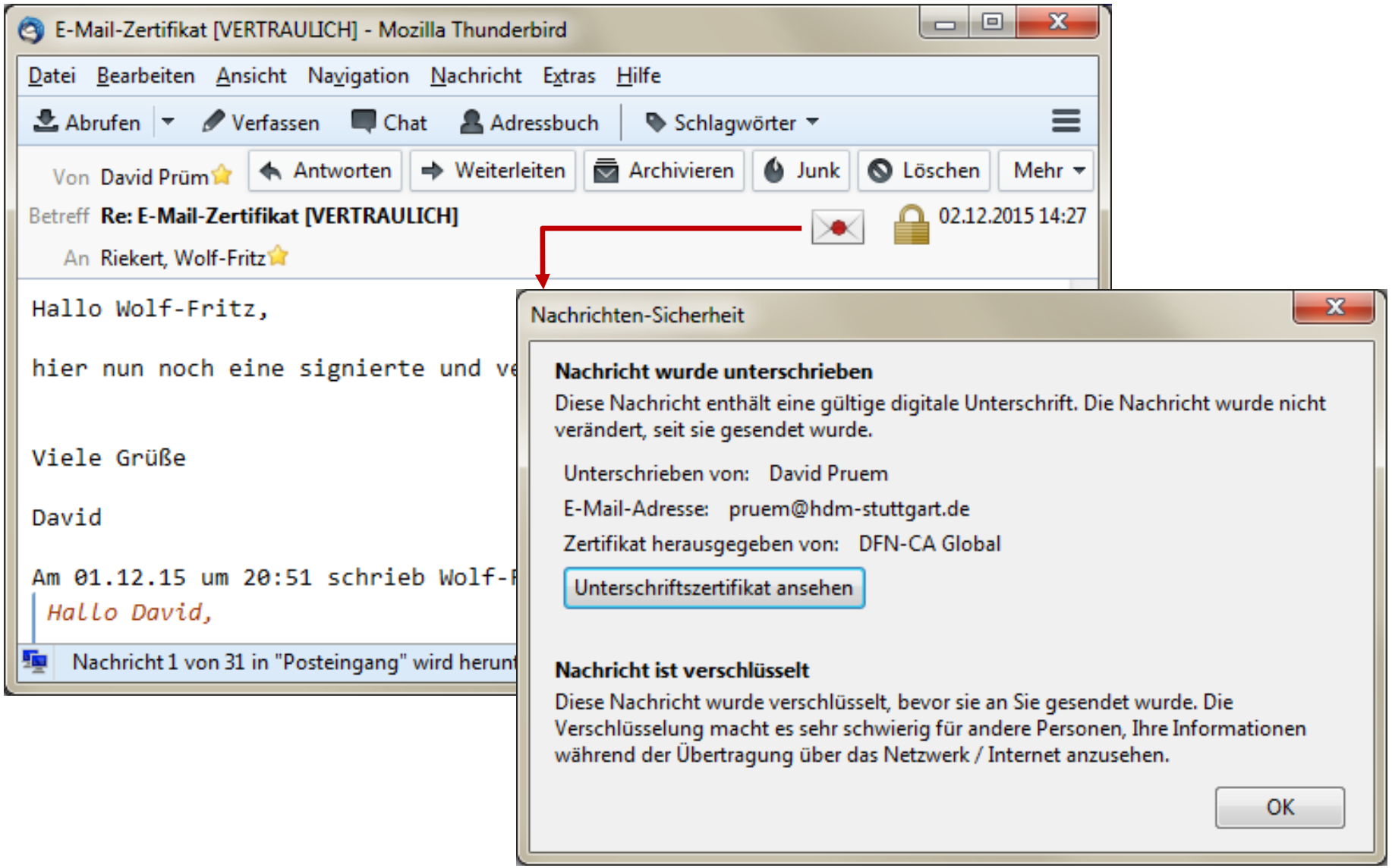
SIGNIERTE EMAILS MIT S/MIME

HOCHSCHULE DER MEDIEN



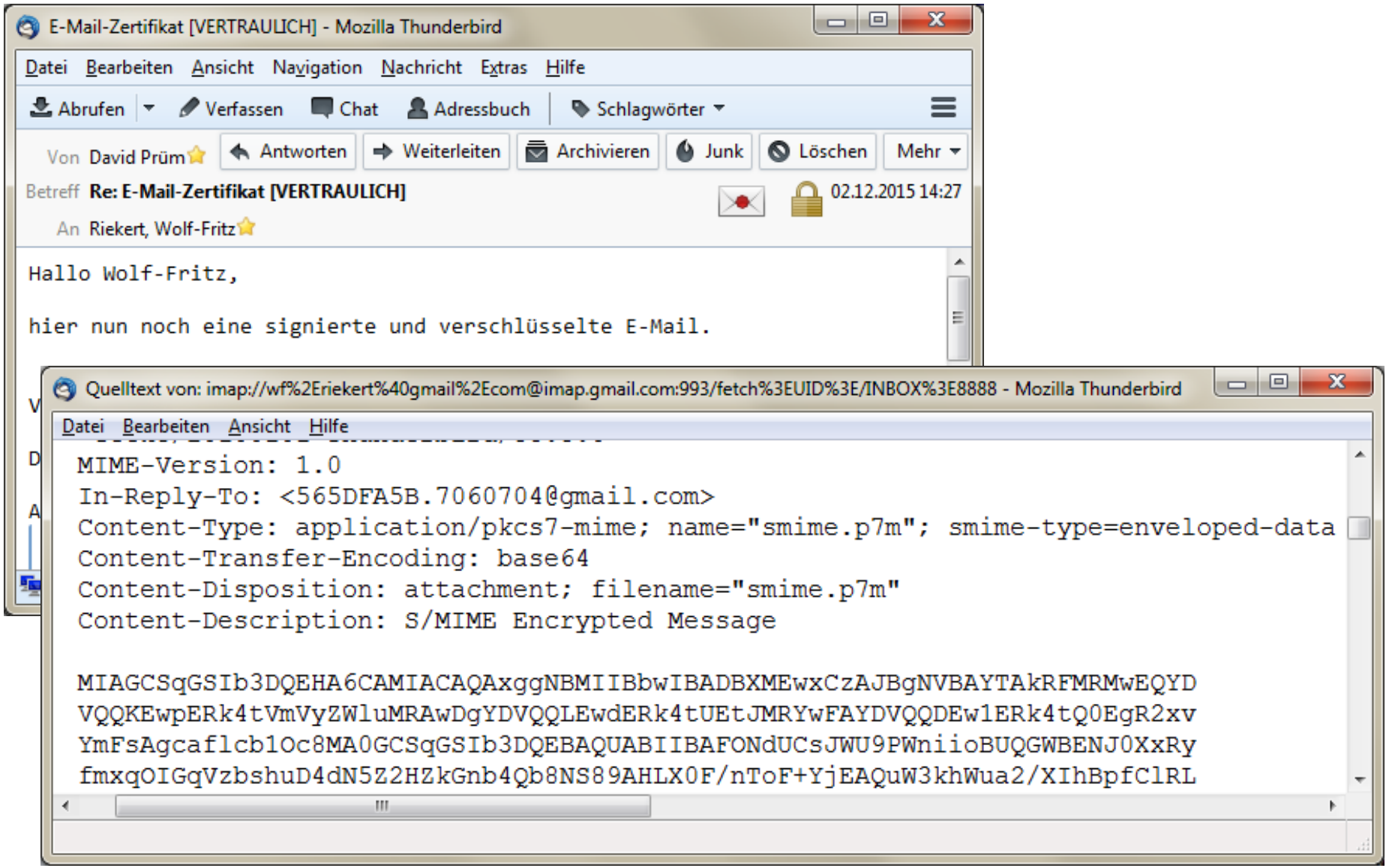
VERSCHLÜSSELTE E-MAILS MIT S/MIME

HOCHSCHULE DER MEDIEN



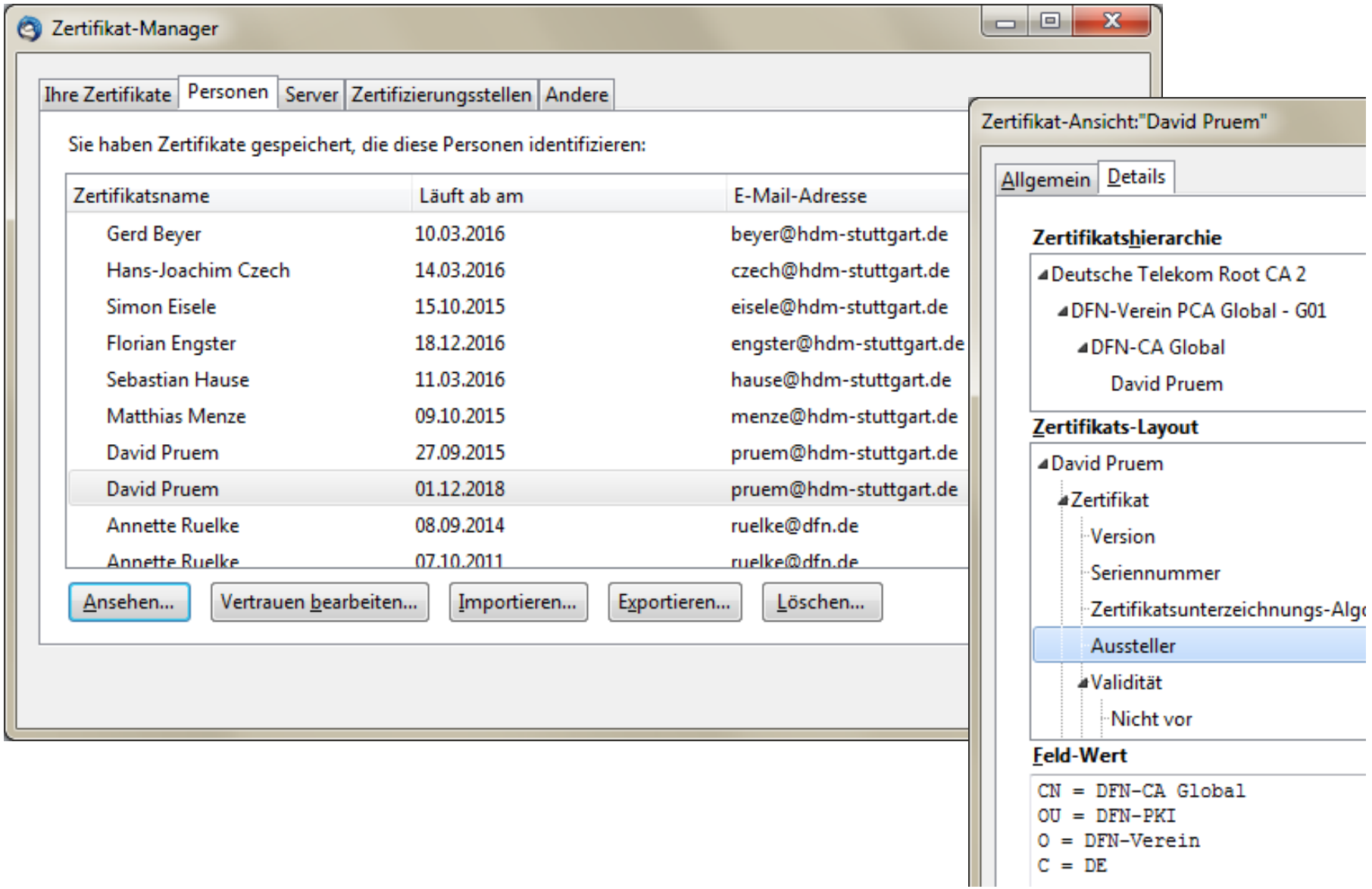
VERSCHLÜSSELTE E-MAILS MIT S/MIME: DER QUELLTEXT

HOCHSCHULE DER MEDIEN



ZERTIKATSPEICHER EINES MAIL-CLIENTS (THUNDERBIRD)

HOCHSCHULE DER MEDIEN



STEGANOGRAPHIE

Alternatives Verfahren zum Schutz von Nachrichten:

Steganographie = Verstecken von Nachrichten in einer anderen unverfänglichen Nachricht

Beispielsweise wird auf die Information in einem Bild oder einem Musikstück weitere Information gepackt, wobei das Bild bzw. das Musikstück unsichtbar bzw. unhörbar verändert wird.

Ggf. werden zusätzlich noch Kryptographietechniken angewandt.

Vorteil der Steganographie: Die Nachricht wird als solche von Uneingeweihten gar nicht erkannt.

TEIL 7: AUFBAU VON WEBSITES

Wesentliches Ziel dieser Lehreinheit ist der Aufbau einer Website mit Hilfe von HTML und CSS.

Hierfür sind folgende Kenntnisse erforderlich:

- Allgemeine Funktionsweise des WWW (bereits vermittelt, hier nochmals kurz wiederholt)
- Web-Seitengestaltung mit der Hypertext Markup Language (HTML)
- Übertragung von Dateien (insbesondere HTML-Dateien, Grafiken, CSS-Formatvorlagen) auf einen Web-Server mit Hilfe von sicherem FTP (FTP über SSH).

Diese Kenntnisse werden im Folgenden vermittelt.

DAS WORLD WIDE WEB (WWW)

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

Server: Web-Server (z.B. Apache HTTP Server, Microsoft Internet Information Services)

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

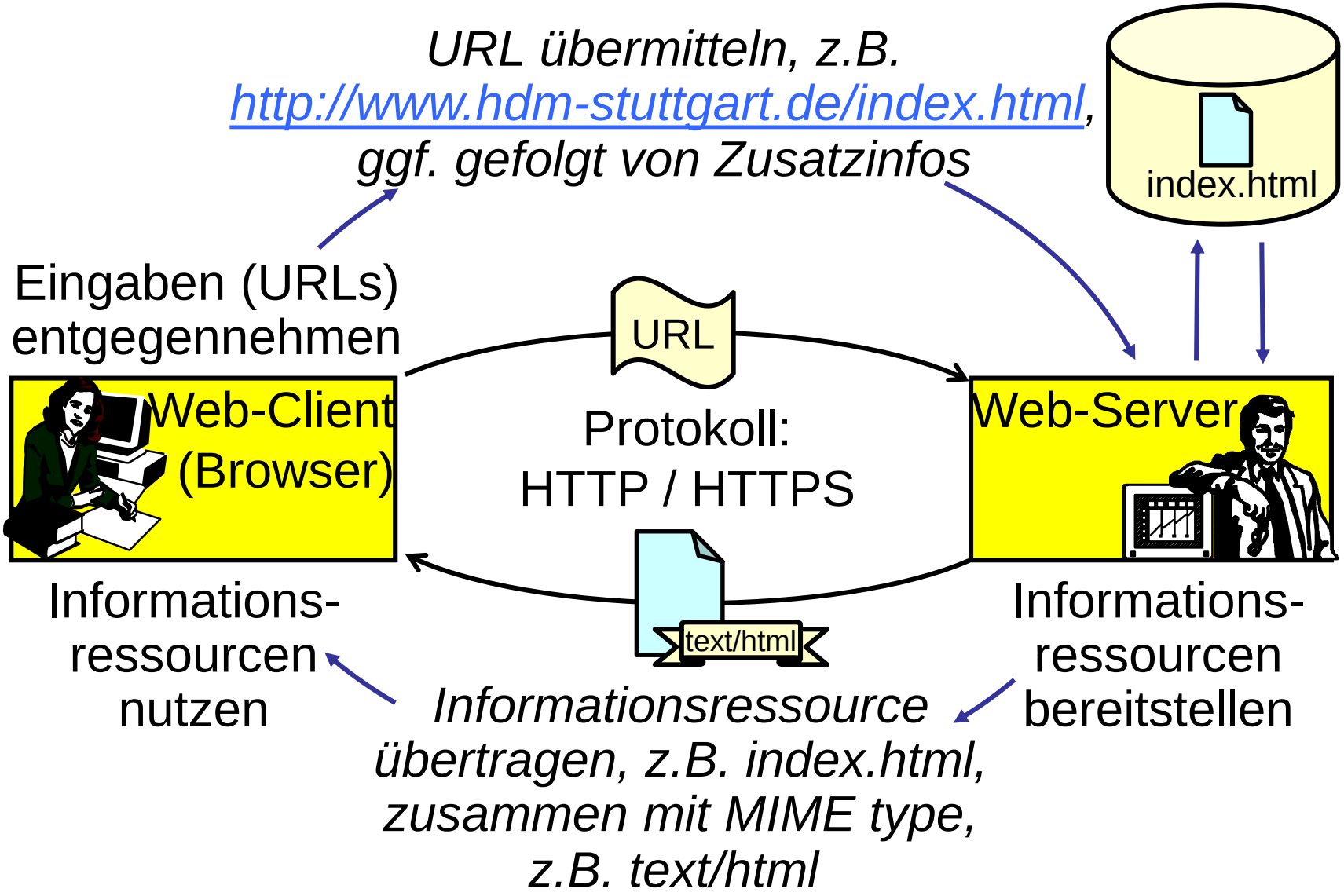
Art des Dienstes: Verbindungsloser Anfrage/Antwort-Dienst

Protokolle: Hypertext Transfer Protokoll (HTTP), sichere Protokollvariante HTTPS (HTTP Secure, verschlüsselt, signiert)

Transportprotokoll: TCP (verbindungsorientiert!) über Port 80 (HTTP) bzw. Port 443 (HTTPS)

WEB-CLIENT (BROWSER) UND WEB-SERVER (WIEDERHOLUNG)

HOCHSCHULE DER MEDIEN



UNIFORM RESOURCE LOCATOR (URL) (WIEDERHOLUNG)

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, z.B. **http:** bzw **https:** für Hypertext Transfer Protocol (Secure)

//Domain = Bezeichnung des Servercomputers im Internet

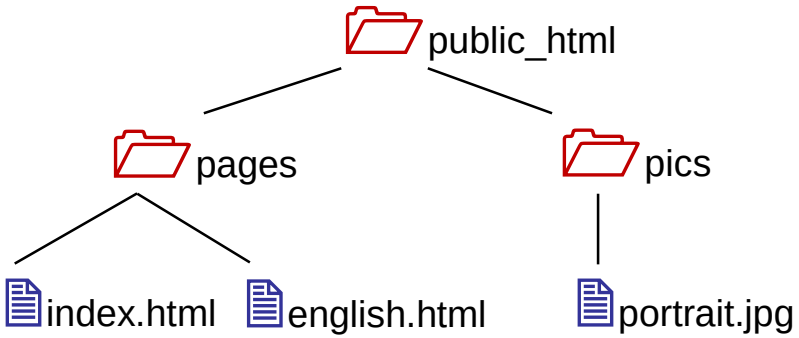
:Port = Kommunikationsport des Web-Server-Programms, i.d.R. nicht erforderlich, da Standardwert = 80

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

URLs: VARIANTEN

Relative URLs: Webseiten 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 Webseite, hier index.html)
- ../pics/portrait.jpg (liegt im Nachbarverzeichnis pics)



Andere Protokolle: Außer http: und https: ist auch **ftp:** möglich (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).

