ZSL
Zentrum für Schulqualität
und Lehrerbildung
Baden-Württemberg

Networking Academy

Application Layer

Andreas Grupp
Andreas.Grupp@zsl-rstue.de

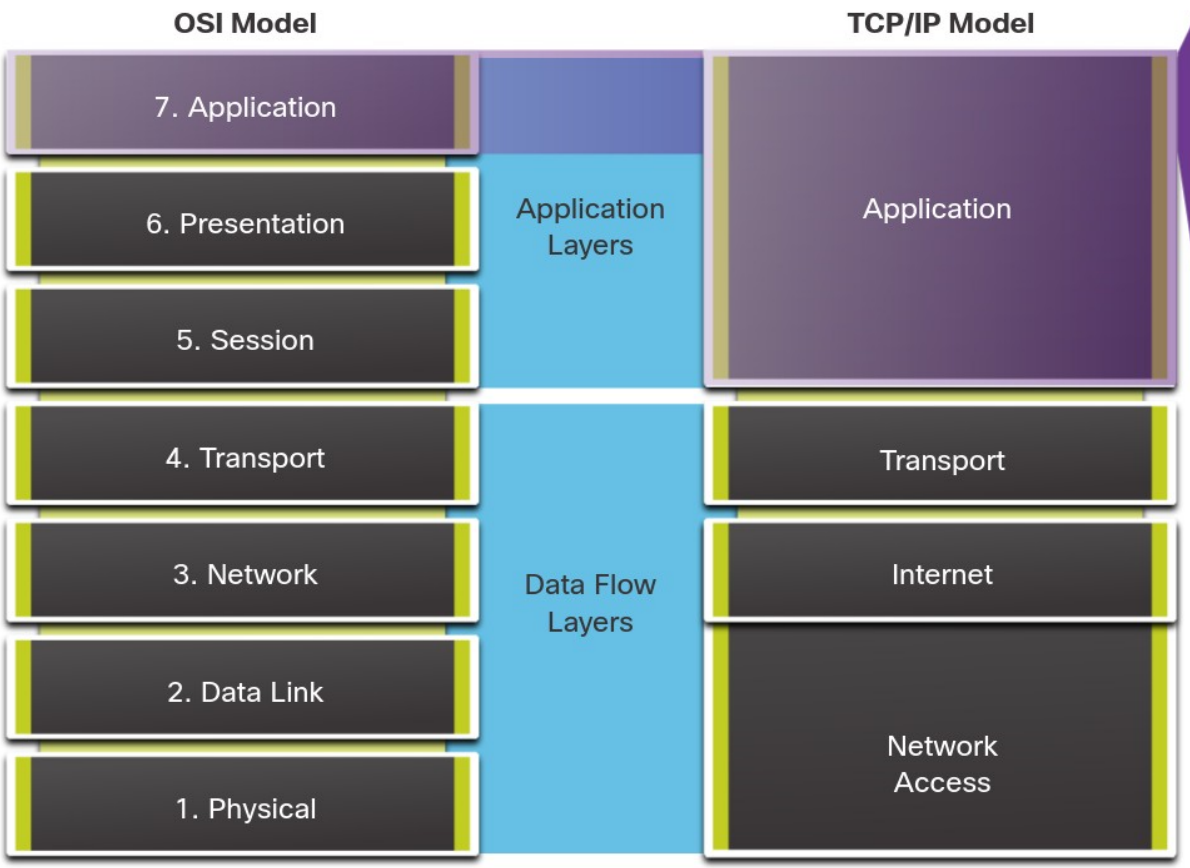
Carina Haag
carina.haag@zsl-rsma.de

Tobias Heine
tobias.heine@zsl-rsma.de

Uwe Thiessat
uwe.thiessat@gbs-sha.de

Application-Layer, unterschiedlich definiert

TCP/IP-Application-Layer umfasst auch die Aufgaben der OSI-Layer „**Presentation**“ und „**Session-Layer**“



Domain Name System
Hypertext Transfer Protocol
Simple Mail Transfer Protocol
Post Office Protocol
Dynamic Host Configuration Protocol
File Transfer Protocol
Internet Message Access Protocol

Application-Layer ist die Schnittstelle zwischen einer Anwendung und der Netz-Kommunikation.

Ein paar der gängigen Protokolle sind hier aufgelistet.

Im realen TCP/IP-Modell sind einige Protokolle im Betriebssystem, andere direkt in der Anwendung programmiert.

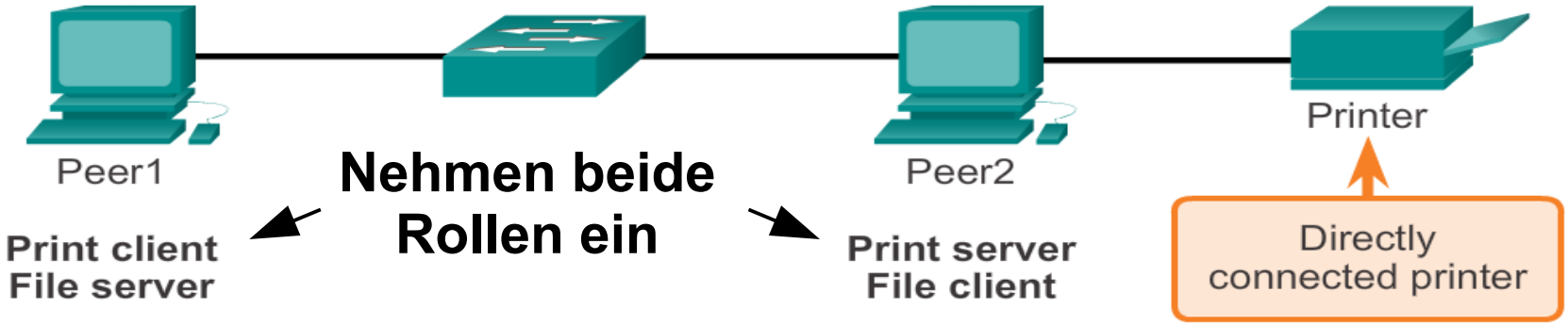
Teilaufgaben der OSI-Layer 5, 6 und 7 = TCP/IP-Applic.-Layer

