Rechnernetze: (1) Einleitung

Prof. Dr. Klaus-Peter Kossakowski

Gliederung der Vorlesung

- **Einführung und Historie des Internets**
- **Schichtenmodell**
  - Dienst, Protokoll, Internet-Modell
  - Einordnung von IT-Sicherheit
- **Netzwerk als Infrastruktur**
- **Layer 7: Anwendungsschicht**
- **Layer 7/4: Socketprogrammierung**
- **Layer 4: Transportschicht**
- **Layer 3: Netzwerkschicht**
- **Layer 2: Sicherungsschicht**

Inhalte dieses Kapitels

In diesem Kapitel lernen Sie die wichtigsten Aufgaben und Arten von Rechnernetzen kennen und erhalten eine Vorstellung davon, wie Kommunikation im Netz stattfindet und wie sie mit Hilfe von Protokollen konzeptionell aufgebaut ist.

Die abstrakten Modelle des modernen Protokoll-aufbaus werden hier gemeinsam mit dem Kommunikationsablauf zwischen den Protokoll-schichten und der Verteilung von Sicherheit besprochen.

Auch Informationen über die Entstehung des Internets gehören mit zur Einführung.

Ziele dieses Kapitels

Sie können die möglichen Aufgaben von Rechnernetzen, die Arten der Kommunikation und Adressierung benennen und unterscheiden.

Sie können das Schichtenmodell im Internet erklären sowie Schichten und Protokolle korrekt benennen und unterscheiden.

Sie können das Konzept von Protokollen und deren Schichtung sowie das Hinzufügen von Headern erklären.

Sie können Vor- und Nachteile bei der Platzierung von Sicherheitsfunktionen in unterschiedlichen Schichten des Schichtenmodells erklären.

Gliederung der Vorlesung

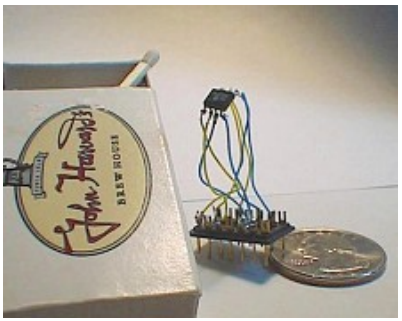
- **Einführung und Historie des Internets**
- **Schichtenmodell**
  - Dienst, Protokoll, Internet-Modell
  - Einordnung von IT-Sicherheit
- **Netzwerk als Infrastruktur**
- **Layer 7: Anwendungsschicht**
- **Layer 4: Transportschicht**
- **Layer 3: Netzwerkschicht**
- **Layer 2: Sicherungsschicht**

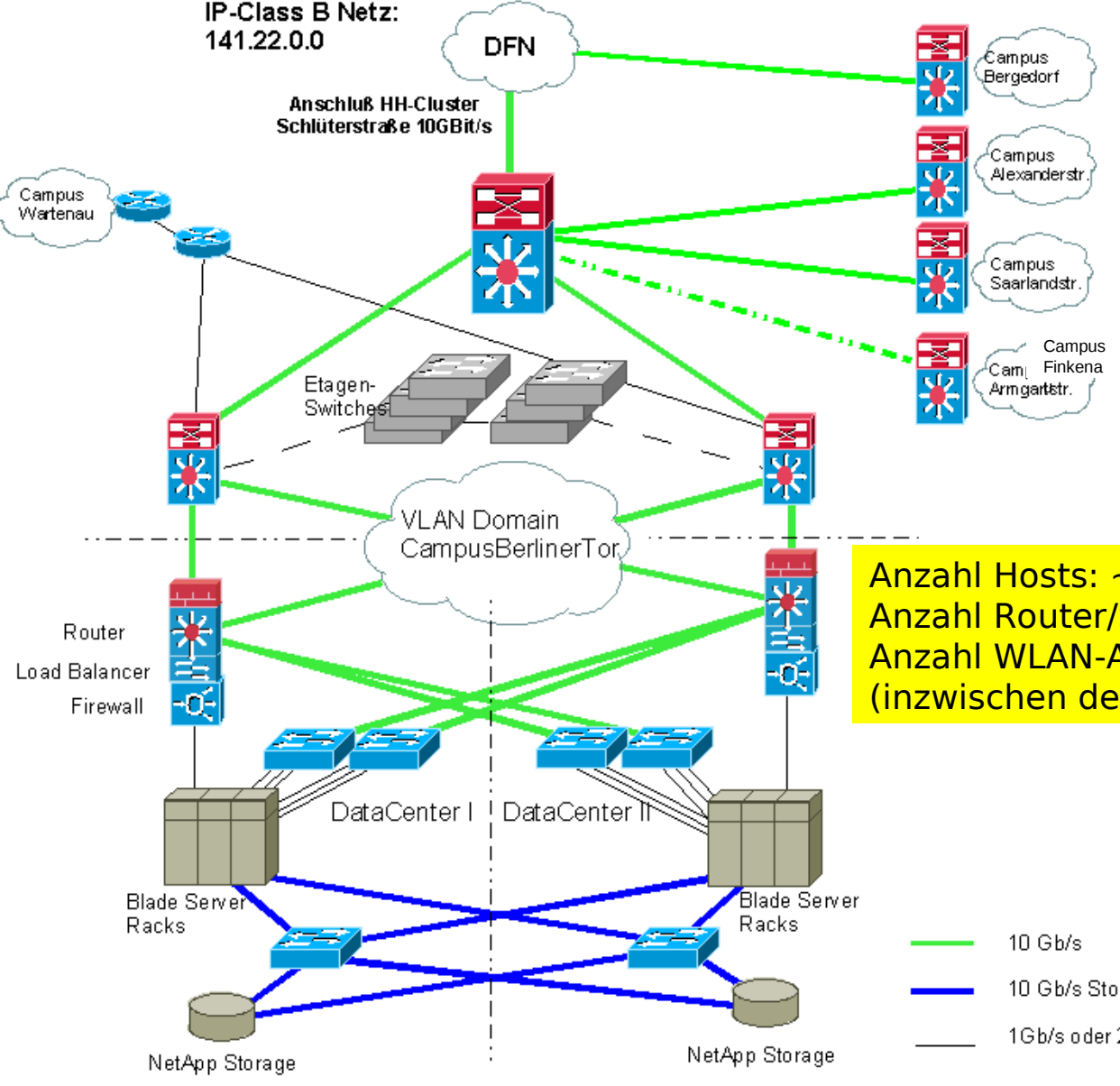
Cooles Internet

IP-Bilderrahmen
http://www.ceiva.com

Web-Toaster mit Wettervorhersage
(kommerziell nicht erfolgreich)

Der kleinste Webserver der Welt !?
http://www-ccs.cs.umass.edu/~shri/iPic.html





Anzahl Hosts: ~ 1.500
Anzahl Router/Switches: ~ 300
Anzahl WLAN-Access Points: ~ 300
(inzwischen deutlich anders)

Was ist das Internet?

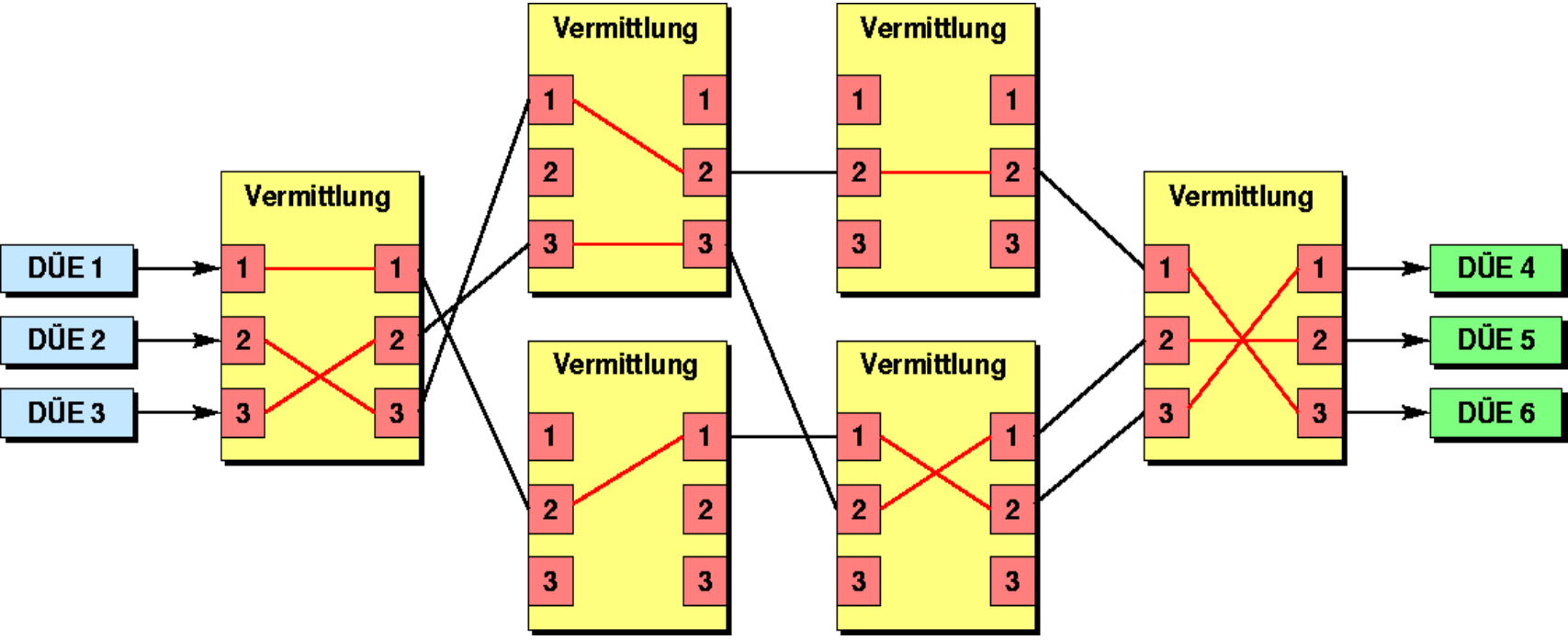
Internet als “Netzwerk von Netzwerken”

- Lose vs. Hierarchisch
- Öffentliches Internet vs. privates Intranet
- Protokolle zum Steuern, Senden, Empfangen von Nachrichten

Internet Standards

- IETF: Internet Engineering Task Force
  http://www.ietf.org
- World Wide Web Consortium (W3C)
  http://www.w3.org

Leitungsvermittlung beim Telefon



Strukturierung von Netzen

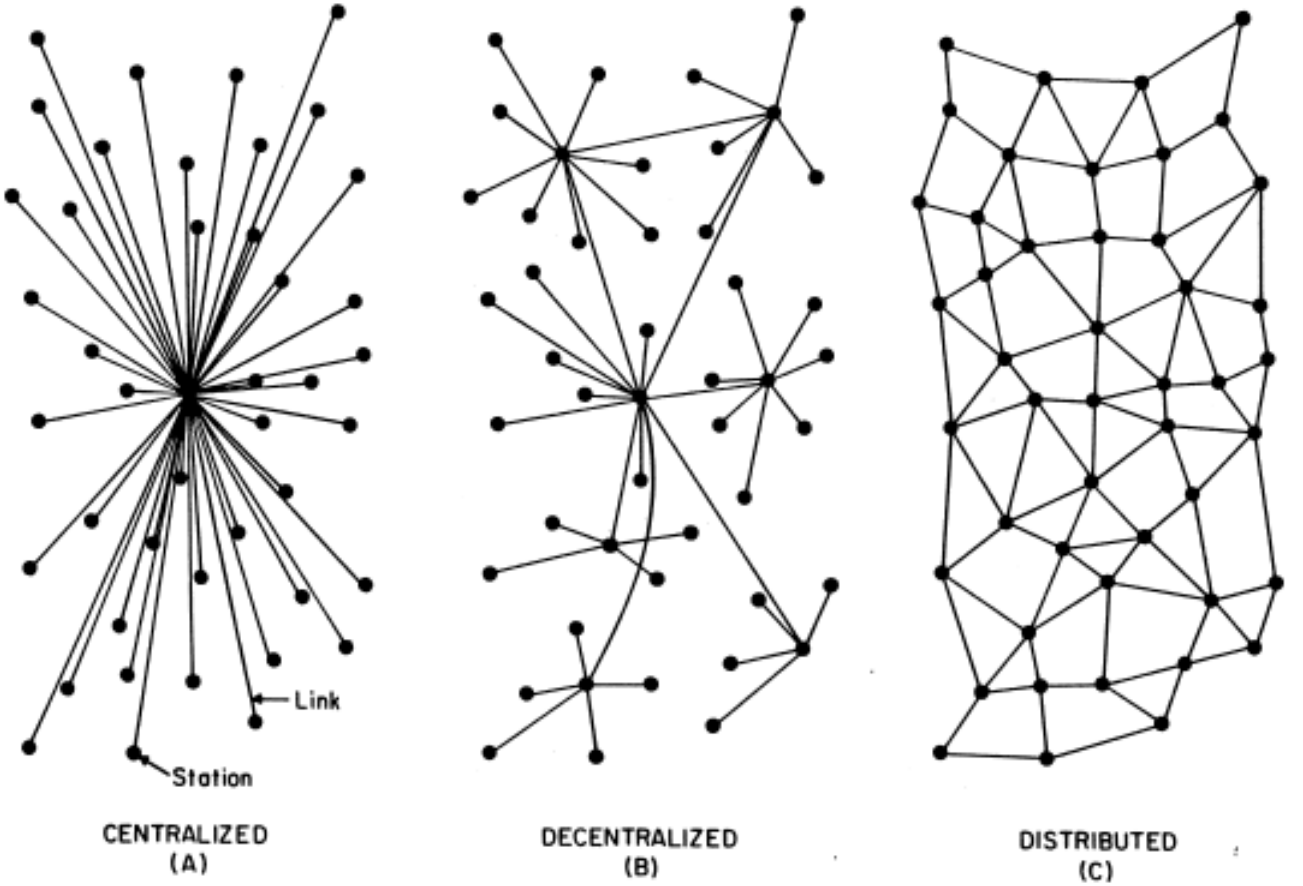
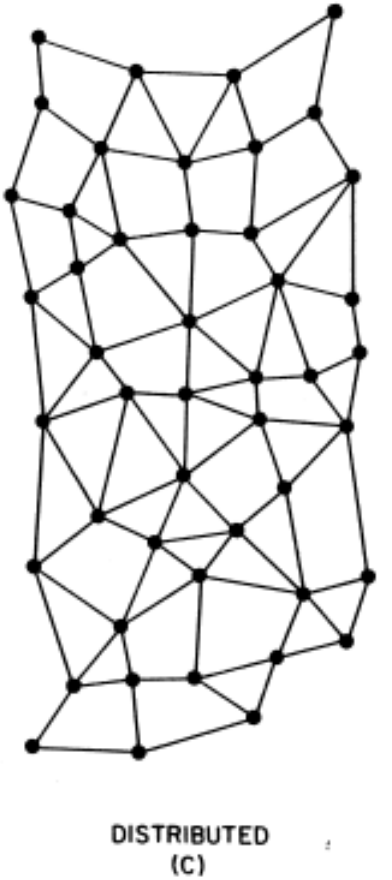


