Multimedia, Future Internet und Netzwerk-Virtualisierung

Dr. Christian Baun

christian.baun@h-da.de

31.5.2012

Ausbildung und beruflicher Werdegang

- 2005: Diplom in Informatik an der FH Mannheim
- 2006: Master of Science an der HS Mannheim
- 2006 – 2011: Wissenschaftlicher Mitarbeiter am Steinbuch Centre for Computing des Karlsruher Instituts für Technologie (bis 09/2009 Forschungszentrum Karlsruhe GmbH)
  - 2006 – 2008: D-Grid Integrationsprojekt
    - Referenzinstallation
    - Integration zusätzlicher Komponenten und nachhaltiger Betrieb
  - 2008 – 2011: Open Cirrus Cloud Computing Testbed
    - Betrieb und Optimierung von privaten Clouds
    - Entwicklung von Cloud-Werkzeugen
- 2011: Promotion an der Universität Hamburg
  - Titel: „Untersuchung und Entwicklung von Cloud Computing-Diensten als Grundlage zur Schaffung eines Marktplatzes“
- Seit Oktober 2011: Vertretungsprofessur an der HS Darmstadt

Lehrveranstaltungen und Veröffentlichungen (2006 – 2012)

- 21 eigenverantwortliche Lehrveranstaltungen an der HS Darmstadt, HS Mannheim, Universität Heidelberg und Universität Karlsruhe (TH)
  - 5x Betriebssysteme
  - 4x Systemsoftware
  - 4x Cluster, Grid und Cloud Computing
  - 3x Seminar Cloud Computing
  - 2x Netzwerke
  - ...
- 50 Veröffentlichungen
  - 4 Bücher über Netzwerke, Cloud Computing und Verteilte Systeme
  - 2 Buchbeiträge
  - 8 Konferenzbeiträge auf internationalen Konferenzen
  - 17 Artikel (u.a. Informatik Spektrum, PIK, iX und c't)
  - 19 Vorträge auf Konferenzen und Workshops

`https://www.fbi.h-da.de/organisation/personen/baun-christian.html`
`http://www.informatik.hs-mannheim.de/~baun/`

Agenda

- Status des Internet und seine Reformierbarkeit
- Übertragungsverfahren für Videos im Internet
- Mobile IP
- Varianten der Netzwerkvirtualisierung
- Lösungsmöglichkeiten für das „Future Internet“

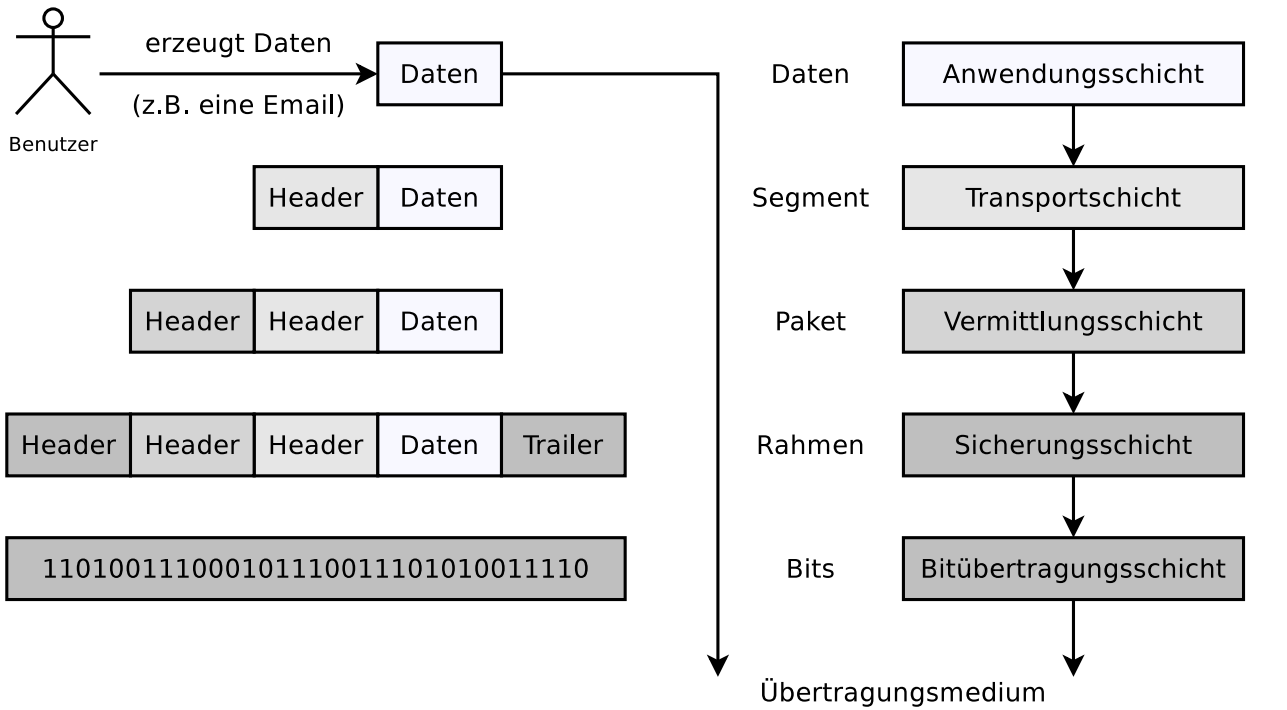
Internet

- Das **Internet**...
  - hat zahlreiche Aspekte unseres Alltags verändert
    - Kommunikation
    - Arbeit
    - Konsum
    - Freizeit
  - bietet zahllose Informationen, die in kurzer Zeit gefunden werden können
  - ist heute (fast) überall verfügbar
  - kann mit verschiedensten Geräten verwendet werden
- Viele Menschen würden dieser Aussage zustimmen:
  - „Das Internet steht für **Modernität**“

Was macht das Internet aus? Woraus besteht es?

