



IPv6 – Chance und Risiko für den Datenschutz im Internet

22. November 2011

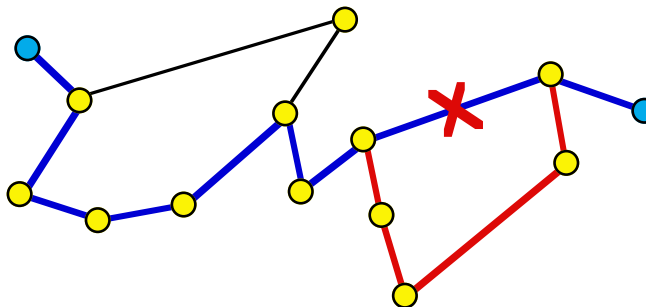
Prof. Dr. Hannes Federrath

<http://svs.informatik.uni-hamburg.de/>

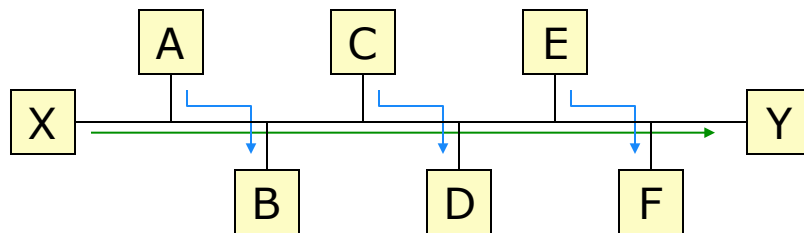
Adressen sind erforderlich für das Routing

- Anforderungen

- **Einfachheit:** Router besitzen wenig Speicher und Rechenleistung, Wegewahl soll wenig Zeit kosten
- **Stabilität:** Router sollen lange ohne Neustart laufen
- **Robustheit:** Router sollen alternative Wege bei Ausfall einer Route finden