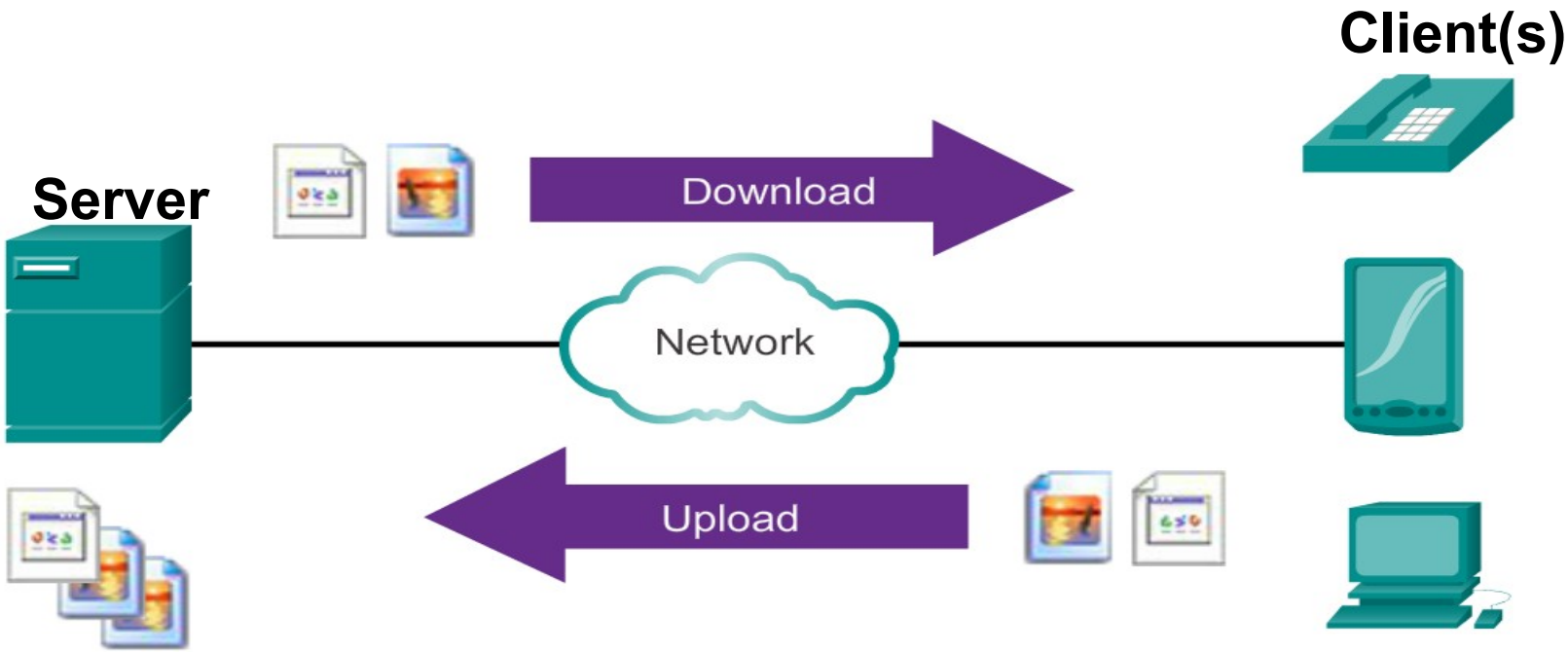
- Application Layer (OSI-7): Interface zwischen Anwendungen und den darunter liegenden Netzwerkschichten. Typische Vertreter wären:
  - HTTP, SMTP, POP, IMAP, FTP, TFTP, BOOTP, DHCP oder DNS – um nur ein paar Vertreter zu nennen
- Presentation Layer (OSI-6):
  - Formatierung / Darstellung von Daten in einem zum Zielgerät kompatiblen Format, z.B. MPEG, PNG, ...
  - Daten-Komprimierung, so dass Ziel-Gerät wieder entpacken kann.
  - Daten-Verschlüsselung b. Senden, Entschlüsselung beim Empfang.
- Session Layer (OSI-5):
  - Initiieren, aufrechterhalten und Neustart von Sessions (Sitzungen), die unterbrochen wurden oder über einen längeren Zeitraum inaktiv waren.

Ein paar Protokolle des TCP/IP-Application-Layers

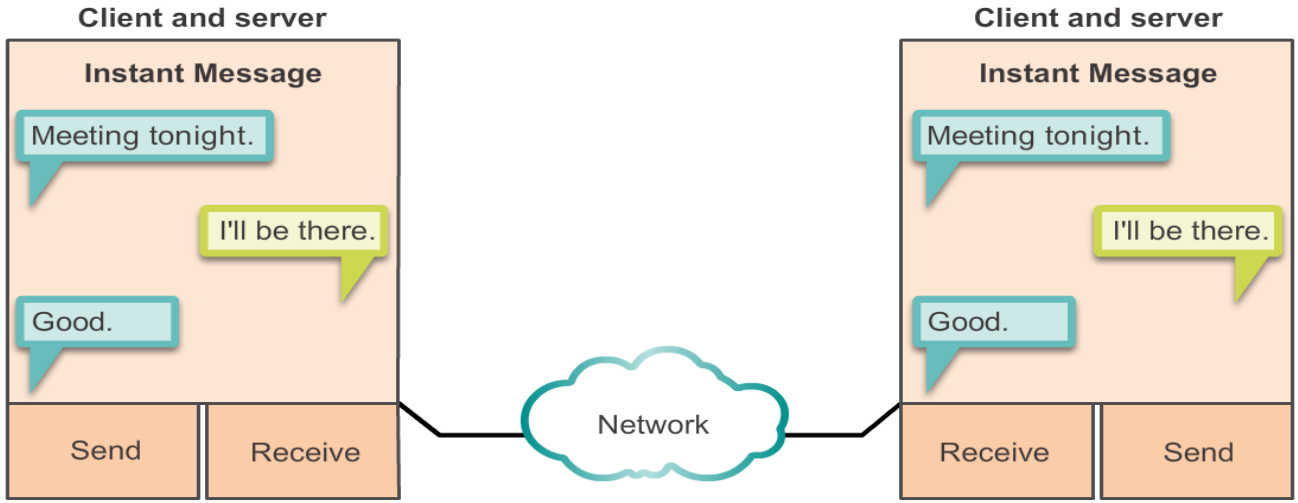
- DNS - Domain Name System (or Service) – TCP, UDP Client 53
- BOOTP - Bootstrap Protocol – UDP Client 68, Server 67
- DHCP - Dynamic Host Configuration Protocol – UDP Client 68, Server 67
- E-Mail, verwendet verschiedene Protokolle
  - SMTP - Simple Mail Transfer Protocol, TCP 25 (Anmerk. 465, 587)
  - POP3 - Post Office Protocol, TCP 110
  - IMAP - Internet Message Access Protocol, TCP 143 (Anmerk. 993)
- FTP - File Transfer Protocol – TCP 20 to 21 + Datenkanal
- TFTP - Trivial File Transfer Protocol – UDP client 69
- HTTP - Hypertext Transfer Protocol – TCP 80, 8080
- HTTPS - HTTP Secure – TCP, UDP 443

Peer-to-Peer vs. Client-Server-Netzwerk-Modell





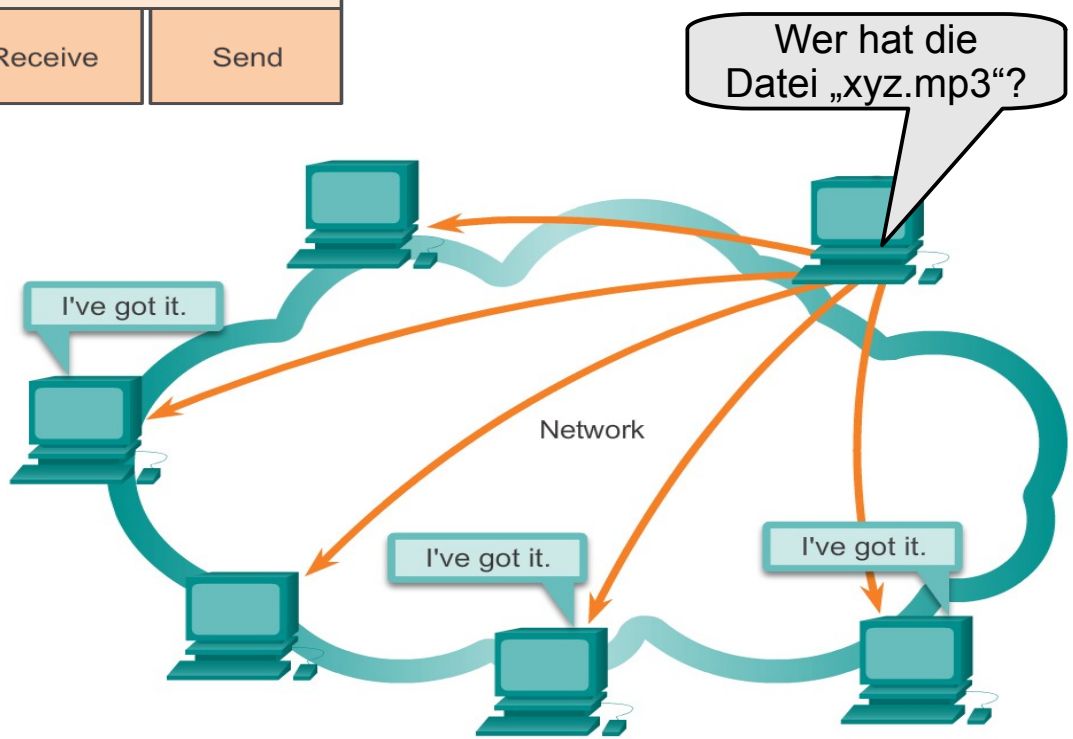
Auch im Anwendungsbereich: P2P-Applikationen