FIG. 1 — Centralized, Decentralized and Distributed Networks

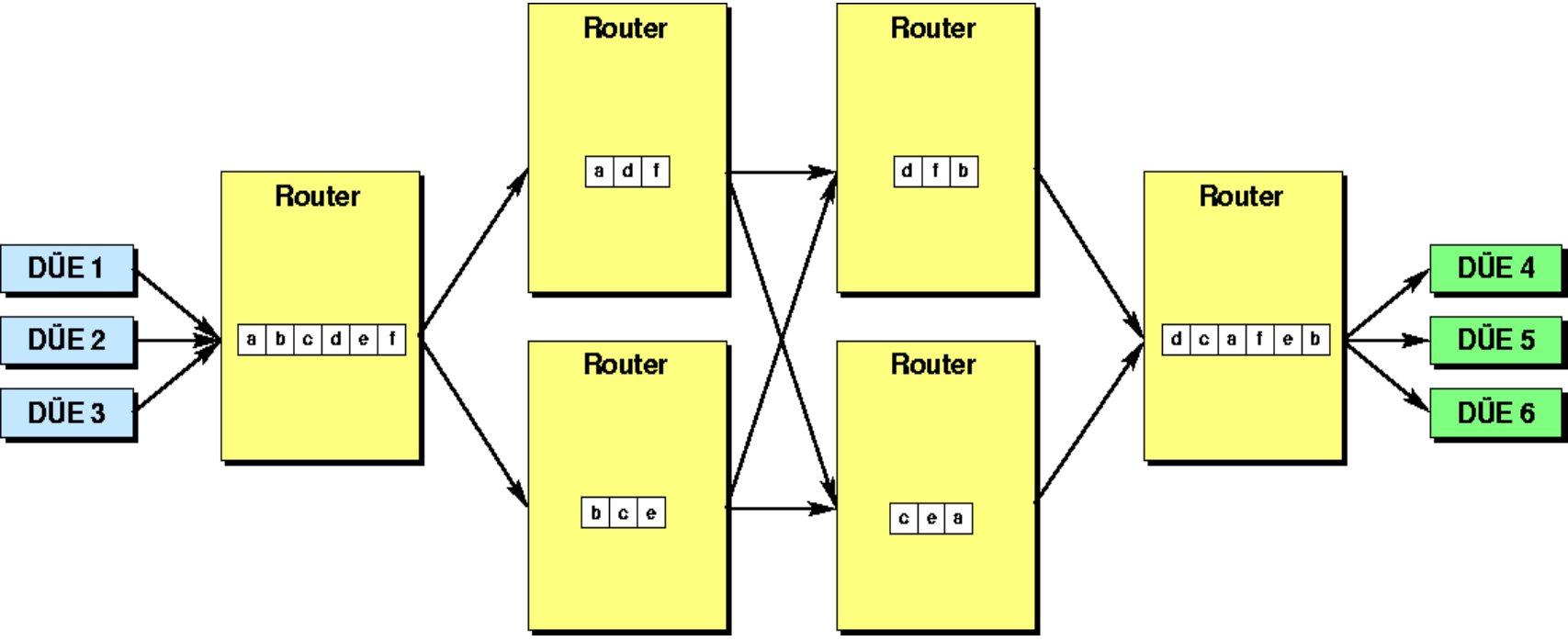
Wichtige Jahre

- **1961 / Kleinrock: Warteschlangentheorie zeigt die Effizienz der Paketvermittlung**

  Bei Ausfall eines Teils des Netzes muss der Rest autark weiterarbeiten können. Damit waren sowohl eine Hierarchie als auch eine zentrale Instanz ausge- schlossen, die Instanzen mussten verteilt sein.



Nunmehr also Paketvermittlung

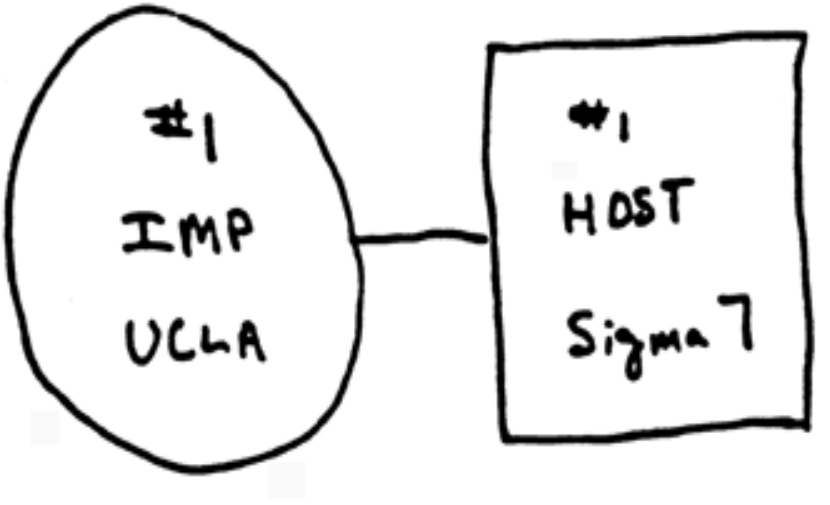


Wichtige Jahre

- 1961 / Kleinrock: Warteschlangentheorie zeigt die Effizienz der Paketvermittlung
- 1968: Ausschreibung der Advanced Research Project Agency (ARPA) zu einem Verbindungsnetz (UCLA, UCSB, SRI, UoU)
- 1969: Der erste ARPAnet-Knoten geht in Betrieb

ARPAnet im September 1969

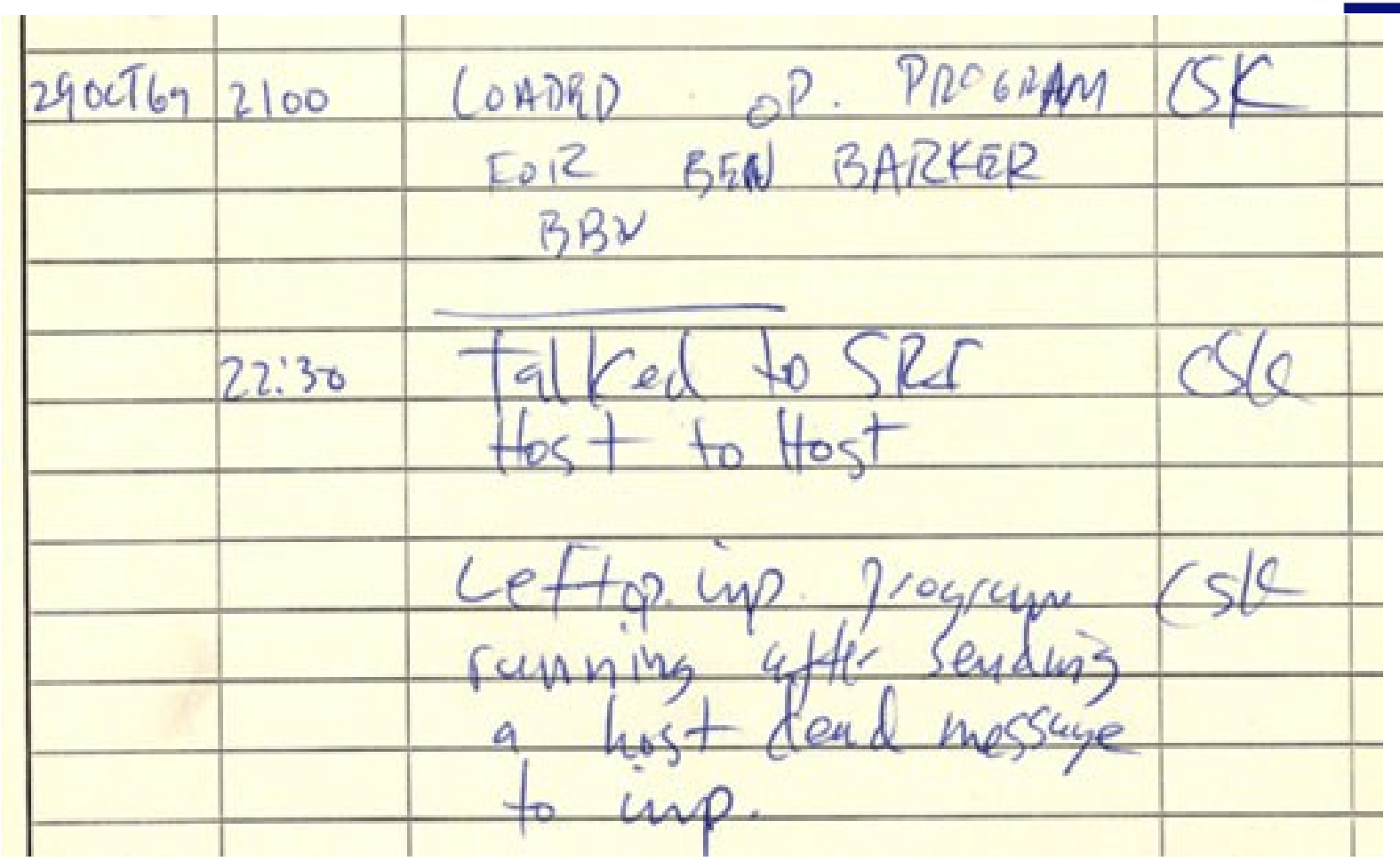
Das Team bei BBN



Einschränkungen des ARPAnet

- **Beschränkt**
  - maximal 64 Interface Message Processor (IMPs)
  - mit je 16 Host Interfaces
- **Beim Einsatz von Mainframes starke Einschränkung**
- **Spätere Einführung lokaler Netze erfordert massive Steigerung der Host-Anzahl**

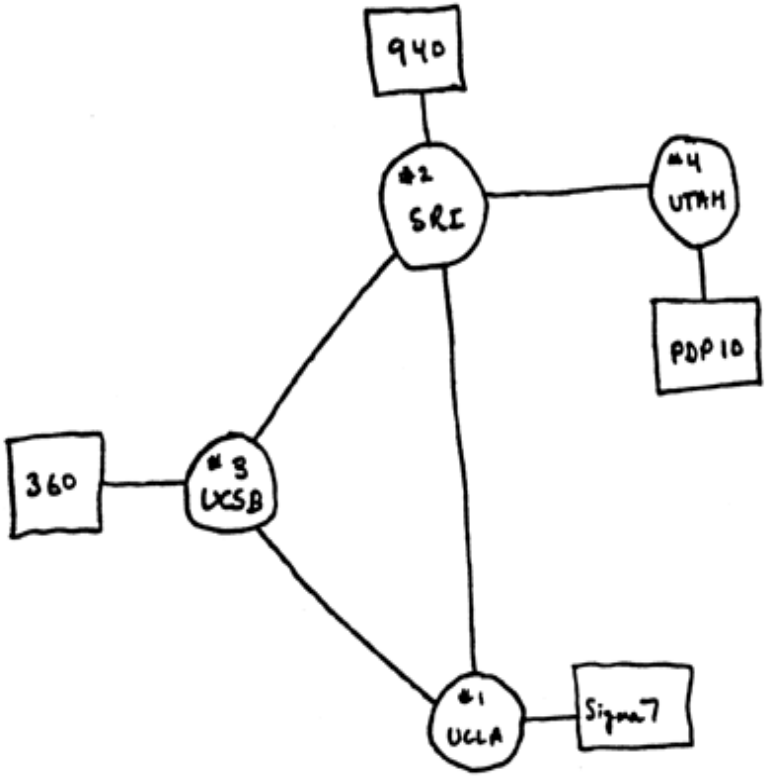
ARPAnet im Oktober 1969



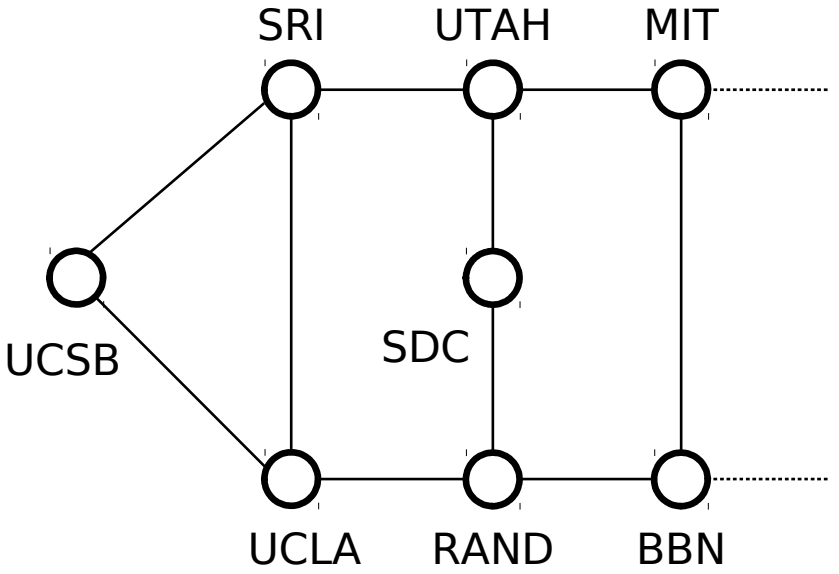
29Oct69	2100	LOADED IMP. PROGRAM FOR BBN BARKER BBN	CSK
	22:30	talked to SRI Host to Host	CSK
		Left IMP. program running after sending a host dead message to IMP.	CSK