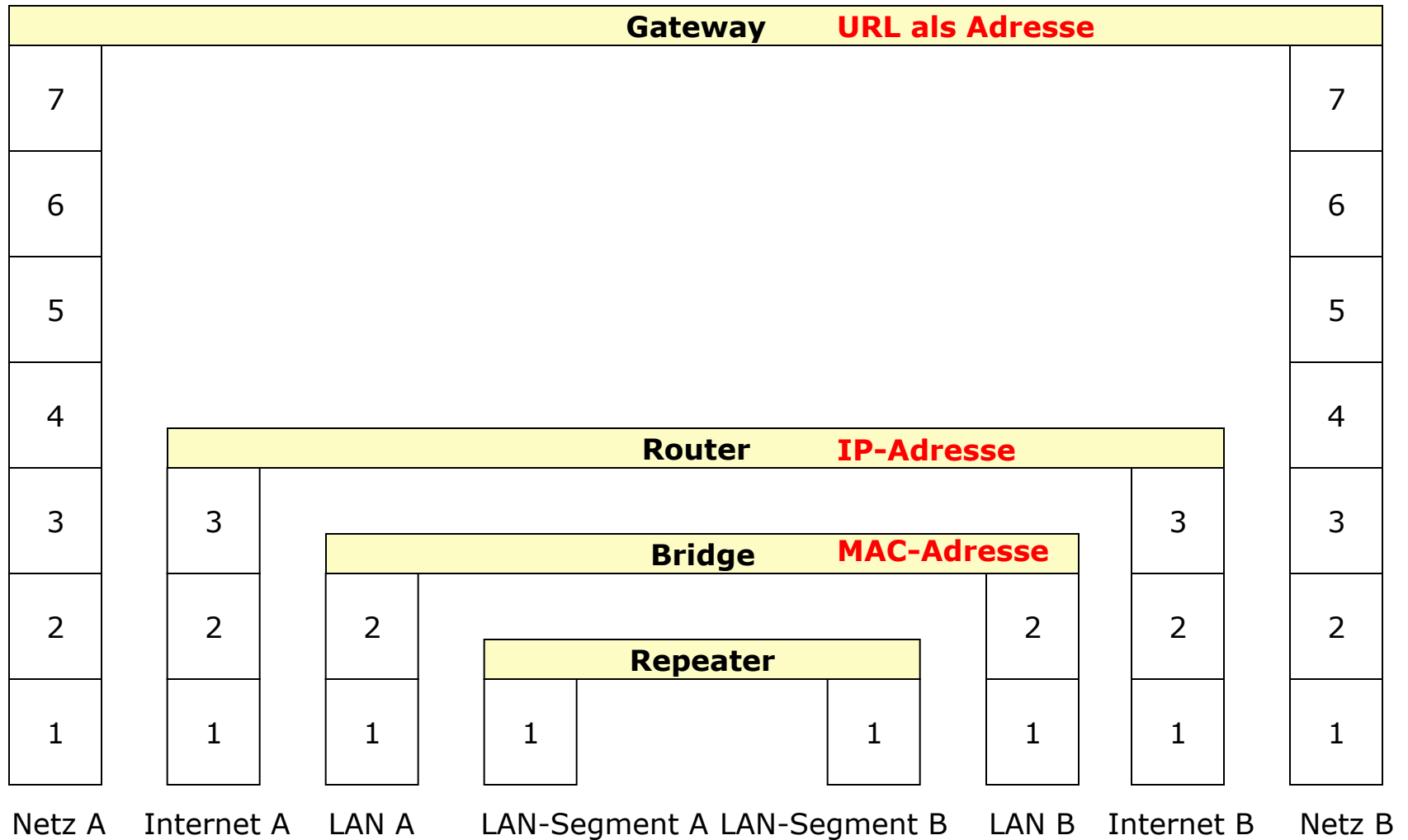
- **Fairness**
- **Optimalität**



Optimalität: Wenn A, B, C, D, E, F gemeinsam voll auslasten können, sollten X und Y warten

