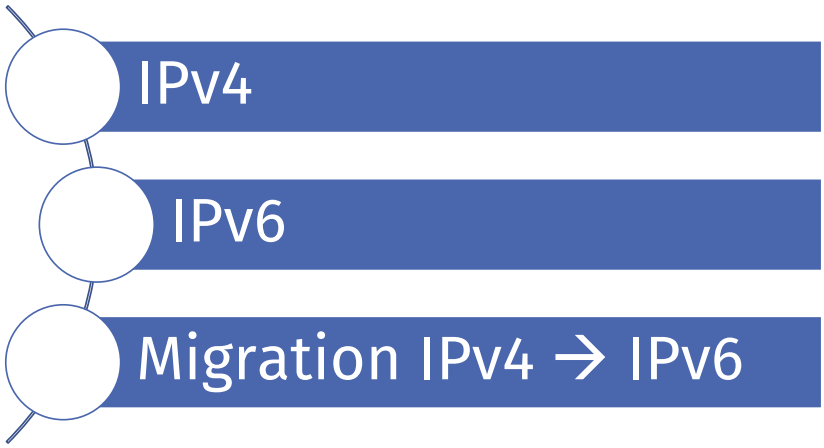
2. Internet Protocol

DIE INTERNET-PROTOKOLLWELT

28

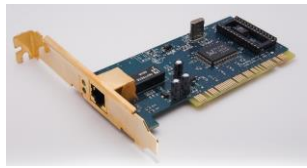
Übersicht



29

Wiederholung: Die Internet-Protokollhierarchie

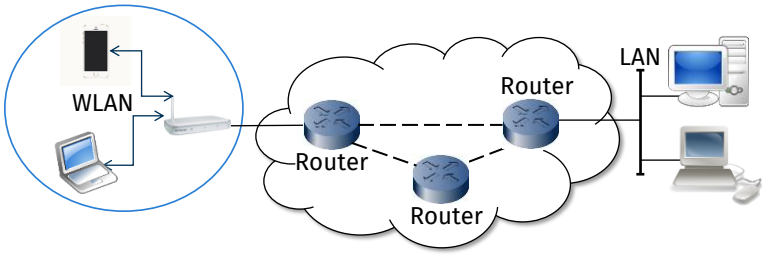
Anwendungsschicht	Anwendungsspezifische Funktionen zusammengefasst in Anwendungsprotokollen
Transportschicht	Ende-zu-Ende-Datenübertragung zwischen zwei Anwendungsinstanzen
Internet-Schicht	Paketvermittlung im Netz
Sicherungsschicht	Schnittstelle zum physikalischen Medium: Rechner-Netzanschluss, *Network-to-Host*, N2H
Bitübertragungsschicht	



Das Protokoll IP (Internet Protocol) [RFC 791]

Historie:
- Entwickelt vom amerikanischen Verteidigungsministerium (*Department of Defense*, DoD)
- Bereits 1969 im damaligen ARPANET eingesetzt (ursprünglich 4 Hosts!)

Realisierung und Entwicklung:
- IP = das am meisten genutzte Vermittlungsschichtprotokoll
- Weiterentwicklung im Projekt *IP next generation*, IPng, der *Internet Engineering Task Force*, IETF, zu IPv6