Manche Anwendungen kommunizieren auch direkt – ohne zentralen Server. Meist aber für Vermittlung Start über zentralen Server

Datei-Sharing über P2P-Applik. z.B. mit eDonkey, eMule, Shareaza, BitTorrent (Teile), Bitcoin, LionShare. Oft auch Verwendung des Gnutella-Protokolls (ganze Dateien).

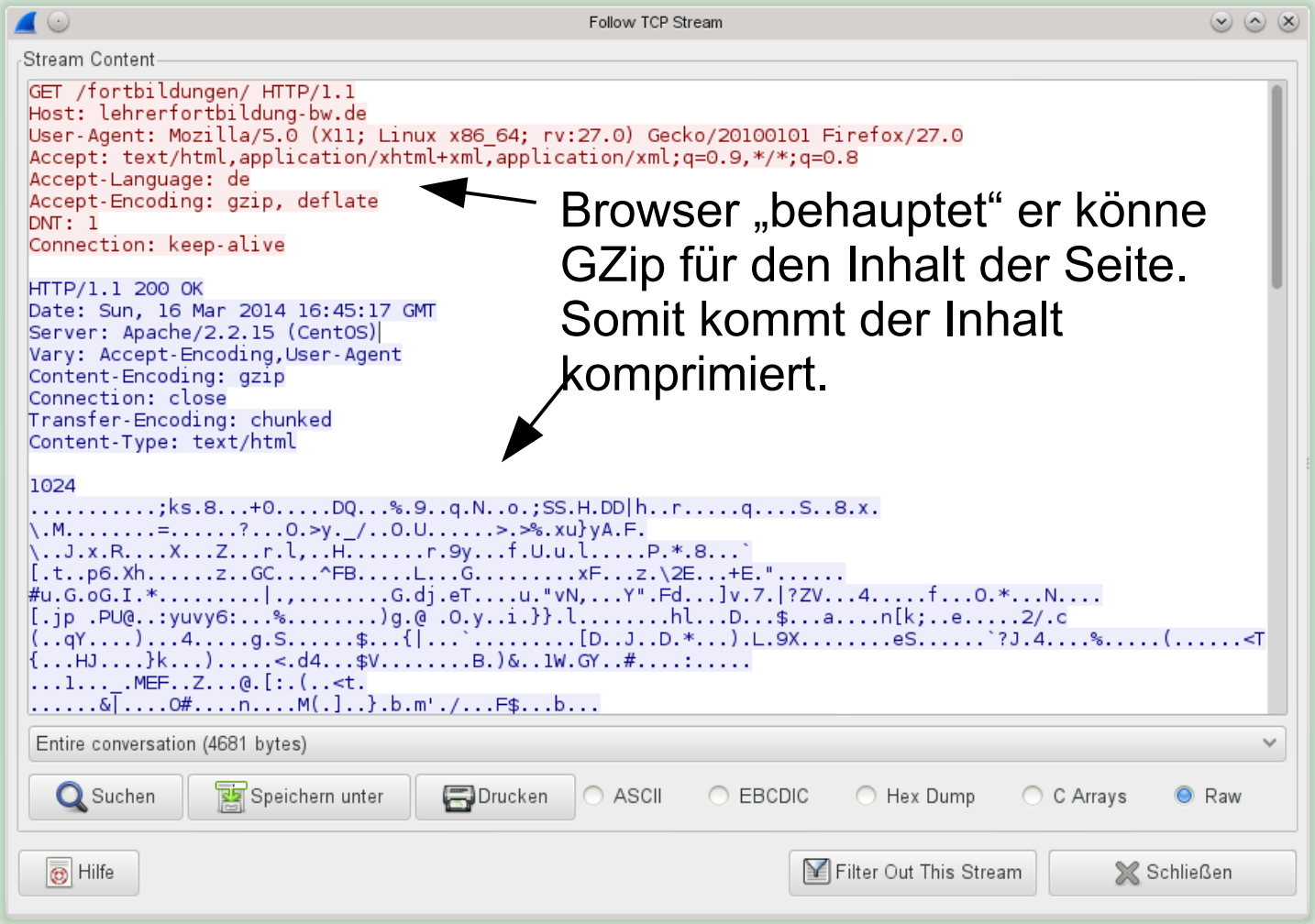
Rechtlich nicht unbedenklich!