Fairness: X und Y sollten jedoch nicht benachteiligt werden

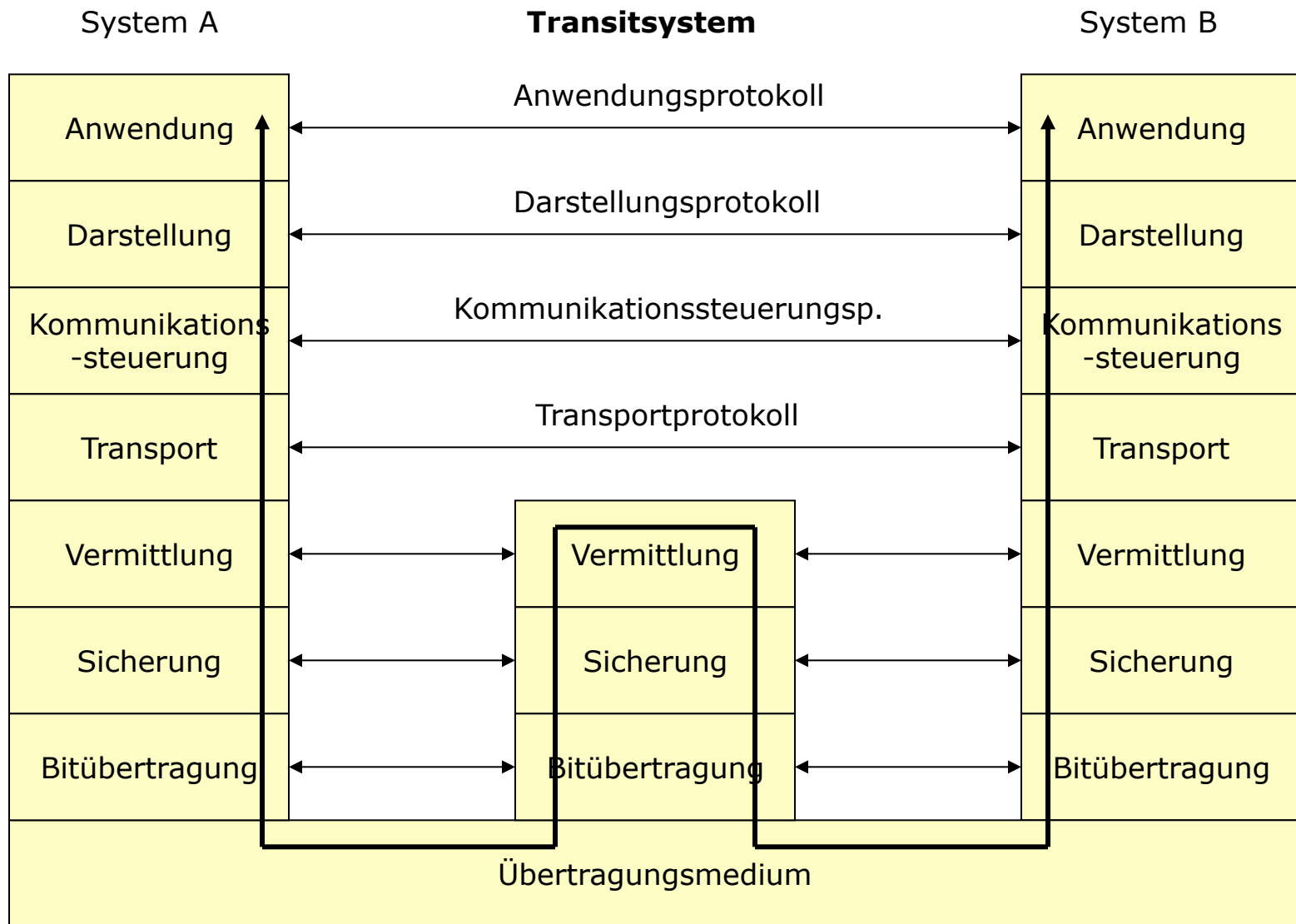
Bezeichnungen der Funktionseinheiten beim «Internetworking»