ARPAnet im Dezember 1969

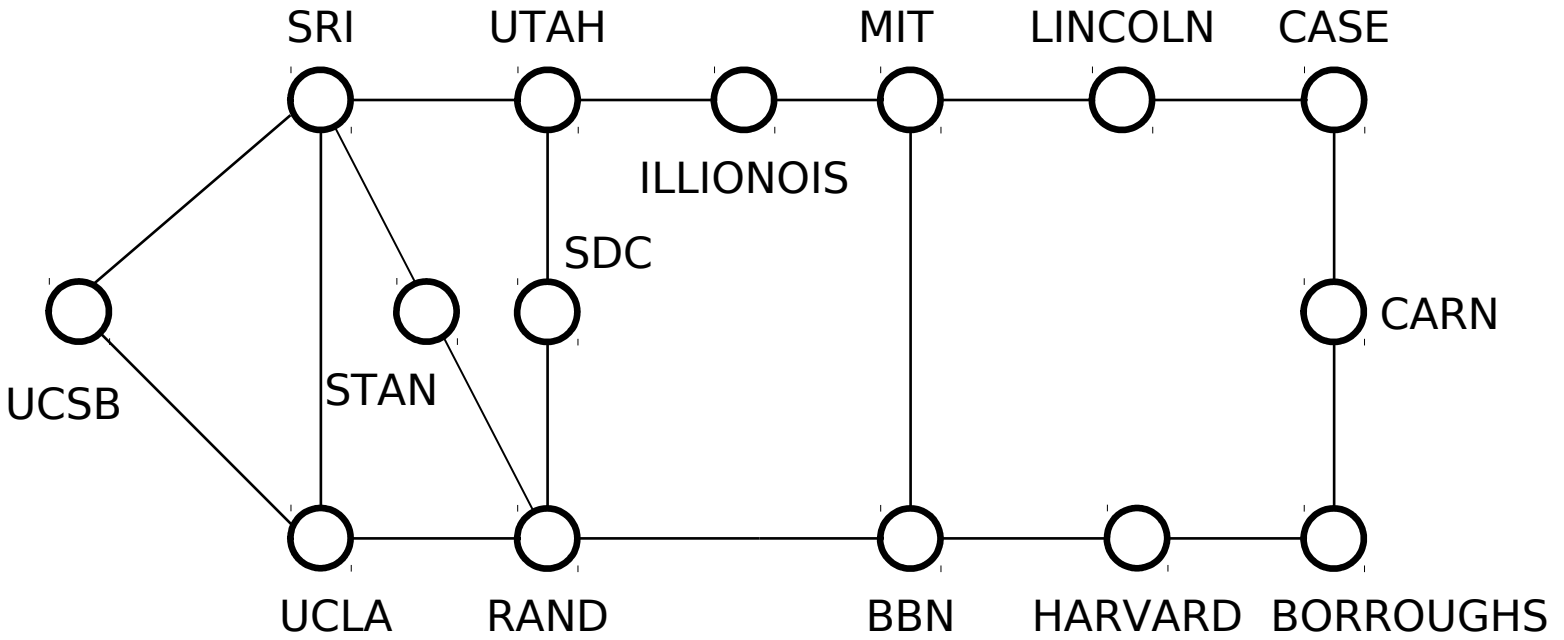
Honeywell 516
mit 12 KB Speicher



ARPAnet 1970



ARPAnet 1971

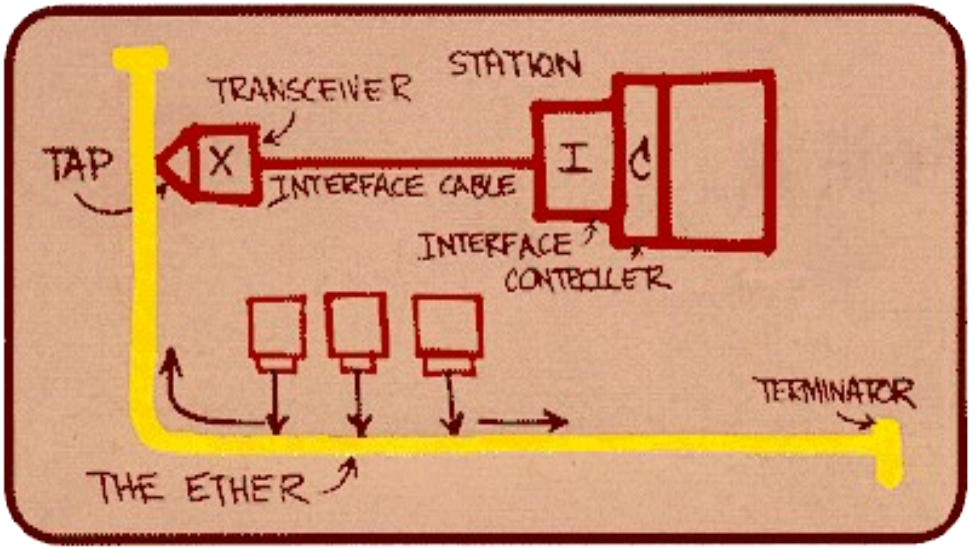


Wichtige Jahre (2)

- 1970: ALOHAnet Satelliten-Netzwerk
- 1973 Metcalve und Boggs: Ethernet

Ethernet als Zugang zum LAN

Bob Metcalfe entwarf einen Zugriffsalgorithmus auf ein gemeinsames Medium – das Local Area Network – bereits während des Studiums.



Ethernet (Metcalfe und Boggs, 1973)

Wichtige Jahre (2)

- 1970: ALOHAnet Satelliten-Netzwerk
- 1973 / Metcalve und Boggs: Ethernet
- 1974 / Cerf und Kahn: Internetworking-Prinzipien

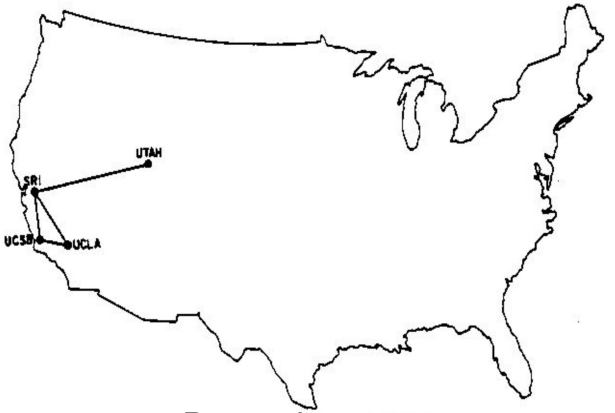
Internetworking als Paradigma

- **Verknüpfung existierender lokaler Netzwerke macht es zum „Netz der Netze“**
- **Autonomie aller Teilnetze**
  - “Best effort”-Dienstmodell – keine SLAs
  - Zustandslose Router
- **Anders als beim bisherigen Network Control Program (NCP) wird das Netzwerk nicht mehr als zuverlässig angesehen**
  - Betrachtung der Übertragung als Strom
  - Flusskontrolle und Fehlerkontrolle nötig

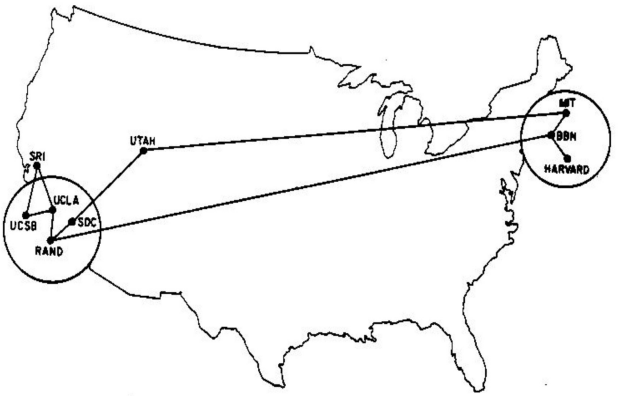
Wichtige Jahre (2)

- 1970: ALOHAnet Satelliten-Netzwerk
- 1973 Metcalve und Boggs: Ethernet
- 1974 / Cerf und Kahn: Internetworking-Prinzipien
- bis 1979: Entwicklung der TCP/IP-Basisprotokolle
- bis 1980: Integration in Berkeley UNIX
- 1980: TCP/IP wird Standard des US DoD

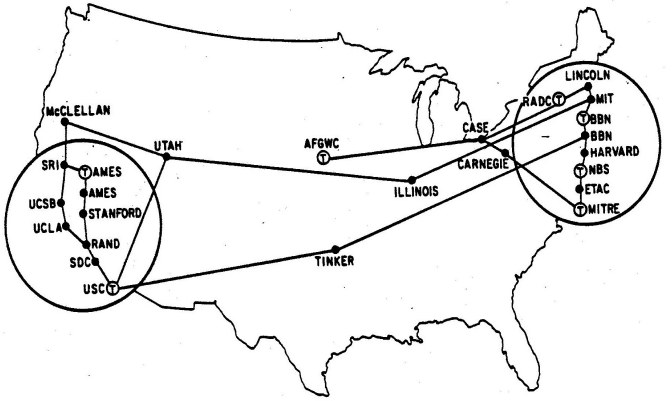
ARPAnet Entwicklung



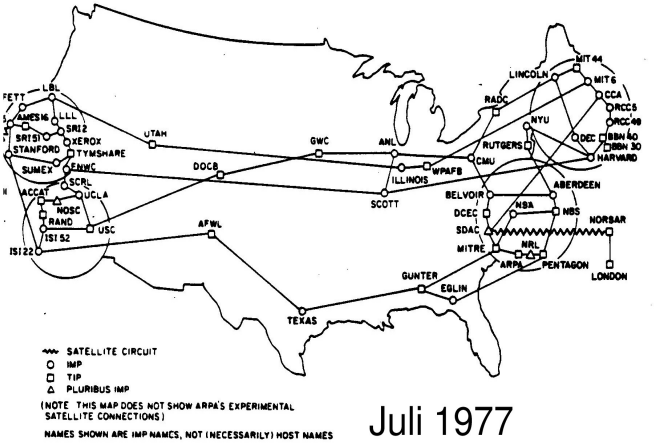
Dezember 1969



Juni 1970



März 1972



Juli 1977

Wichtige Jahre (3)

- **1.1.1983: Umstellung von NCP auf TCP/IP an nur einem Tag!!**
  - MILNET wird vom ARPAnet abgetrennt
- **bis 1984: ISO/OSI Referenzmodell**
- **1984: Mehr als 1.000 Hosts im ARPAnet**
- **1986: NSFnet wird gegründet**
  - Backbone-Geschwindigkeit beträgt 56Kbps

Wichtige Jahre (4)

- **bis 1990: viele neue Netzwerke**
  - CSnet (USA, Wissenschaftsnetz)
  - BITnet (Unis)
  - Minitel (BTX-Frankreich)
  - DFN (Deutschland) und viele andere europäische Forschungsnetze entstehen
  - 100.000 Rechner im weltweiten Netzverbund
- **1990: ARPAnet wird abgeschaltet und vollständig durch das NSFnet abgelöst**

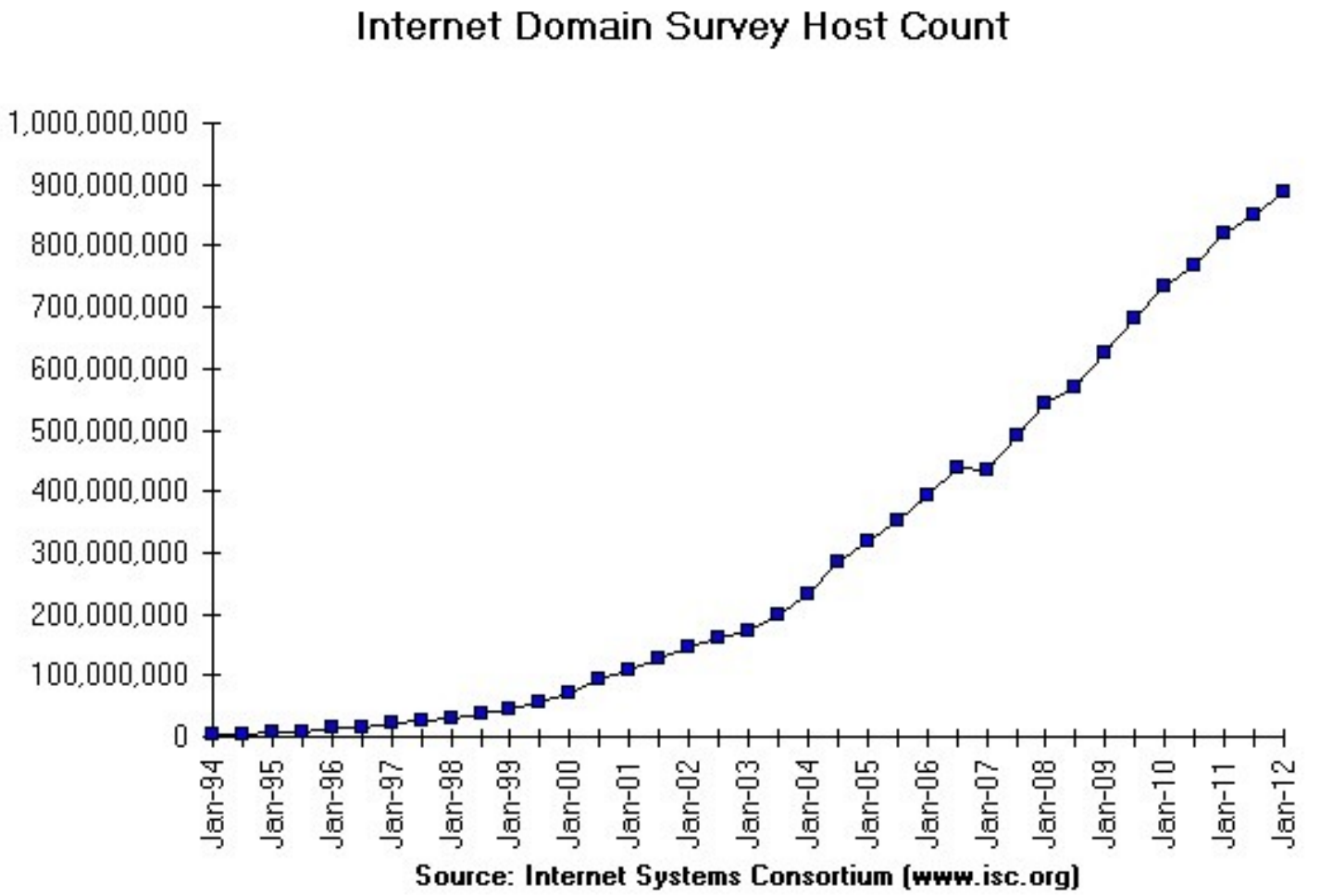
Wichtige Jahre (5)

- ab 1990: Entwicklung des WWW
- 1993: ca. 70.000 Rechner im dt. Internet
- 1994: Mosaic, erster „richtiger“ Browser
- 1995: Ende der staatlichen Dominanz, die die bisherige Netzwerkentwicklung trieb, und Beginn der Kommerzialisierung
- 1995: SUN bringt die Sprache JAVA heraus
- 1995: Netscape wird gegründet
- 1996: Internet-Telefonie

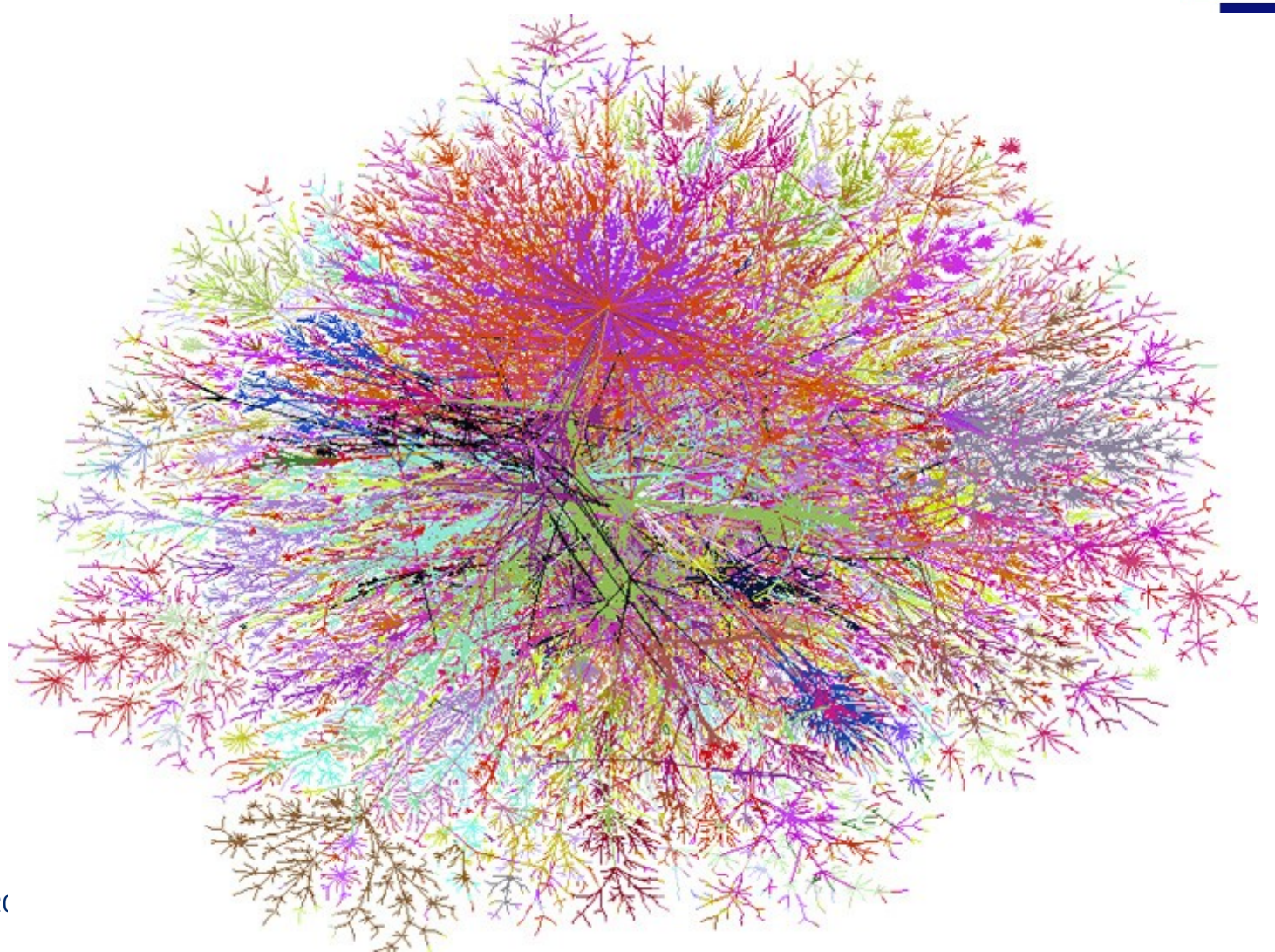
Wichtige Jahre (6)

- **ab 1998: Beginn des „Hypes“**
- **1999: Beginn der IPv6-Adressvergabe**
- **2000: Internet-Blase platzt und Abflauen der Internet-Euphorie**
- **ab 2005: Web 2.0**
  - Soziale Netzwerke
- **ab 2013: Snowden-Effekt**
  - Überwachungsmöglichkeiten staatlicher Bedarfsträger wird offenkundig

Das Wachstum bis 2012



Internet Topologie heute ...