HTML: HYPERTEXT MARKUP LANGUAGE

- Hypertext Markup Language (HTML) = Dokumentenbeschreibungssprache des WWW
  - ⇨ Web-Seiten werden durch HTML-Dateien beschrieben
  - ⇨ Hypertext: Die Dokumente sind über Links verknüpft
  - ⇨ Markup: Die Bedeutung der Dokumentinhalte wird durch Markierungen mit der HTML-Sprache festgelegt.
- HTML legt primär die logische **Struktur** von Dokumenten fest: Überschriften, Absätze, Abbildungen, Tabellen, Links
- Mit Formatvorlagen in der Sprache CSS (Cascaded Style Sheets) kann die genaue Darstellung (das **Layout)** festgelegt werden.
- Gestaltung von HTML-Seiten
  - ⇨ im HTML-Quelltext mit einem reinen Texteditor
  - ⇨ oder mit einem so genannten WYSIWYG-Editor („*What You See Is What You Get*“)

EIN EINFACHES HTML-BEISPIEL


```
<!doctype html>
<html>
  <head>
    <meta charset="utf-8" />
    <title>Riekerts Homepage</title>
  </head>

  <body>
    <h1>Willkommen!</h1>
    <img src="riekert.jpg" alt="Foto Riekert" />
    <p>Wolf-Fritz <em>Riekert</em><br />
      <a href="http://www.hdm-stuttgart.de">
        HdM Stuttgart
      </a>
    </p>
  </body>
</html>
```

HTML

- HTML besteht aus Elementen
  - ⇨ Elemente sind markiert durch „Tags“ (sprich „Tägs“)
  - ⇨ Syntax: **<tagname>** *Inhalt* **</tagname>** (Start-Tag, Ende-Tag)
  - ⇨ Anordnung nacheinander (z.B.: ****…****…****…****) oder verschachtelt (z.B.: ****…****…****…****)
  - ⇨ Manche Tags haben keinen Ende-Tag, z.B. **
**, wird oft gekennzeichnet durch einen Schrägstrich: **
**
- Manche Tags haben Attribute
  - ⇨ Syntax: **<tagname attributname = "***Wert***">**
- Die Tags werden im Browser nicht angezeigt
  - ⇨ Sie „sagen“ dem Browser, was der Tag-Inhalt bedeutet
  - ⇨ z.B. dass es sich um eine Überschrift oder einen Hyperlink handelt

EINIGE BEISPIELHAFTE HTML-ELEMENTE

HOCHSCHULE DER MEDIEN

HTML-Element	Anfangskennung	Endekennung
HTML-Wurzel	`<html>`	`</html>`
Kopfteil	`<head>`	`</head>`
Metadaten	`<meta … />`	
Dokumenttitel	`<title>`	`</title>`
Dokumentrumpf	`<body>`	`</body>`
Überschrift Gr. 1	`<h1>`	`</h1>`
Überschrift Gr. 2	`<h2>`	`</h2>`
Absatz (paragraph)	`<p>`	`</p>`
Zeilenwechsel (break)	` `	
Betont (emphasized)	`<em>`	`</em>`
Hyperlink	`<a href = "URL">`	`</a>`
Graphik	`<img src = "URL" />`	

ERSTELLEN VON WEB-SEITEN: DAS HTML-GRUNDGERÜST

HOCHSCHULE DER MEDIEN

```
<!doctype html>
<html>
  <head>
    <meta charset="utf-8" />
    <title>Titel der Seite</title>
  </head>

  <body>
    <h1>Hauptüberschrift</h1>
    <h2>Unterüberschrift</h2>
    <img src="foto.jpg" alt="Ein Foto" />
    <p>Ein Absatz (Fließtext) mit einem Link:
       <a href=„http://www.hdm-stuttgart.de“ />
       HdM Stuttgart </a>
    </p>
  </body>
</html>
```

BLOCK-ELEMENTE UND INLINE-ELEMENTE

Es gibt zwei Arten von HTML-Elementen: **Block-Elemente** und **Inline-Elemente**

Block-Elemente

- Block-Elemente erzwingen eine neue Zeile davor und danach
- Block-Elemente nehmen die volle Breite
- Beispiele: **p** (Absatz), **h1**, **h2**, **h3**, … (Überschriften)
- Block-Element ohne weitere Eigenschaften: **div**

Inline-Elemente

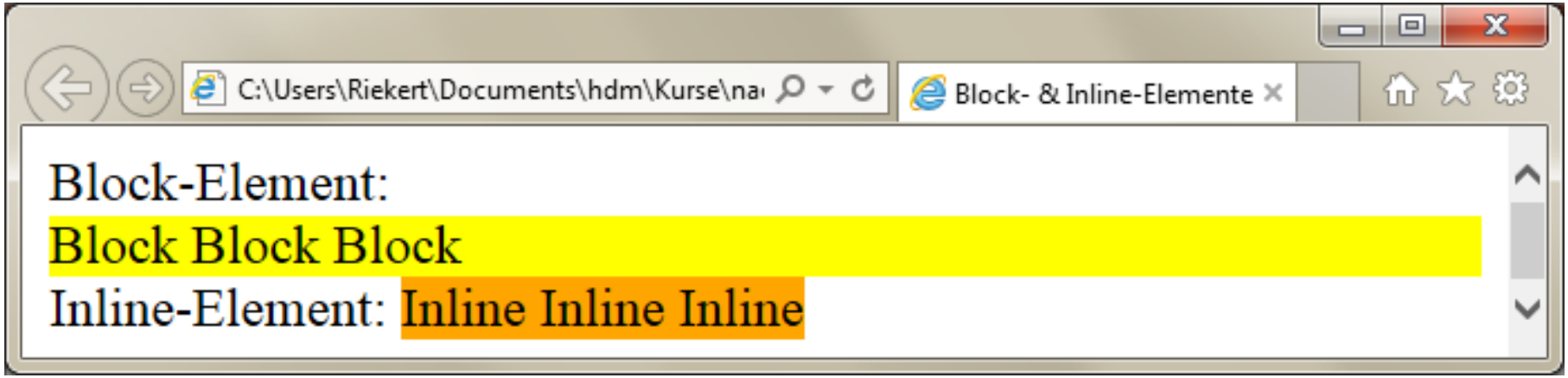
- Inline-Elemente erzwingen **keine** neue Zeile
- Inline-Elemente sind nur so breit wie der Inhalt
- Beispiele: **a** (Hyperlink), **em** (Betonung) …
- Inline-Element ohne weitere Eigenschaften: **span**

UNTERSCHIED INLINE-ELEMENT UND BLOCK-ELEMENT

HTML-Code-Ausschnitt:

```
…
Block Element:
        <div style="background:yellow;"> Block Block Block </div>

Inline Element:
        <span style="background:orange;"> Inline Inline Inline </span>
…
```



WOHLGEFORMTHEIT

HTML-Dokumente bezeichnet man als **wohlgeformt**, wenn sie die Syntax von XML (einer Sprachfamilie HTML-artiger Sprachen) einhalten. Insbesondere muss Folgendes gelten:

- Start-Tags, die kein End-Tag haben, soll man mit einem schließenden Schrägstrich kennzeichnen (z.B. `<br />`)
- Konsistente Groß-/Kleinschreibung (nicht: `<b> … </B>`)
  - ⇨ Empfehlung: Durchweg Kleinschreibung verwenden!
- Kein Überlappen von Tags (also nicht: `<b><i>…</b></i>`)
- Alle Attribute müssen einen Wert haben, der in Anführungszeichen (" " oder ' ') eingeschlossen ist.
  Verboten: `<tag att=wert>…</tag>` und `<tag att>…</tag>`
  Richtig: `<tag att="wert"> … </tag>`

Wohlgeformtheit ist nicht zwingend gefordert, aber sinnvoll.

VALIDITÄT

- Der Browser kann HTML-Dokumente nur darstellen, wenn sie korrektes HTML enthalten. Man nennt sie dann valide.
- Valide **HTML-Dokumente** erfüllen folgende Forderungen:
  - ⇨ Sie erfüllen die allgemeine HTML-Syntax (Notation von Tags, Attributen usw.), ggf. Wohlgeformtheit
  - ⇨ Sie enthalten nur definierte Elemente und Attribute.
- Überprüfung im „Validator“ (http://validator.w3.org/) oder in komfortablem HTML-Editor (z.B. Dreamweaver)
  - ⇨ Es gibt verschiedene HTML-Versionen. Die aktuellste Version ist HTML 5; diese sollte bei der Validitätsprüfung eingestellt sein.

HTML: LITERATUR UND INTERNETRESSOURCEN

HOCHSCHULE DER MEDIEN

Beim Erstellen von Web-Seiten mit Texteditoren benötigt man ein Handbuch, um HTML-Befehle nachzuschlagen.

Hier zwei Empfehlungen:

- SELFHTML e.V.: SELFHTML-Wiki. Ein Online-Handbuch zu HTML, CSS und Javascript in Form eines Wiki. http://wiki.selfhtml.org/
- Stefan Münz und Clemens Gull (2013): HTML5-Handbuch. 9. Aufl. Haar bei München: Franzis Verlag GmbH. Online: http://webkompetenz.wikidot.com/docs:html-handbuch

ERSTELLUNG VON WEB-SEITEN

- Auf Ihrem PC oder persönlichen Laptop einen Ordner für alle Ihre Web-Dateien (HTML, JPG, CSS, PHP…) erstellen.
- Für HTML-Code geeigneten Editor starten
  - ⇨ eine **neue Web-Seite erstellen**
  - ⇨ Web-Seite in dem dafür eingerichteten Ordner im lokalen Dateisystem **speichern**
- **Vorschau** mit Web-Browser (Mozilla Firefox, Google Chrome, Safari, Internet-Explorer, …), am besten mehrere Browser verwenden
- Seite mit sicherem **FTP** (SFTP über SSH) auf den Web-Server kopieren
- **Ergebnis** auf Web-Server mit Web-Browser **anschauen**

WEB-SEITEN-EDITOREN

Zum Erstellen von Web-Seiten können verschiedene Arten von Editoren verwendet werden:

- einfache Text-Editoren wie Editor bzw. Notepad (in Windows integriert) oder Textedit (in MacOs integriert). Speichern als reinen Text (plain text) mit Encoding UTF-8.
- Text-Editoren mit Syntaxunterstützung: Brackets (Windows und Mac), Textwrangler (Mac), Notepad++ (Windows), Phase 5 (Windows), alle zum freien Download
- Editoren mit WYSIWYG-Unterstützung („What you see is what you get“): Professionell und kostenpflichtig: Adobe Dreamweaver (in einigen Laboren installiert). Freie Alternativen: Microsoft Expression Web 4, Microsoft Visual Studio Community, Mozilla Seamonkey Composer.

WEB-SEITE ERSTELLEN MIT EINEM REINEN TEXTEDITOR

HOCHSCHULE DER MEDIEN

```
<!doctype html>
<html>
  <head>
    <meta charset="utf-8" />
    <title>Wolf-Fritz Riekerts Homepage</title>
  </head>
  <body>
    <h1>Wolf-Fritz Riekert</h1>
    <p><em>Dies ist meine Homepage</em></p>
    <p><img src="riekert.jpg" width="132" height="131"
          alt="Foto Riekert" /></p>
    <p><a href="http://www.hdm-stuttgart.de">
          Hochschule der Medien Stuttgart</a></p>
    <p><a href="lehrveranstaltungen.html">
          Lehrveranstaltungen</a></p>
  </body>
</html>
```

Allgemeiner Rahmen, kann immer gleich bleiben

Erscheint als Titel von Browserfenster bzw. Tab

Texte eingeben und z.B. als Überschrift <h1>, Absatz <p> oder „betont“ („emphasized“) auszeichnen

Bild einbetten

relative URL

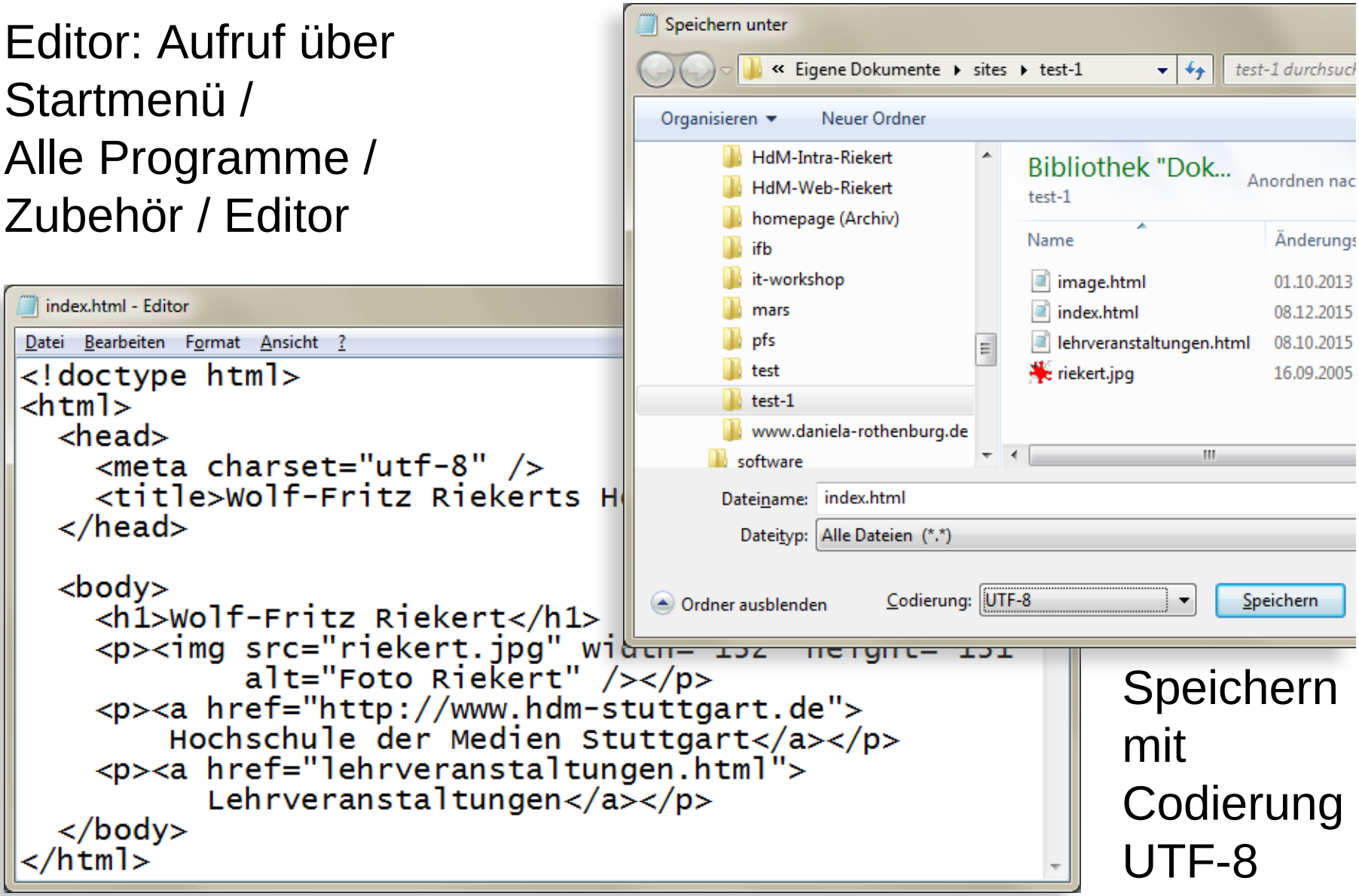
Hyperlink, absolute URL

Hyperlink, relative URL, d.h. Datei liegt in selbem Verzeichnis.