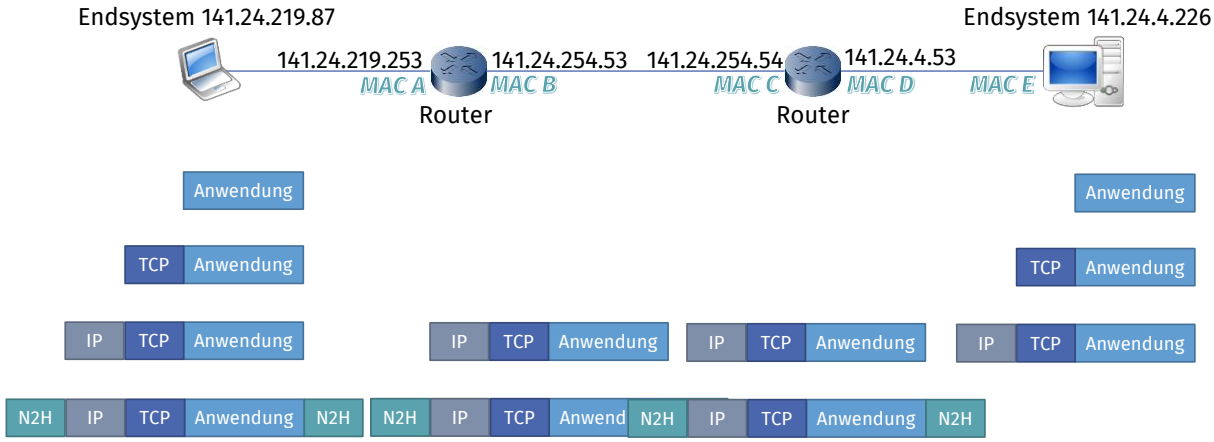


Eigenschaften von IP

- Paketvermittelt
- Verbindungslos (Datagrammdienst)
- Ungesicherte Übertragung:
  - Datagrammverlust
  - Duplizierung von Datagrammen
  - Nichteinhalten der Reihenfolge
  - (Theoretisch) endloses Kreisen von Paketen
  - Keine Behandlung von nicht behebbaren Fehlern der darunter liegenden Schicht
  - Anzeige von (fatalen) Fehlern mit dem Protokoll *Internet Control Message Protocol*, ICMP
- Keine Flusskontrolle
- Keine explizite Staukontrolle
- Einsatzbereich von privaten bis hin zu öffentlichen Netzen
- Weltweit eindeutige (hierarchische) Adressierung notwendig

32

Interworking mit IP

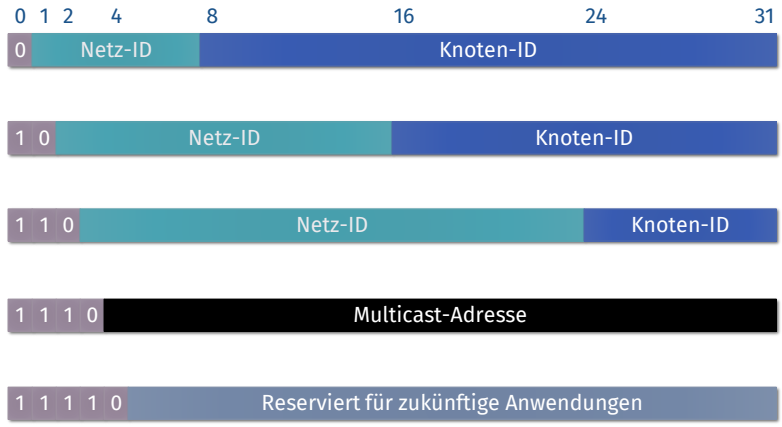


33

IPv4-Adressen (ursprüngliche Einteilung)

Adressklassen (32 Bit):

1. **Class A** für Netze mit bis zu 16 Mio. Knoten
2. **Class B** für Netze mit bis zu 65.536 Knoten
3. **Class C** für Netze mit bis zu 256 Knoten
4. **Class D** für Gruppenkommunikation (Multicast)
5. **Class E**, noch reserviert für zukünftige Anwendungen



IPv4-Subnetzadressen

- IPv4-Adresse (hier Klasse B):