Surfen im Web → http-Verbindung

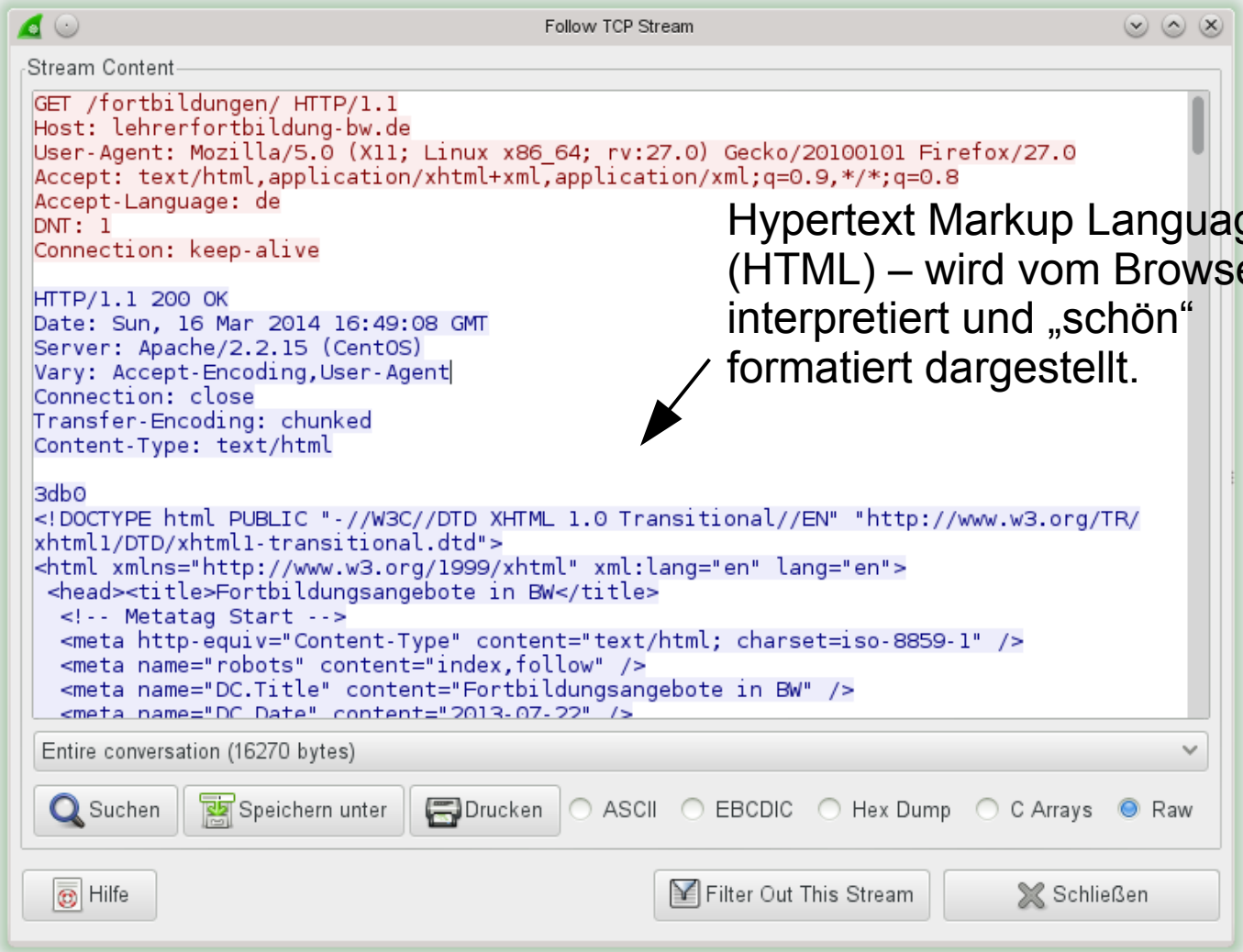
http://lehrerfortbildung-bw.de/fortbildungen/ ← Gewünschte Ressource auf betreffendem Host

Hostnamen – wird über DNS auf IP-Adresse aufgelöst!



Browser „behauptet“ er könne GZip für den Inhalt der Seite. Somit kommt der Inhalt komprimiert.

http-Verbindung ohne Komprimierung



Hypertext Markup Language (HTML) – wird vom Browser interpretiert und „schön“ formatiert dargestellt.

Ein paar wenige Details zu http

- Request / Response Protokoll
- Message Typen:
  - GET – z.B. für ganz normale Anfragen an eine Site
  - PUT – z.B. für Formulardaten von Client → Server
  - POST – z.B. Dateiupload von Client → Server
- Unterstützung für Authentifizerung
- Default ist unverschlüsselt → Server-Port 80
- Verschlüsselt via https → Server-Port 443

https in Aktion ...

Verschlüsselung über Secure Socket Layer (SSL) / Transport Layer Security (TLS) unterbindet das Mitlesen.
Entspricht einer Funktionalität des OSI-Layers-6

E-Mail und der Application-Layer (1)

- E-Mail ist ein Store-and-Forward-Verfahren
  - Absender liefert bei „*Ausgangs-Postamt*“ die zu versendende E-Mail ab. Verwendetes Protokoll ist „*Simple Mail Transfer Protocol*“

    → SMTP des Mail-Programms (MUA) an Mailserver (MTA) des Absenders
  - Prüft welches „*Postamt*“ für Empfänger-Domain zuständig ist …

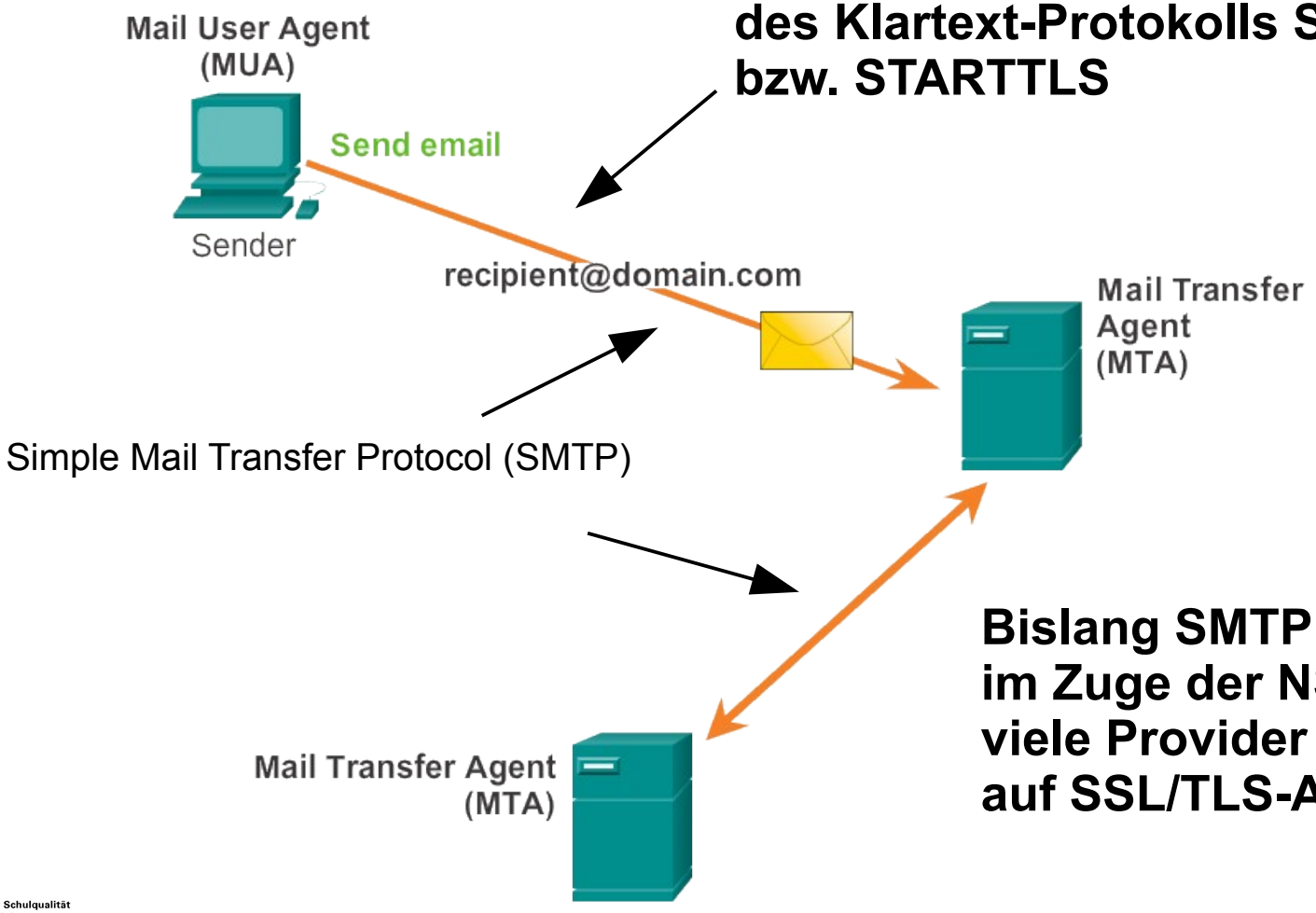
    → DNS-Anfrage nach MX-Eintrag der Domain

    … und leitet Mail an dieses „*Postamt*“ weiter

    → Mail wird per SMTP an Ziel-Mailserver (MTA) ausgeliefert

E-Mail und der Application-Layer (2)

Bei diesem Vorgang Authentifizierung erforderlich → normalerweise Absicherung des Klartext-Protokolls SMTP via SSL/TLS bzw. STARTTLS



Bislang SMTP meist im Klartext, im Zuge der NSA-Affäre stellen viele Provider in Deutschland auf SSL/TLS-Absicherung um.