EDITIEREN VON HTML-CODE MIT DEM „EDITOR“ UNTER WINDOWS

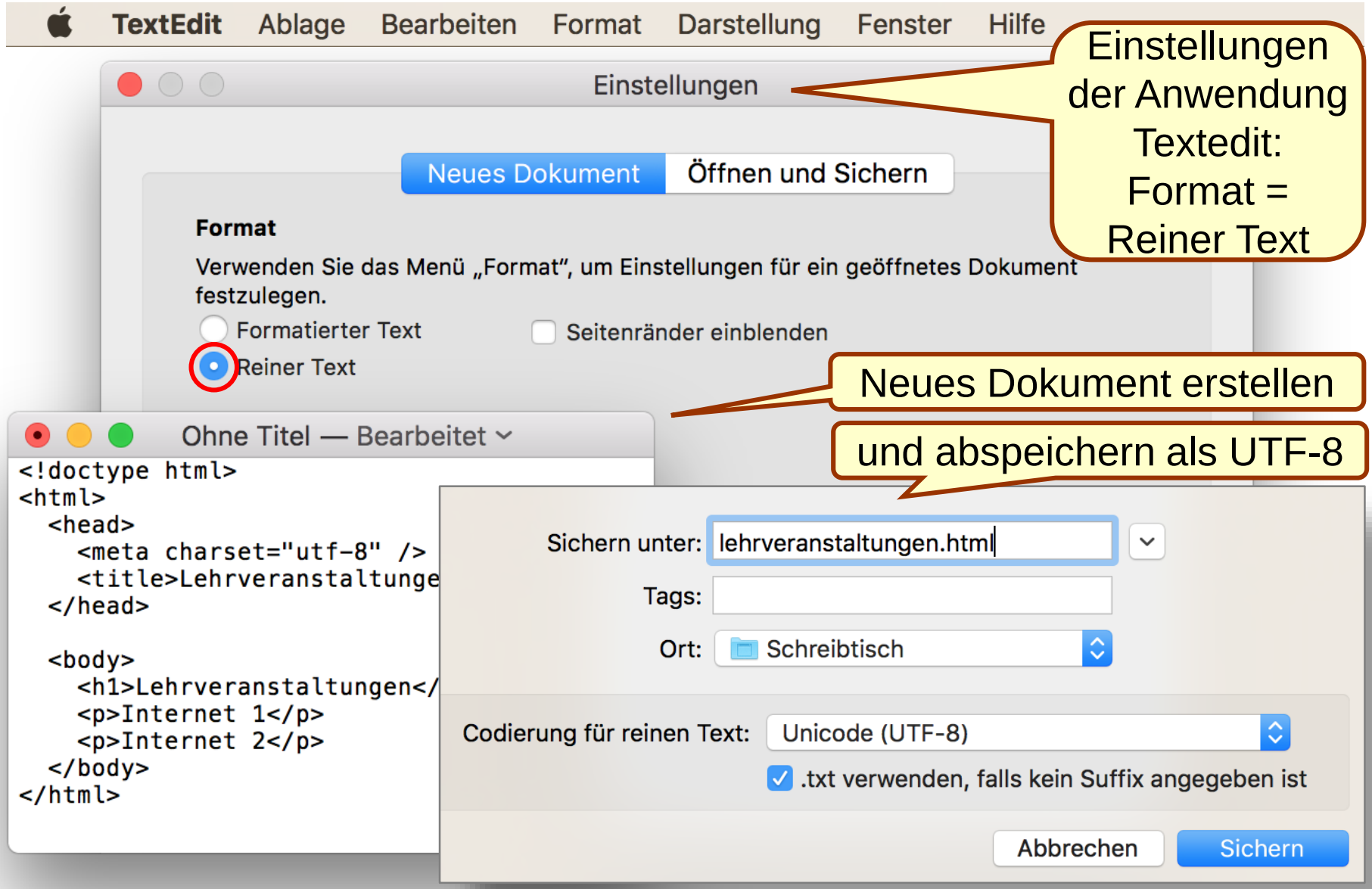
HOCHSCHULE DER MEDIEN

Editor: Aufruf über
Startmenü /
Alle Programme /
Zubehör / Editor



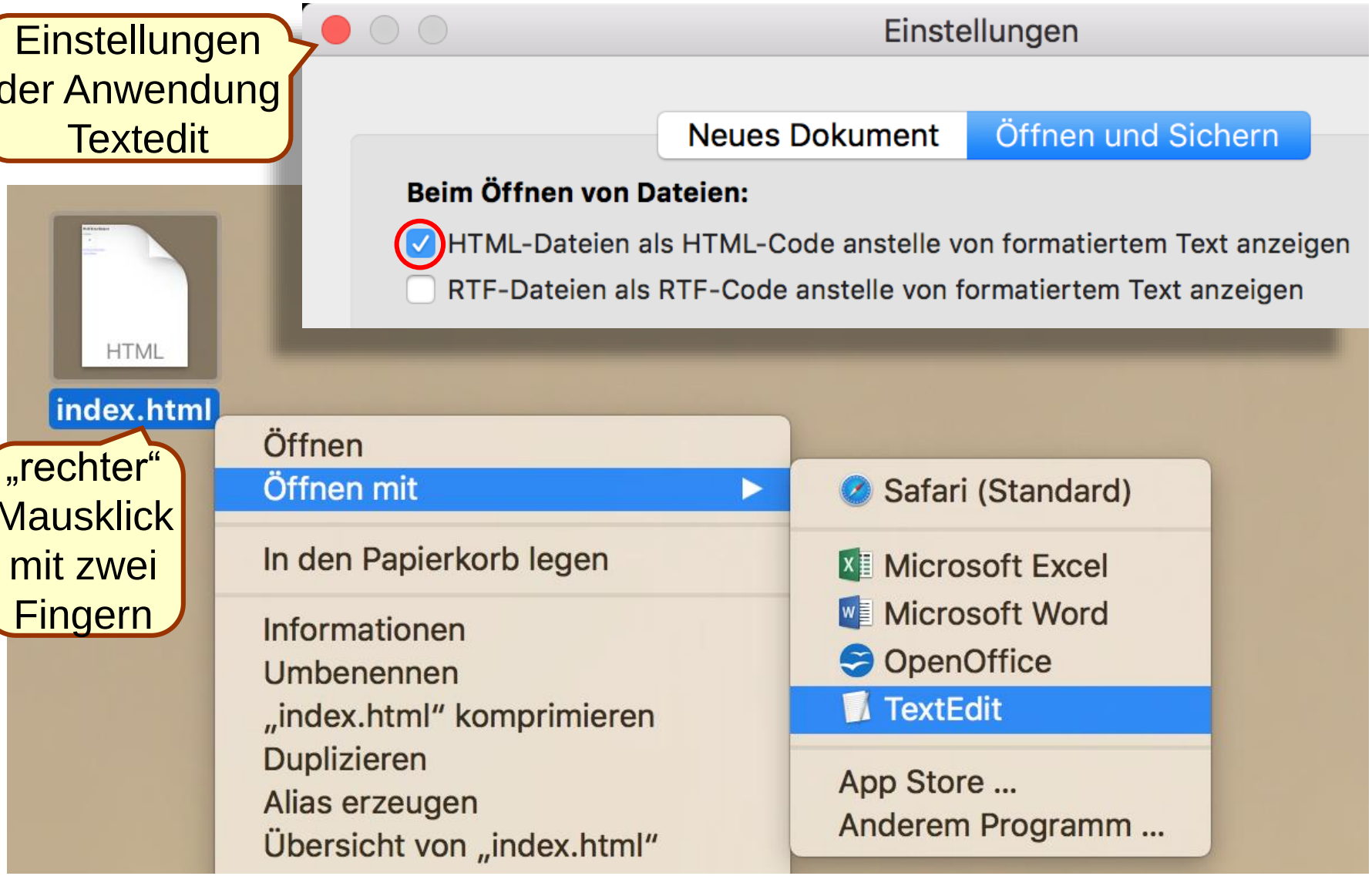
Speichern mit Codierung UTF-8

TEXTEDIT: HTML-DOKUMENTE NEU ERSTELLEN AUF DEM MAC



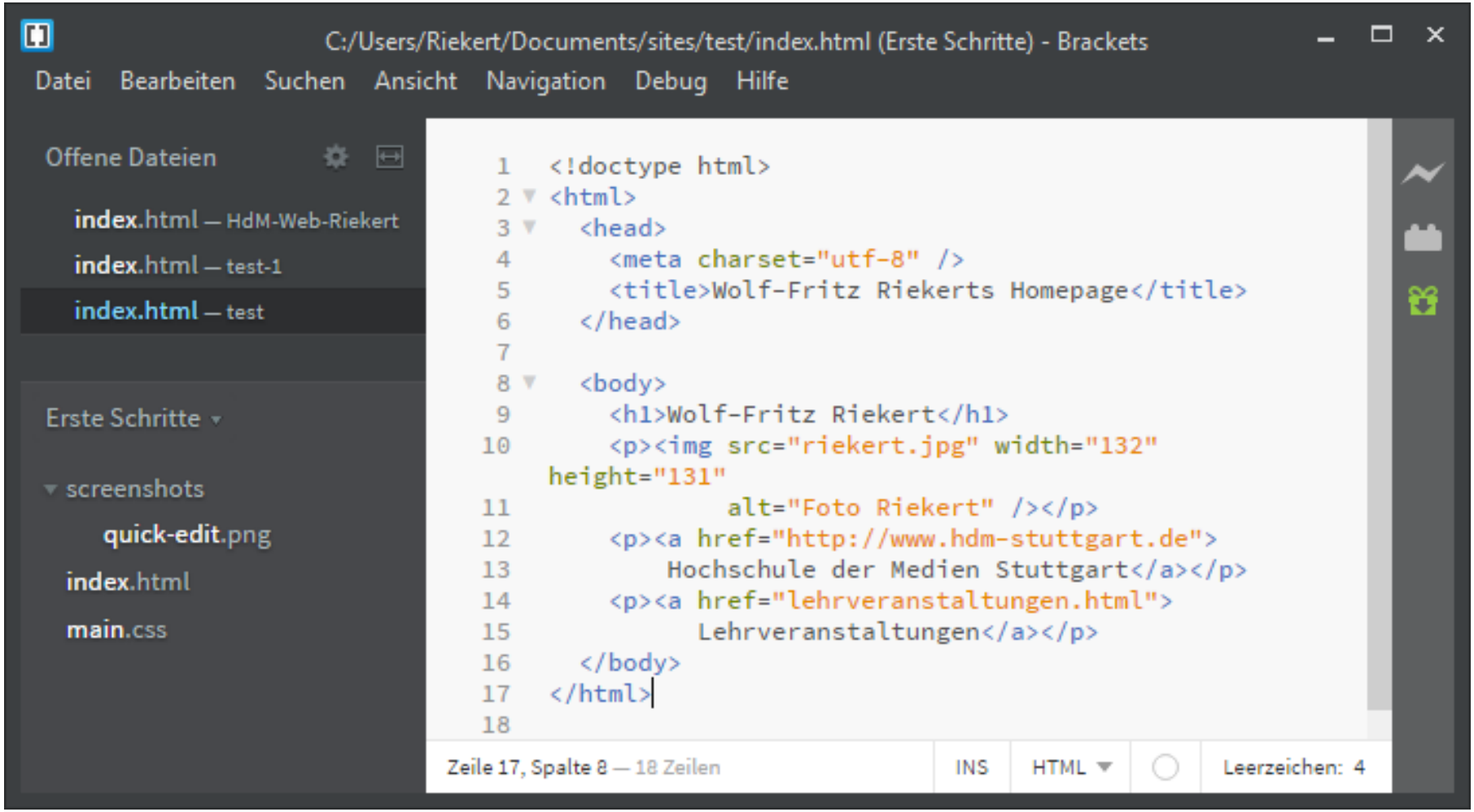
TEXTEDIT: HTML-DOKUMENTE BEARBEITEN AUF DEM MAC

HOCHSCHULE DER MEDIEN



BRACKETS: EIN HTML-EDITOR MIT SYNTAXUNTERSTÜTZUNG

HOCHSCHULE DER MEDIEN



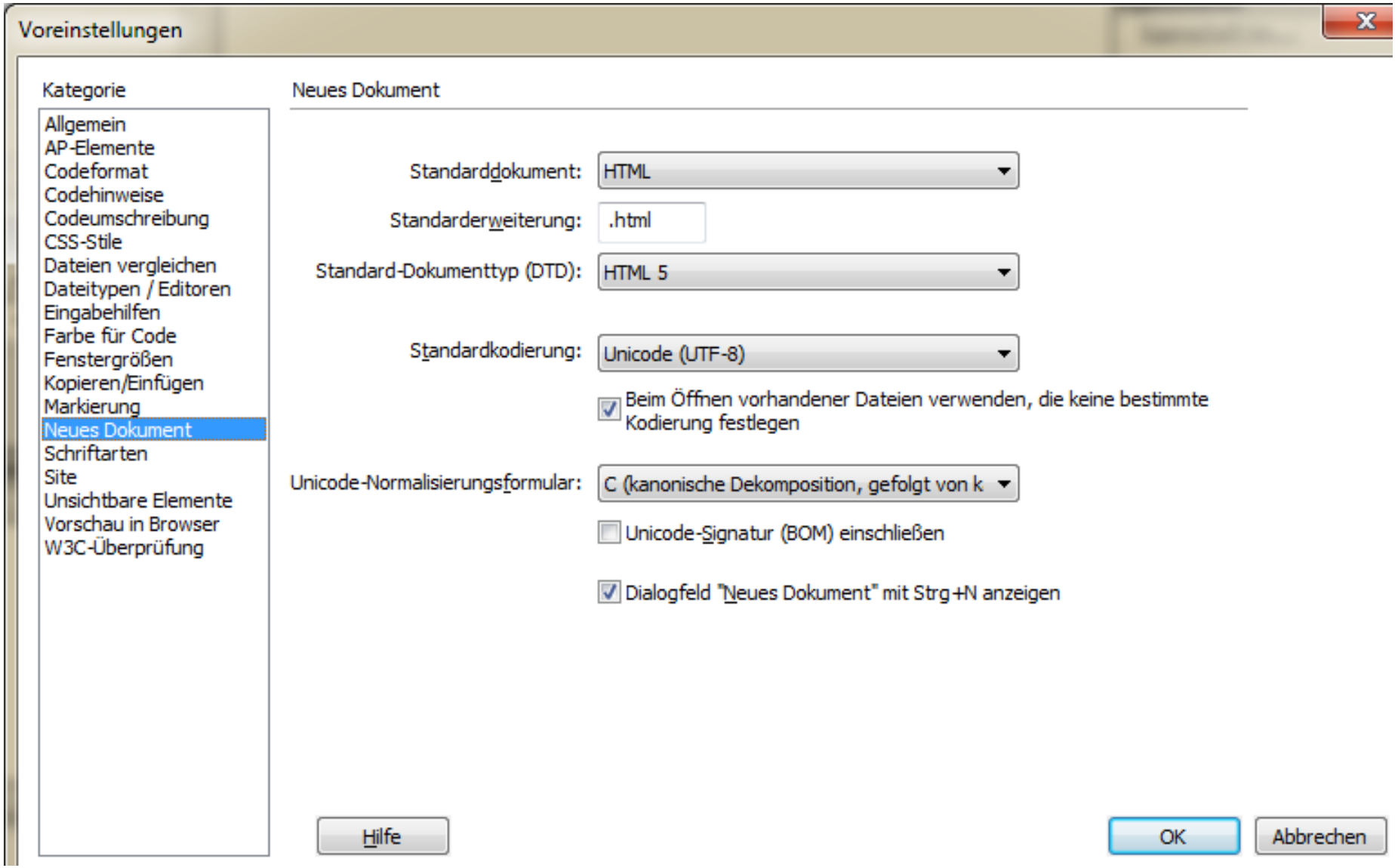
Brackets: ein HTML-Editor mit Syntaxunterstützung.
Freier Download für Windows und Mac unter http://brackets.io

WEB-SEITEN MIT EINEM WYSIWYG-EDITOR BEARBEITEN

- **Voreinstellungen** vornehmen: HTML 5, Unicode (UTF-8), wenn möglich.
- Eigentliche Erstellung der Web-Seite ähnlich wie in Word:
  - ⇨ **Texte** nach Belieben schreiben. Formate ändern usw.
  - ⇨ **Bilder** (JPG, GIF, PNG) einfügen (eigentlich nur verknüpfen)
    - Am besten aus selbem Verzeichnis wie HTML-Datei
  - ⇨ **Hyperlinks** einfügen
    - Textbereich oder Grafik mit der Maus markieren
    - mit Schaltfläche ***Verknüpfung*** URL festlegen
- Sichern mit Menü ***Datei - Speichern unter***
  - ⇨ Als Namen für die Startseite verwendet man **index.html**
  - ⇨ Weitere Web-Seiten erhalten beliebige Namen mit Endung **.html**