Packets on the Internet:

http://www.youtube.com/watch?v=4VxPazlA0Zc

Gliederung der Vorlesung

- **Einführung und Historie des Internets**
- **Schichtenmodell**
  - Dienst, Protokoll, Internet-Modell
  - Einordnung von IT-Sicherheit
- **Netzwerk als Infrastruktur**
- **Layer 7: Anwendungsschicht**
- **Layer 7/4: Socketprogrammierung**
- **Layer 4: Transportschicht**
- **Layer 3: Netzwerkschicht**
- **Layer 2: Sicherungsschicht**

Das Kommunikationsproblem

- Heterogene Anwendungslandschaft
- Verteilte Applikationen
- Heterogene Rechnerarchitekturen
- Heterogene Netzwerk-Infrastruktur

Jeder ‘Teilnehmer’ des Netzes soll mit jedem anderen Teilnehmer sinnvoll kommunizieren können!

Kommunikation als Hauptaufgabe

- **Die Aufgabe von Rechnernetzen ist es, Kommunikation zwischen den Teilnehmern zu ermöglichen**
- **Kommunikation ist dabei sehr vielfältig:**
  - Prozesse schicken einander Nachrichten
  - Rechner (Betriebssysteme) vergeben Aufträge und warten auf die Bearbeitung
  - Mitglieder einer Benutzergruppe verständigen sich über einen Status
  - …

Aufgaben von Rechnernetzen

- **Lastverbund**
  - Verteilung von Aufgaben an mehrere Rechner
  - Beseitigung von Engpässen
  - Nutzung freier Ressourcen
- **Leistungsverbund**
  - Zusammenarbeit von Rechnern verschiedener Funktionalitäten
  - Virtuelle Universalmaschine

Aufgaben von Rechnernetzen (2)

- **Verfügbarkeitsverbund**
  - Redundanz durch Systemdoppelung
  - Problem bleibt Redundanz der Daten
- **Datenverbund**
  - Gemeinsamer Zugriff auf Datenbestände
  - Redundanzfreie und ortsungebundene Datenhaltung

Aufgaben von Rechnernetzen (3)

- **Funktionsverbund**
  - Geteilte Ressourcennutzung (Massenspeicher, Software,...)
  - Virtualisierte Funktionsumgebung für z.B. Walking User Support
- **Nachrichtenverbund**
  - Kommunikation zum Austausch von Nachrichten
  - Ortsungebundene Erreichbarkeit

Grundtypen von Verbindungen bzw. Netzwerken

- **Punkt-zu-Punkt-Netzwerke:**
  - Netzwerk zwischen zwei Hosts bzw. Vermittlungsknoten über dedizierte Leitungen
  - Glasfaser, Richtfunk
- **Broadcast-Netzwerke:**
  - Netzwerk zwischen vielen Hosts/Gateways über geteilte (shared) Leitungen
  - Ethernet, WLAN, Bluetooth

Grundtypen von Adressierungen

- **Unicast:**
  - Teilnehmer A kommuniziert mit B
- **Broadcast:**
  - Teilnehmer A kommunizert an alle angeschlossenen Teilnehmer im LAN I
- **Multicast:**
  - Teilnehmer A kommuniziert an ausgewählten Adressatenkreis irgendwo
- **Anycast:**
  - Teilnehmer A kommuniziert an interessierte Teilnehmer irgendwo

Zwei elementare Kommunikationsarten

- **Synchron: Telefon, Terminal, Video-Konf.**
  - Gemeinsame Aktion von Sender und Empfänger
  - Erfordert gleichzeitige Bereitschaft aller Partner
- **Asynchron: SMS, Email, Instant Messager**
  - Sender und Empfänger operieren losgelöst voneinander
  - Puffermechanismen speichern Objekte für späteren (wahlfreien) Zugriff zwischen

Umsetzung im Internet

- **Synchron → Verbindungsorientiert**
  - Aufbau einer expliziten Verbindung zwischen den Partnern (Handshake)
  - Speichern von Zustandsinformationen im Endsystem
- **Asynchron → Verbindungslos**
  - Kein Verbindungsaufbau
  - Übertragung von einzelnen Nachrichten

Dienste als Abstraktion

Wohldefinierte und benötigte Funktionen

- ausgelagertes Leistungspaket beim Dienstgeber (Server)
  - Dienstfunktion
  - Dienstprimitiven
  - Dienstprozeduren
- Inanspruchnahme durch Dienstnehmer (Client)

Dienste als Abstraktion (2)

Dienstgüte

- Angemessenheit
- Zugänglichkeit
- Technische Leistung
  - Antwortzeit
  - Genauigkeit
  - ...
- Kosten
- Zuverlässigkeit
- Sicherheit: Vertraulichkeit, Integrität, ...

Dienste als Abstraktion (3)

Client-Server Modell

- Rollenzuweisung:
  - Server erbringt
  - Client erfragt einen Dienst
- Kommunikationsform:
  - n Clients : 1 Server – viele mit einem
- Fast alle Internet-Dienste

Dienste als Abstraktion (4)

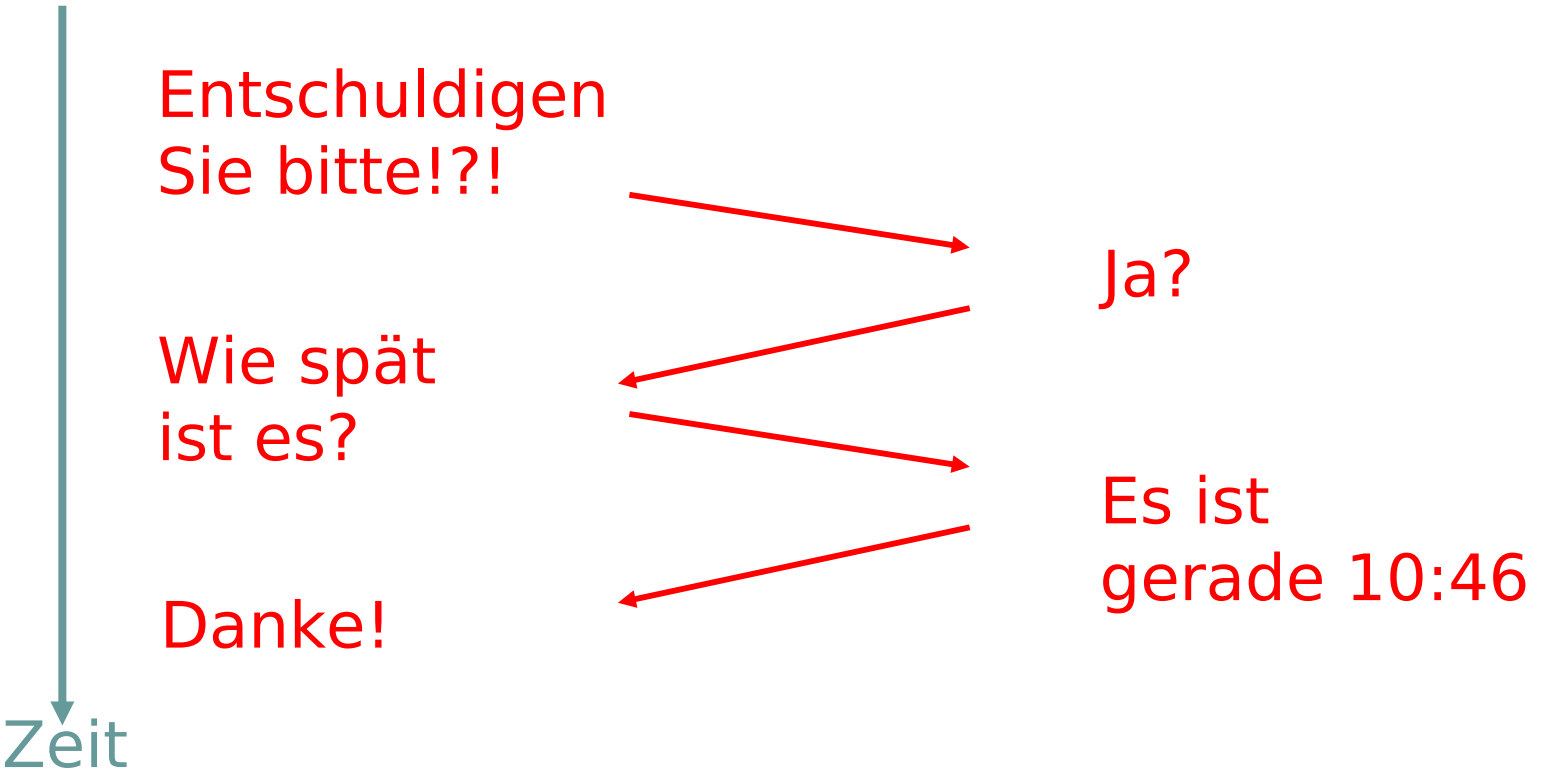
Peer-to-Peer Modell

- Rollenzuweisung:
  - Teilnehmer sind gleichartig
  - Rolle wird bzw.
  - Aufgaben werden dynamisch zugeteilt
- Kommunikationsform:
  - n : m Systeme – viele mit vielen
- Ausgewählte Internet-Anwendungen
  - Filesharing
  - Tauschbörsen
  - VCoIP

Protokolle

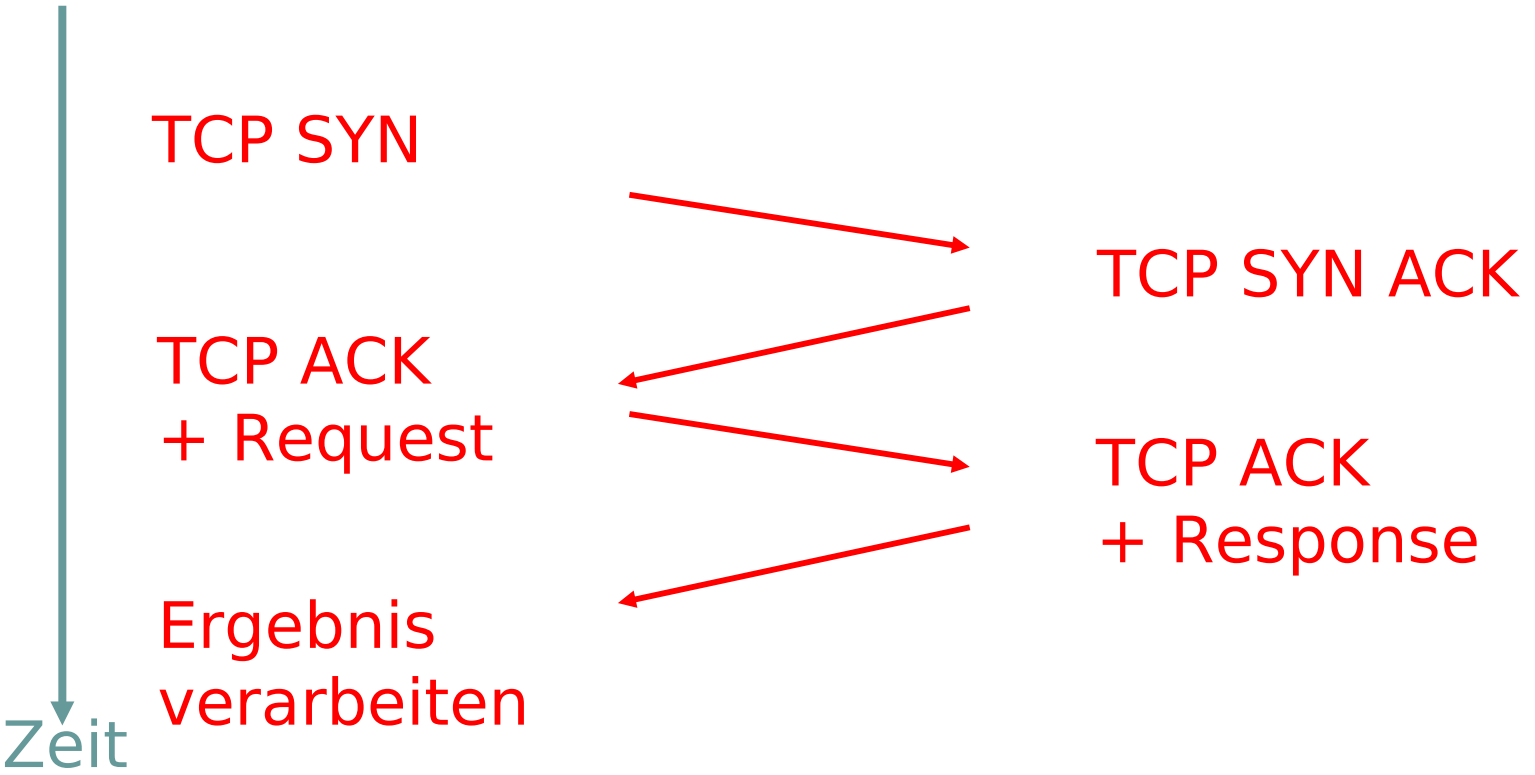
Protokolle im Beispiel

Menschliches Kommunikationsprotokoll



Protokolle im Beispiel (2)

Internet-Kommunikationsprotokoll



Protokolle im Beispiel (3)

Internet-Kommunikationsprotokoll

Definition: Protokoll

Ein Protokoll definiert zwischen allen kommunizierenden Einheiten

- das Format und
- die Reihenfolge aller Nachrichten

die ausgetauscht werden, sowie die Aktionen,

- die beim Senden und / oder beim Empfang einer Nachricht oder eines anderen Ereignisses

unternommen werden.