Jede Schicht (Layer)...

- behandelt via **Protokolle** bestimmte Aspekte der Kommunikation
- ist in sich abgeschlossen
  - Einzelne Protokolle können verändert oder ersetzt werden, ohne alle Aspekte der Kommunikation zu beeinflussen



Die eigentlichen Nachrichten entsprechend dem jeweiligen Anwendungsprotokoll

Daten für den Transport verpacken
Ende-zu-Ende-Kommunikation
Adressierung der Prozesse mit Portnummern

Paketweiterleitung über physische Abschnitte
Weiterleitung der Pakete und Wegermittlung
Logische Adressen

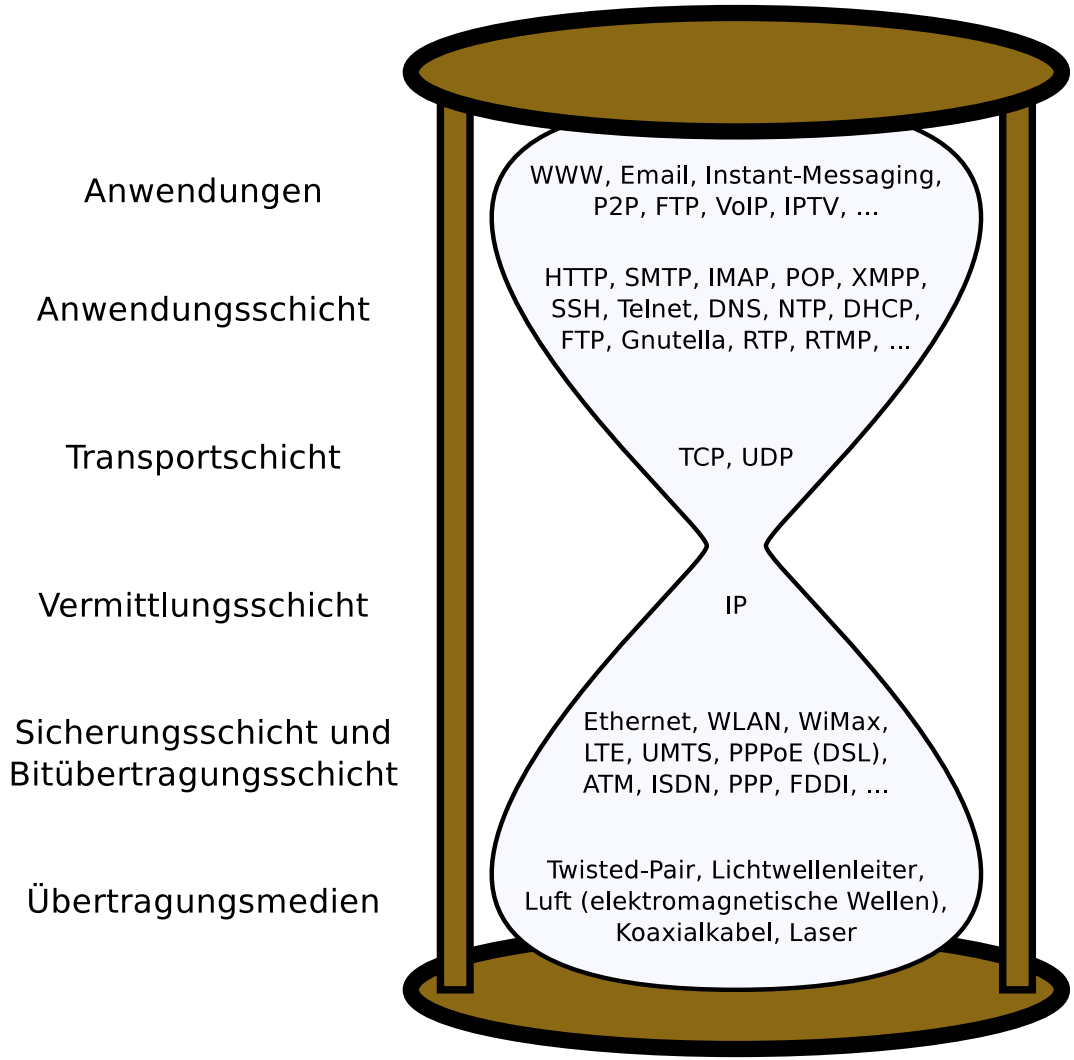
Fehlerfreien Datenaustausch gewährleisten
Zugriff auf das Übertragungsmedium regeln
Physische Adressen

Physischer Anschluss ans Übertragungsmedium
Kodierung der Daten mit Leitungscodes

Können wirklich alle Protokolle einfach ersetzt werden? Wann ist das zuletzt geschehen?

Realität im Internet

- Kommunikation soll für jede Anwendung über jedes (physische) Netzwerk möglich sein
- Transportschicht und Vermittlungsschicht sind die Middleware zwischen den Anwendungen und Vernetzungstechnologien
  - Die Protokolle dieser Schichten sind die **Kernprotokolle**



Ist das Internet (die Kernprotokolle!) wirklich modern? Gab es Änderungen in den letzten Jahren?

Einige Änderungen an den Kernprotokolle des Internet

- 1983: **TCP/IP** wird im Arpanet eingefügt
  - Wenige hundert Knoten sind betroffen
  - Das Arpanet wird dadurch zu einem Subnetz des noch jungen Internet
- Mitte der 1980er Jahre: **Überlastkontrolle** wird nötig
  - Integration in TCP, obwohl es genauso bei UDP hilfreich wäre
    - Keine Etablierung einer neuen Schicht oder Anpassung von IP
- 1993: **Classless Interdomain Routing** (CIDR) wird eingeführt
  - Unterteilung des IPv4-Adressraums mit Klassen ist unflexibel
  - Subnetze sind nun möglich
    - IPv4-Adressraum wird damit effizienter genutzt

1993: NCSA Mosaic, der erste populäre Browser, erscheint und das WWW wird langsam populär.
Seit 1993: Keine großen Änderungen an den Kernprotokollen, sondern nur kleine Verbesserungen!