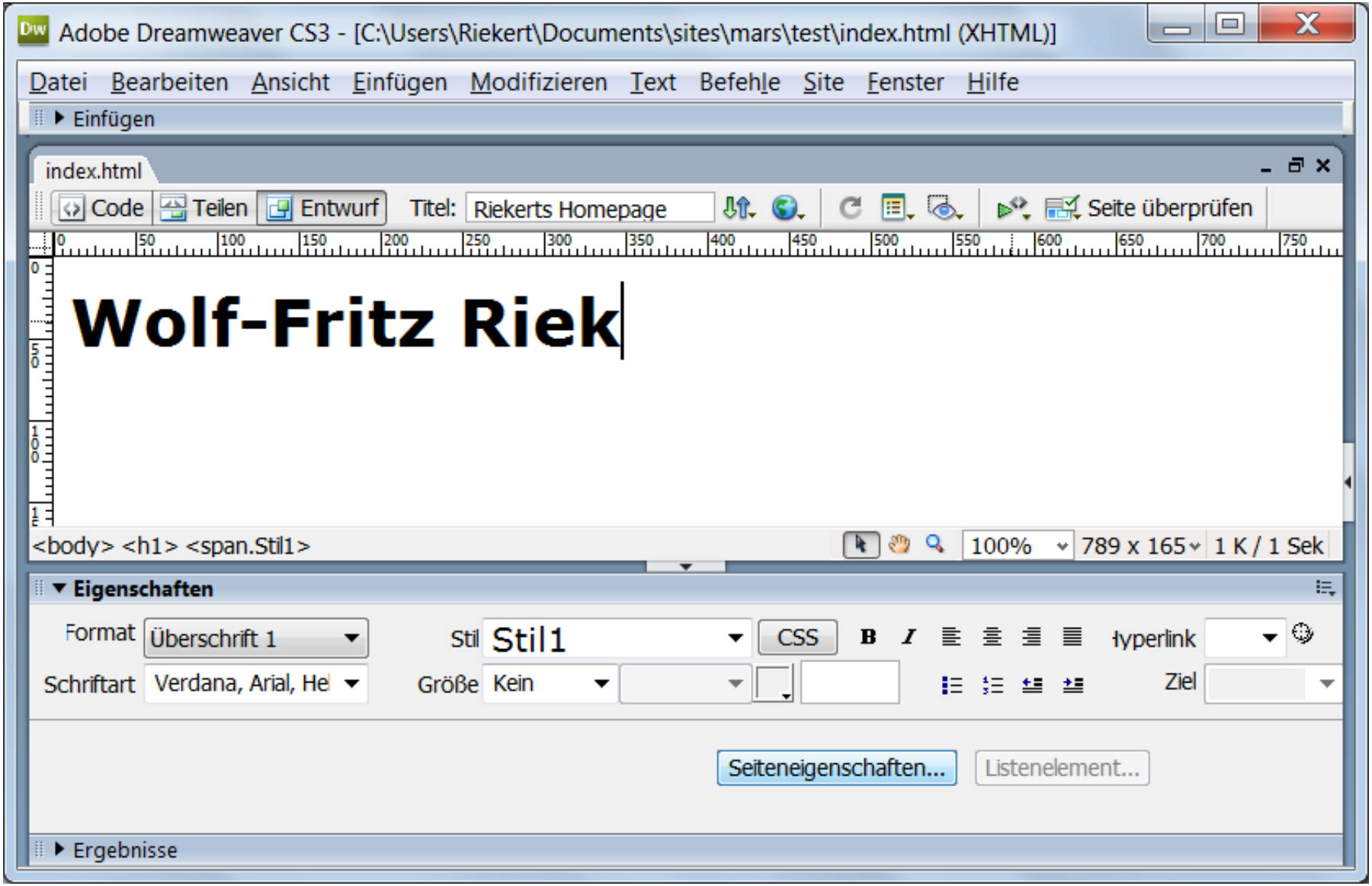
DREAMWEAVER: VOREINSTELLUNGEN

HOCHSCHULE DER MEDIEN



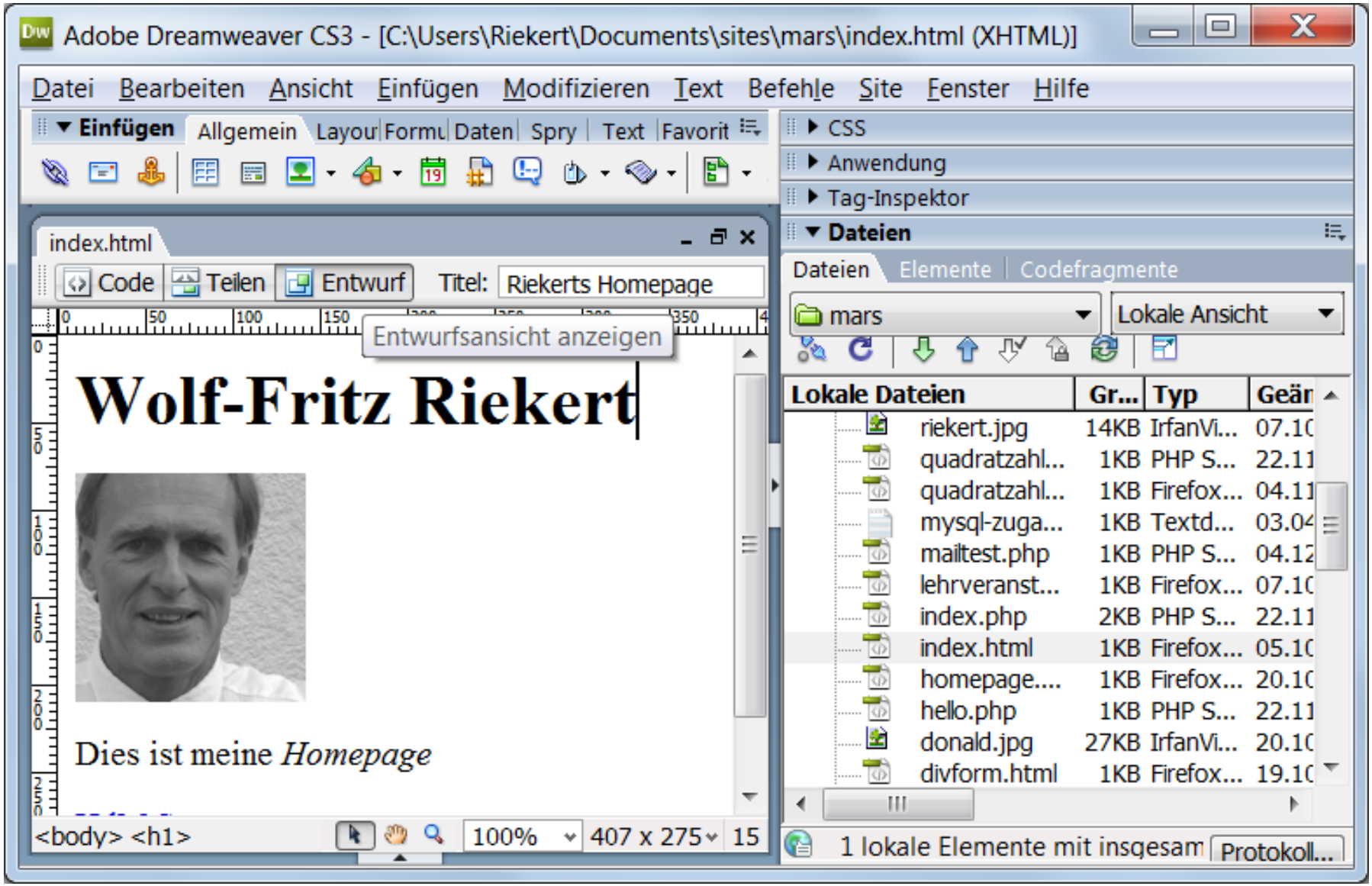
DREAMWEAVER:
NEUE Web-Seite ERSTELLEN

HOCHSCHULE DER MEDIEN



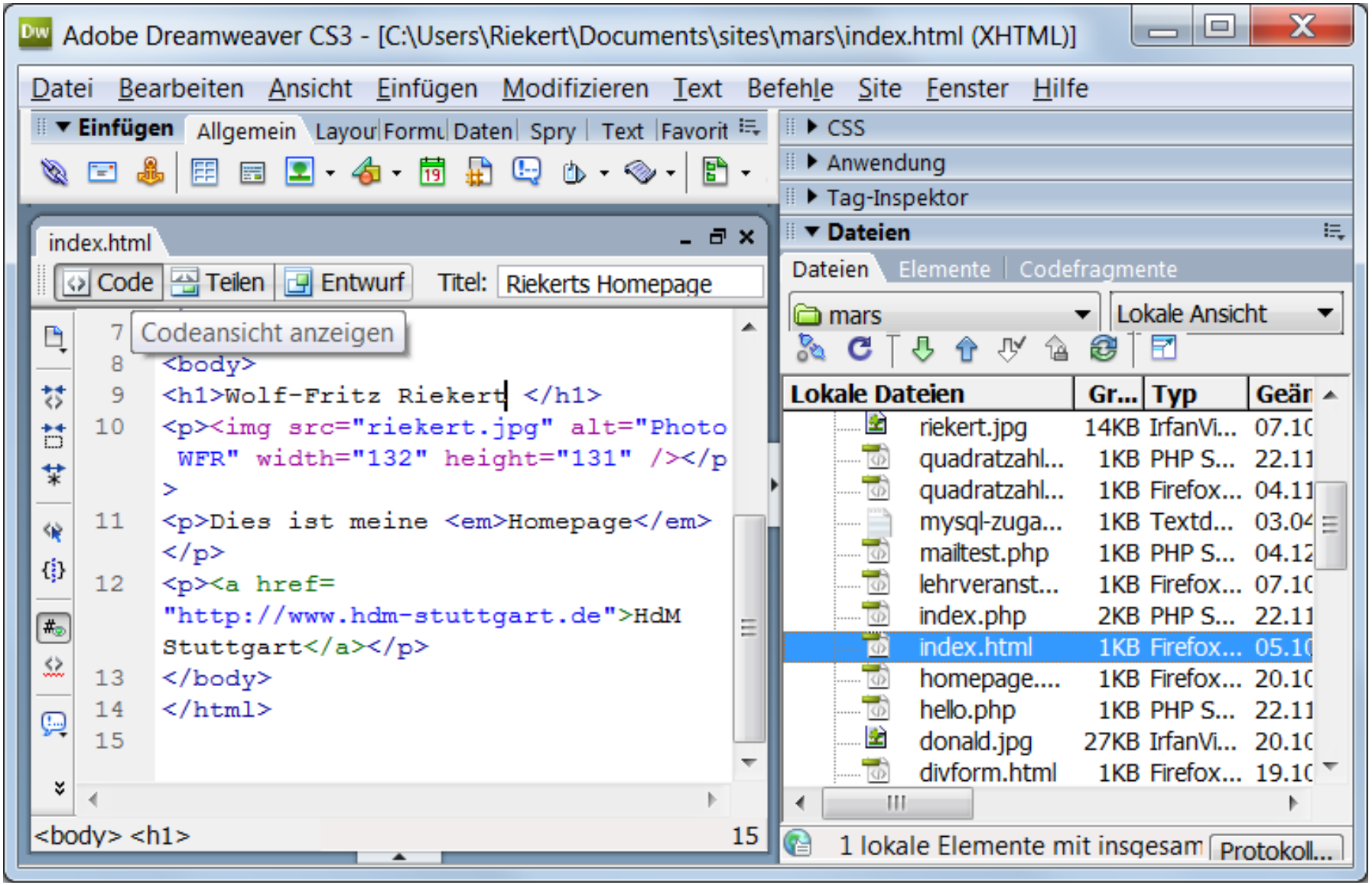
DREAMWEAVER: ENTWURFSANSICHT

HOCHSCHULE DER MEDIEN



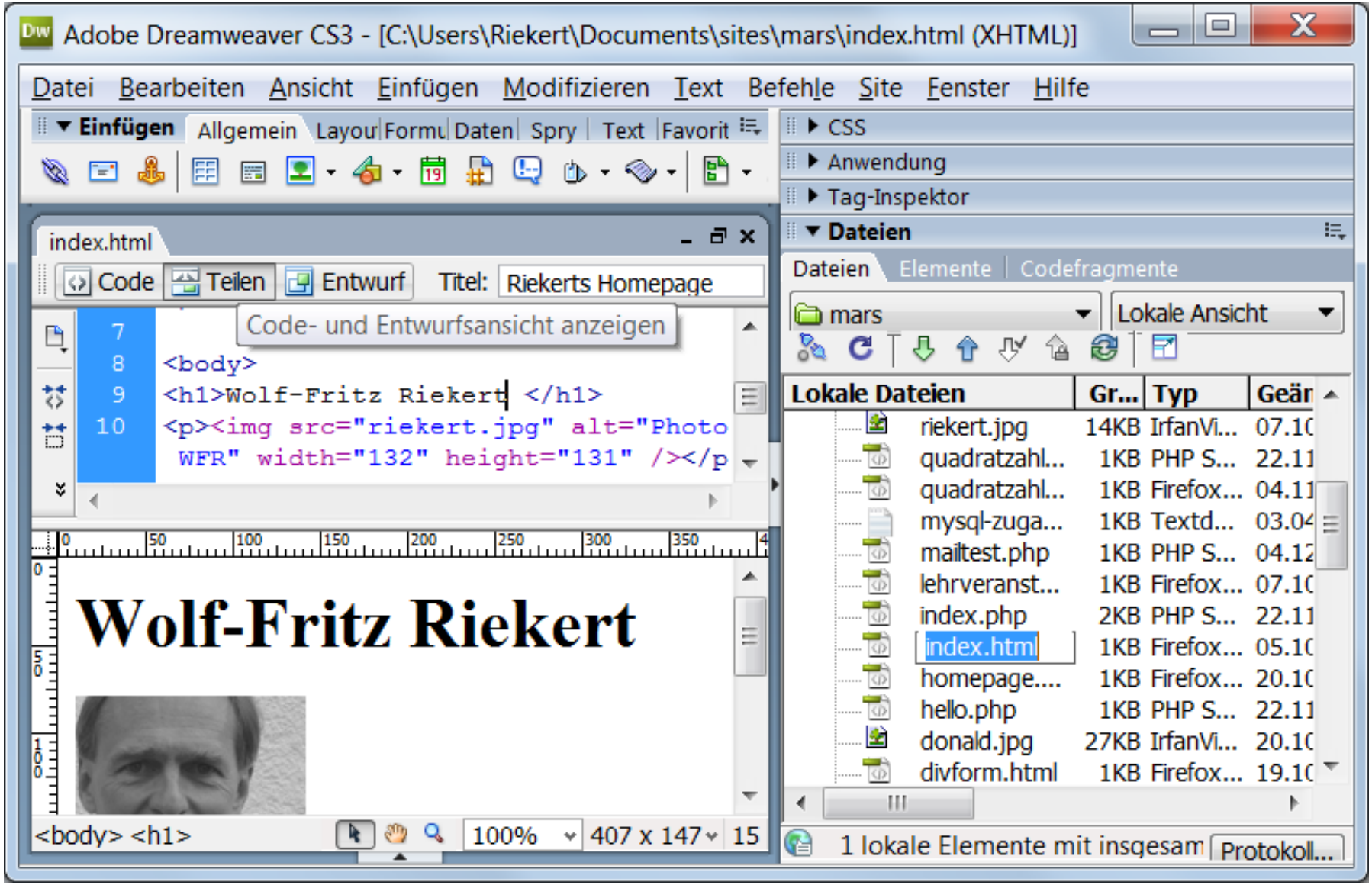
DREAMWEAVER: CODEANSICHT

HOCHSCHULE DER MEDIEN



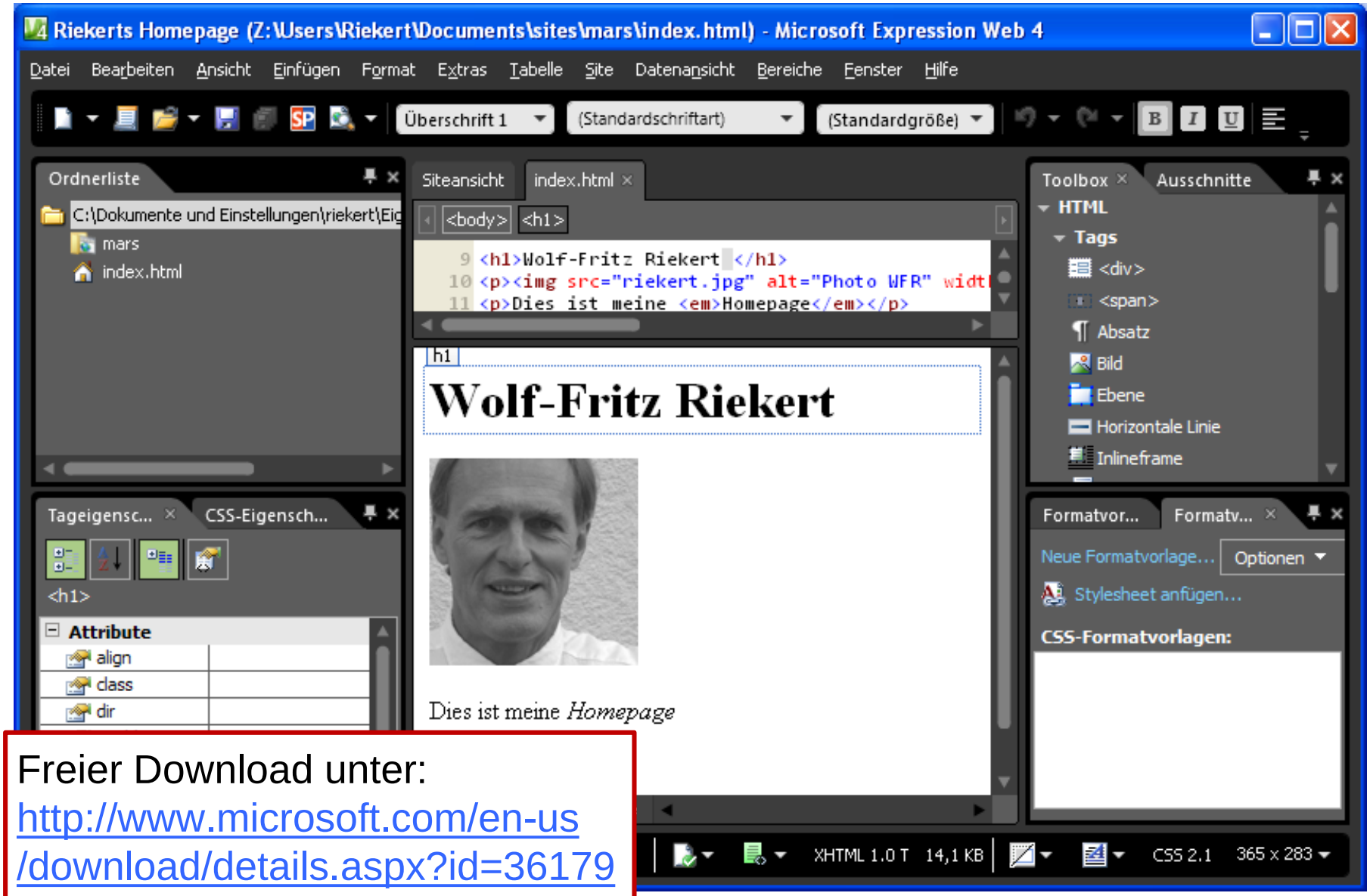
DREAMWEAVER: GETEILTE ANSICHT

HOCHSCHULE DER MEDIEN



ALTERNATIVE ZU DREAMWEAVER: MICROSOFT EXPRESSION WEB

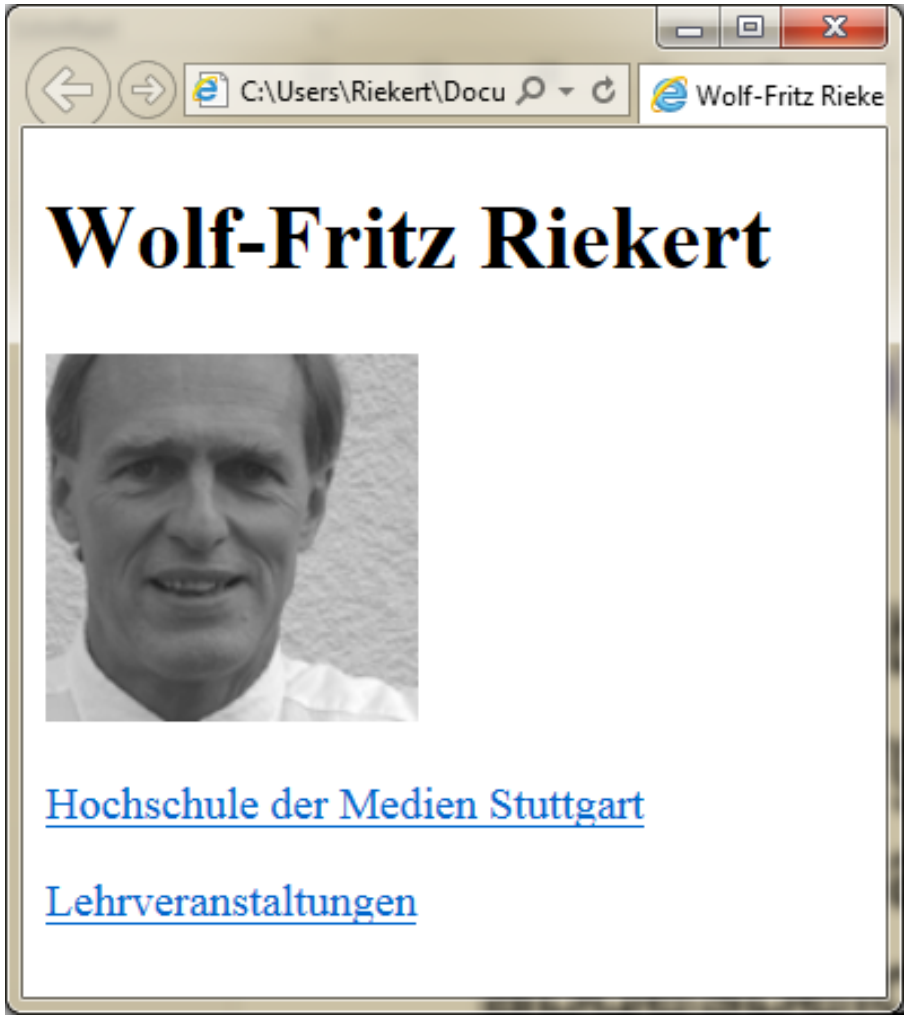
HOCHSCHULE DER MEDIEN



Freier Download unter:
http://www.microsoft.com/en-us/download/details.aspx?id=36179

ANZEIGE DES ERGEBNISSES

- Einen Ordner im lokalen Dateisystem anlegen
- Dort die erzeugte(n) Web-Seite(n) abspeichern
- Vorschau: Web-Seite(n) mit einem Browser anzeigen.