Protokolle bilden die „Sprache“

Zur Kommunikation untereinander benötigen Rechner eine gemeinsame Sprache:

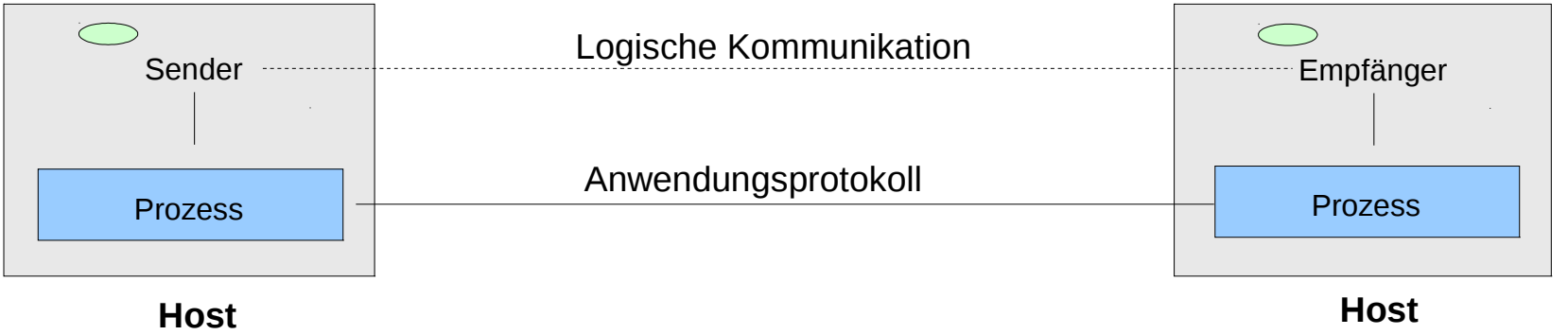
- Protokolle erbringen definierte Dienstleistungen gegenüber dem Nutzer bzw. der übergeordneten Schicht
- Abbildung unterschiedlicher Anforderun-gen oder Kontexte führen zur Existenz vieler Protokolle
- Offene Standards müssen verabredet werden, damit Protokolle universell sind

Aufgabe von Protokollen

Funktionsmechanismen höherer Kommunikationsprotokolle sind:

- Adressierung
- Einbettung von Daten (encapsulation)
- Segmentierung + Reassemblierung von Datenpaketen
- Fehlererkennung und -behebung
- Flusssteuerung (flow control)
- Verbindungskontrolle (connection control)

Das Internet-Modell?



Protokollschichtung als Lösung

Für die Kommunikation in heterogenen, offenen Systemen ist eine konzeptionelle Gliederung der Funktionalitäten unerlässlich:

- Gliederung des Gesamtproblems in Ebenen
- Jede Ebene löst einen Teil des Problems
- Jede Ebene arbeitet mit den direkt benachbarten Ebenen zusammen
- Voraussetzung dafür sind kompatible Implementierungen und diese gibt es nur bei präzise definierten Schnittstellen!

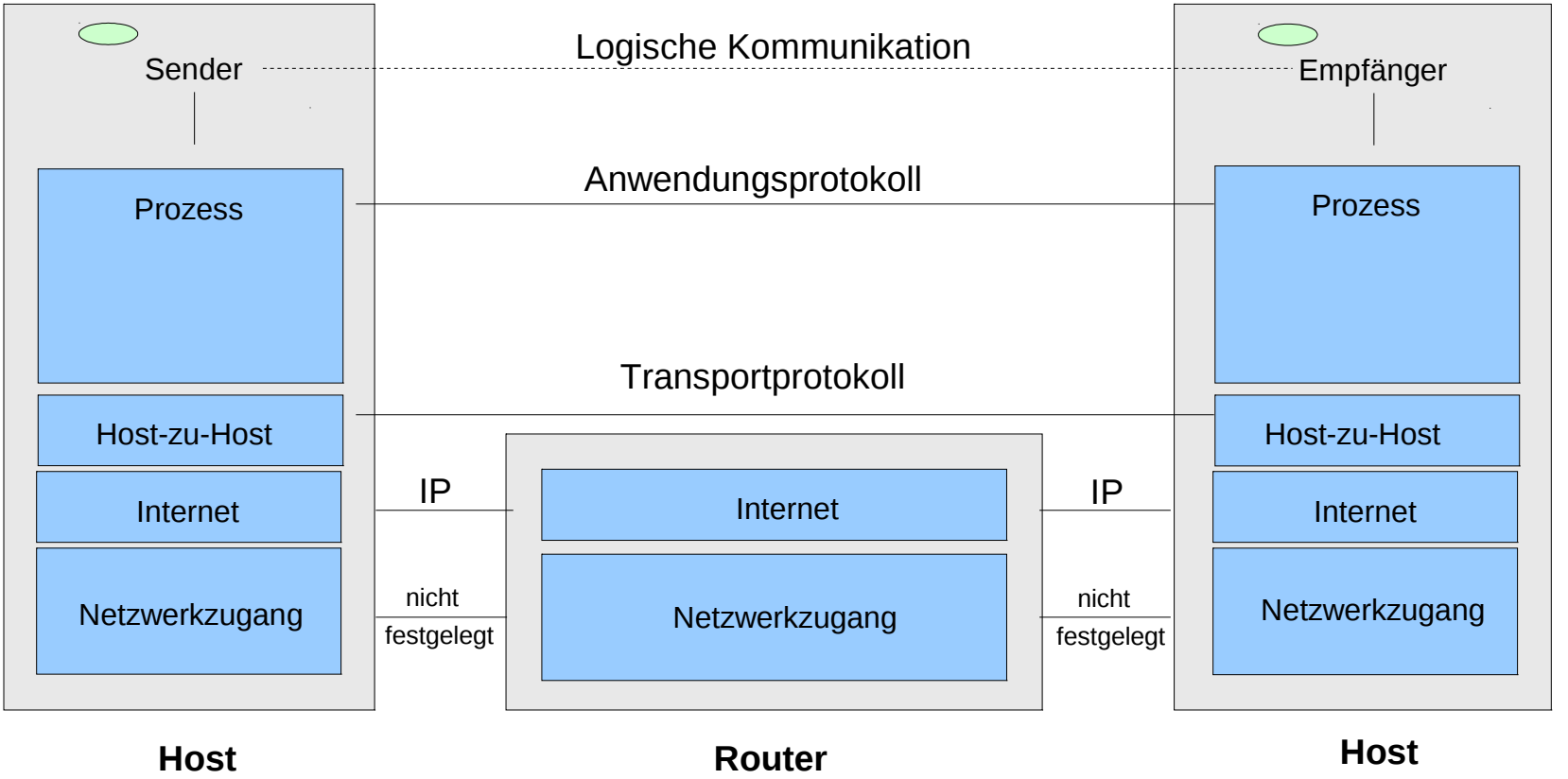
Das Internet-Modell?

Das Internet-Modell

Kommunikationsarchitektur des US DoD

- **Bestandteile des Modells:**
  - Process:
    Implementiert durch Anwendung
  - Host-to-Host: Ablaufumgebung für kommunizierende Prozesse
  - Internet: Ermöglicht die Kommunikation, vermittelt zwischen Rechnern (hosts)
  - Network Access: Stellt Zugriff auf Übertragungsmedien bereit

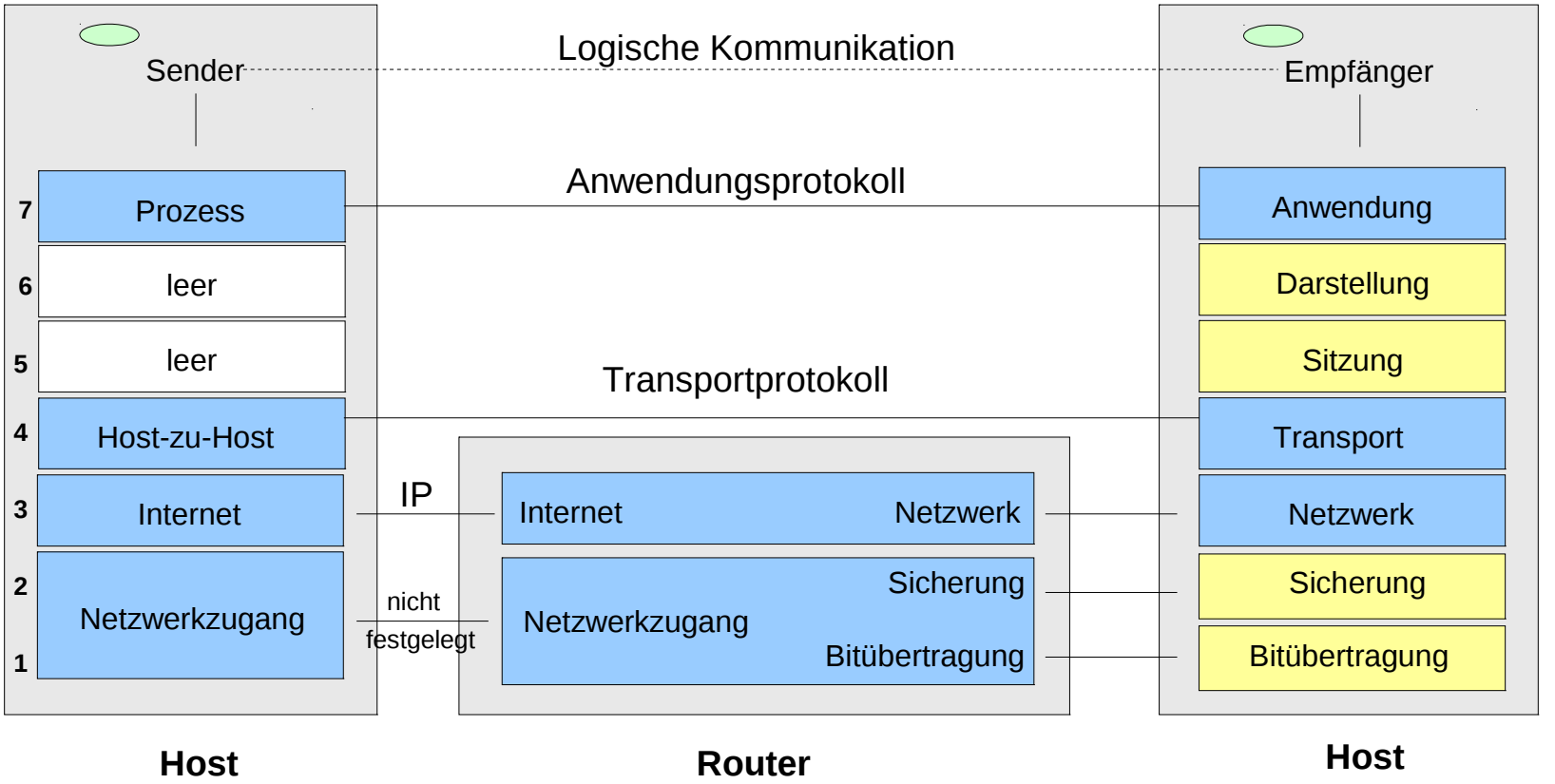
Das Internet-Modell



Das ISO/OSI-Modell

- **ISO (International Organization of Standardization) beauftragte 1977 einen Unterausschuss mit der Entwicklung einer Kommunikationsarchitektur für/zwischen offenen Systemen**
- **Aufgabe des Modells:**
  - Referenz zur Beschreibung von Protokollen und Funktionen
  - Standardisierungsgrundlage für Protokolle
  - Keine Spezifikation für Implementierungen

Internet-Modell vs. ISO/OSI



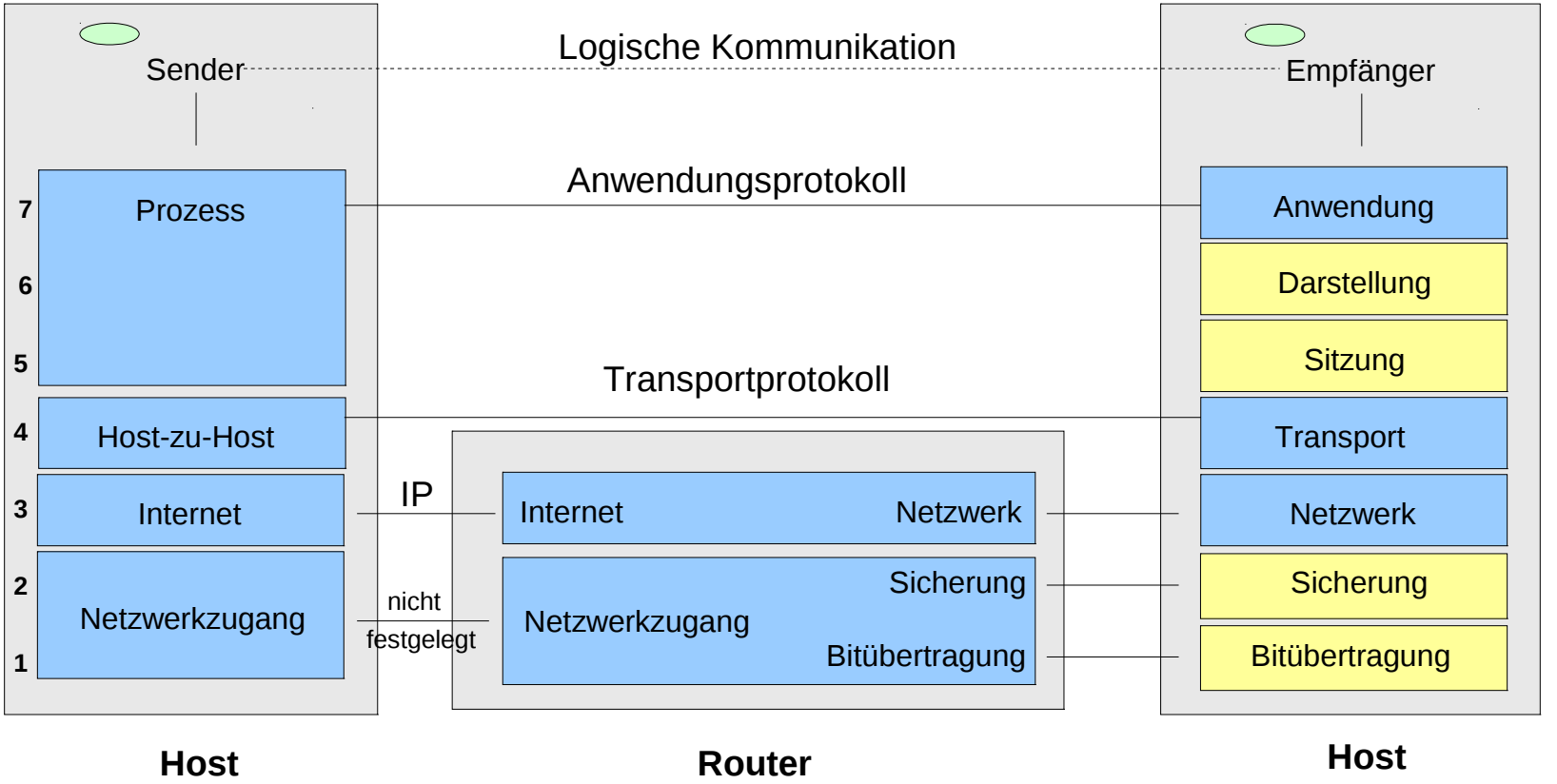
Das ISO/OSI-Modell (2)

- **Anwendungsschicht / application layer:**
  = Process (FTP, SMTP, HTTP, ...)
- **Transportschicht / transport layer:**
  = Host-to-Host (TCP, UDP)
- **Netzwerkschicht / network layer:**
  = Internet (IP)
- **Sicherungsschicht / data link layer:**
  - Datentransfer zwischen benachbarten Netzwerkelementen: PPP, HDLC, Ethernet
- **Bitübertragungsschicht / physical layer**

Zwei Schichten mehr ...