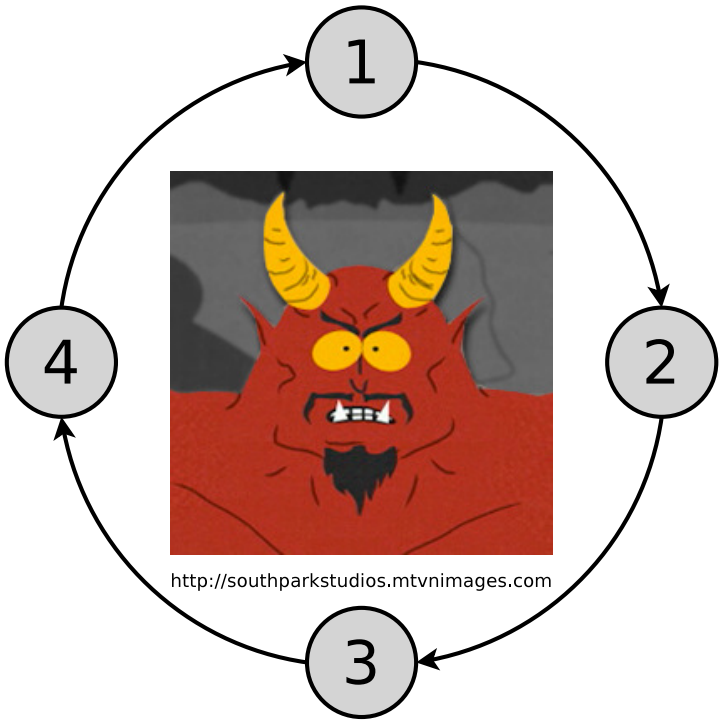
Status des Internet und seine Reformierbarkeit

- „**Why the Internet only just works**“(2006) von Mark Handley
  `http://www.cs.ucl.ac.uk/staff/M.Handley/papers/only-just-works.pdf`
- Zusammenfassung:
  - Erweiterungen und Verbesserungen an den Kernprotokollen...
    - fanden seit 1993 kaum statt
    - müssen rückwärtskompatibel sein, was die Möglichkeiten hemmt
    - benötigen Dekaden bis zur Etablierung
  - Wir können das Internet auch nicht abschaffen und ein neues und besseres Internet erschaffen
- Fazit: **Das Internet ist verknöchert!**
  - Seine Kernprotokolle sind kaum reformierbar

Was ist der Grund für diese Stagnation?
Warum ist die Etablierung neuer Kernprotokolle so schwierig?

Etablierung besserer Kernprotokolle ist schwierig

- Etablierung eines neuen Vermittlungsprotokolls: **(fast) unmöglich**
- Etablierung eines neuen Transportprotokolls: **schwierig**
  1. Anwendungsentwickler implementieren es nur, wenn es Ende-zu-Ende funktioniert (Firewalls und Router mit NAT!)
  2. Betriebssystementwickler implementieren es nur, wenn populäre Anwendungen es verwenden
  3. Entwickler von Firewall- und NAT-Lösungen unterstützen es nur, wenn es in populären Betriebssystemen implementiert ist
  4. Neue Protokolle funktionieren nicht Ende-zu-Ende, weil Firewalls und Router mit NAT es nicht kennen