- Web-Seite(n) mit (sicherem) FTP auf ein freigegebenes Verzeichnis auf dem Web-Server kopieren.
- Anzeige der Web-Seite(n) via URL mit Web-Browser von überall auf der Welt



FTP (FILE TRANSFER PROTOCOL)

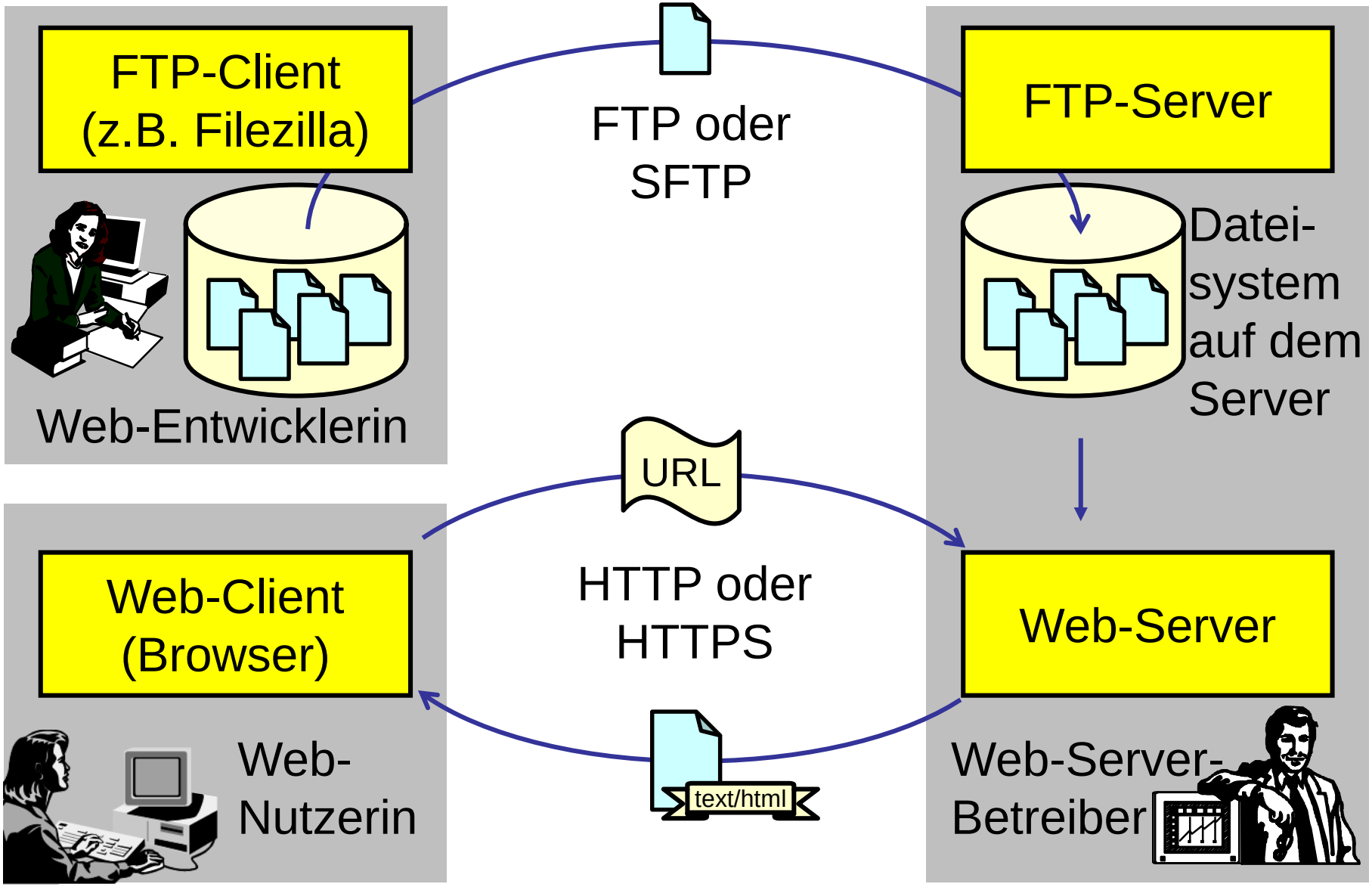
Frage: Wie kommen die Web-Seiten auf den Web-Server?

Antwort: Mit **FTP** (File Transfer Protocol): einem der ältesten Verfahren zur Übertragung von Dateien zwischen Computern im Internet

- Web-Server bieten i.d.R. einen FTP-Dienst an.
- Nutzung mit verschiedenen **FTP-Clients**:
  - ⇨ Windows-basierter FTP-Client **Filezilla** (hier erklärt)
  - ⇨ Eingebaute FTP-Funktion in HTML-Editoren, z.B. Dreamweaver oder Expression Web
- Problem: Der normale FTP-Dienst verschlüsselt Passwörter und Daten nicht
- Abhilfe: Neuere verschlüsselte FTP-Dienste verwenden: sicheres SFTP über SSH (alternativ: FTP über TLS)

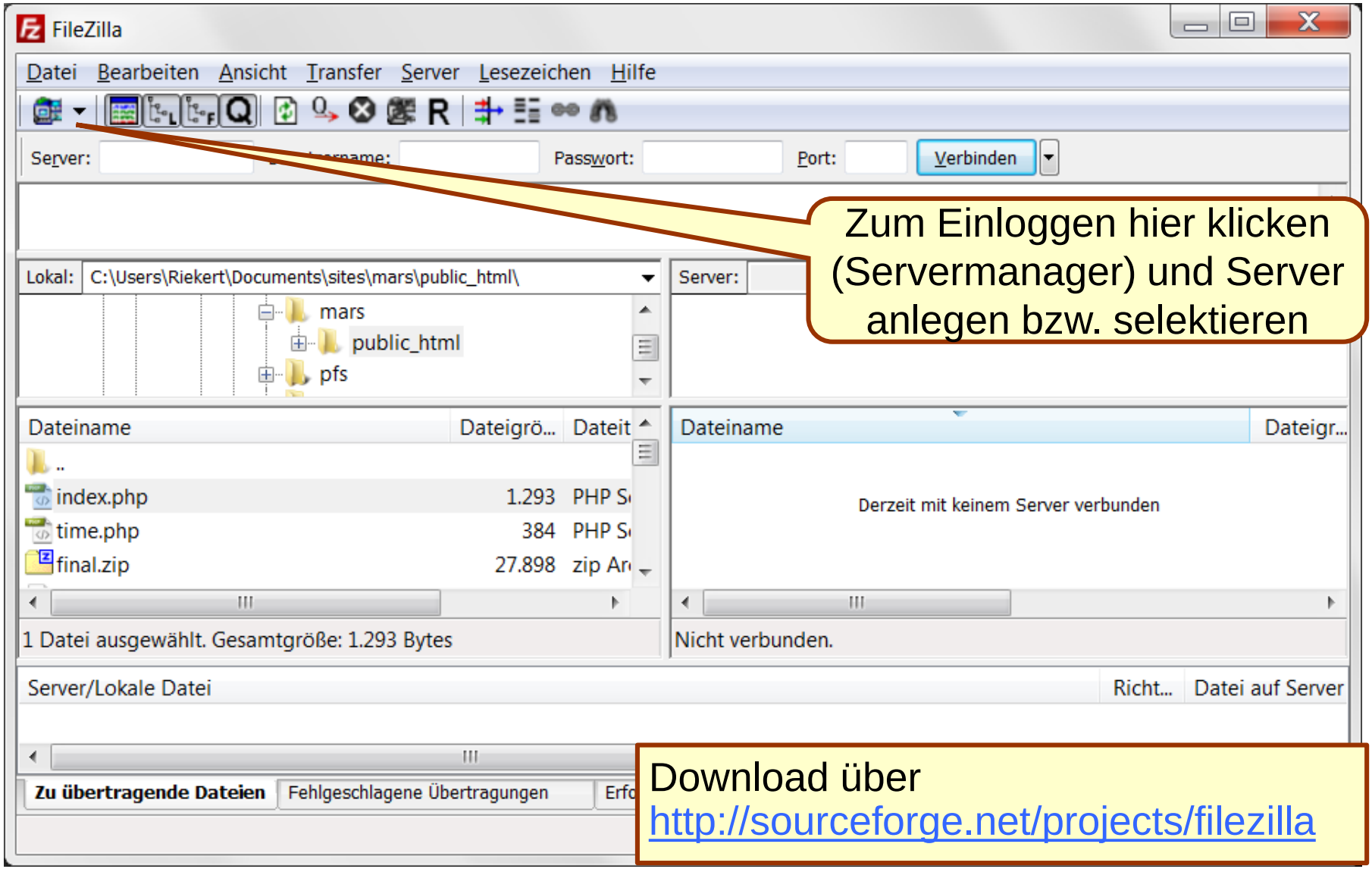
DER FTP-DIENST ÜBERTRÄGT WEB-SEITEN AUF DEN SERVER