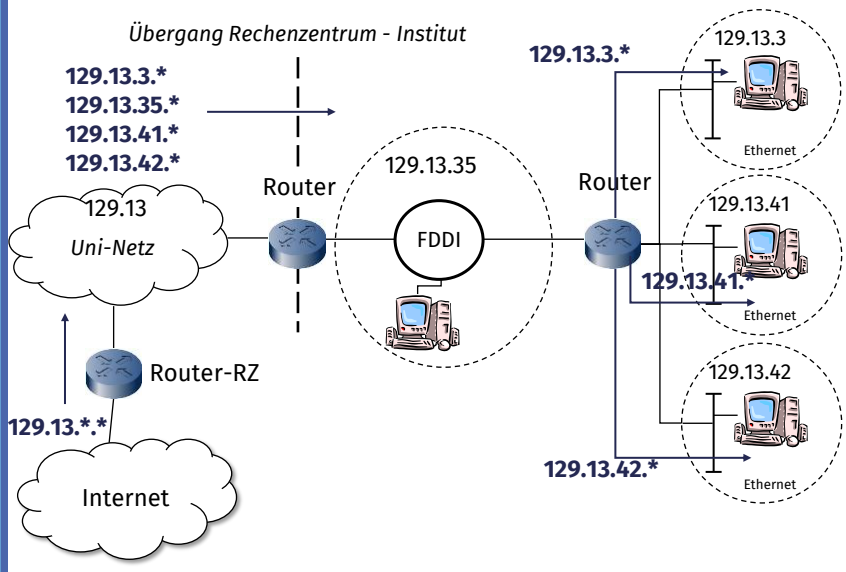
- Subnetzmaske: Adressteil für Netz und Subnetz (durch Folge von „1“)
- Beispiel:

IP-Adresse:	129.	13.	3.	64
Subnetzmaske:	255.	255.	255.	0
	1111 1111	1111 1111	1111 1111	0000 0000
Netzwerk:	129.	13.		
Subnetz:			3.	
Endsystem:				64

- Netz-ID: Adressklasse
- Subnetz-ID nicht immer vorhanden (z. B. bei Subnetzmaske **255.255.0.0** in obigem Beispiel)

IPv4-Subnetze

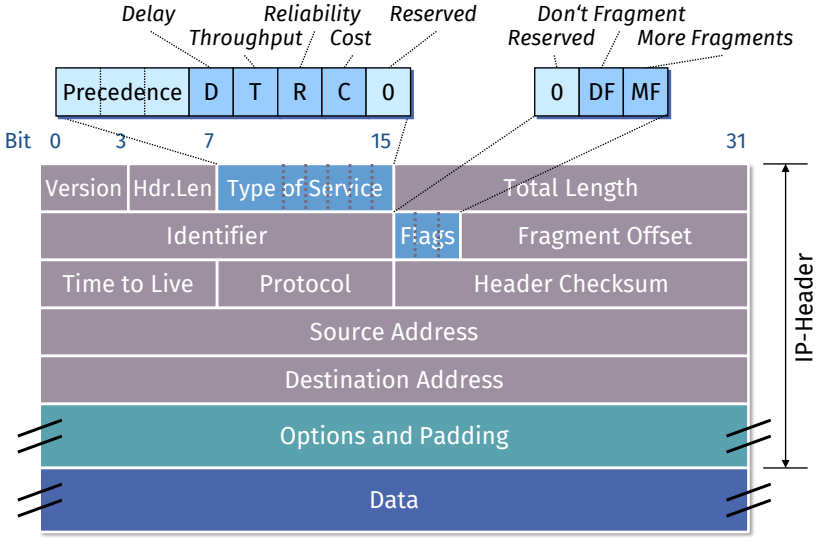
Beispiel



36

IPv4-Datagramm: Aufbau

(klassisch)



37

IPv4-Datagramm: Felder

Version	Versionsnummer für IP
Header Length	Länge des IP Headers in 32-bit-Worten
Type of Service, TOS/ Differentiated Services	Dienstgüteunterstützung
Total Length	Länge des gesamten Datagrammes
Identifier	Identifikation der Dateneinheit
Flags	Notwendig für Segmentierung
Fragmentation Offset	zur Reassemblierung
Time to Live	Lebenszeitbegrenzung des Pakets
Protocol	Protokoll der darüber liegenden Schicht (z. B. 6=TCP, 17=UDP)
Header Checksum	Fehlerüberprüfung für Header
Source/Destination Address	Quell- und Zielrechner
Options	zusätzliche Dienstleistungen
Padding	für 32-Bit-Ausrichtung (Options)
Data	Benutzerdaten

Wegewahl bei IP

Routingtabelle auf **jedem** System, die üblicherweise über Routingprotokolle gefüllt wird

Bestimmung des Eintrags, der die Weiterleitung festlegt, anhand der Zieladresse:

- Durchsuche Host-Adressen
- Durchsuche Netzwerkadressen
- Suche nach Default-Eintrag

Ziel ist...	Route	MAC-Rahmen wird adressiert an...
... direkt erreichbar	Direct Route	Zielsystem
... nur indirekt erreichbar	Indirect Route	Router

Beispiel der Adressierung

IP-Paket adressiert an...