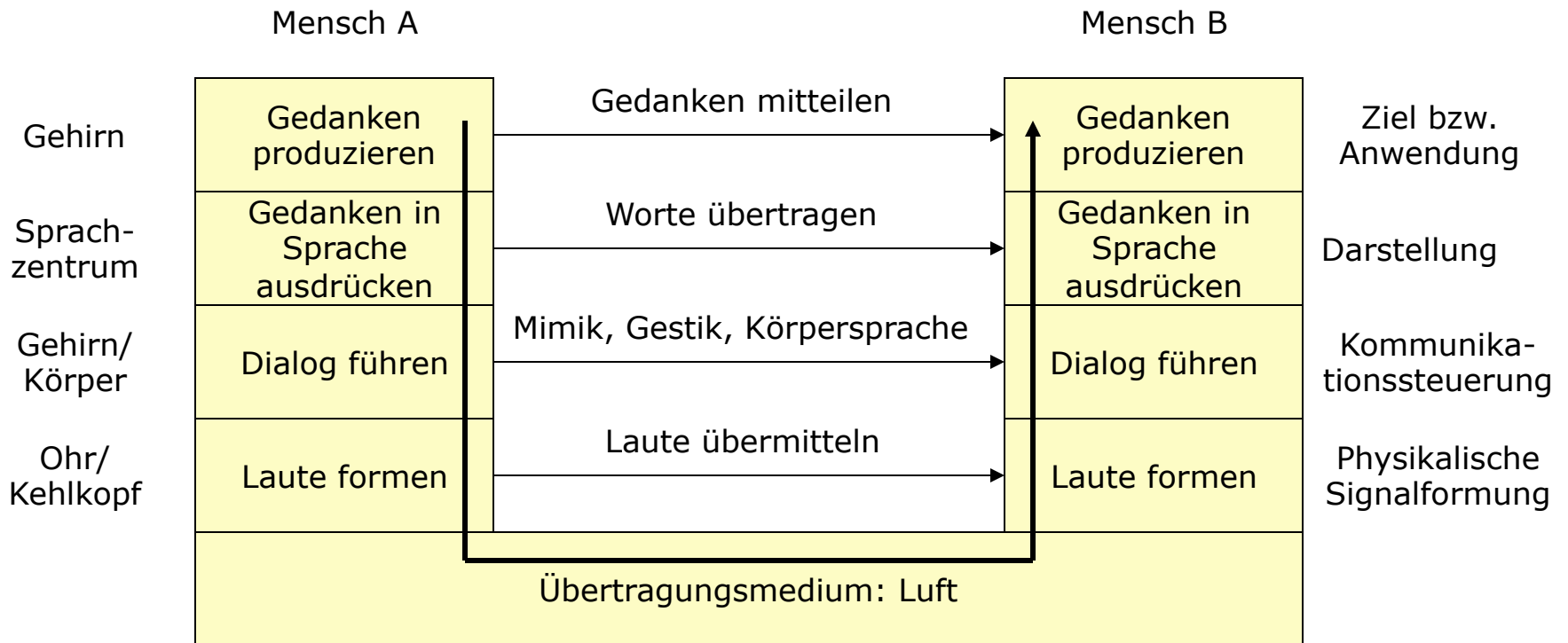
OSI-Modell: Aufgaben der 7 Schichten

Application Layer	Anwendung	Anwendungsunterstützende Dienste Netzmanagement
Presentation Layer	Darstellung	Umsetzung von Daten in Standardformate Interpretation dieser gemeinsamen Formate
Session Layer	Kommunikations- steuerung	Prozess-zu-Prozess-Verbindung Prozesssynchronisation
Transport Layer	Transport	Logische Ende-zu-Ende-Verbindungen in Abstraktion der technischen Übertragungssysteme
Network Layer	Vermittlung	Wegbestimmung im Netz: Routing Datenflusskontrolle
Data Link Layer	Sicherung	Logische Verbindungen mit Datenpaketen Elementare Fehlererkennungsmechanismen
Physical Layer	Bitübertragung	Nachrichtentechnische Hilfsmittel für die Übertragung von Bits