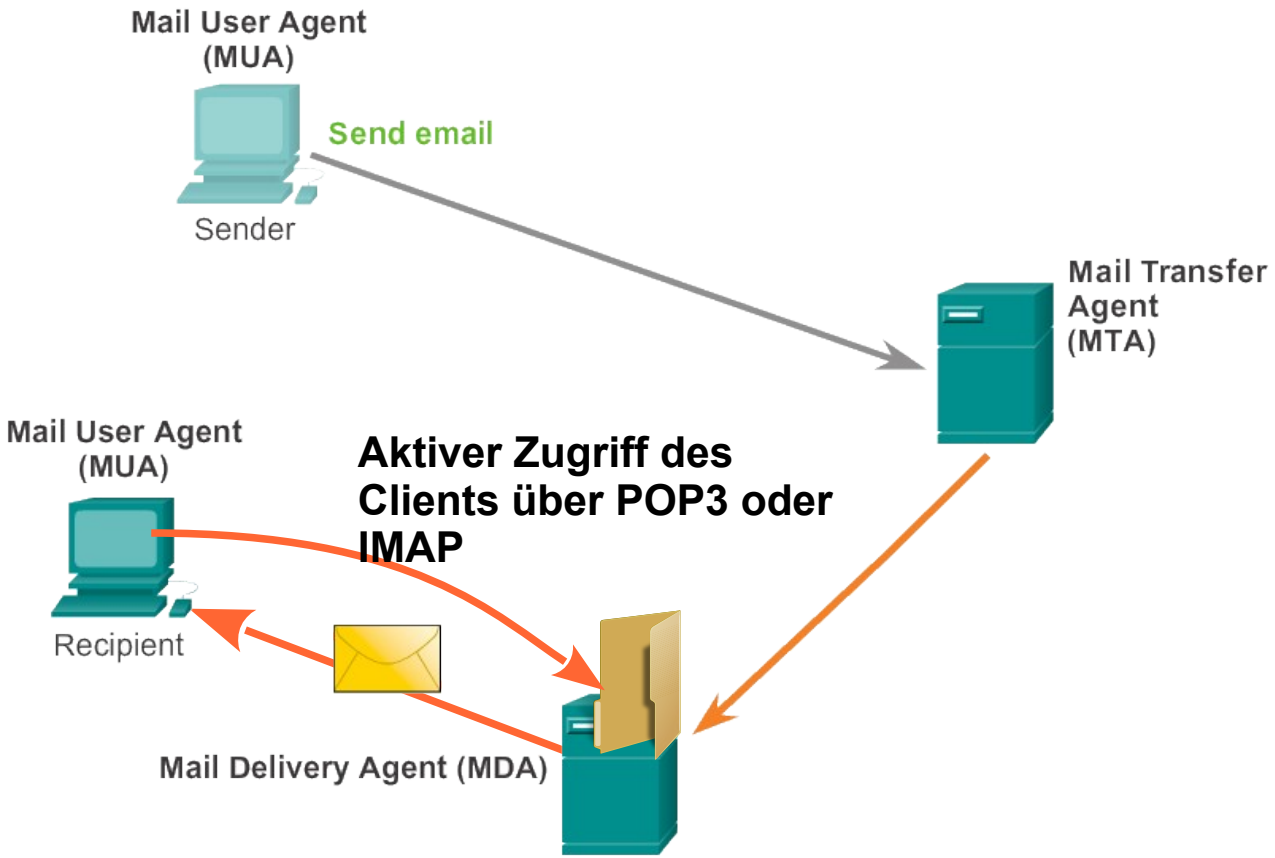
E-Mail und der Application-Layer (3)

- Ziel-Mailserver (MTA) einer Domain prüft ob Empfänger existiert, Quotas nicht überschritten sind, ggf. Spam- und Virenkontrolle, …

  → nach „*Eingangskontrolle*“ Ablage der Mail im Postfach des Empfängers.

- Auslieferung ist ein Request- und Response-Verfahren – Zugriff auf Postfächer erfolgt
  - aktiv vom Empfänger selbst. Verwendet dazu ...
  - Post Office Protocol (POP), oder
  - Internet Message Access Protocol (IMAP)

E-Mail und der Application-Layer (3)



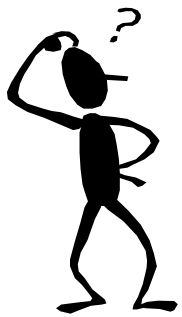
Absicherung der Kommunikation mit Postfach erfolgt heute im Normalfall auch über SSL/TLS

E-Mail und der Application-Layer (4)

- SMTP – auf Port 25
  - Authentf. User auf Port 465 (SSL/TLS) bzw. 587 (STARTLS)
- POP3 – auf Port 110 (SSL-Port 995)
  - primär für Abholung von Mails
  - löscht (ohne andere Einstellung) Mail auf MDA!
  - keine Ordnerstruktur auf MDA möglich
  - wenig/keine Protokoll-Features zur Mailverwaltung
- IMAP – auf Port 143 (SSL-Port 993)
  - alle Fähigkeiten von POP3. Zusätzlich
  - Mailverwaltung auf Server, z.B. Ordner, Suchen …
  - oft kostenpflichtig

Kommunikation im Internet

- Rechner müssen eindeutig identifizierbar sein.
- IP-Protokoll verwendet hierfür nummerische Adressen (bei IPv4 z.B. 84.158.95.179)



74.125.43.104
141.69.160.40
160.44.68.26

Für Menschen ist die Verwendung von IP-Adressen unzumutbar!

IP-basierende Rechner erhalten deshalb einen eindeutigen Namen der leichter merkbar ist!

213.165.64.71 ↔ www.gmx.de

Die Auflösung von IP-Adresse in den Namen u. umgekehrt leistet das **D**omain **N**ame **S**ystem (DNS)

Aufbau von Rechnernamen

Diese Namen sind streng hierarchisch aufgebaut.

Rechnername:

- Frei wählbar
- www nur Konvention!!

Subdomains:

- z.B. Abteilung, Standort, ...