- **Darstellungsschicht / presentation layer:**
  - Konventionen zur einheitlichen Darstellung von Zeichen und Datentypen mit ASN.1
- **Sitzungsschicht / session layer:**
  - Dienste zur Verwaltung von Sessions (Wiederaufnahme etc.)
  - wurde im Internet nicht wirklich benötigt (jedenfalls in der Theorie – in der Praxis wird dies oft in die Anwendung integriert!)

Internet-Modell vs. ISO/OSI (2)



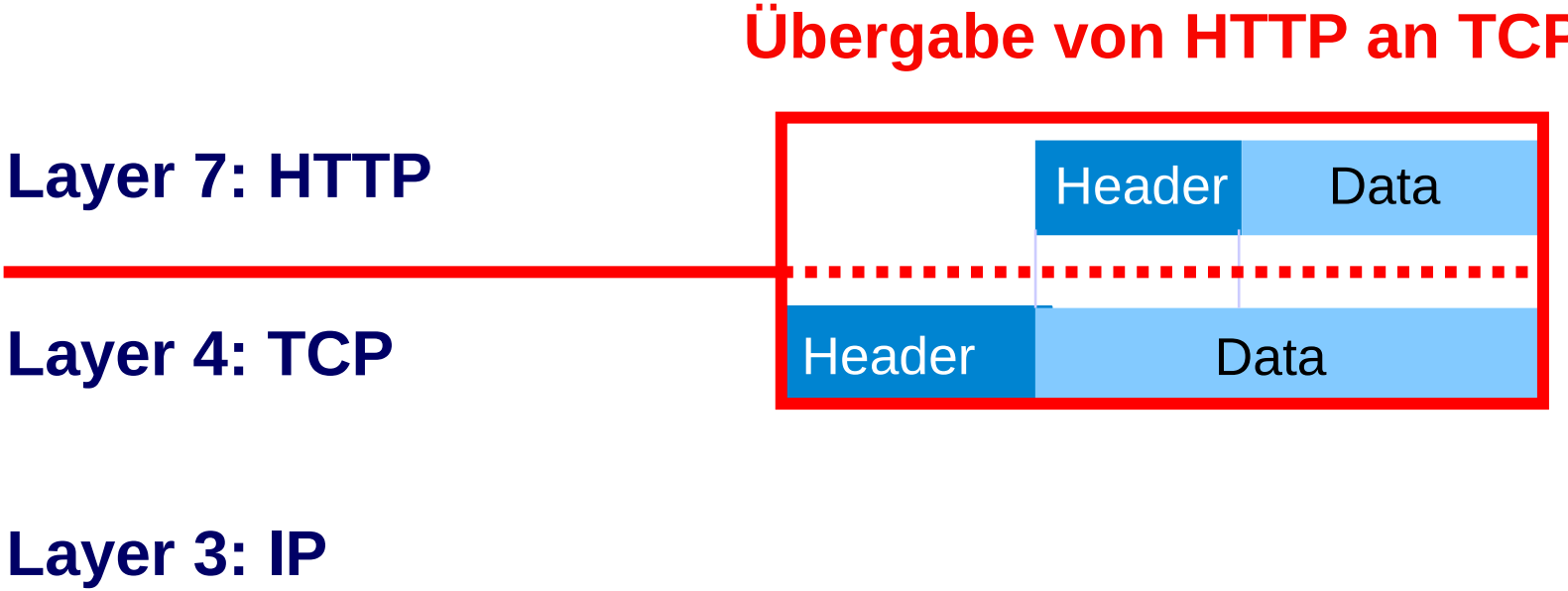
Protokollschichtung

- **Jede Schicht implementiert genau einen Dienst a.k.a. Service**
  - definiert dazu eigene interne Aktionen
  - verwendet dazu Dienste der unteren Schicht
  - Logische Kommunikation verläuft immer horizontal innerhalb derselben Schicht
- **Reale Kommunikation verläuft innerhalb eines Rechners immer vertikal durch alle Schichten**

Protokollschichtung (2)

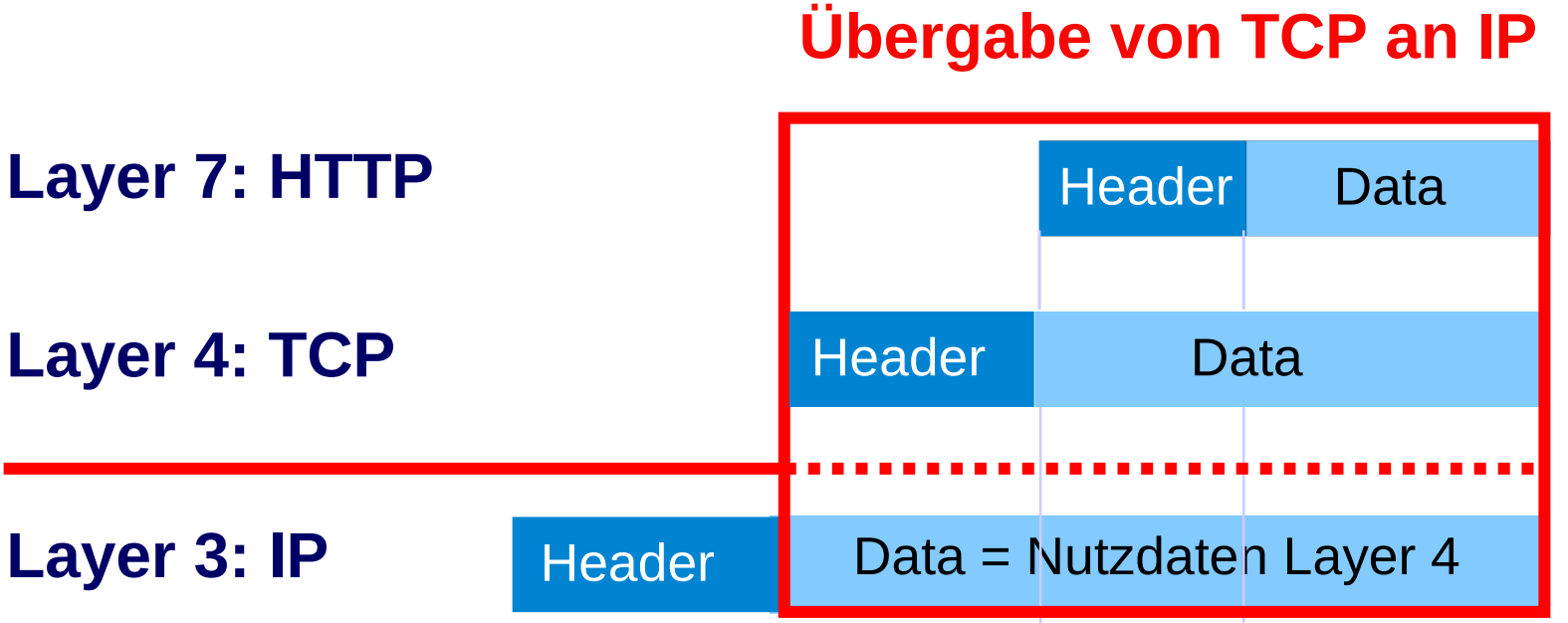
- **Jede Schicht implementiert genau einen Dienst a.k.a. Service**
- **Reale Kommunikation verläuft innerhalb eines Rechners immer vertikal durch die Schichten**
  - Daten kommen von der höheren Schicht
  - Headerinformationen für Empfänger werden hinzugefügt
  - Evtl. Verarbeitung / Transformationen
  - Weitergabe an untere Schicht

Protokollschichtung (3)



Data der höheren Schicht werden als Payload bezeichnet und (üblicherweise) nicht verarbeitet!

Protokollschichtung (4)



IP-Adresse adressiert Rechner und
wird erst durch die Schicht 3 hinzugefügt.

Optionale Protokollfunktionen

- **Verbindungsaufbau / -abbau**
  - Handshake mit einem Partner auf derselben logischen Schicht
- **Fehlerkontrolle**
  - Fehlererkennung und -behebung
- **Flusskontrolle**
  - Vermeiden der Überlastung eines Knotens

Optionale Protokollfunktionen (2)

- **Segmentierung und Reassemblierung**
  - Aufteilung großer Datenblöcke durch den Sender und Zusammensetzen beim Empfänger
- **Multiplexen**
  - Gemeinsame Nutzung einer einzigen Verbindung durch mehrere gleichartige Verbindungen der jeweils höheren Schicht

Verbindungskontrolle

Protokolle können Daten mit unterschiedlicher Zielsetzung übertragen. Deshalb sind Protokolle entweder

- Verbindungsorientiert
  = connection-oriented

oder

- Verbindungslos
  = connectionless

Verbindungskontrolle (2)

Verbindungsorientiert
= connection-oriented

- zustandsbehafteter, gesicherter Transfer
- zwischen beteiligten Partnern
- drei ausgezeichnete Phasen zwischen diesen Partnern:
  - Verbindungsaufbau
  - Datentransfer (optional)
  - Verbindungsabbau

Verbindungskontrolle (3)

Verbindungslos
= connectionless

- zustandsloser, ungesicherter Transfer
- zwischen unabhängigen Partnern

Fehlerkontrolle

Protokolle können unterschiedlich zuverlässig sein

- **Zuverlässige Protokolle**
  - bieten Schutz vor Datenverlust/-zerstörung
  - verifizieren Pakete nach Erhalt und quittieren
  - haben Overhead
- **Unzuverlässige Protokolle**
- **k-zuverlässige Protokolle**

Fehlerkontrolle (2)

- **Zuverlässige Protokolle**
- **Unzuverlässige Protokolle**
  - beachten Datenverluste nicht
  - verifizieren und quittieren Pakete nicht
  - Fehlererkennung und -korrektur kann nur in übergeordneten Schichten erfolgen
- **k-zuverlässige Protokolle**
  - stellen sicher, dass wenigstens immer k aus insgesamt k+n Paketen zuverlässig ankommen

Flusskontrolle

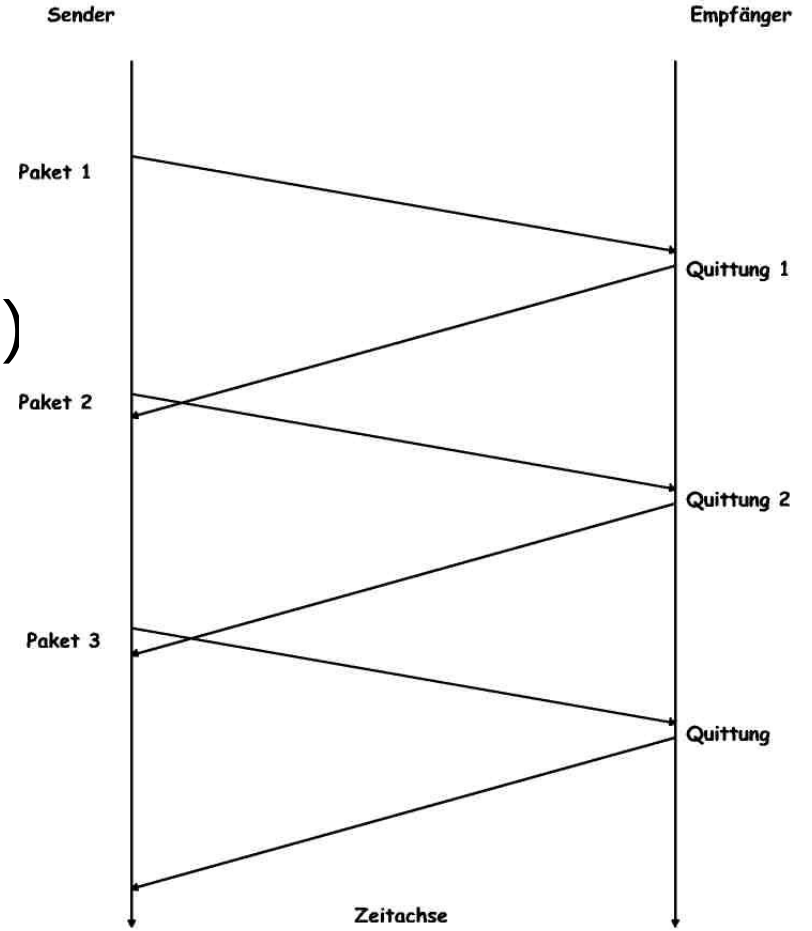
Bestimmte Protokolle können den tatsächlichen Datenfluss an die verfügbaren Ressourcen von Sendern, Empfängern und das Netzwerk anpassen, indem sie

- **verfügbare Sende- und Empfangspuffer miteinander abgleichen**
- **Übertragungen im Netz messen und interpretieren**
- **Kommunikationsverhalten auf alle Leistungsgrößen einstellen**

Realisierung in einer Verbindung

Empfänger sendet Quittungen:

- Zustandsmeldungen (Verbindungskontrolle)
- Empfangsbestätigung (Sicherung)
- Bekanntgabe von Empfangspuffern (Flußkontrolle)



Konsequenzen der Paketvermittlung

- **Store and forward:**
  - Pakete werden vollständig an den nächsten Knoten übertragen (“Hop”) und warten dort auf den nächsten Hop
- **Die aggregierten Ressourcenanforderungen in einem Vermittlungsknoten können die verfügbare Kapazität übersteigen**
  - Stau:
    Pakete müssen in einer Warteschlange auf die weitere Verarbeitung bzw. Übertragung über eine Verbindung warten

Bewertung der Paketvermittlung

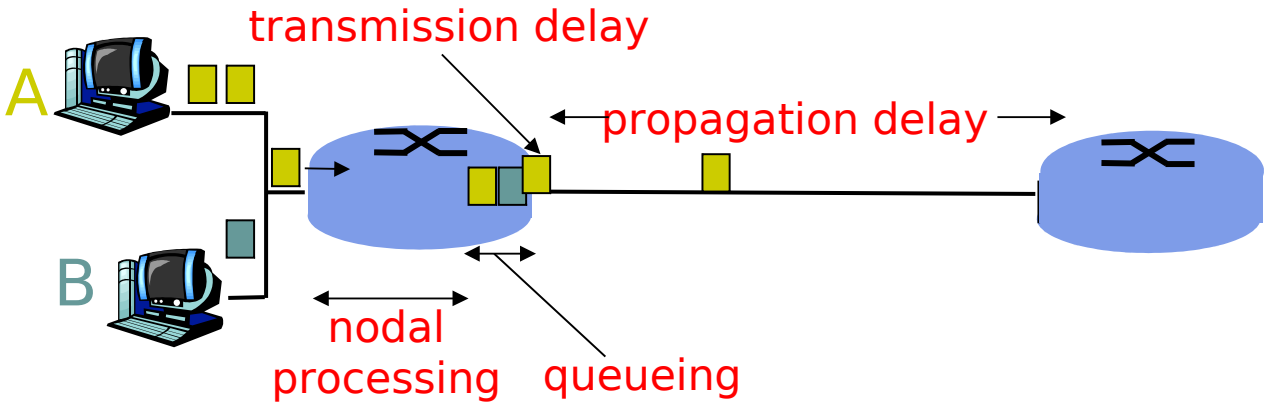
- **Durch Paketvermittlung ist eine bessere Auslastung des Netzes erreichbar**
  - keine Ruhephasen
  - dynamische Aufteilung der Ressourcen
  - kein Overhead für Leitungsreservierung
- **Problemfälle:**
  - Stau
  - Überlastung