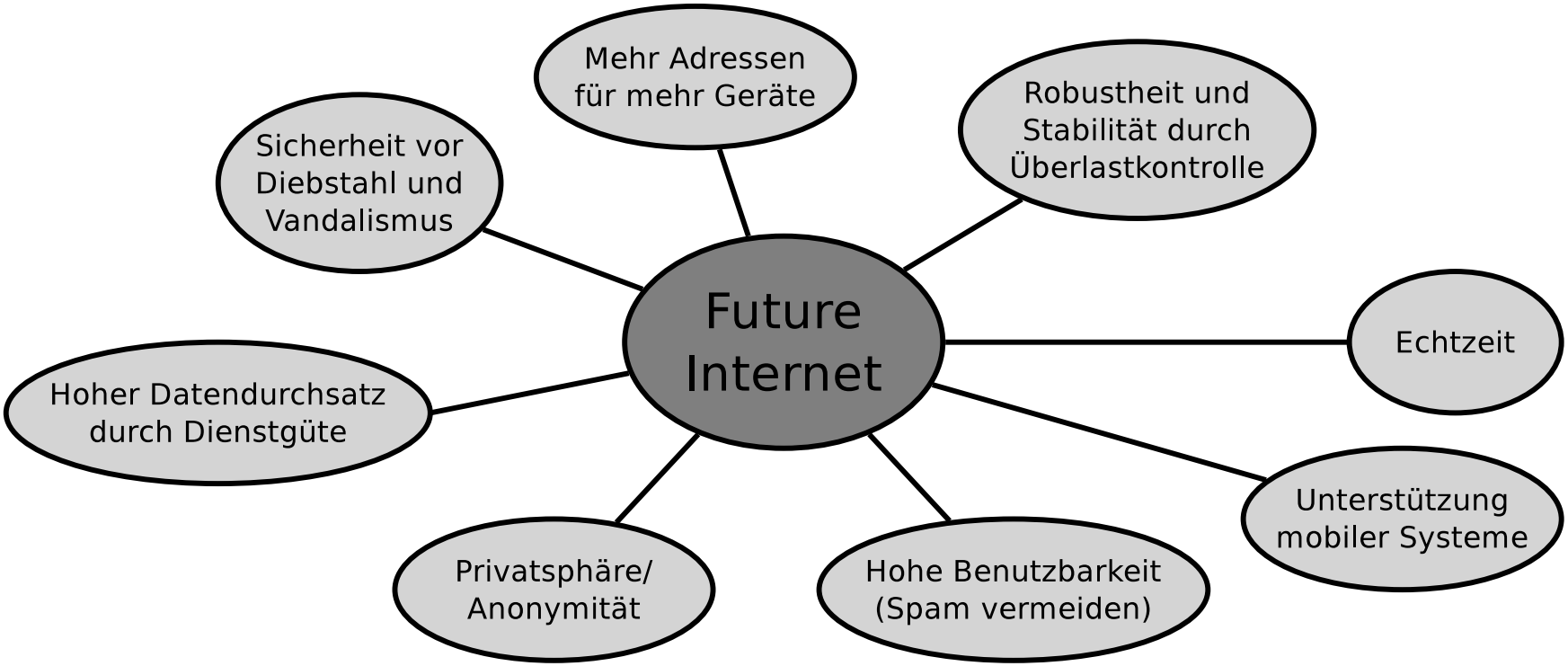


Nicht das Internet ändert sich, aber die Anforderungen

- **Konzentration der Dienste** führt zu stärkerer Netzbelastung
  - Beispiele: VoIP, IPTV (Multicast), TV on-demand,... ($\Longrightarrow$ **Echtzeit**)
  - Konzentration der Dienste erfordert **Dienstgüte** (Quality of Service)
- Spam verringert die **Benutzbarkeit** und muss reduziert werden:
  - Spam via Email heute
  - Spam over Internet Telephony (SPIT) vielleicht in Zukunft
- **Gefahren** müssen bekämpft werden:
  - Diebstahl und Vandalismus durch Viren, Würmer, Phishing, Spyware,...
- **Überlastkontrolle** für beliebige Anwendungen wird dringender
  - Unterschiede bzgl. der Leitungskapazität nehmen zu
- **Mobile Systeme** sind heute Standard
  - Wechsel der IP sind für zahlreiche Anwendungen (z.B. SSH) ein Problem
- **Adressknappheit** in der Vermittlungsschicht ist ein Problem
  - NAT ist eine Lösung, aber Hardware mit NAT hemmt neue Entwicklungen (Protokolle)
- **Anonymität** ist von Benutzern erwünscht

„Future Internet“

- Unter diesem Schlagwort sucht man Lösungen für die aktuellen Anforderungen an das Internet



- Die Themengebiete Multimedia und Netzwerkvirtualisierung spielen hier eine große Rolle

Multimedia

- Das Internet ermöglichte bis zur Entwicklung des WWW nur den Austausch von Dateien und Textnachrichten
  - Erst die Browser Viola (1992) und Mosaic (1993) konnten auch Grafiken anzeigen
- Multimedia im Internet ist heute meist gleichbedeutend mit **Videos**
- Aktuelle Entwicklung:
  - 02.06.2010: „Annual Cisco Visual Networking Index Forecast Projects Global IP Traffic to Increase More Than Fourfold by 2014“
    `http://newsroom.cisco.com/dlls/2010/prod_060210.html`
    - Hauptgrund: Video
    - 2014 soll der monatliche Datenverkehr bei 64 Exabyte liegen
    - 2014 soll die Summe aller Video-Angebote (IPTV, VoD, Internet Video) mehr als 91% des globalen Datenverkehrs ausmachen
    - Schon 2010 übertraf der Video-Datenverkehr den P2P-Datenverkehr
  - 14.05.2012: „Online-Videokonsum steigt in Deutschland kräftig an“
    `http://heise.de/-1575372`

Übertragungsverfahren für Videos im Internet

- **Download**
  - Webserver überträgt (z.B. via HTTP) statische Videodaten
  - Client verwendet ein Browser-Applet oder ein entsprechendes Programm, das die Videodaten vollständig herunterlädt oder teilweise puffert
- **Streaming**
  - Streaming-Server überträgt einen Datenstrom mit Videodaten zum Client
  - Die Datenverbindung unterliegt einer Qualitätskontrolle
  - Über ein Übertragungsprotokoll können Server und Client in Echtzeit Zustände, Qualitätsmetriken und Metadaten austauschen

Download-Verfahren

- **Podcast**
  - Enthält nur die URL einer Datei zum Download
  - Server agiert als einfacher Webserver ohne zusätzliche Funktionalität
- **Progressiver Download**
  - Applet oder HTML5-fähiger Browser puffert einen Teil (z.B. 5s) der Videodaten
    - Nach dem Puffern kann der Client das Video abspielen, während das Applet den Rest des Videos im Hintergrund puffert
  - Modifizierte Videodateien sind nötig, die den Header mit den Metadaten am Dateianfang besitzen
    - Der Header befindet sich sonst standardmäßig am Dateiende
- **HTTP-Pseudo-Streaming**
  - Videos können an jeder beliebigen Stelle mit einem Keyframe starten
    - Arbeitsweise: Webserver können Dateien erst ab einem bestimmten Offset in der Datei übertragen
  - Ein serverseitiges Modul muss „*on-the-fly*“ einen Header vor die Videodaten hängen, wenn der Client das Video anfragt