Domain:

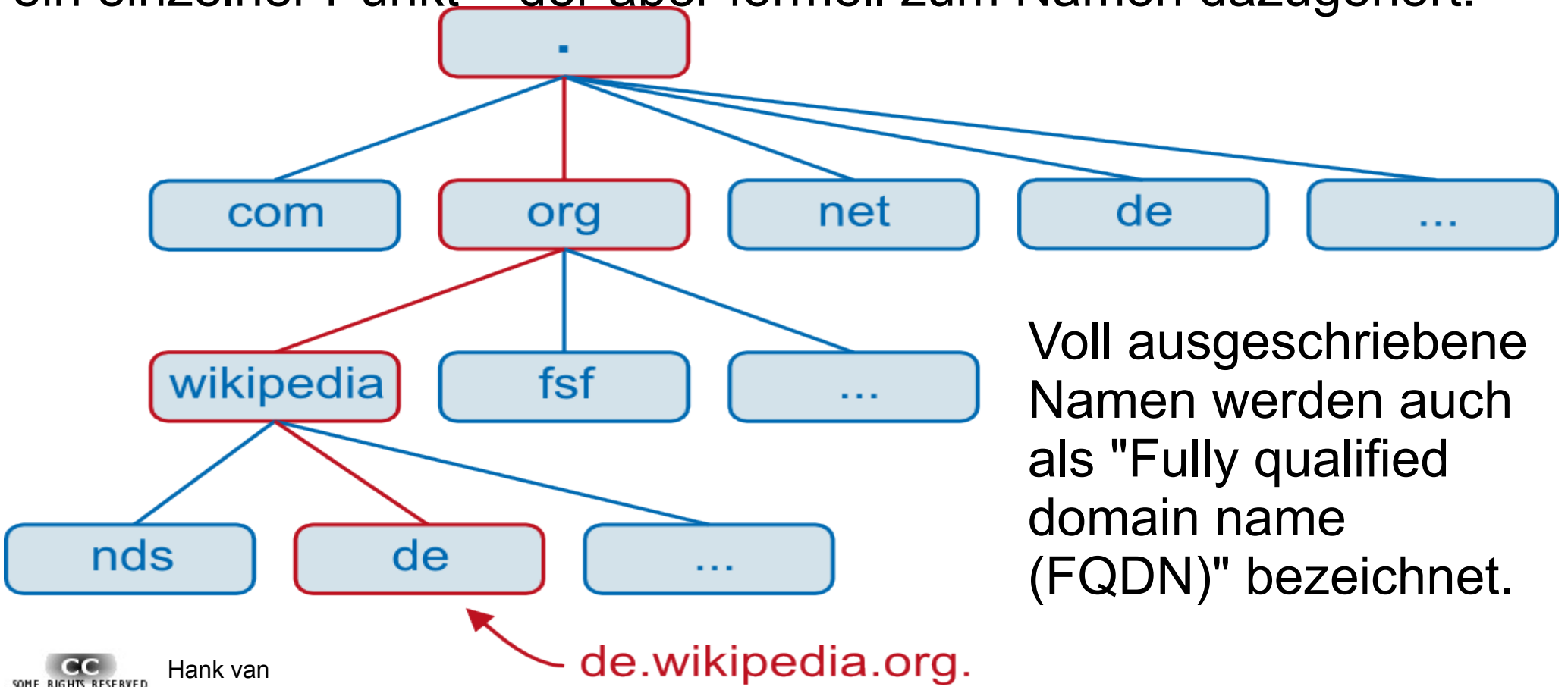
- Kennzeichen eines einzelnen Netzwerks

Top-Level-Domain:

- Landkürzel (de, uk, at ...)
- oder Gruppenkürzel, z.B.
  com = commercial
  org = organisation

Der DNS Namensraum

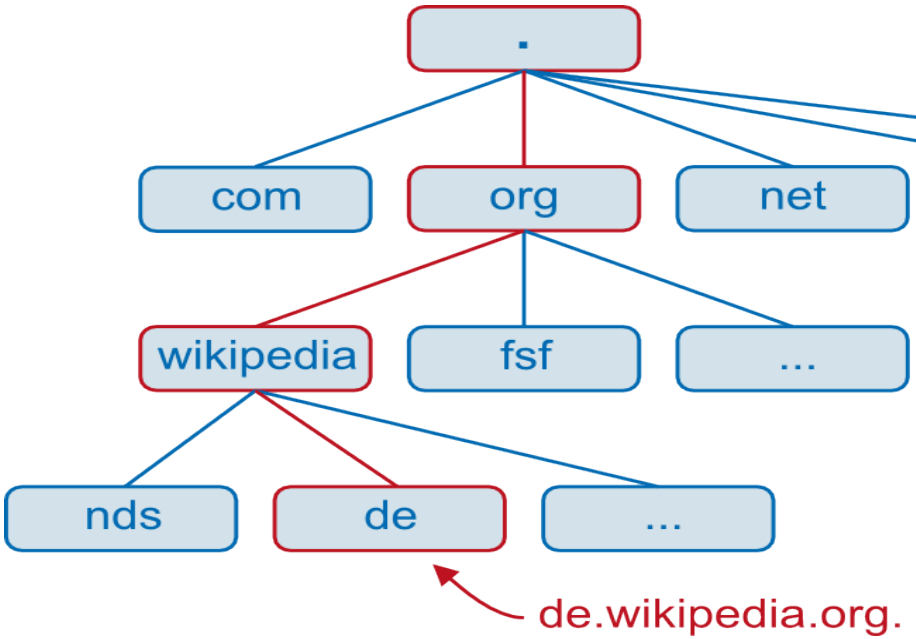
Oberhalb der Top-Level-Domains ist "Root" –
ein einzelner Punkt – der aber formell zum Namen dazugehört!



Voll ausgeschriebene Namen werden auch als "Fully qualified domain name (FQDN)" bezeichnet.

Hank van Helvete, Wikipedia

Delegationen im Namensraum



Der gesamte Namensraum ist für einen DNS-Server nicht zu bewältigen. Deshalb werden jeweils Untermengen zur Verwaltung an andere DNS-Server "**delegiert**".

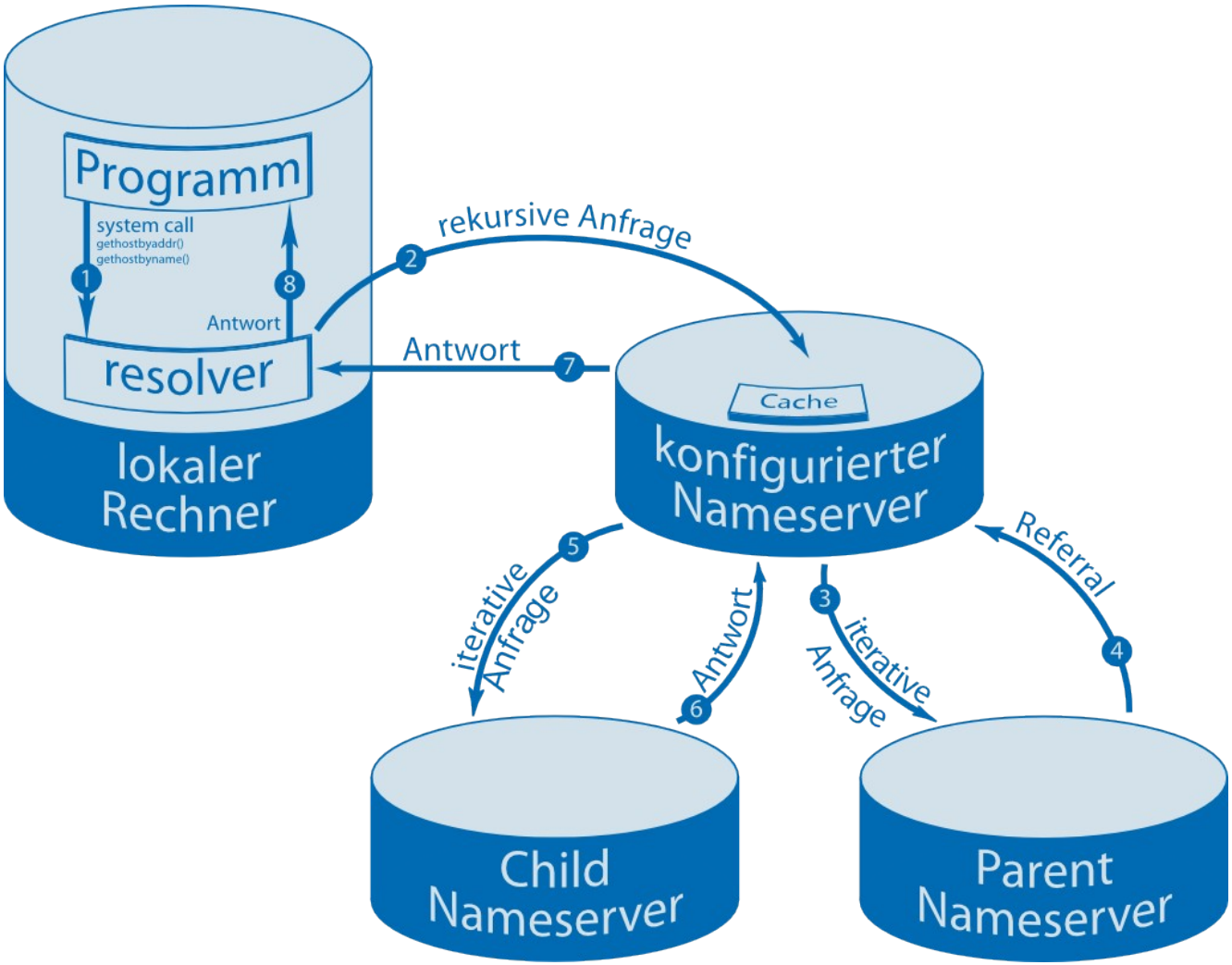
Delegationsbereiche werden "Zone" genannt.