Bewertung der Paketvermittlung

- **Durch Paketvermittlung ist eine bessere Auslastung des Netzes erreichbar**
- **Unvorhersagbare Paketverzögerungen und möglicher Verlust**
  - Stau
  - Überlastung
- **Zuverlässiger Datentransfer und Überlastkontrolle müssen ggf. von höheren Protokollschichten geleistet werden**
- **Keine garantierten Paketzustellzeiten möglich**

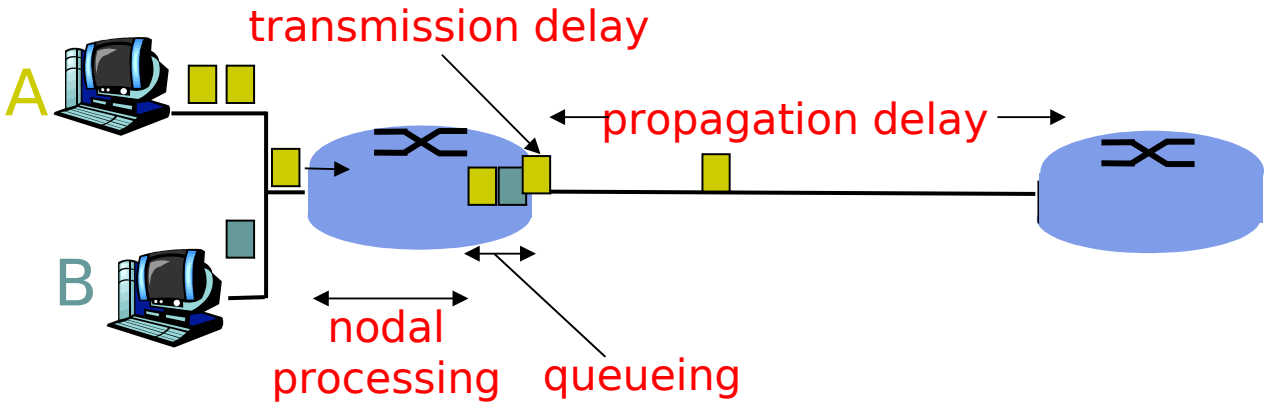
Verzögerungsarten

- **Verarbeitungsverzögerung = nodal processing**
  - Prüfung auf Bitfehler
  - Routing-Entscheidung über Ausgang



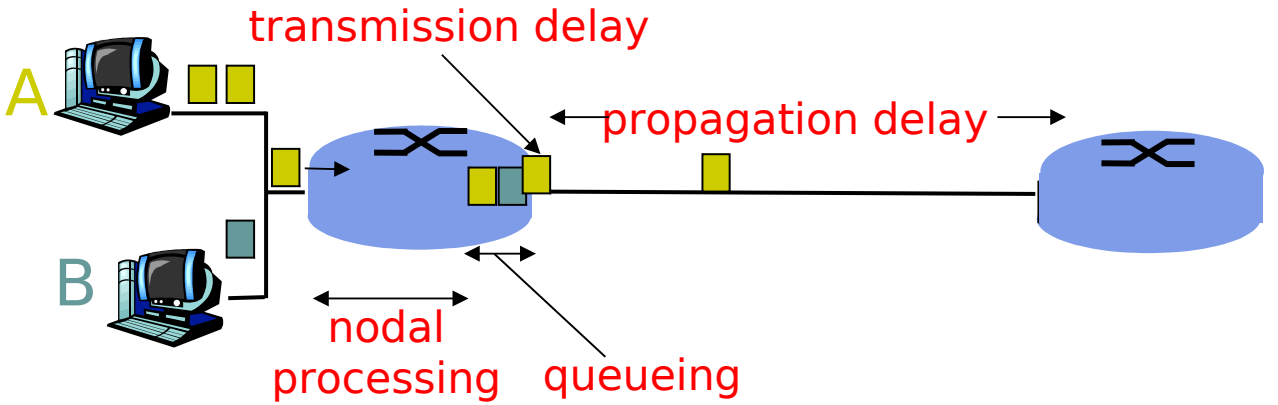
Verzögerungsarten (2)

- **Warteschlangenverzögerung = queueing**
  - Wartezeit im Puffer vor der Ausgangsleitung
  - Hängt stark von Verkehrslast im Router ab



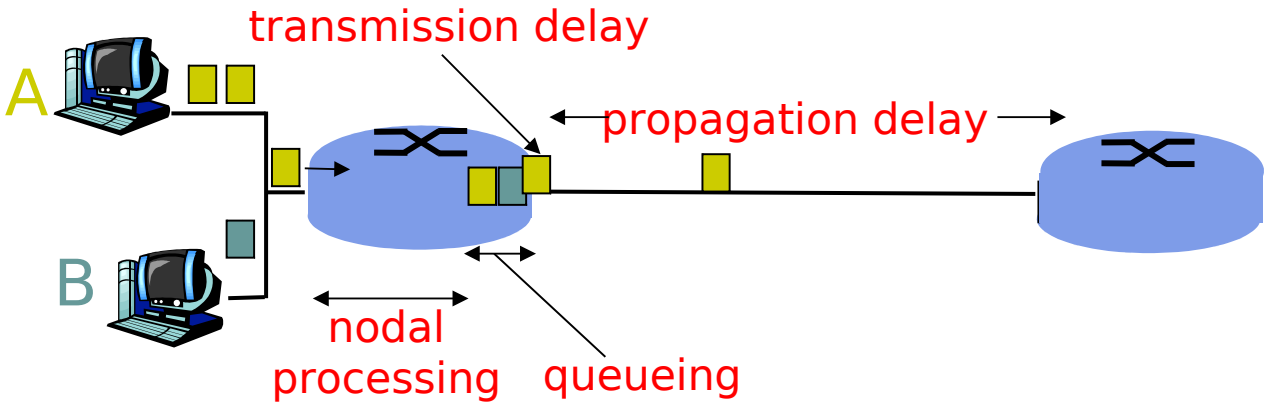
Verzögerungsarten (3)

- **Übertragungsverzögerung = transmission delay**
  - R = Übertragungsrate [bit/s]
  - L = Paketlänge [bit]
  - Übertragungsverzögerung = L/R [s]



Verzögerungsarten (4)

- **Ausbreitungsverzögerung = propagation delay**
  - d = Länge der physikalischen Leitung [m]
  - v = Ausbreitungsgeschwindigkeit [m/s]
  - Ausbreitungsverzögerung = d/v [s]

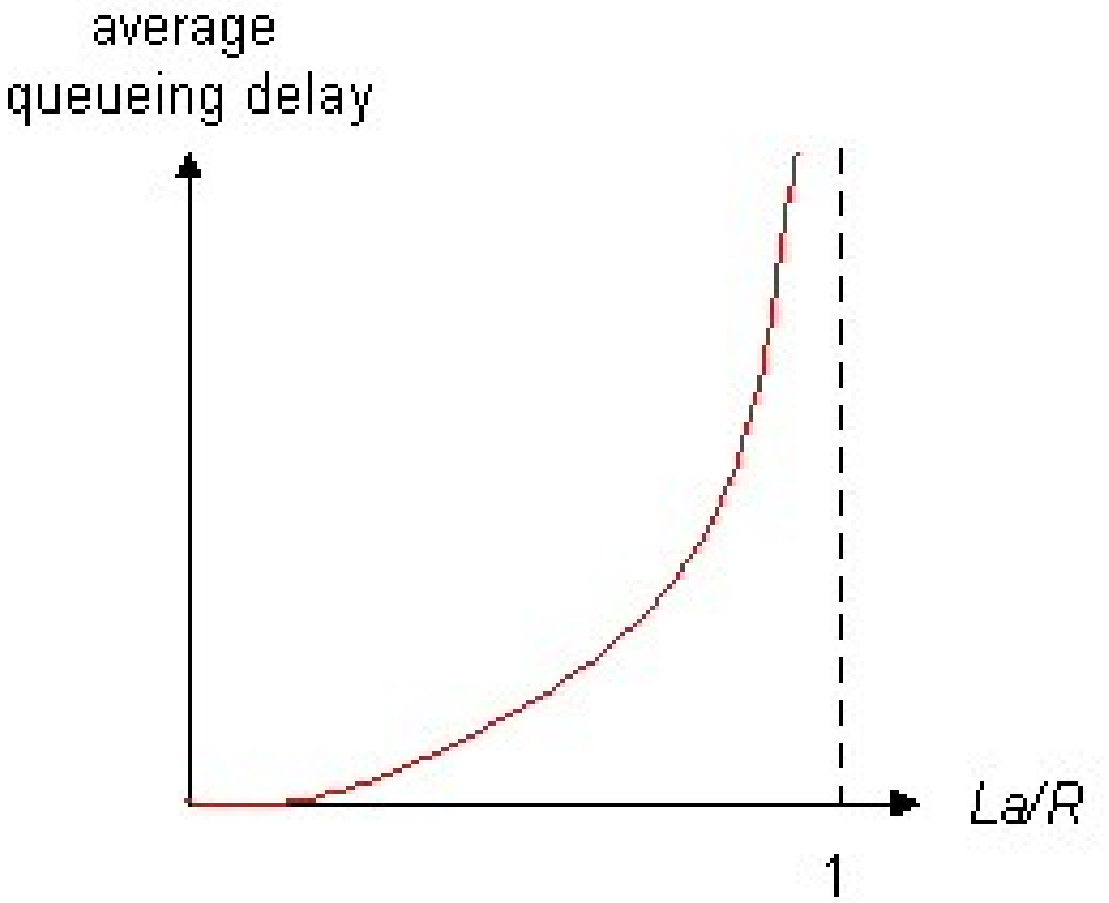


Warteschlangenverzögerungen

Last = Verkehrsintensität [Pakete]

- R = Übertragungsrate [bit/s]
- L = Paketlänge [bit]
- a = durchschnittliche Ankunftsrate [Pakete/s]

Warteschlangenverzögerungen



Warteschlangenverzögerungen

Last = Verkehrsintensität [Pakete]

- **R = Übertragungsrate [bit/s]**
- **L = Paketlänge [bit]**
- **a = durchschnittliche Ankunftsrate [Pakete/s]**

La/R ~ 0:
durchschnittl. Warteschlangenverzögerung klein
La/R → 1:
Verzögerung wird groß
La/R > 1:
Ankunftsrate übersteigt Übertragungsrate
durchschnittl. Warteschlangenverzögerung ist unendlich!

Und ist Paketverzögerung ein wirkliches Problem?

Und ist Paketverzögerung ein wirkliches Problem?

Ja, klar …

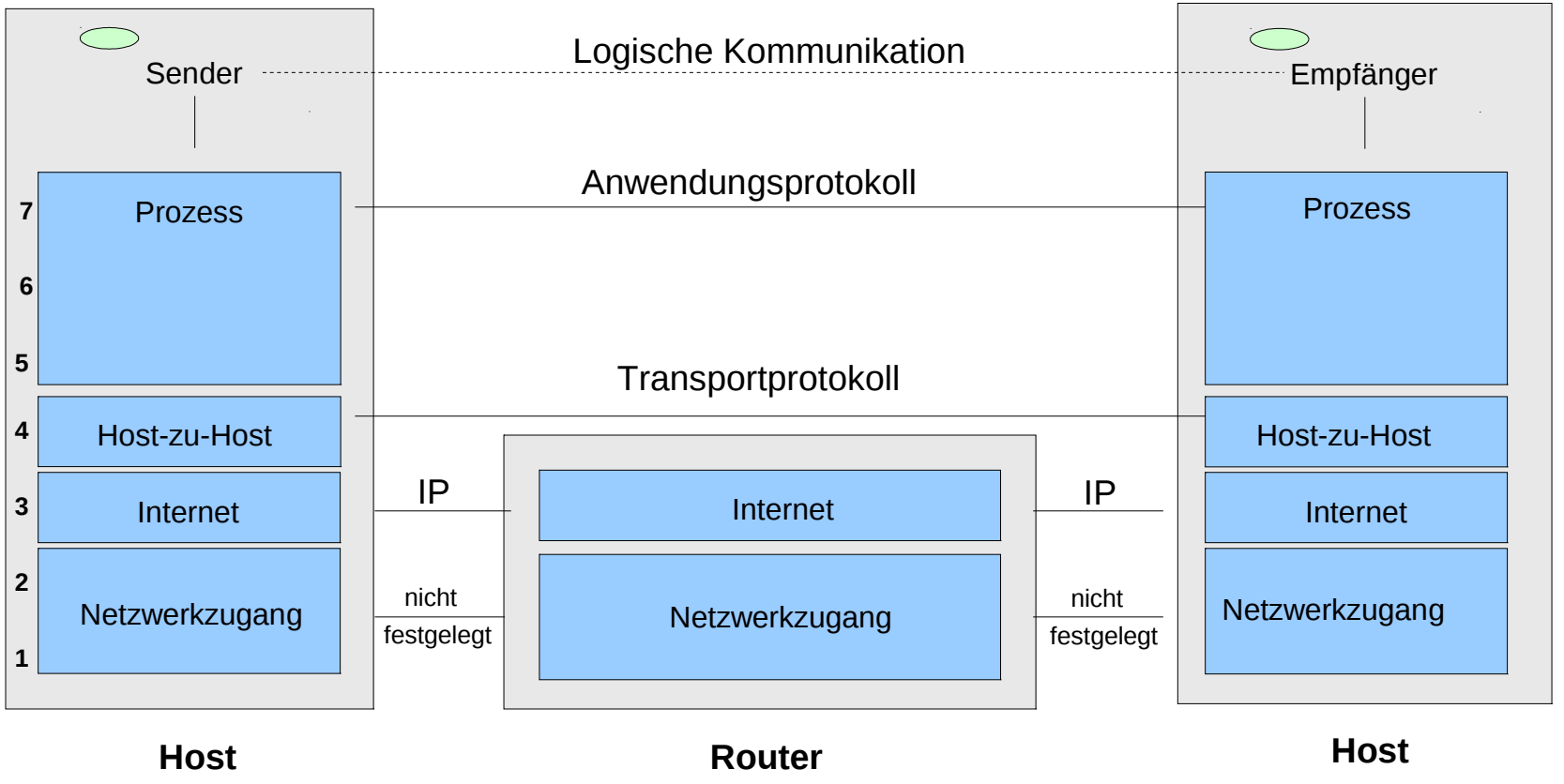
Und ist Paketverzögerung ein wirkliches Problem?

- Also wie schaffen wir ein der Leitungs-vermittlung ähnliches Verfahren?

Und ist Paketverzögerung ein wirkliches Problem?