HOCHSCHULE DER MEDIEN



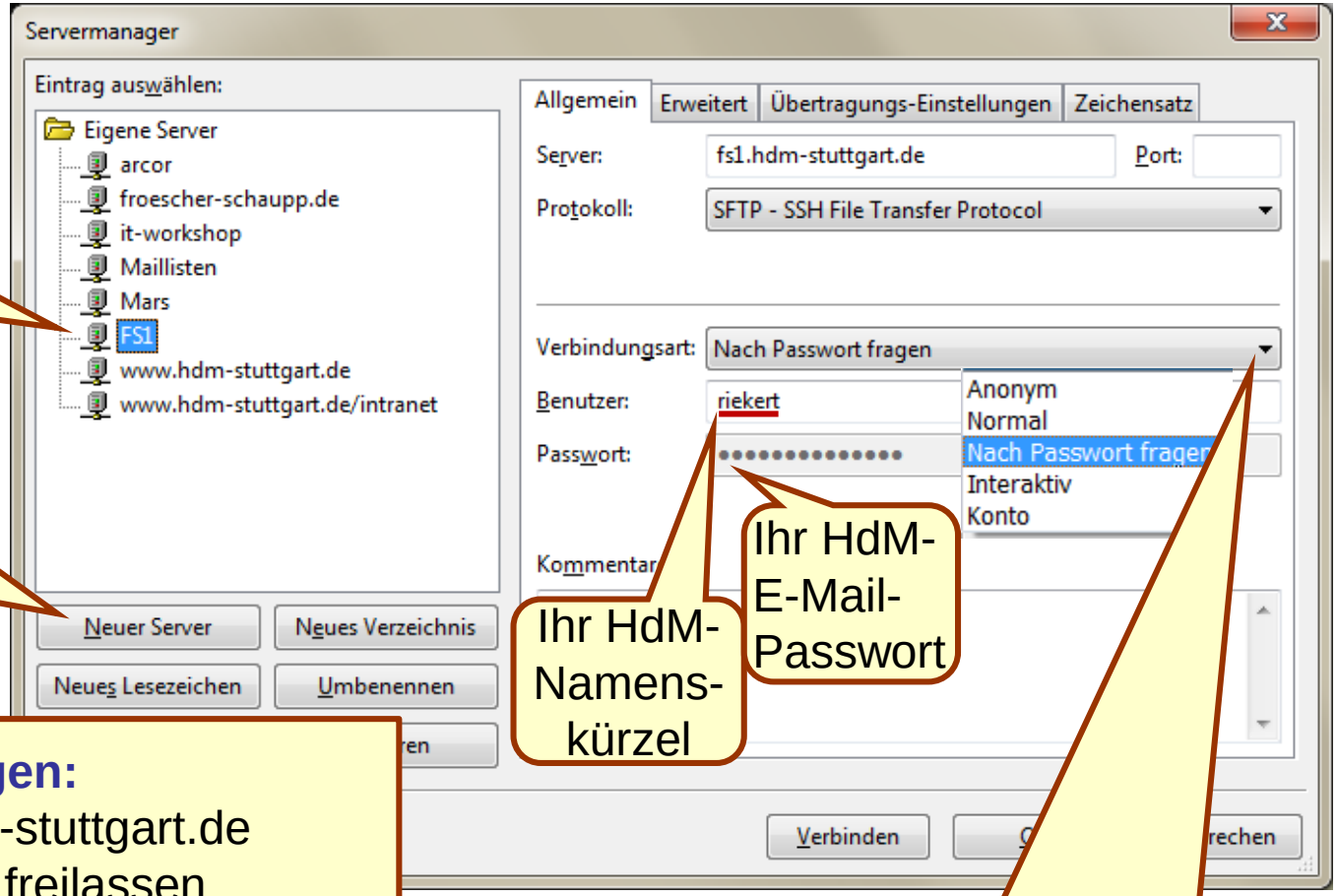
FILEZILLA: FENSTER-BASIERTER FTP-CLIENT

HOCHSCHULE DER MEDIEN



FILEZILLA: SERVERMANAGER

HOCHSCHULE DER MEDIEN



Hier Server selektieren

Beim ersten Mal neuen Server FS1 anlegen

Ihr HdM-Namens-kürzel

Ihr HdM-E-Mail-Passwort

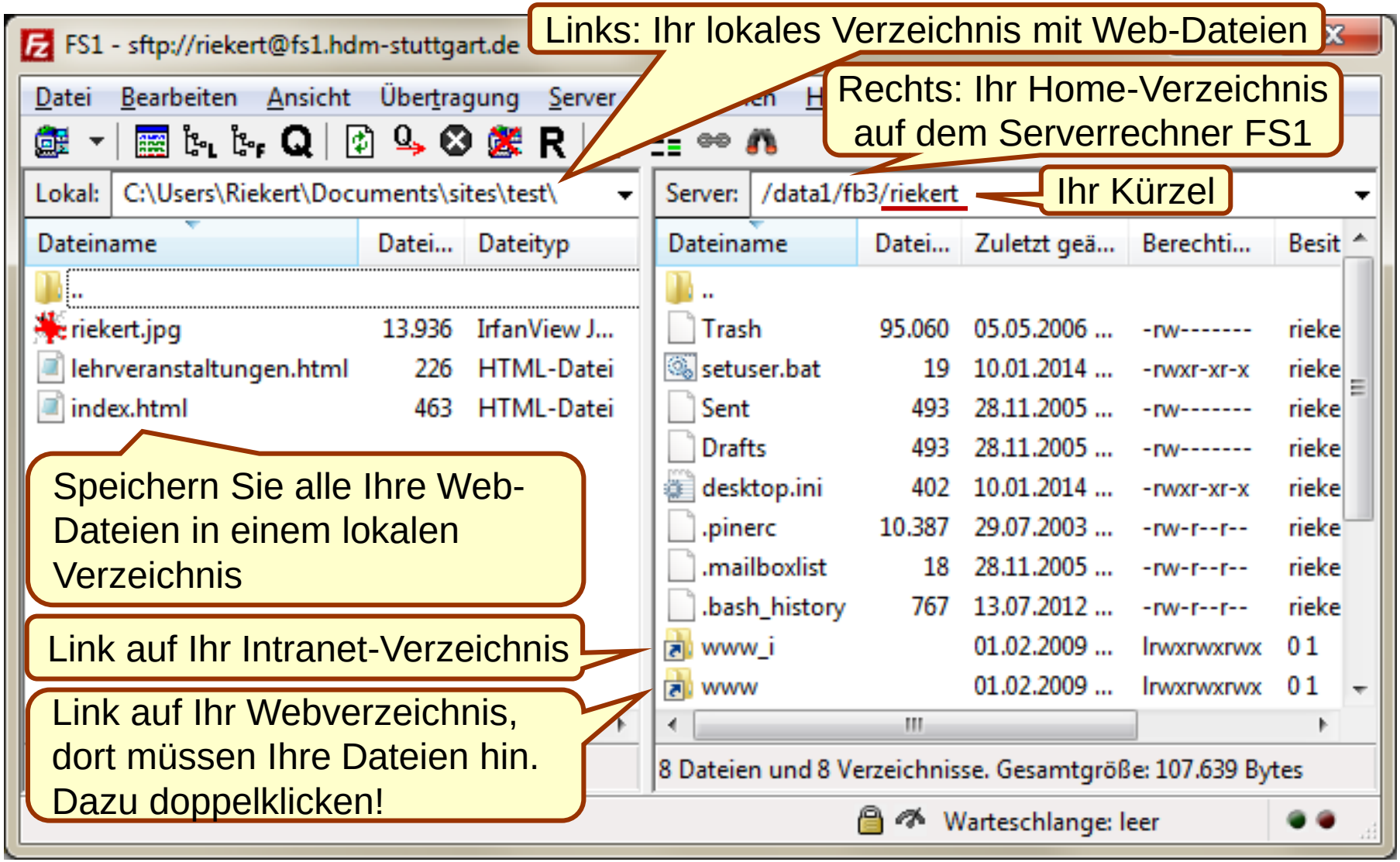
Server-Einstellungen:

Host:	fs1.hdm-stuttgart.de
Port:	22 oder freilassen
Protokoll:	SFTP über SSH
Benutzer:	HdM-Namenskürzel
Passwort:	wie für E-Mail

Verbindungsart:
Empfohlen: **Nach Passwort fragen**!
Auf eigenem Rechner auch: Normal

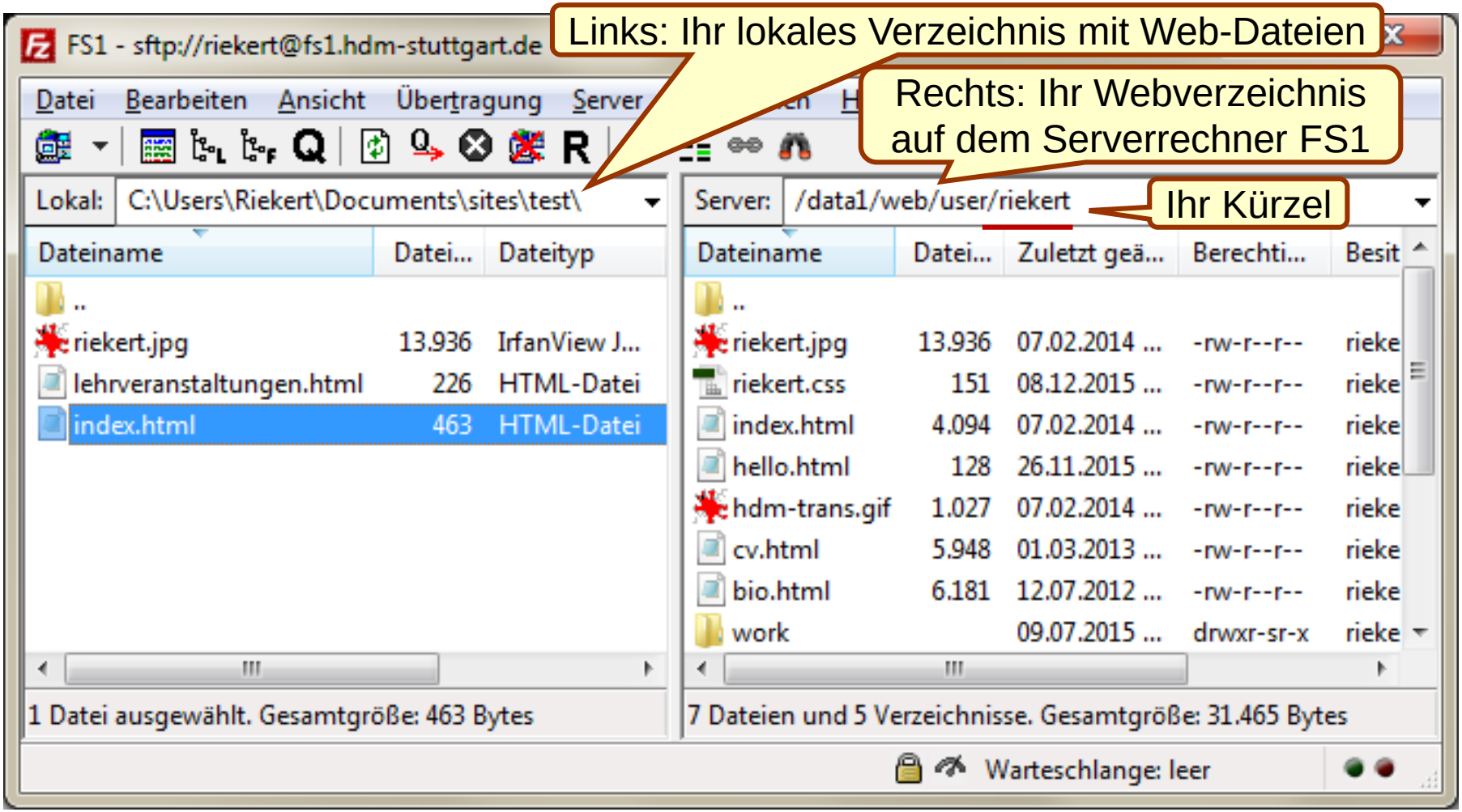
FILEZILLA: DARSTELLUNG DER DATEISYSTEME LOKAL UND FERN

HOCHSCHULE DER MEDIEN



FILEZILLA: FILETRANSFER

HOCHSCHULE DER MEDIEN



Dateien können durch Ziehen auf den Server kopiert werden.

SPEICHERORT VON WEB-DATEIEN AUF DEM WEB-SERVER

Die Web-Dateien (HTML-Seiten, Grafiken, ggf. PHP-Skripte) müssen auf ein Verzeichnis des Web-Servers kopiert werden, das für das Web freigegeben ist.

- Auf Linux/Unix-Systemen mit dem Apache-Web-Server ist dafür i.d.R. das Unterverzeichnis public_html des persönlichen Homeverzeichnisses vorgesehen.
- Auf dem Web-Server der HdM befinden sich die Web-Dateien im Verzeichnis /data1/web/user/<namenskürzel>, erreichbar über den Link www vom Homeverzeichnis.
- Dateien in diesem Unterverzeichnis können vom Web aus mit der URL http://rechnername/~*username*/*dateiname* angesprochen werden. Beispiele:
  - ⇨ http://www.hdm-stuttgart.de/~xy999/datei.html
  - ⇨ http://www.hdm-stuttgart.de/~xy999/ erreicht die Seite http://www.hdm-stuttgart.de/~xy999/index.html

HOMEPAGES AUF DEM WEB-SERVER DER HdM

HOCHSCHULE DER MEDIEN

- Geben Sie Ihrer Homepage den Dateinamen **index.html**!
- Speichern Sie diese Datei auf dem Web-Server der HdM ab (mittels FTP über SSH auf fs1.hdm-stuttgart.de, siehe oben)
- Verwenden Sie das Verzeichnis, das über den Link **www** erreichbar ist (erscheint z.B. als /data1/web/user/xy999 [1])
  - ⇨ Ihre Homepage hat dann z.B. die URL: http://www.hdm-stuttgart.de/~xy999/index.html
  - ⇨ Den Dateinamen index.html dürfen Sie im Browser weglassen. Es genügt, folgende URL einzugeben: http://www.hdm-stuttgart.de/~xy999

---

[1] xy999 ist hier der Platzhalter für Ihr eigenes Namenskürzel.
[2] ~ ist das Tilde-Symbol (unter Windows: zugleich AltGr und + drücken; auf dem Mac: zugleich Alt und n, dann Leerzeichen)

WEITERE SEITEN AUF DEM WEB-SERVER DER HdM

HOCHSCHULE DER MEDIEN

- Für weitere Seiten sowie für CSS-Dateien, Bilder und andere Mediendateien verwenden Sie Namen in Kleinschreibung, ohne Sonderzeichen, ohne Umlaute, mit Endung .html, .css bzw. .jpg usw. je nach Dateityp.
- Speichern Sie diese Dateien im selben Verzeichnis wie die Homepage auf dem Web-Server ab. Für größere Websites können Sie auch Unterverzeichnisse verwenden.
- Mit dem Browser erreichen Sie die Dateien unter der URL: https://www.hdm-stuttgart.de/~xy999/*dateiname.html* bzw. https://www.hdm-stuttgart.de/~xy999/*dateipfad.html*.
- In index.html und Ihren weiteren Web-Seiten können Sie diese Dateien mit relativen URLs (s.o.) referenzieren; d.h. als URL genügt der Dateiname bzw. -pfad, das Protokoll „http:“ bzw. „https:“ und der Hostname des Servers entfallen.

REFERENZIERUNG VON URLS IM HTML-CODE UND IM BROWSER

index.html

```
<!doctype html>
<html>
  <head>
    <meta charset="utf-8" />
    <title>Meine Homepage</title>
  </head>

  <body>
    <p><img src="img/foto.jpg" alt="Mein Foto" /></p>

    <p><a href="http://www.hdm-stuttgart.de/">
          HdM Stuttgart</a></p>
    <p><a href="hobbys.html"> Hobbys</a></p>
  </body>
</html>
```

Homepage index.html, im Browser erreichbar unter http://www.hdm-stuttgart.de/~xy999/index.html oder noch kürzer: http://www.hdm-stuttgart.de/~xy999

Relative URL. Das Bild liegt im Unterverzeichnis img (relativ zu index.html). Im Browser erreichbar z.B. unter http://www.hdm-stuttgart.de/~xy999/img/foto.jpg

Absolute URL, genauso im Browser erreichbar

Relative URL, Die HTML-Datei hobbys.html liegt im selben Verzeichnis wie index.html. Im Browser erreichbar z.B. unter http://www.hdm-stuttgart.de/~xy999/hobbys.html

ERGEBNIS AUF DEM WEB-SERVER MIT DEM BROWSER BETRACHTEN

HOCHSCHULE DER MEDIEN

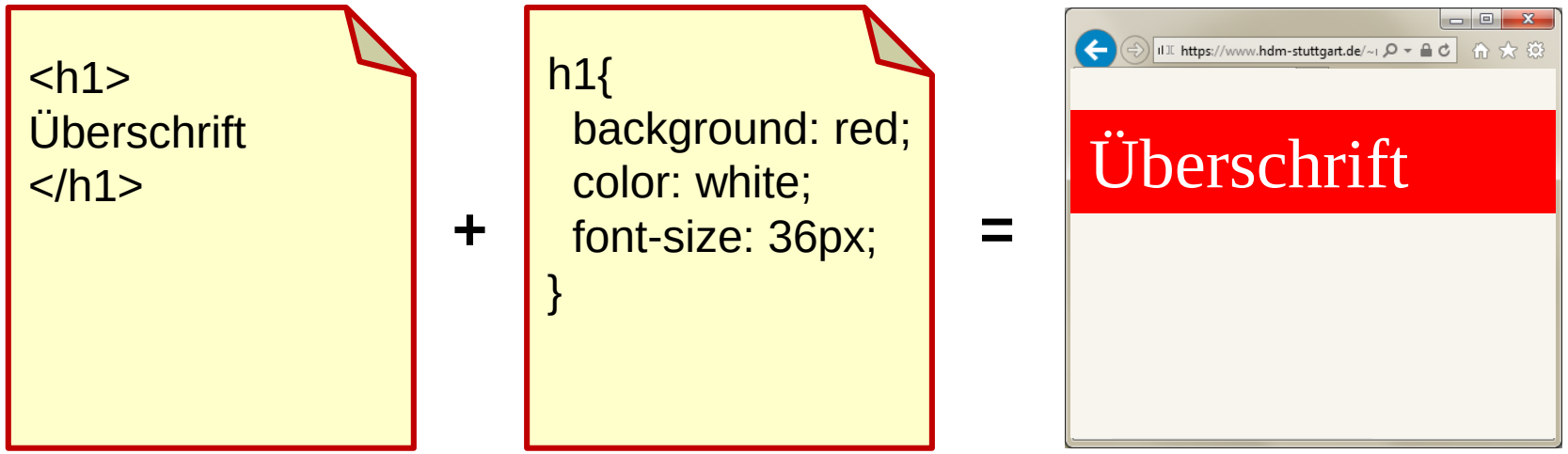
Die Homepage index.html des Users riekert auf dem Web-Server der HdM. Analog ist die Homepage index.html des Users mit dem Kürzel xy999 im Browser unter der URL http://www.hdm-stuttgart.de/~xy999 erreichbar

CSS (CASCADED STYLE SHEETS)

- Mit HTML werden **Inhalt** und **Struktur** einer Web-Seite beschrieben:
  - ⇨ HTML legt fest: Welche Elemente der Web-Seite sind Absätze, Überschriften, Hervorhebungen, Links … ?
  - ⇨ Die Darstellung der Web-Seite kann mit HTML nicht genau festgelegt werden. Je nach Browser kann das Aussehen der HTML-Elemente variieren.
- Erst mit **CSS** (Cascaded Style Sheets) wird die **Darstellung** einer Web-Seite eindeutig festgelegt:
  - ⇨ CSS beschreibt das Aussehen der einzelnen HTML-Elemente auf einer Website.
  - ⇨ Mit CSS können Eigenschaften wie Farbe, Schrifttyp, Schriftgröße, Layout usw. für jedes HTML-Element festgelegt werden.

WIE FUNKTIONIERT CSS?