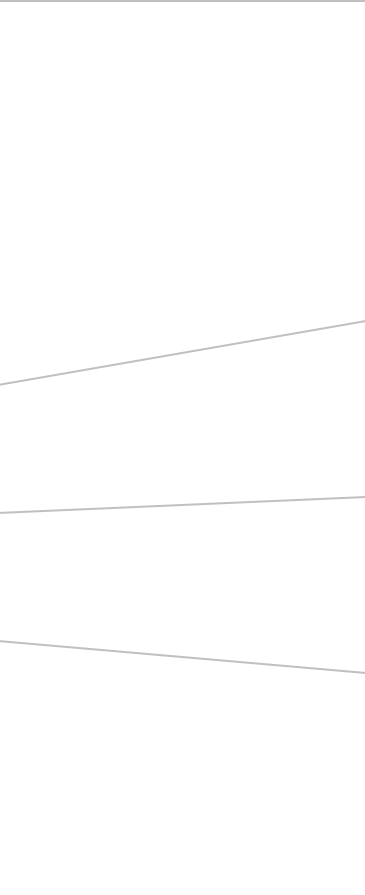
Schichten im OSI-Modell



Ebenenmodell der Mensch-zu-Mensch-Kommunikation



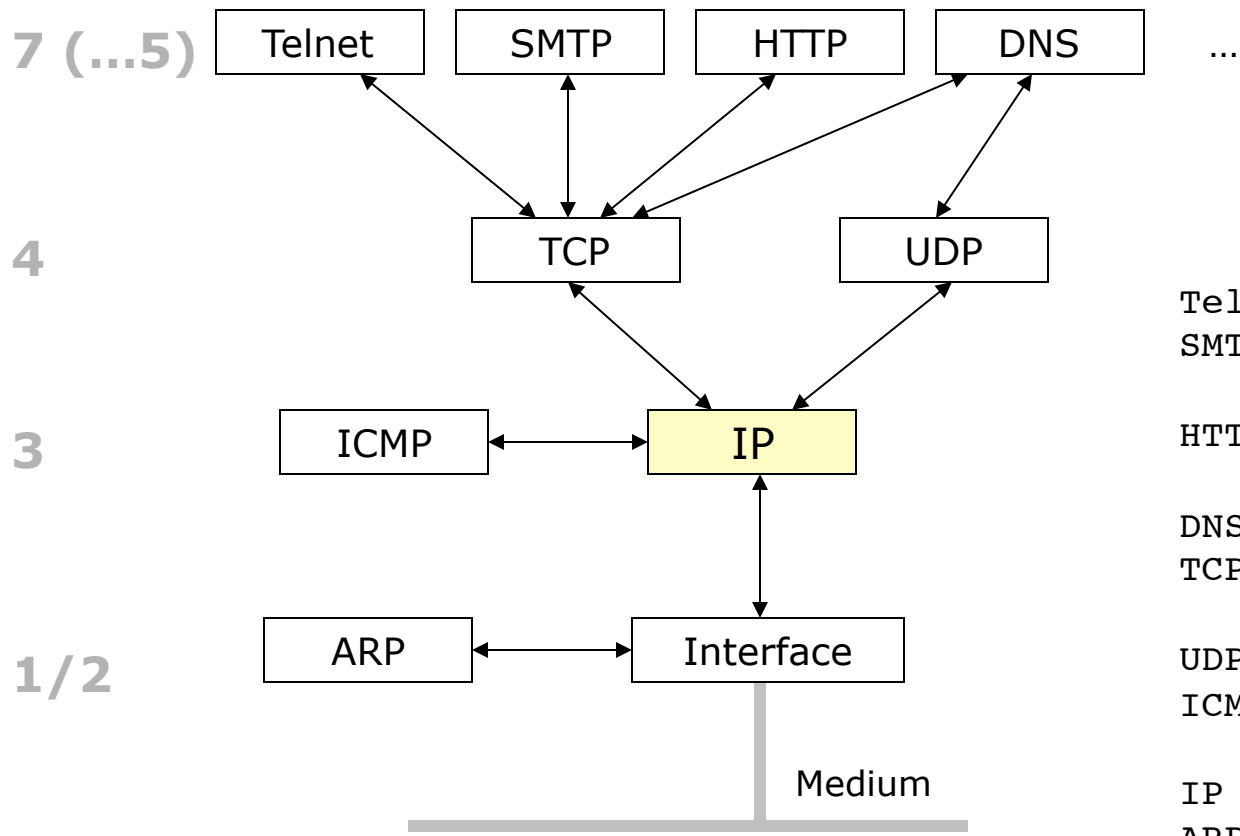
Schichtenmodelle OSI und Internet

7	A	Application Layer		Application Level
6	P	Presentation Layer		Telnet, FTP, SMTP, DNS, HTTP, ...
5	S	Session Layer		
4	T	Transport Layer		Transmission Level
3	N	Network Layer		TCP, UDP
2	DL	Data Link Layer		
1	PH, PHY	Physical Layer		Internet Level
			IP, ICMP	
			Network Level	
			MAC-Adresse Ethernet, ...	