- de-Zone ist an mehrere, redundante DENIC-Nameserver delegiert
- schule.de-Zone ist z.B an diverse Nameserver des ODS e.V. weiterdelegiert.
- ...

DNS-Namensraum – Fazit

- Verteiltes System – kein Server weiß alles!
- Ausgehend von Root-Nameservern werden Teiläste des Namensraums als Zonen delegiert.
- Innerhalb der Hauptzonen können erneut Teiläste als Zonen delegiert werden – usw.
- Im einzelnen Namen sind die Punkte potentielle Delegationsgrenzen (nicht zwingend delegiert!).
- Pro Zone üblicherweise mehrere, redundante Nameserver die hier "autoritativ" sind.
- Autoritative Nameserver in "primär" (einer) und einen oder mehrere "sekundäre" Nameserver aufgeteilt (früher Master- und Slave-Server).

DNS-Anfrage eines Hosts



Hank van Helvete, Wikipedia

DNS-Beispielanfrage

Source	Destination	Protocol	Info
p549E5D84.dip.t-dialin.net	G.ROOT-SERVERS.NET	DNS	Standard query A www.hes.fn.bw.schule.de
G.ROOT-SERVERS.NET	p549E5D84.dip.t-dialin.net	DNS	Standard query response
p549E5D84.dip.t-dialin.net	Z.NIC.de	DNS	Standard query A www.hes.fn.bw.schule.de
Z.NIC.de	p549E5D84.dip.t-dialin.net	DNS	Standard query response
p549E5D84.dip.t-dialin.net	dns1.shuttle.de	DNS	Standard query A www.hes.fn.bw.schule.de
dns1.shuttle.de	p549E5D84.dip.t-dialin.net	DNS	Standard query response
p549E5D84.dip.t-dialin.net	arbi.informatik.uni-oldenb	DNS	Standard query A www.hes.fn.bw.schule.de
arbi.informatik.uni-oldenburg	p549E5D84.dip.t-dialin.net	DNS	Standard query response A 129.143.233.11

Reihenfolge der Namensauflösung (eines DNS-Servers):

1. Anfrage an Root-Server ⇒ Verweis auf "de"-Nameserver
2. Anfrage an einen der "de"-Nameserver (hier Z.NIC.de) ⇒ Verweis auf Nameserver von "schule.de"
3. Anfrage an einen der Nameserver von "schule.de" (hier dns1.shuttle.de) ⇒ Verweis auf NS von "bw.schule.de"
4. Anfrage an einen der NS von "bw.schule.de" (hier arbi.informatik.uni-oldenburg.de) ⇒ IP-Adresse als autoritative Antwort!
   Grund: Die verwaltete Zone enthält neben der Subdomain "bw.schule.de" auch noch alle darin enthalten Subdomains.

(Bsp. einer iterativen DNS-Anfrage, typisch für Nameserver

DNS-Ressourcen

- Verbreitetster DNS-Server → *Berkeley Internet Name Domain (BIND)* oder entsprechend dem zugehörigen Binary oft nur *named*
- Gespeicherte Ressource-Records:
  - A – IPv4 Adresse zu einem Namen
  - AAAA – IPv6 Adresse zu einem Namen
  - NS – Authoritativer Name Server
  - CNAME – zu Alias gehörender Canonical name
  - MX - Mail eXchange Record
- **`ipconfig /displaydns`** → Windows DNS-Cache

DNS-Diagnostik mit nslookup

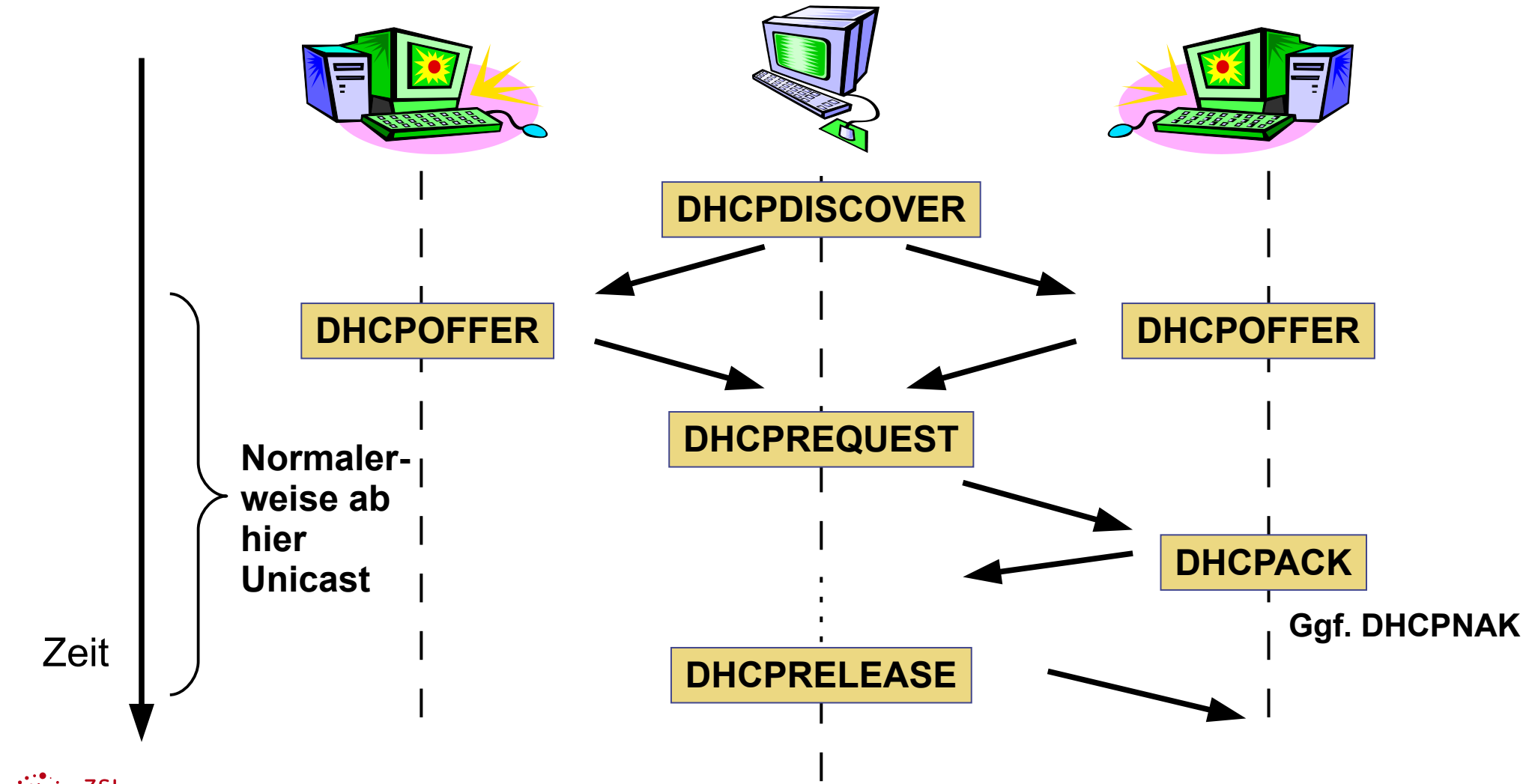
Beispiel um Nameserver zu einer Domain abzufragen:

```
C:\>nslookup
Standardserver:  server.grupp.private
Address:  172.16.0.1

> set type=ns
> schule.de
Server:  server.grupp.private
Address:  172.16.0.1

Nicht autorisierte Antwort:
schule.de       nameserver = dns1.Shuttle.de
schule.de       nameserver = ws-mue1.win-ip.dfn.de
schule.de       nameserver = dns.schule.de
schule.de       nameserver = arbi.Informatik.Uni-Oldenburg.de
```