- Mit HTML werden die Elemente einer Web-Seite definiert (im Beispiel eine Überschrift 1. Ordnung)
- Mit CSS wird das Aussehen der Elemente definiert (im Beispiel roter Hintergrund, weiße Schrift, Größe 28pt)
- Im Browser wird beides zusammengeführt („gerendert“)



INTERAKTIVES TESTEN VON HTML- UND CSS-CODE

HOCHSCHULE DER MEDIEN

Das Zusammenspiel von HTML und CSS lässt sich auf der Website http://jsbin.com leicht ausprobieren.
HTML- und CSS-Code in den zugehörigen Teilfenstern eingeben und das Ergebnis im Output-Teilfenster betrachten.

CSS:
AUFBAU EINER CSS-STILREGEL

Der Selektor bestimmt die Elemente, deren Aussehen festgelegt werden soll.

```
Selektor {
    Eigenschaft : Wert;
    ...
}
```

Der Wert kann z.B. die Farbe sein, die das Element annehmen soll

Die Eigenschaft bestimmt das Aussehen der selektierten Elemente. Eigenschaften können z.B. Farbe, Größe, Schriftart u.a. sein

CSS: SELEKTOREN

Selektoren stellen die Verbindung zu den Elementen des HTML-Dokuments her. Es gibt drei Arten von Selektoren:

- **Elementname-Selektoren**:
  Beispiel: Der Selektor **h1** selektiert Überschriften 1. Ordnung wie z.B. diese: <h1>Überschrift</h1>
- **Klassen-Selektoren**:
  Beispiel: Der Selektor **.rot** selektiert alle HTML-Elemente mit dem Attribut class="rot", z.B. dieses:
   Inline-Element der Klasse "rot"
- **Id-Selektoren**:
  Beispiel: Der Selektor **#main** : selektiert das HTML-Element mit dem Attribut id="main", z.B. so:
  Absatz mit Id "main"

CSS:
BEISPIELE FÜR STILREGELN

HOCHSCHULE DER MEDIEN

Stilregel

mit Elementnamen-Selektor

```
h1 {
      color: blue;
}
```

Alle h1-Elemente (Überschriften der Ordnung 1) werden blau dargestellt

mit Klassen-Selektor

```
.rot {
      color: red;
}
```

Färbt alle HTML-Elemente mit dem Attribut **class="rot"** rot.
Achtung: Erfordert Anpassungen im HTML-Code

mit Id-Selektor

```
#main {
      color: green;
}
```

Färbt das HTML-Element mit dem Attribut **id="main"** grün.
Achtung: Erfordert Anpassungen im HTML-Code

Bedeutung

CSS: ABSTÄNDE ZWISCHEN HTML-ELEMENTEN FESTLEGEN

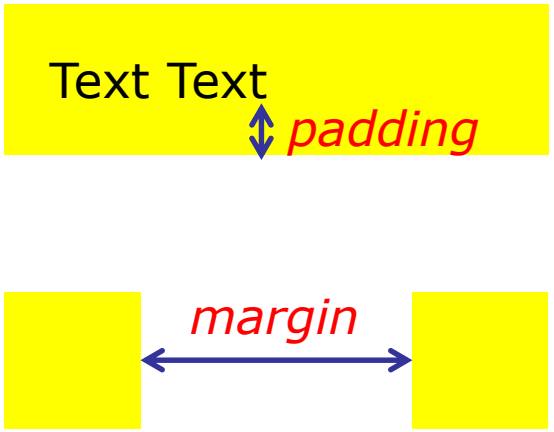
Mit CSS-Eigenschaften können Abstände zwischen Elementen festgelegt werden

padding erhöht den Abstand von Text zum Boxenrand
z.B. padding: 10px;

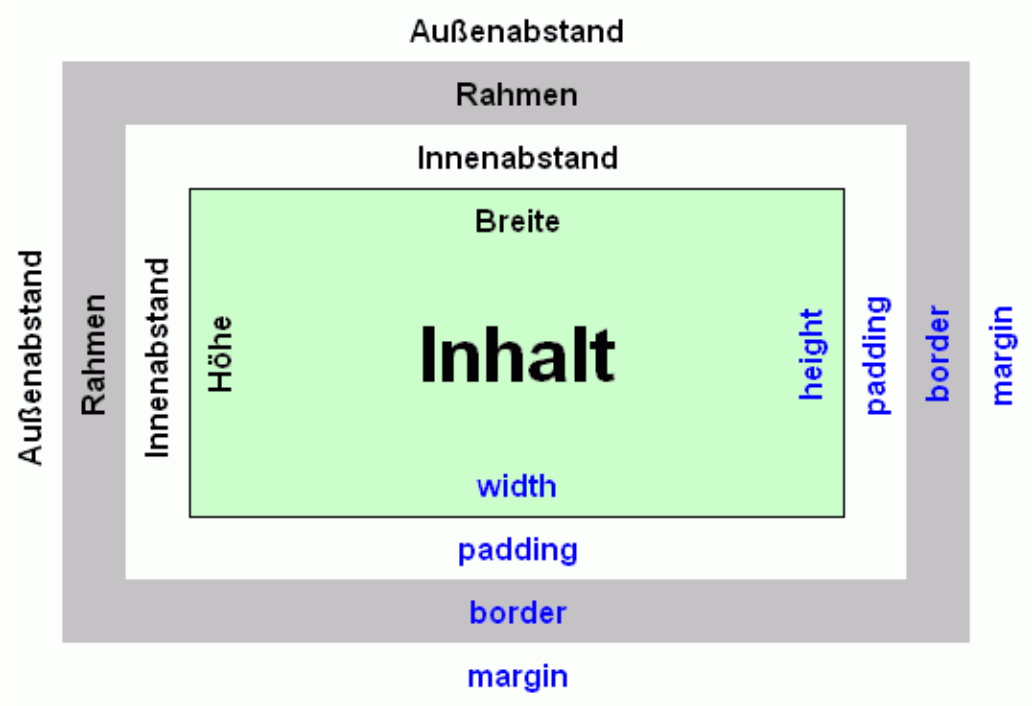
margin erhöht den Abstand eines Elements zu einem anderen
z.B. margin-right: 50px;

border erzeugt einen Rahmen um das Element
z.B. border: 2px solid black;

Beispiel:



CSS: DAS „BOX-MODELL“



Width und height: Breite und Höhe des Inhalts des Elements
Padding: Innenabstand des Modells zum Rahmen
Border: Rahmen des Elements
Margin: Außenabstand des Elements

Padding, Margin und Border lassen sich auch separat für oben (top), rechts (right), unten (bottom), links (left) festlegen. – z.B. *border-bottom: 5px;*

Achtung! Der für das Element benötigte Platz auf dem Bildschirm setzt sich aus height/width, padding, border und margin zusammen.

CSS: LIVE-BEISPIEL MIT VERSCHIEDENEN BOXEN

HOCHSCHULE DER MEDIEN

HTML

```
<!DOCTYPE html>
<html>
   <head>
     <title>Meine HTML-Seite
     </title>
     <meta charset="utf-8" />
   </head>
   <body>
     <h1>Überschrift</h1>
     <h1 id="spezial">
         Überschrift
         spezial</h1>
     <h1>Überschrift</h1>
     <div id="dingsda"></div>
     <div class="gelbumrahmt">
         text text</div>
     <div class="gelbumrahmt">
         mehr text</div>
   </body>
</html>
```

CSS

```
/* Ein Elementname-Selektor
*/
h1{
  color: red;
}

/* Id-Selektoren */
#spezial{
  color: blue;
}
#dingsda{
  background: black;
  height: 50px;
  width: 50px;
}

/* Ein Klassenselektor */
.gelbumrahmt{
  background: yellow;
  margin-top: 10px;
  border: 2px solid black;
}
```

Output

Run with JS | Auto-run JS

Überschrift

Überschrift spezial

Überschrift

text text

mehr text

Live Demo: http://jsbin.com/pacefe/1/edit?html,css,output

CSS: NOCH EIN LIVE-BEISPIEL

HOCHSCHULE DER MEDIEN

Live Demo: http://jsbin.com/jevegis/970/edit?html,css,output

GRUNDLEGENDE EIGENSCHAFTEN IN CSS_STILREGELN

Schrift:

font-size = Schriftgröße (z.B. 12pt)
font-family = Schriftart (z.B. Verdana)
color = Farbe (z.B. red)

Rahmen:

border = kompletter Rahmen um Element
border-left = nur Links Rahmen an Element

Hintergrund:

background-color = Hintergrundfarbe (z.B. green)
background-image = Hintergrundbild (URL)

Vollständige Liste zum Nachschlagen: http://www.css4you.de

WIE WIRD CSS IN HTML EINGEBUNDEN? (1)

HOCHSCHULE DER MEDIEN

```
<!DOCTYPE html>
   <head>
      <title>Meine Webseite</title>
   </head>
   <body>
      <p style="font-size:12px;">
         Das HTML-Element ‘p’ dass mich u
gestylt.
      </p>
   </body>
</html>
```

So lieber nicht!!!

Style-Angabe als Attribut des HTML-Elements:
Im Normalfall lieber nicht.

WIE WIRD CSS IN HTML EINGEBUNDEN? (2)

HOCHSCHULE DER MEDIEN

```
<!DOCTYPE html>
   <head>
      <title> Meine Webseite</title>
      <style type="text/css">
         p { font-size: 13px; }
      </style>
   </head>
   <body>
      <p>Das HTML-Element ‘p’ dass mich umgibt wird mit CSS
gestylt.</p>
   </body>
</html>
```

Auch so lieber nicht!!!

Style-Angabe im <head>-Element im Normalfall lieber nicht.

WIE WIRD CSS IN HTML EINGEBUNDEN? (3)


```
<!DOCTYPE html>
   <head>
      <title>Meine Webseite</title>
      <link href="tutorial.css" rel="stylesheet" type="text/css" />
   </head>
   <body>
      <p>Das HTML-Element ‘p’, das mich umgibt,
         wird mit CSS gestylt.</p>
   </body>
</html>
```

Die Auslagerung der Stilregeln in eine CSS-Datei ist übersichtlicher und professionell: Darstellung (= CSS) und Inhalt/Struktur (= HTML) sind voneinander getrennt und können von unterschiedlichen Personen bearbeitet werden.

STATISCHE UND DYNAMISCHE WEB-SEITEN

Die bisher betrachteten Web-Seiten waren alle **statisch**.

- D.h. sie sehen immer gleich aus, wenn man sie aufruft.

Im Gegensatz dazu gibt es **dynamische Web-Seiten**.
Deren Inhalte sind abhängig von der Situation, z.B.

- von äußeren Bedingungen, z.B. Wetterbericht
- vom Zeitablauf, z.B. Video-Streaming-Seiten
- von Benutzereingaben, z.B. Fahrplanauskunft oder E-Shop

Dynamische Web-Seiten können nicht allein mit HTML definiert werden

- Man benötigt eine **Web-Applikation**
  - ⇨ d.h. ein Software-Programm, das die Inhalte erzeugt

APPLIKATIONEN UND WEB-APPLIKATIONEN

- Herkömmliche **Applikationen** oder **Anwendungen** sind Software-Programme, die von einem Datenträger (z.B. CD-ROM) auf einem PC installiert werden
  - ⇨ Installieren bedeutet Kopieren des Programms auf die Festplatte und Anpassen an die Betriebssystem- und Hardware-Umgebung (z.B. angeschlossener Drucker)
- **Web-Applikationen** sind Software-Programme, die von einem Web-Server bereitgestellt werden und über den Web-Browser gestartet werden.
  - ⇨ **Clientseitige Programme** laufen im Web-Browser ab. Zugrundeliegende Technologie: z.B. Javascript, Flash…
  - ⇨ **Serverseitige Programme** laufen im Web-Server ab. Verschiedene Technologien möglich, wir konzentieren uns auf die serverseitige Programmiersprache **PHP.**

PHP

- PHP: Beispiel einer **Skriptsprache** (Programmiersprache) zur serverseitigen Erzeugung von dynamischen Web-Seiten
- **Ziel** der nachfolgenden Lehreinheit:
  - ⇨ Verstehen der allgemeinen **Funktionsweise**
  - ⇨ **Nicht** das Erlernen der Programmiersprache PHP
- PHP ist eingebettet in HTML
  - ⇨ Dateinamenserweiterung **.php** statt .html
  - ⇨ Die festen Anteile einer Web-Seite werden weiterhin durch die bekannten HTML-Befehle erzeugt
  - ⇨ Die variablen Anteile werden durch die Sprachelemente der PHP-Skriptsprache erzeugt.
  - ⇨ Kennzeichnung der PHP-Sprachelemente durch besondere Tags

TAGS ZUR EINBETTUNG VON PHP-CODE IN HTML-CODE

- Einbettung von PHP mit einem Script-Tag:

```
<script language="php">

// Hier kann PHP-Code geschrieben werden.

</script>
```

- Kurzform (So genannte „XML-konforme Einbettung“):

```
<?php

// Hier kann PHP-Code geschrieben werden.

?>
```

EIN „HELLO WORLD“ SCRIPT IN PHP

hello.php

Dateinamensendung muss **.php** sein!

```
<!doctype html>
<html>
 <head>
  <meta charset="utf-8" />
  <title>Beispiel</title>
 </head>
 <body>
  <?php
   echo "Hallo, ich bin ein PHP-Skript!";
  ?>
 </body>
</html>
```

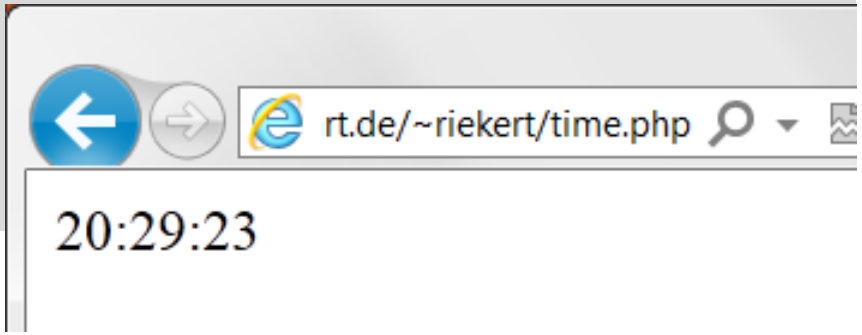
echo = PHP-Ausgabeanweisung

DIE ERSTE „DYNAMISCHE“ WEB-SEITE

time.php

```
<!doctype html>
<html>
 <head>
  <meta charset="utf-8" />
  <title>Uhrzeit</title>
 </head>
 <body>
  <?php
   echo date("H:i:s");
  ?>
 </body>
</html>
```

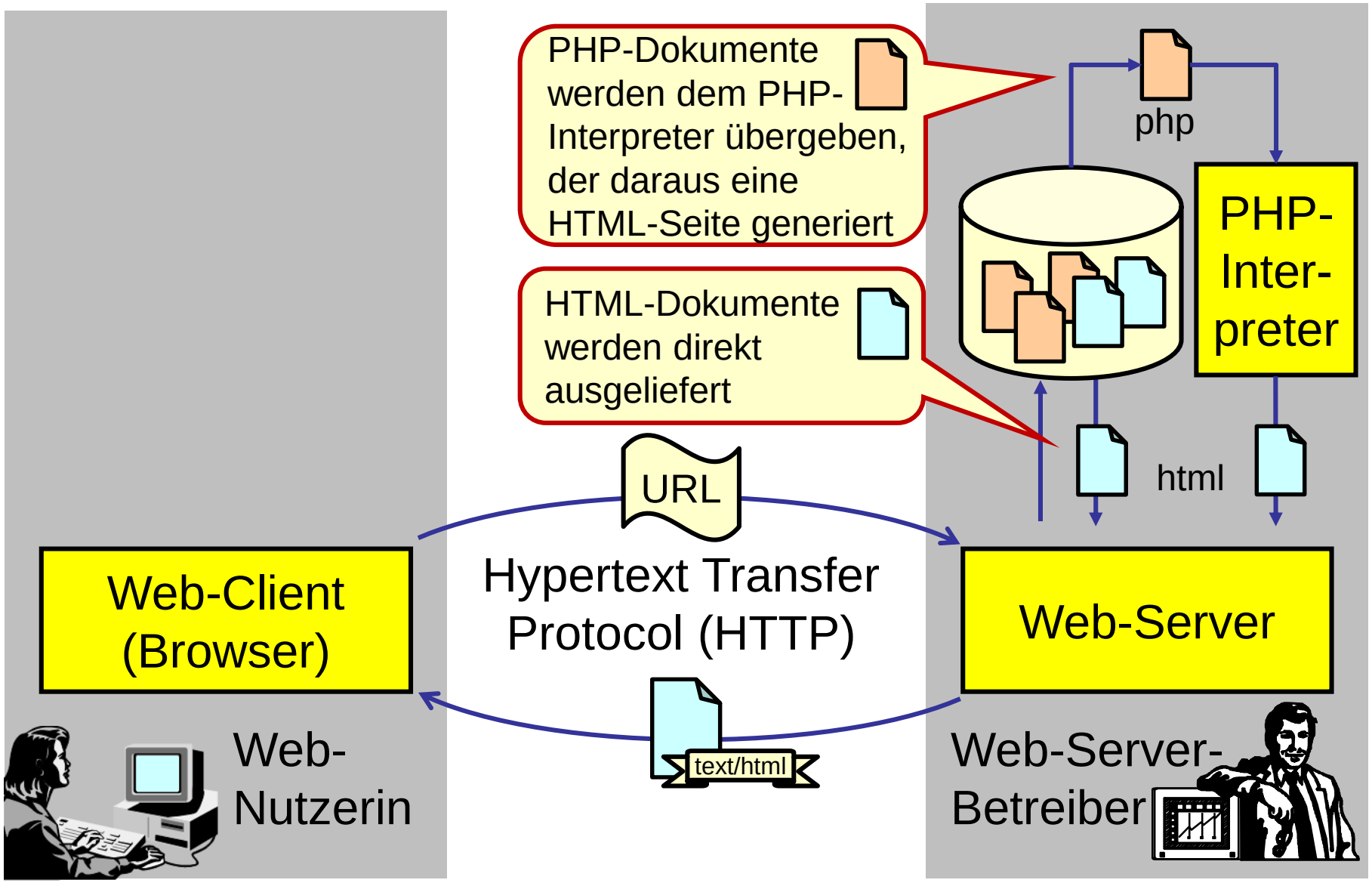
date = Funktion zur Bestimmung von Datum/Uhrzeit im Format (24-)Stunden-Minuten-Sekunden ("H:i:s")