OSI

Internet

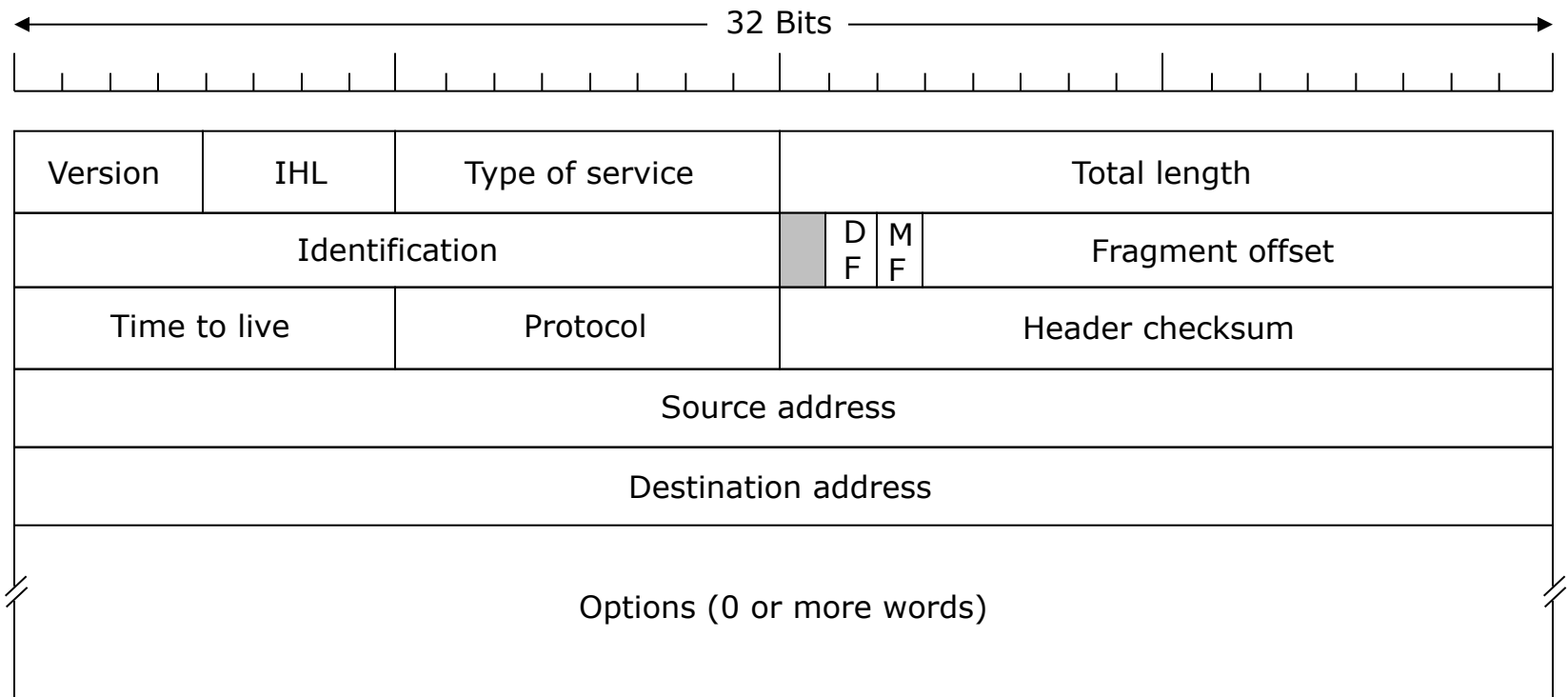
Protokollebenen



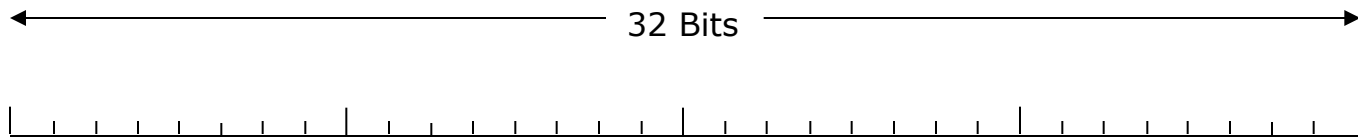
- Telnet Teletype Network
- SMTP Simple Mail Transfer Protocol
- HTTP Hypertext Transmission Protocol
- DNS Domain Name System
- TCP Transmission Control Protocol
- UDP User Datagram Protocol
- ICMP Internet Control Message Protocol
- IP Internet Protocol
- ARP Adress Resolution Protocol

Header des IPv4-Protokolls

IPv4-Adresse hat 4 Byte = 32 Bit



Der feste IPv6-Header



Version	Priority	Flow label		
Payload length		Next header	Hop limit	
Source address (16 Bytes)				
IPv6-Adresse hat 16 Byte = 128 Bit				
Destination address (16 bytes)				

Die IPv6-Erweiterungsheader

Erweiterungsheader	Beschreibung
Optionen für Teilstrecken (Hop-by-Hop)	Verschiedene Informationen für Router
Routing	Definition einer vollen oder teilweisen Route
Fragmentierung	Verwaltung von Datengrammfragmenten
Authentifikation	Echtheitsüberprüfung des Senders
Verschlüsselung	Vertraulichkeit des Inhalts (Payload)
Optionen für Ziele	Zusätzliche Informationen für das betreffende Ziel

IP Version 6

- IPv6
 - Erweiterung des Adressraums
 - 4 Byte-Adressen (IPv4) → 16-Byte-Adressen (IPv6)
 - bessere Unterstützung der QoS-Anforderungen von Echtzeitanwendungen: Priorisierung von IP-Paketen
 - Streaming
 - Verbesserung der Sicherheit
 - Authentication Header
 - Encapsulated Security Payload

IPSec/IPv6

- IPSec/IPv6 schließt eine Lücke bzgl. Sicherheitsfunktionen auf der Netzwerkschicht

	IPv4	IPv6
Anwendungsschicht	Pretty Good Privacy (PGP), S/MIME, Secure Shell (SSH)	
Transportschicht	Secure Sockets Layer/Transport Layer Security (SSL/TLS)	
Vermittlungsschicht	—	Authentication Header (AH) zur Integritätssicherung von Datagrammen MD 5, SHA-1 Encapsulated Security Payload (ESP) zur Verschlüsselung von Datagrammen DES/CBC
Schichten 1/2	Challenge Handshake Protocol (CHAP, Passwort), Encrypt Control Protocol (ECP), Wireless Equivalent Privacy (WEP)	