Streaming-Protokolle

- Video-Streaming ist das Übertragen eines Datenstroms von Videodaten vom Server zum Client mit **Qualitätskontrolle**
  - Ein Streaming-Protokoll ermöglicht es, sowohl Live-Aufnahmen mit geringer Zeitverzögerung als auch Videodateien von einem persistenten Speicher zu übertragen
- Ein Streaming-Protokoll besteht aus mindestens zwei einzelnen Streams
  - **Transportstrom**
    - Übermittelt die eigentlichen Nutzdaten (Video)
  - **Kontrollstrom**
    - Stellt die Dienstgüte (Quality of Service) sicher
    - Ziel: Unterbrechungsfreie Wiedergabe auf dem Client
    - Ist ein anwendungsspezifischer QoS auf der Anwendungsschicht
- Für Streaming ist ein Streaming-Server zwingend notwendig
  - Beispiele: Adobe Flash Media Server, RealNetworks Helix Server,...
- Populäre Streaming-Protokolle: **RTP** und **RTMP**

Real-Time Transport Protocol (RTP)

- Verwendet das User Datagram Protocol (UDP) zum Transport
- Komponenten:
  - Transport Protokoll
    - Überträgt die Nutzdaten (Video)
  - RealTime Streaming Protocol (**RTSP**)
    - „*Netzwerk-Fernbedienung*“
    - Steuerung des Video-Stroms (z.B. Start, Stop, Pause,. . .)
  - Real Time Control Protocol (**RTCP**)
    - Aushandlung und Einhaltung von Quality-of-Service-Parametern
    - Tauscht Steuernachrichten zwischen Server und Client aus
    - Durch Rückmeldungen (Sender- und Empfängerberichte) erfolgen Anpassungen der Übertragungsrate

Real Time Messaging Protocol (RTMP)

- Verwendet das Transmission Control Protocol (TCP) zum Transport
- Benötigt keine zusätzlichen Kontrollprotokolle wie RTSP und RTCP
  - Enthält außer Nachrichten zur Übermittlung der Nutzdaten auch Nachrichten zur Steuerung des Servers, Übertragung der Video-Metadaten und Anpassung der Übertragungsrate (QoS)
- Kommunikation ist **direkt** via TCP/IP oder **getunnelt** via HTTP möglich
  - Tunnel-Variante: RTMP-Nachrichten werden in HTTP-Antwortnachrichten verpackt, um Firewalls zu überwinden

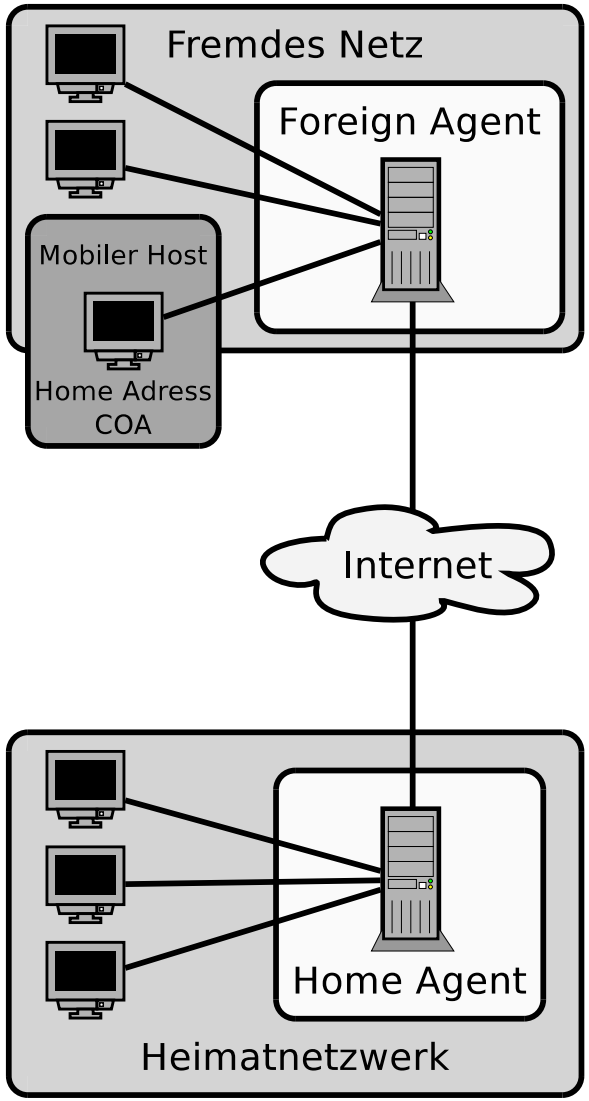
Mobile Systeme

- Bei Downloads oder Streaming darf sich die IP nicht ändern
- Mobile Systeme werden aber zunehmend populär
  - Cisco (2010): „*Der globale Datenverkehr durch mobile Geräte steigt zwischen 2009 und 2014 um das 39-fache auf 3,5 Exabyte pro Monat*“

    Quelle: `http://newsroom.cisco.com/dlls/2010/prod_060210.html`
- Lösung: **Mobile IP**

Mobile IP

- Jedes Endgerät erhält zwei IP-Adressen
  - Home Address und Care-Of-Address (COA)
- Verlässt das Endgerät sein Heimatnetz, meldet es sich beim Foreign Agent im fremden Netz an und erhält von diesem eine COA zugewiesen
  - Die COA teilt das Endgerät seinem Home Agent im Heimatnetz mit
- Datenpakete leitet der Home Agent via IP-to-IP-Kapselung an die COA und damit über den Foreign Agent an den Mobile Host weiter
  - Bei IP-to-IP-Kapselung (*Tunneling*) werden IP-Pakete als Nutzdaten eines anderen IP-Pakets verpackt
- So können mobile Geräte das Netzwerk wechseln und dabei ihre IP behalten