AUSFÜHRUNG VON PHP-SCRIPTS

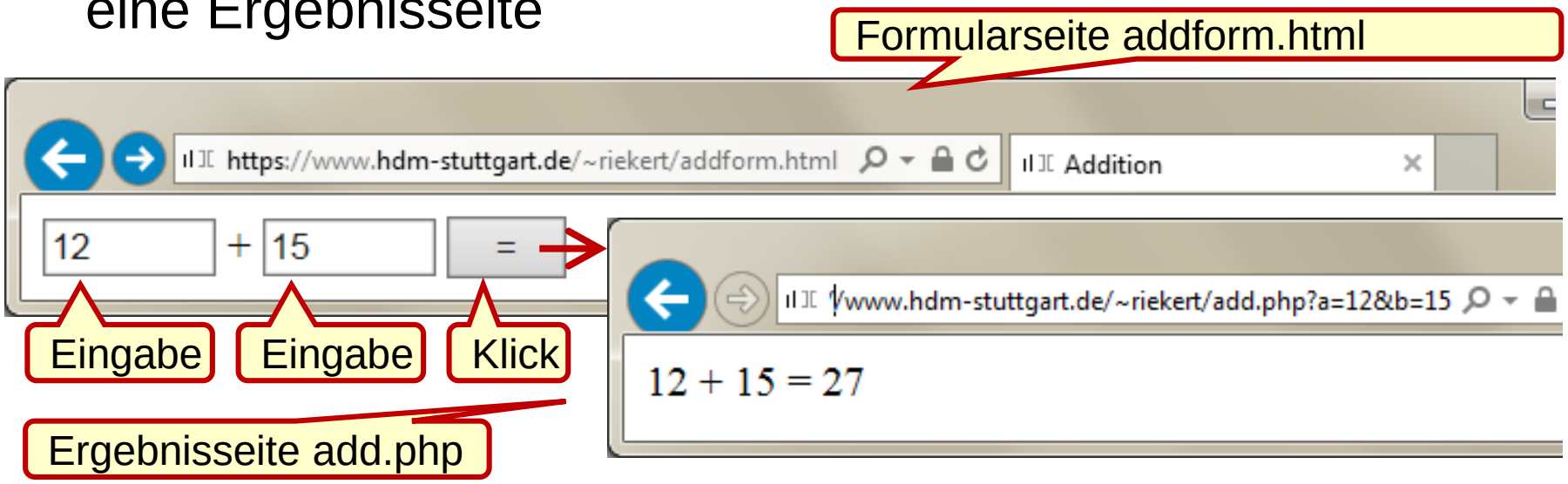
- Von einem Internetbrowser aus wird eine URL mit Dateinamensendung .php abgerufen.
- Der Web-Server ist so konfiguriert, dass er angeforderte Dateien mit Endung .php an den PHP-Interpreter übergibt.
- Der PHP-Interpreter verarbeitet die PHP-Dateien, indem er
  - ⇨ den eingebetteten PHP-Code ausführt und
  - ⇨ aus der PHP-Datei eine HTML-Seite erzeugt.
- Die erzeugte HTML-Seite sieht aus wie die PHP-Datei, nur sind die Teile innerhalb der PHP-Tags durch Text ersetzt, der durch eingebettete PHP-Ausgabeanweisungen generiert wurde, z.B. durch den Befehl **`echo`**.
- Diese HTML-Seite wird an den Web-Server übergeben, der diese dann an den Internetbrowser zur Anzeige überträgt.

AUSFÜHRUNG VON PHP-SCRIPTS



FORMULARE UND PHP-SKRIPTE

- Ein Formular ist eine HTML-Seite, die Benutzereingaben ermöglicht.
- Die Benutzereingaben können als so genannte Parameter an ein PHP-Skript übergeben werden.
- Dieses PHP-Skript führt dann in Abhängigkeit von den Parametern eine Aktion (z.B. Berechnung) aus und erzeugt eine Ergebnisseite

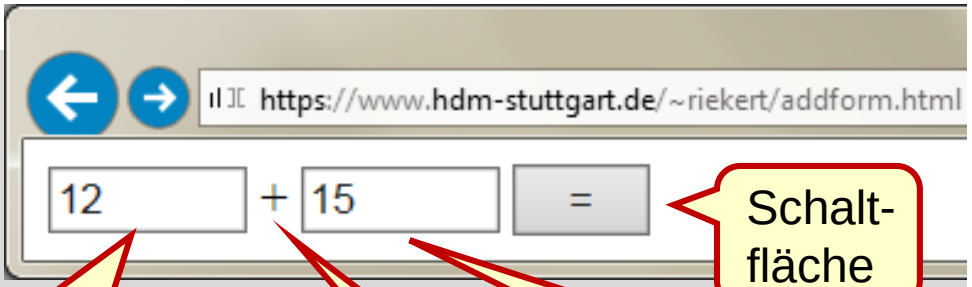


ADDITION: DAS FORMULAR

HOCHSCHULE DER MEDIEN

addform.html

```
<!doctype html>
<html>
 <head>
   <meta charset="utf-8" />
   <title>Addition</title>
 </head>
 <body>
   <form action="add.php" method="get">
     <input type="text" name="a" size="5" /> +
     <input type="text" name="b" size="5" />
     <input type="submit" value="  =  " />
   </form>
 </body>
</html>
```



Schalt-fläche

Eingabefeld „a“

Text

Eingabefeld „b“

form-Tag zur Definition des Formulars

URL eines PHP-Skripts: erzeugt nächste Seite nach dem Abschicken des Formulars.

Eingabefeld „a“

Angezeigter Text „+“

Eingabefeld „b“

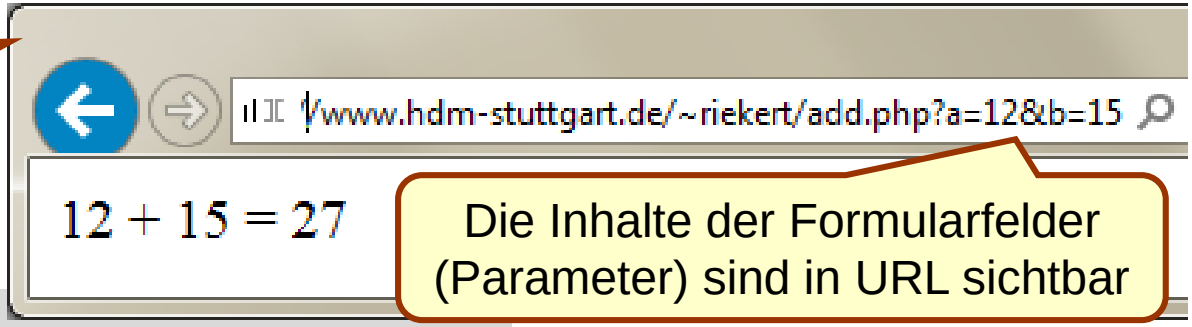
Schaltfläche zum Abschicken des Formulars

ADDITION: DAS PHP-SKRIPT

HOCHSCHULE DER MEDIEN

Ausgabe des Skripts

Das PHP-Skript



Die Inhalte der Formularfelder (Parameter) sind in URL sichtbar

add.php

```
<!doctype html>
<html>
 <head>
  <title>Summe</title>
  <meta charset="utf-8" />
 </head>
 <body>
  <?php
     $a=$_GET["a"]; $b=$_GET["b"];
     echo $a . " + " . $b . " = " . ($a+$b);
   ?>
 </body>
</html>
```

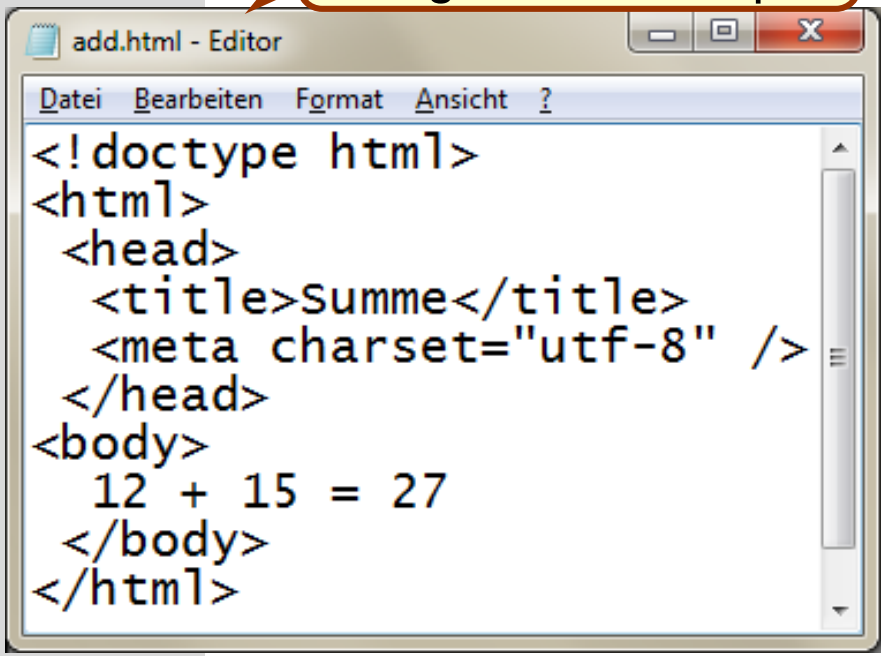
Übernahme der Parameter „a“

… und „b“

Ausgabe des Ergebnisses

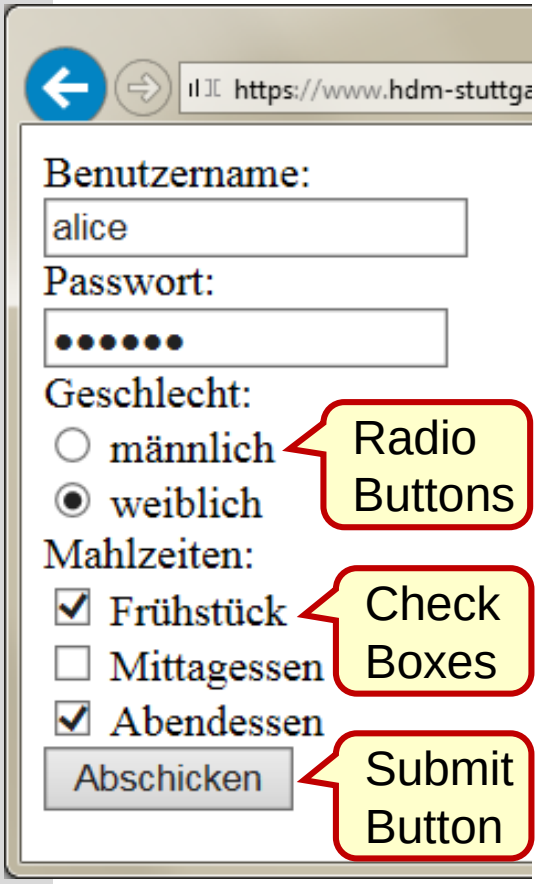
Berechnung der Summe

Seitenquelltext der Ausgabe des Skripts

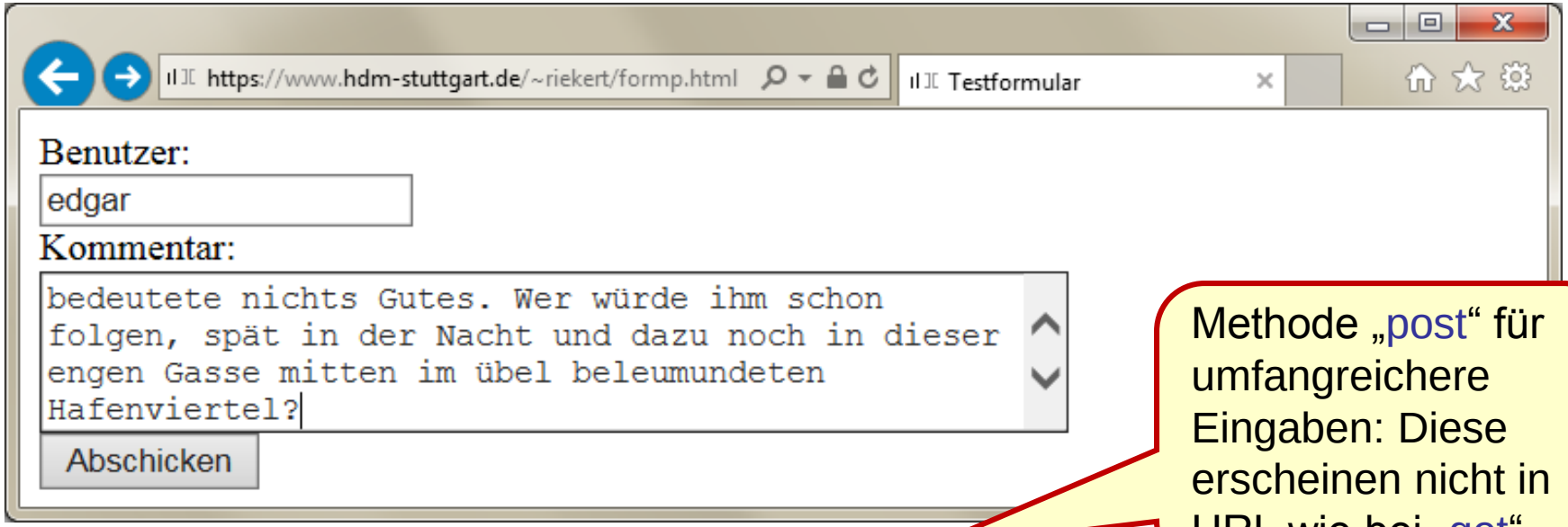


EIN KOMPLEXERES FORMULAR


```
<form name="testformular" method="get"
      action="formeval.php">
Benutzername: <br />
<input type="text" name="benutzername" /> <br />
Passwort: <br />
<input type="password" name="passwort" /> <br />
Geschlecht: <br />
<input type="radio" name="geschlecht"
       value="m" /> männlich <br />
<input type="radio" name="geschlecht"
       value="w" /> weiblich <br />
Mahlzeiten: <br />
<input type="checkbox" name="fruehstueck"
       value="ja" /> Frühstück <br />
<input type="checkbox" name="mittagessen"
       value="ja" /> Mittagessen<br />
<input type="checkbox" name="abendessen"
       value="ja" /> Abendessen<br />
<input type="hidden" name="version" value="1.0" />
<input type="submit" value="Abschicken" />
</form>
```



FORMULARE
FÜR UMFANGREICHE EINGABEN



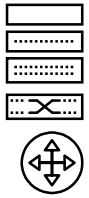

```
<form name="testformular" method="post"
      action="https://www.hdm-stuttgart.de/~riekert/formeval.php">
Benutzer: <br />
<input type="text" name="benutzer" /> <br />
Kommentar: <br />
<textarea name="kommentar" rows="4" cols="60">
Hier kann ein längerer Text eingetragen werden!
</textarea>
<input type="submit" value="Abschicken" />
</form>
```

Methode „post“ für umfangreichere Eingaben: Diese erscheinen nicht in URL wie bei „get“

Sie können diese URL eintragen, um Ihre Formulare zu testen.

textarea: Geeignet für umfangreichere Texteingaben.

LEGENDE DER NETZWERKSYMBOLE



Hub, diverse Verteiler

Switch

Router

WLAN-(DSL-)Router

WLAN-Access-Point

Laptop (mit WLAN-Interface)

Arbeitsplatz-PC

Servercomputer

Browser

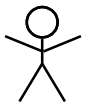
Prozess

Lokales Netzwerk
Broadcastnetz

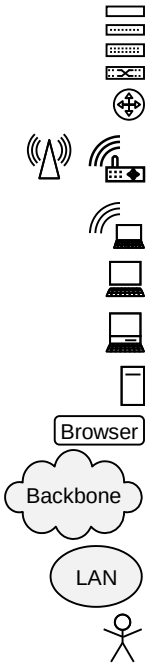
Lokales Netzwerk
(Hintergrund für
Komponenten)

Verbundnetz
(z.B. Internet)

Verbundnetz
(Hintergrund für
Komponenten)



Benutzer(in)



Kleine
Symbole