Fakten

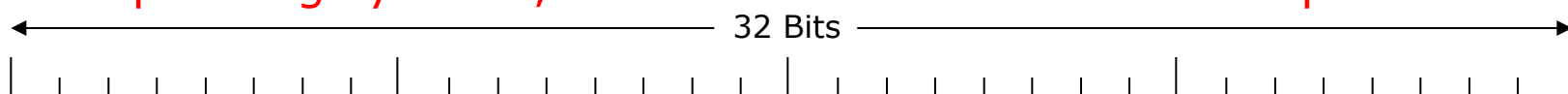
- IPv4
 - Adresse hat 32 Bit
 - Adressvorrat ist heute bereits zu klein, um jedem Gerät jederzeit eine eindeutige Kennung (IPv4-Adresse) zuzuteilen
- IPv6
 - Adresse hat 128 Bit
 - Adressvorrat ermöglicht eindeutige Kennung (IPv6-Adresse) aller Geräte
 - Eingebaute Priorisierung kann Netzneutralität gefährden
 - Verwendung der MAC-Adresse (Schicht 2) als Teil der IP-Adresse ermöglicht auch Identifizierung trotz Adreßwechsel
 - Privacy Extensions (RFC 4941): zufällige MAC-Adresse erzeugen und regelmäßig wechseln

Von IPv4 bekannte »Schutzfunktionen«

- Adressersetzung ist weiterhin möglich
 - Network Address Translation (NAT)
 - kann weiterhin unterstützt werden, ist aber meist nicht mehr zwingend erforderlich
 - Verwendung von Proxies ebenfalls weiterhin möglich
 - Beachte: auch bei IPv4 trotz NAT Identifizierbarkeit
- Dynamische Adressvergabe ist weiterhin möglich
 - Sensibilität der ISPs vorausgesetzt, könnten IP-Adressen von DSL-Zugängen weiterhin dynamisch zugeteilt werden
 - Beachte: Eine statische IP-Adresse ist ein Personenpseudonym und unstrittig ein personenbezogenes Datum (und nach einer gewissen Nutzungszeit auch für alle Außenstehenden verkettbar).
 - Eine dynamische IP-Adresse ist lediglich ein personenbezogenes Datum für denjenigen, der die Zuordnungsregel kennt.