Netzwerkvirtualisierung

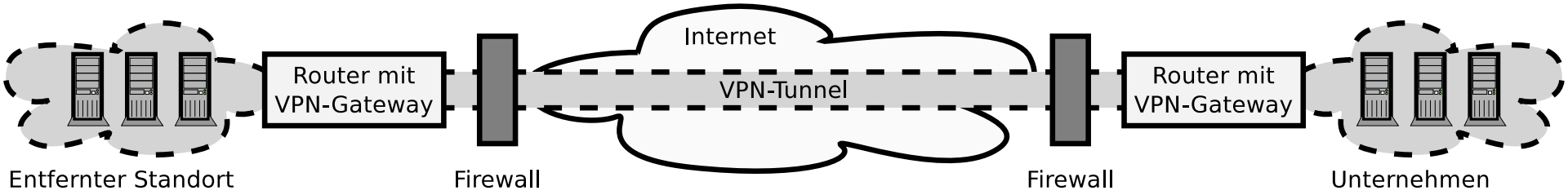
- Schlagwort für unterschiedliche Ansätze, um Netzwerkressourcen zu logischen Einheiten zusammenzufassen oder aufzuteilen
- Vorteile:
  - Unabhängigkeit von den physischen Gegebenheiten
  - Flexibilität
  - Höhere Sicherheit gegenüber Datendiebstahl und menschlichen Fehlern
- Varianten der Netzwerkvirtualisierung:
  - **Virtual Private Networks** (VPN)
  - **Virtual Local Area Networks** (VLAN)

Virtual Private Networks (VPN)

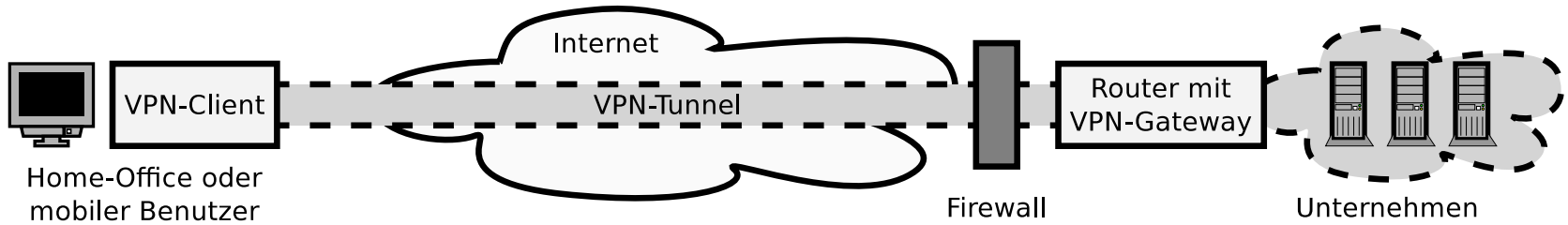
- Sind virtuelle private Netze (logische Teilnetze) innerhalb öffentlicher IP-Netze (z.B. Internet)
  - Ein Teilnehmer kann physisch an einem öffentlichen Netz angeschlossen sein, ist jedoch via VPN einem Netz zugeordnet
- Realisierung: VPN-Tunnel durch das IP-Netz
  - Ein VPN-Tunnel ist eine virtuelle Verbindung zwischen zwei Enden
    - IP-Pakete werden an Tunnelenden mit einem VPN-Protokoll gekapselt, zum anderen Tunnelende übertragen und dort ausgepackt
- Vorteile:
  - VPN-Verbindungen kann man verschlüsseln
    $\Longrightarrow$ Sicherheit
  - Zugriffe ins Internet gehen nicht über das zugeordnete Netz, sondern über das via VPN verbundene Netz
    $\Longrightarrow$ Sicherheit und evtl. freieres Arbeiten

Einsatzmöglichkeiten von VPNs

- **Site-to-Site VPN**
  - Verbindet zwei Standorte zu einem einzigen Netzwerk
  - Szenario: Entfernte Unternehmensstandorte ins Firmennetz integrieren



- **Remote Access VPN** oder **End-to-Site VPN**
  - Integriert einen Rechner in ein entferntes Netzwerk
  - Der VPN-Client baut eine Verbindung zum entfernten VPN-Gateway auf
  - Szenario: Ein Mitarbeiter arbeitet von zuhause über das Firmennetz



Technische Arten von VPNs

- **Layer-2-VPN**
  - Protokollbeispiele: Point-to-Point Tunneling Protocol (PPTP)
  - Site-to-Site VPN oder Remote Access VPN ist möglich
  - VPN-Gateways und VPN-Clients kapseln Rahmen, z.B. PPP-Rahmen (z.B. Modem, ISDN oder DSL) durch zusätzliche Rahmen-Header
- **Layer-3-VPN**
  - Protokoll: Internet Protocol Security (IPsec)
  - Meist Site-to-Site VPN
  - Tunnelmodus: IP-Pakete werden durch zusätzliche IP-Header gekapselt
    - VPN-Client-Software oder Hardwarelösung (VPN-Firewall) nötig
- **Layer-4-VPN**
  - Protokoll: Transport Layer Security (TLS) / Secure Sockets Layer (SSL)
  - Meist Remote Access VPN
  - Sichere Kommunikation via TLS/SSL-Header – kein Tunneling
  - Als Client-Software genügt ein Webbrowser

Beispiele sinnvoller Einsatzgebiete von VPNs

- **Campusnetzwerke** mit WLAN
- Integration von **Home-Office-Arbeitsplätzen** und **entfernten Abteilungen** in das LAN eines Unternehmens oder einer Behörde
  - Identisch hohe Sicherheitsstandards für alle Mitarbeiter
- **Freies** und **anonymes Arbeiten** für Journalisten in schwierigen Ländern
  - Umgehung von Zensurbeschränkungen, wenn man sich mit dem VPN-Gateway verbinden kann
- **Anonymes Surfen** im Internet für Privatpersonen

- Die meisten VPNs basieren auf IPsec (Layer-3-VPN) oder TLS/SSL (Layer-4-VPN)
- IPsec ist meist die Basis für Site-to-Site VPN, da Remote Access VPN einen VPN-Client erfordert
- TLS/SSL ist meist die Basis für Remote Access VPN, da als Client ein Webbrowser genügt