- **Also wie schaffen wir ein der Leitungs-vermittlung ähnliches Verfahren?**
  - "Virtuelle Kanäle": Verhalten der Leitungsvermittlung wird durch Protokolle simuliert
- **Vorgehen umfasst u.a.**
  - Dienstgütegarantien durch Reservierung von Ressourcen (z.B. für Audio/Video – Streaming)
  - Erfüllung von “Quality of Service” - Anforderungen

Das Internet-Modell

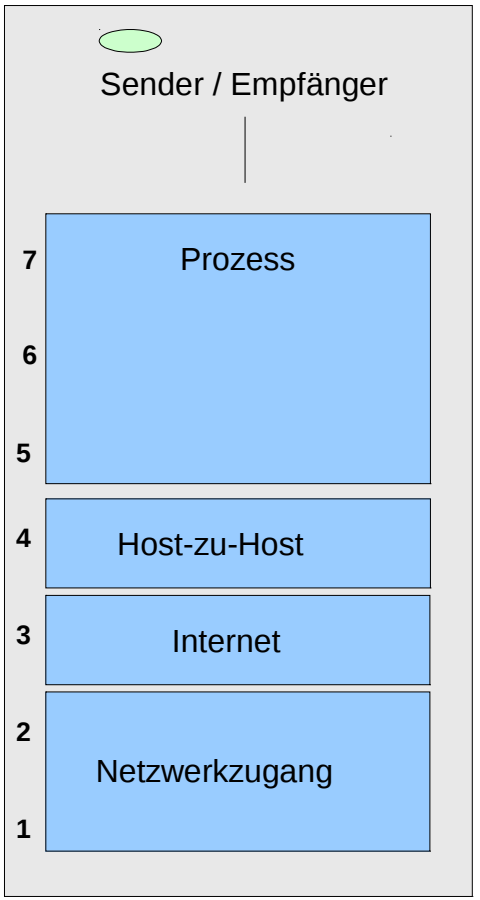


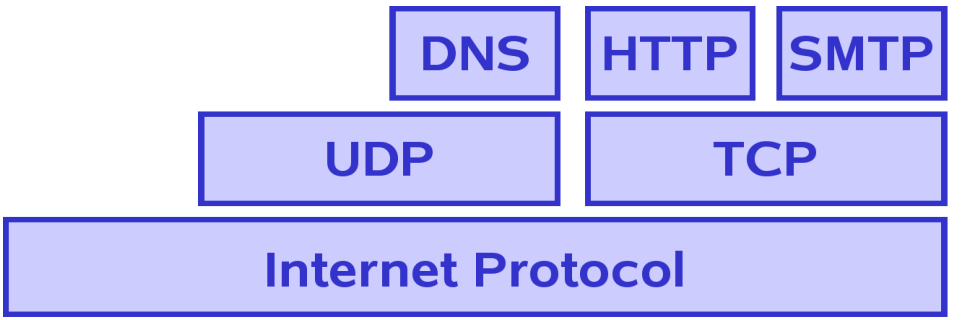
Gliederung der Vorlesung

- **Einführung und Historie des Internets**
- **Schichtenmodell**
  - Dienst, Protokoll, Internet-Modell
  - Einordnung von IT-Sicherheit
- **Netzwerk als Infrastruktur**
- **Layer 7: Anwendungsschicht**
- **Layer 7/4: Socketprogrammierung**
- **Layer 4: Transportschicht**
- **Layer 3: Netzwerkschicht**
- **Layer 2: Sicherungsschicht**

Wohin mit der Sicherheit?

Wohin mit der Sicherheit?





Wohin mit der Sicherheit?

- **Sicherheit kann überall eingebaut werden!**
  - aber es macht nicht überall Sinn!

Wohin mit der Sicherheit?

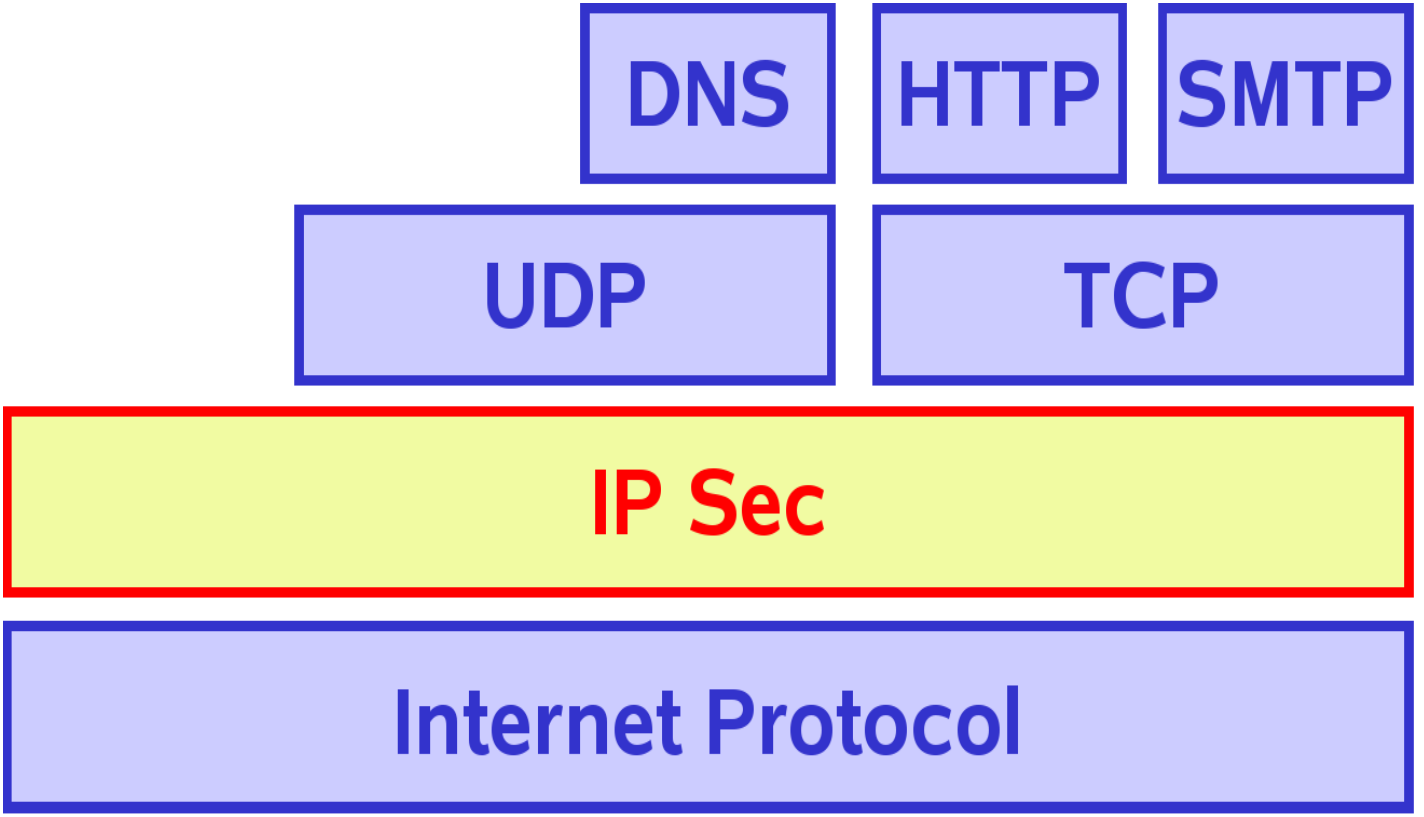
Die gute Nachricht!

- **Sicherheit kann überall eingebaut werden!**
  - aber es macht nicht überall Sinn!

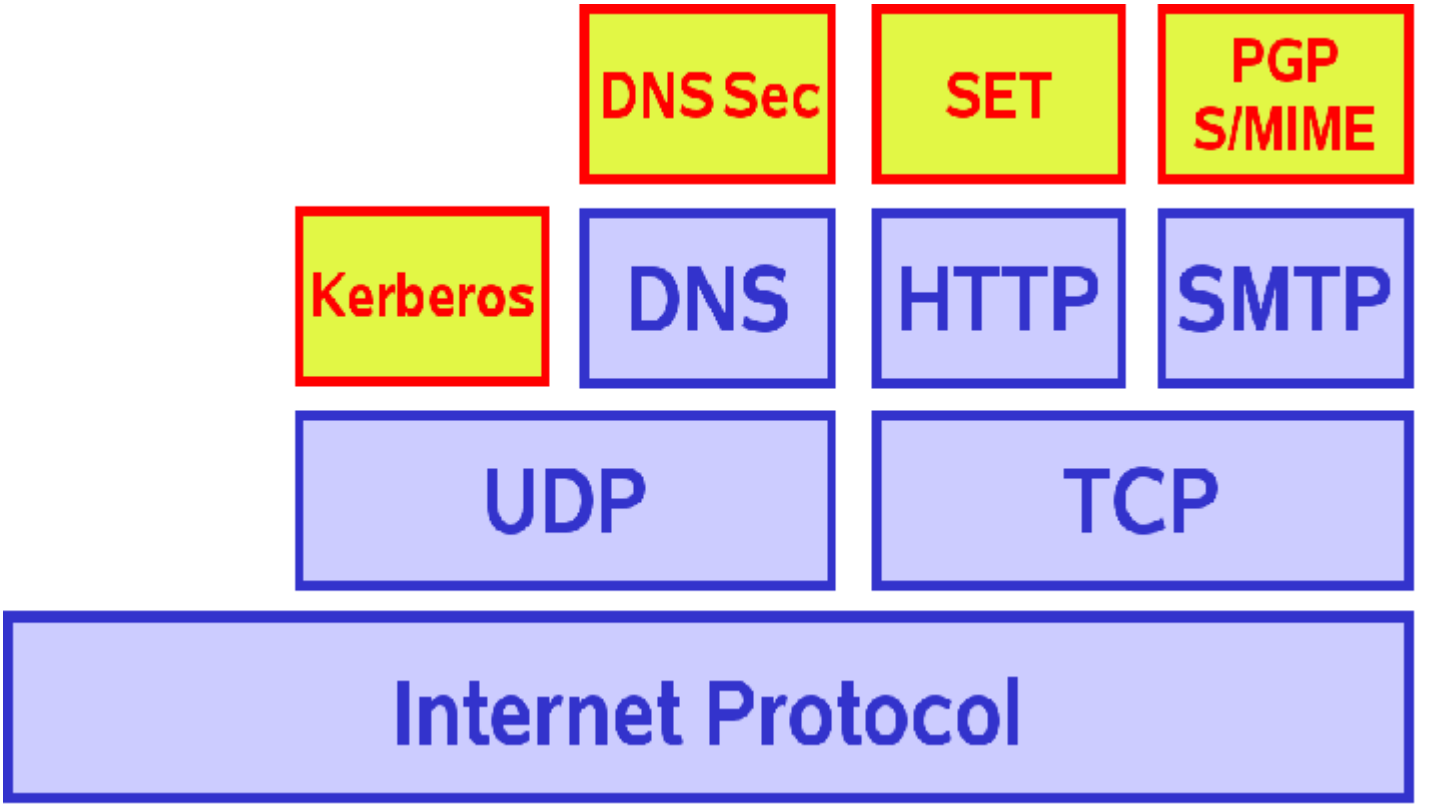
Und jetzt die schlechte Nachricht?

- **Sicherheit muss eingebaut werden!**
  - Tatsächlich nicht überall, aber bestimmt irgendwo!

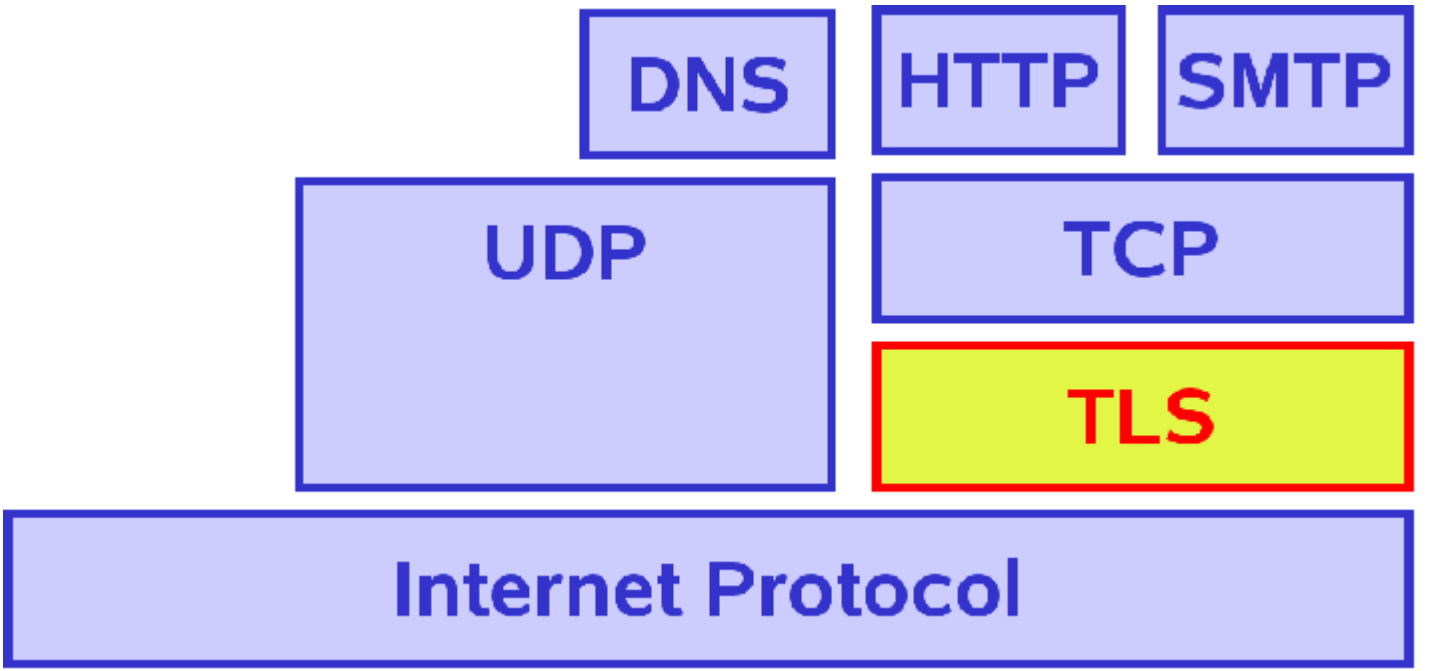
Wohin mit der Sicherheit? (2) - Netzwerk / Internet



Wohin mit der Sicherheit? (3) - Anwendung / Process



Wohin mit der Sicherheit? (4) - Transport / Host-to-Host



Wohin mit der Sicherheit? (5) - Bewertung

Data Link (Network Interface) layer:

- ✓ Schützt den gesamten Verkehr auf dem Link
- ✘ Schützt nur bis zum nächsten Router

Network (Internet) layer:

- ✓ Schützt von Rechner zu Rechner
- ✓ Unsichtbar für die Anwendungen
- ✘ Keine Kontrolle durch Benutzer / Anwendung
- ✘ Passt nicht, weil zustandslos und unsicher
  - Reihenfolge ist üblicherweise wichtig!

Wohin mit der Sicherheit? (6) - Bewertung

Transport (Host-to-Host) layer:

- ✓ Auch Rechner zu Rechner für dieses Prot.
- ✓ Anwendung kann Einfluss nehmen
- ✓ Transport Layer oft zustandsbehaftet
- ✘ Anwendung muss angepasst werden

Application (Process) layer:

- ✓ Exakte Abbildung von Anforderung
- ✘ Skaliert schlecht – jede Anwendung muss angepasst werden

Was machen wir an IT-Sicherheit?

- **Im Rahmen der Vorlesung nur sehr wenig**
- **Wir werden uns beschäftigen mit:**
  - Layer 3:
    - Firewalls
    - IPv6 als sichere Alternative für IPv4
  - Layer 2: (wenn die Zeit reicht)
    - WLAN-Sicherheitsstandards
- **Wir können leider nicht vertiefen:**
  - Verschlüsselung oder digitale Signaturen
  - Angriffserkennung oder sichere Protokolle

Kontakt

Prof. Dr. Klaus-Peter Kossakowski

Email: klaus-peter.kossakowski@haw-hamburg.de

Mobil: +49 171 5767010

http://users.informatik.haw-hamburg.de/~kpk/