Network Address Translation

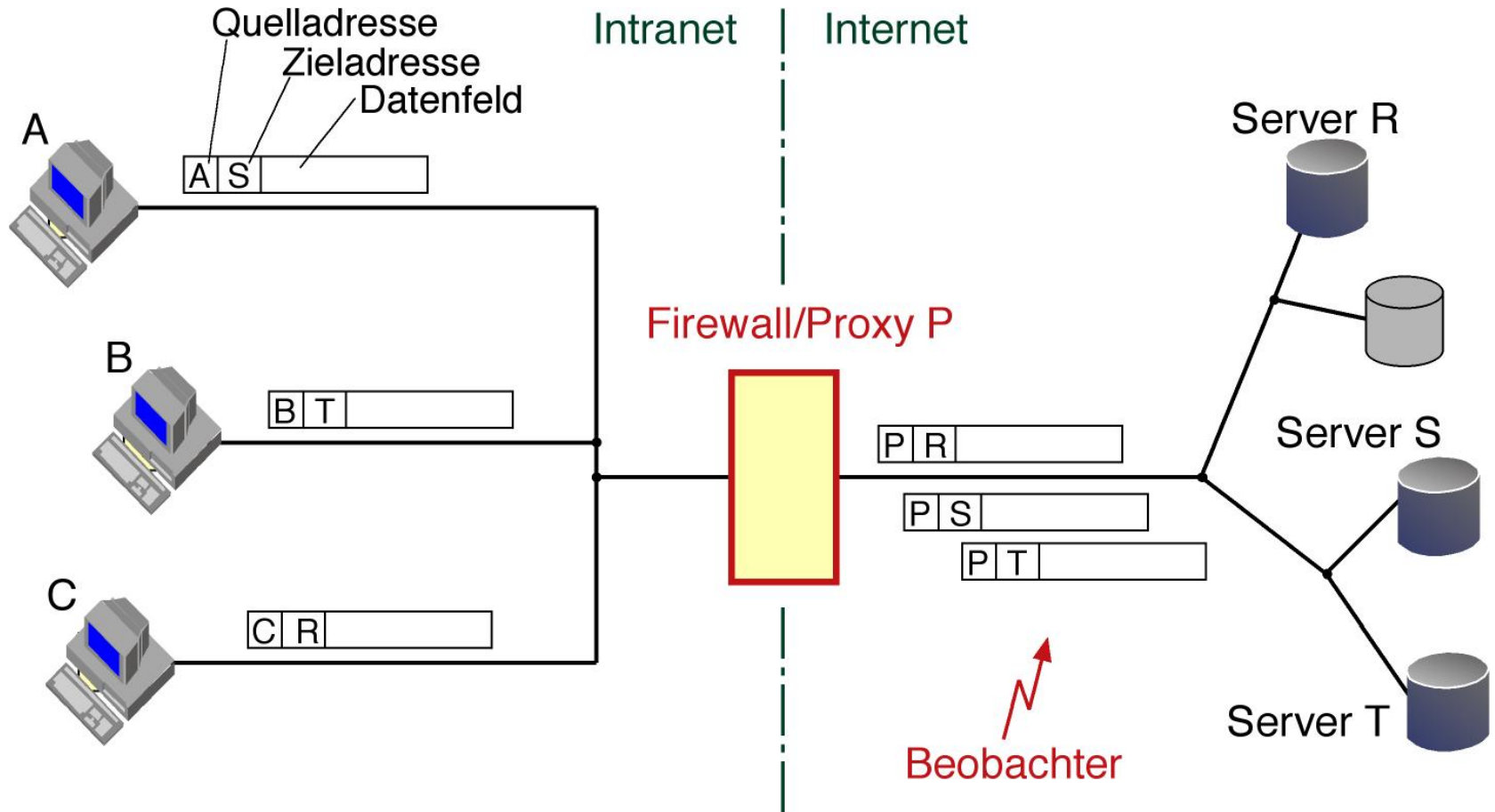
- Kann man feststellen, wieviele Hosts hinter einem NAT-GW sind?
 - S. Bellovin: A Technique for counting NATed hosts. Proc. 2nd ACM SIGCOMM Workshop on Internetmeasurement 2002. <http://www.cs.columbia.edu/~smb/papers/fnat.pdf>
 - Viele Betriebssysteme benutzen das Header-Feld ID als counter: »The technique is based on the observation that on many operating systems, the IP header's ID field is a simple counter.«



Version	IHL	Type of service	Total length			
Identification			D	M	Fragment offset	
			F	F		
Time to live		Protocol	Header checksum			
Source address						
Destination address						
Options (0 or more words)						

Proxies und Network Address Translation

- Schutz vor Beobachtung im Internet



Chancen durch IPv6 aus Datenschutzsicht

- IPsec ist fester Bestandteil von IPv6
 - ermöglicht leichte Verschlüsselung und Authentifizierung
 - Verwendung von Verschlüsselung ist aber nicht zwingend
- Jedes Gerät könnte mehr als eine Adresse erhalten
 - im besten Fall wäre das ein Transaktionspseudonym
 - Autokonfigurationsfunktion in IPv6 ermöglicht funktionsfähige selbst zugewiesene IP-Adressen
 - Beachte: Durch fremd zugewiesenen Präfix bleibt das Gerät bzw. der User jedoch weitgehend beobachtbar (schwacher Schutz, bestenfalls lokal).
- Verbesserte Multicast-Mechanismen und Mobile IP ermöglichen zumindest theoretischen Schutz vor Lokalisierung und Beobachtung
 - Realisierung eines sehr effizienten Mix-basierten Anonymisierungsverfahrens auf IP-Ebene (Schicht 3 des OSI-Referenzmodells) denkbar



Universität Hamburg
Fachbereich Informatik
Arbeitsbereich SVS
Prof. Dr. Hannes Federrath
Vogt-Kölln-Straße 30
D-22527 Hamburg

E-Mail federrath@informatik.uni-hamburg.de

Telefon +49 40 42883 2358

<http://svs.informatik.uni-hamburg.de>