Virtual Local Area Networks (VLAN)

- Verteilt aufgestellte Geräte können via VLAN in einem einzigen virtuellen, logischen Netzwerk zusammengefasst werden
  - VLANs trennen physische Netze in logische Teilnetze (Overlay-Netze)
    - VLAN-fähige Switches leiten Datenpakete eines VLAN nicht in ein anderes VLAN weiter
    - Ein VLAN ist ein nach außen isoliertes Netz über bestehende Netze
  - Zusammengehörende Geräte und Dienste in eigenen VLANs konsolidieren
    - Vorteil: Andere Netze werden nicht beeinflusst
      $\Longrightarrow$ Höhere Sicherheit

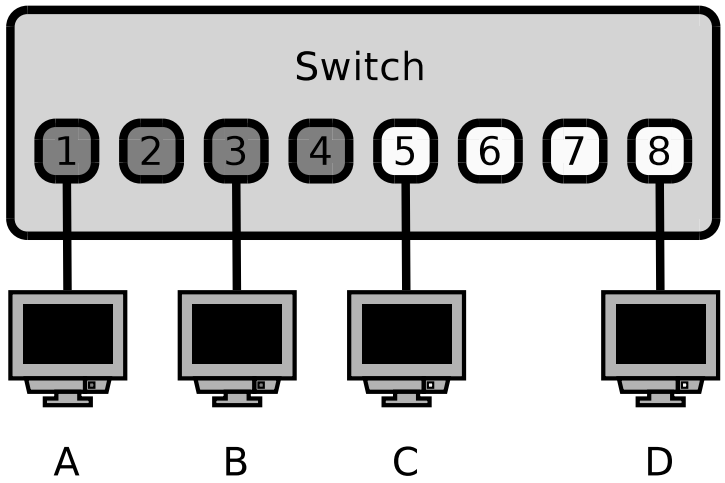
Gute einführende Quellen

Benjamin Benz, Lars Reimann. *Netze schützen mit VLANs*. 11.9.2006
`http://www.heise.de/netze/artikel/VLAN-Virtuelles-LAN-221621.html`
Stephan Mayer, Ernst Ahlers. *Netzsegmentierung per VLAN*. c't 24/2010. S.176-179

Typen von VLANs

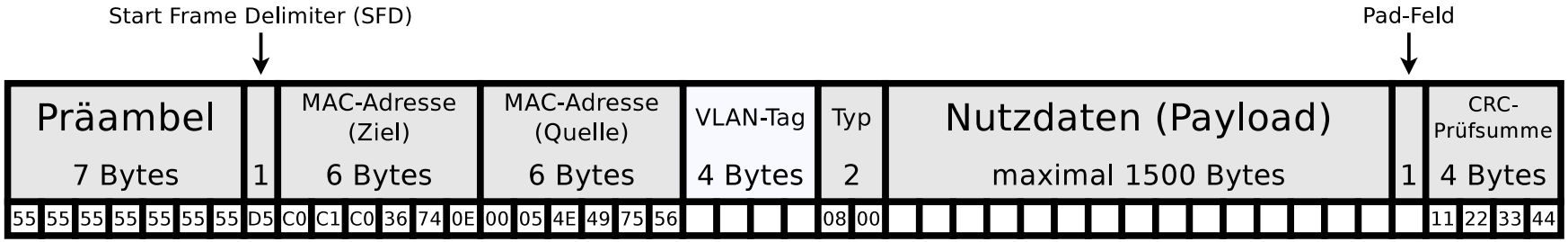
1. Ältester Standard: **Statisches VLAN**
   - Die Anschlüsse eines Switches werden in logische Switches unterteilt
   - Jeder Anschluss ist fest einem VLAN zugeordnet oder verbindet unterschiedliche VLANs
   - Schlecht automatisierbar

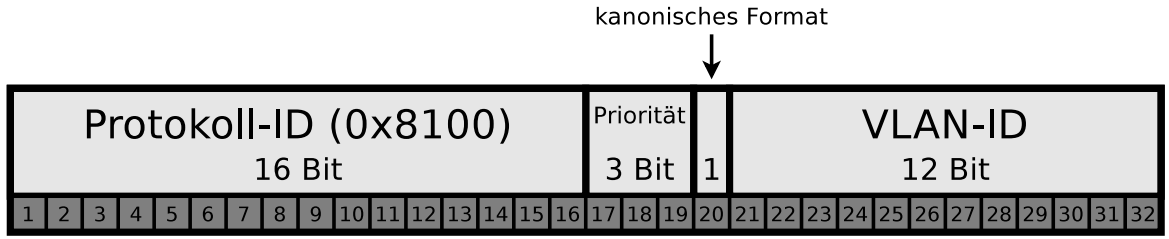
Nur Knoten A und B sowie Knoten C und D können miteinander kommunizieren, obwohl Sie mit dem gleich Switch verbunden sind



2. Aktuell: **Paketbasiertes, dynamisches VLAN** nach IEEE 802.1Q
   - Netzwerkpakete enthalten eine spezielle VLAN-Markierung (*Tag*)
   - Dynamische VLANs können mit Hilfe von Skripten rein softwaremäßig erzeugt, verändert und entfernt werden