Dynamic Host Configuration Protocol – DHCP

- Automatisierte Client-Konfiguration mit IP Adresse (aus Pool), Subnet Maske, Gateway, …
- Zeitbefristete „Leases“
- Nicht sinnvoll für Server, Drucker, Switches, Router, …! Neben DHCP also auch statische IPs
- DHCP-Server je nach Netz auf lokalem Router, auf dediziertem Server, auf ISP-Router, …
- Durchaus auch Sicherheits-Problem → Angreifer bekommen auch IP-Daten! Physikalische Sicherheit für Netze beachten

Ablauf einer IPv4-DHCP-Anfrage



File Transfer Protocol - ftp

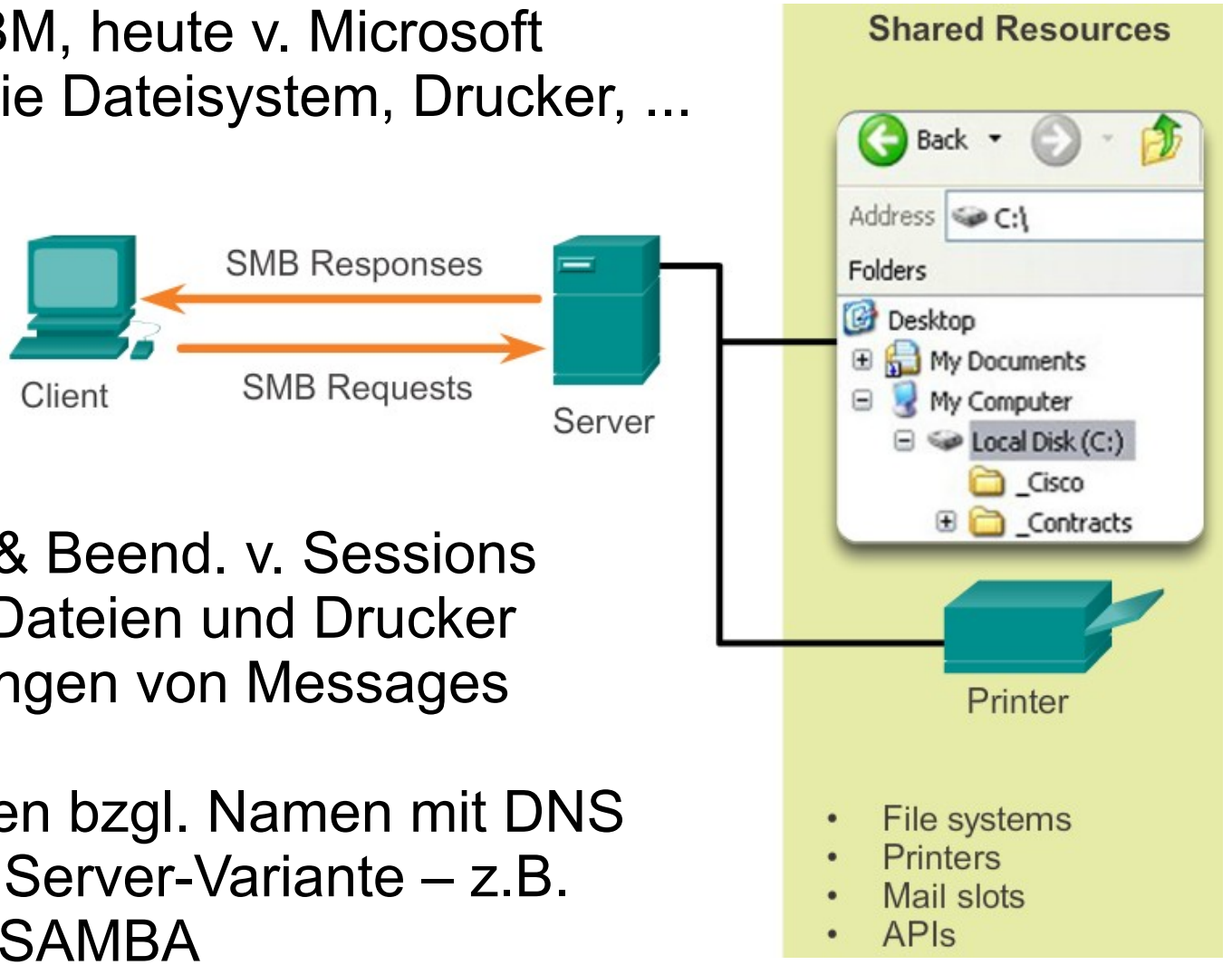
Im aktiven Mode von ftp wird Datenverbindung vom Server zum Client geöffnet. In NAT-Umgebungen ein Problem.

1. Control Connection:
Client öffnet erste Verbindung zum Server. Dient für Control-Kommandos

2. Data Connection:
Client öffnet, im passiven Mode, zweite Verbindung für die eigentliche Datenübertragung

Server Message Block (SMB)

Ursprünglich von IBM, heute v. Microsoft
Ressourcenfreig. wie Dateisystem, Drucker, ...



- Start, Authent. & Beend. v. Sessions
- Kontrolle über Dateien und Drucker
- Senden/Empfangen von Messages

…

Aktuelle Versionen bzgl. Namen mit DNS gekoppelt. Freie Server-Variante – z.B. unter Linux – ist SAMBA

Quizze , Activities, Laborübungen, … dieses Moduls

- Diverse „Check Your Understanding“ wie üblich
- 15.4.8 Lab - Observe DNS Resolution

Fragen