Ethernet-Rahmen mit VLAN-Tag nach IEEE 802.1Q



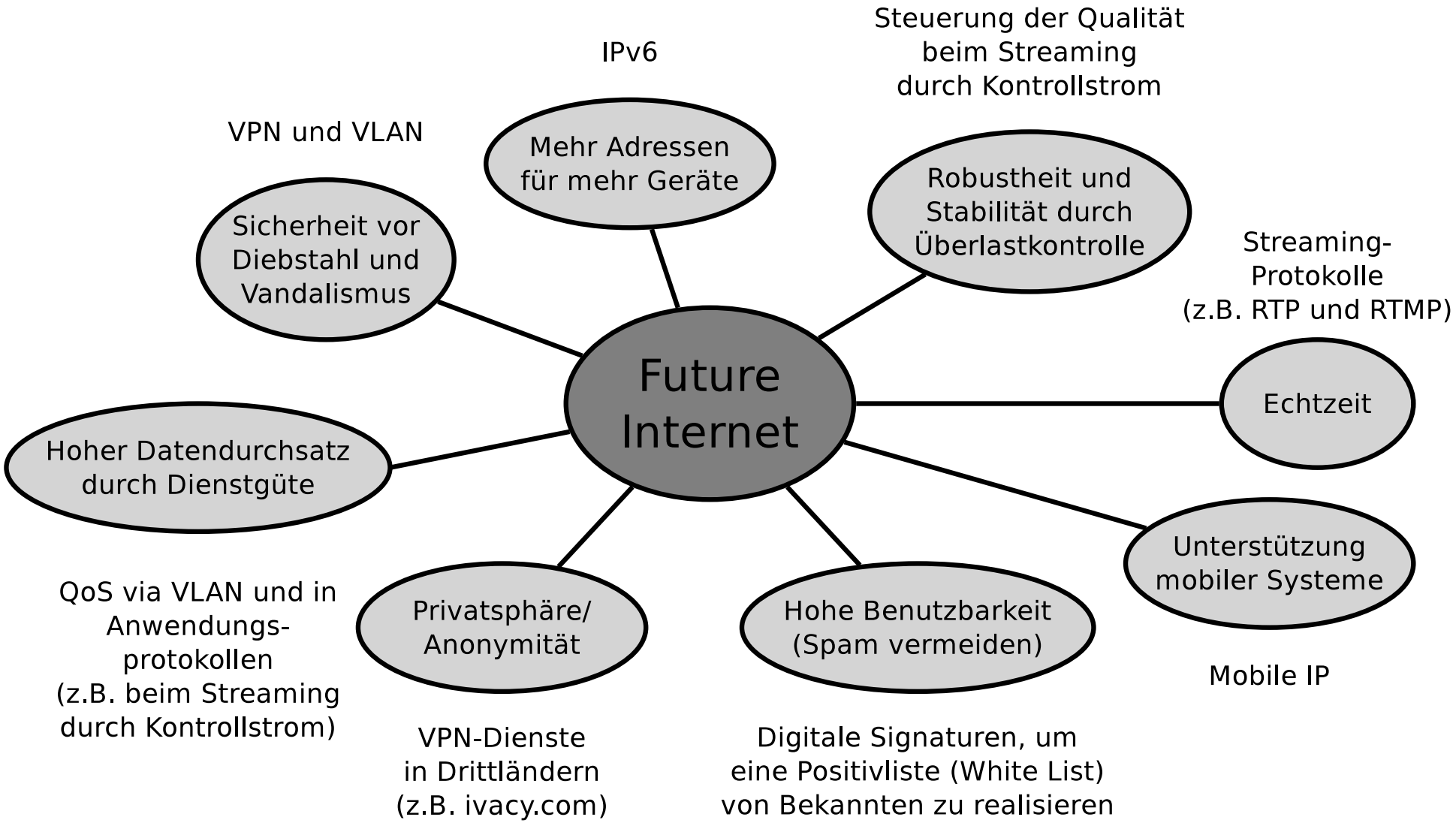


- Die VLAN-Markierung umfasst 32 Bit
- Die Protokoll-ID (16 Bit) hat immer den Wert 0x8100
- 3 Bit repräsentieren die Priorität (QoS)
  - 0 steht für die niedrigste und 7 für die höchste Priorität
  - Damit können bestimmte Daten (z.B. VoIP) priorisiert werden
- Kanonisches Format (1 Bit) $\Longrightarrow$ höchstwertiges Bit der MAC-Adressen
  - 0 = Ethernet, 1 = Token Ring
- 12 Bit enthalten die ID des VLAN, zu dem das Paket im Rahmen gehört

Beispiele sinnvoller Einsatzgebiete von VLANs

- **Telekom Entertain**
  - DSL-Anschluss mit Festnetzanschluss und IPTV
  - Verwendet zwei VLANs, um den IPTV-Datenverkehr zu bevorzugen
    - „Normales“ Internet via PPPoE über VLAN ID 7
    - IPTV ohne Einwahl via VLAN ID 8
- **Eucalyptus**
  - Private Cloud Infrastrukturdienst (IaaS)
  - Jede Virtuelle Maschine (Instanz) ist einer Sicherheitsgruppe zugeordnet
    - Jede Sicherheitsgruppe hat eigene Firewall-Regeln
  - Eucalyptus kann für jede Sicherheitsgruppe ein eigenes VLAN anlegen
    - Isolation des Datenverkehrs der Instanzen anhand der Sicherheitsgruppen
- **Rechenzentren** oder auch **Büro zuhause**
  - Trennung des Datenverkehrs nach ökonomischen Gesichtspunkten
  - Ziel: Absicherung vor Bedienfehlern und fehlerhafter Software
    - Ein VLAN als „Produktionsnetz“ mit den wichtigen Diensten
    - Zusätzliche VLANs für Experimente, Projektarbeit oder Spiele der Kinder

Einige Lösungsmöglichkeiten für das „Future Internet“



Danke für Ihre Aufmerksamkeit!

Die Folien zu diesem Vortrag finden Sie unter:

`http://dl.dropbox.com/u/10971224/Folien_31_5_2012.pdf`

Shortlink:

`http://tinyurl.com/7mtsk84`