- 129.13.35.73 (sioux.telematik.informatik.uni-karlsruhe.de)
- 132.151.1.19 (www.ietf.org)

Aktuelle Routingtabelle:

Destination	*Gateway*	*Flags*	*Refs*	*Use*	*Interface*
Default	i70lr0	UGS	1	13320	tu0
127.0.0.1 (localhost)	localhost	UH	7	242774	lo0
129.13.3	i70r35	UGS	0	6	tu0
129.13.35	mohave	U	11	3065084	tu0
129.13.41	i70r35	UGS	2	4433	tu0
129.13.42	i70r35	UGS	0	4	tu0

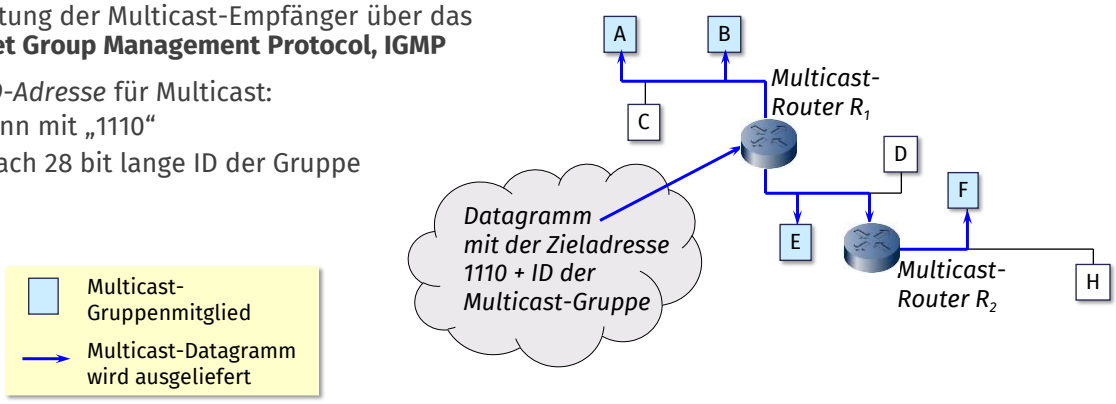
IPv4-Multicasting

IPv4-Datagramm an mehrere Empfänger adressiert

Verwaltung der Multicast-Empfänger über das **Internet Group Management Protocol, IGMP**

Class D-Adresse für Multicast:

- Beginn mit „1110“
- Danach 28 bit lange ID der Gruppe



IPv4-Dienste: Überprüfung des Paketkopfes

Überprüfungen, die nach dem Empfang eines IP-Datagrammes am Header durchgeführt werden:

- Überprüfung der korrekten Länge des Headers
- Test der IP-Versionsnummer
- Überprüfung der korrekten Datagrammlänge
- Prüfsummenbildung über den IP-Header
- Überprüfung der Paketlebenszeit
- Überprüfung der Protokoll-ID
- Überprüfung der Adressklassen beider Adressen (Quell- und Zieladresse)

Bei negativem Resultat eines der oben aufgeführten Tests:

- Paket verwerfen
- Fehlermeldung über ICMP an den Sender des Pakets

IPv4-Dienste: Source Routing

Festlegung des Pfads zum Ziel durch die Protokollinstanz oberhalb von IP

- Options-Feld mit einer Liste von Routern, die den Weg zum Zielknoten beschreiben
- Pointer P → Adresse des nächsten Routers
- Empfangender Router ersetzt die Adresse durch die eigene für das nächste Subnetz
- P → P + 4 [byte] (= nächste Routeradresse)

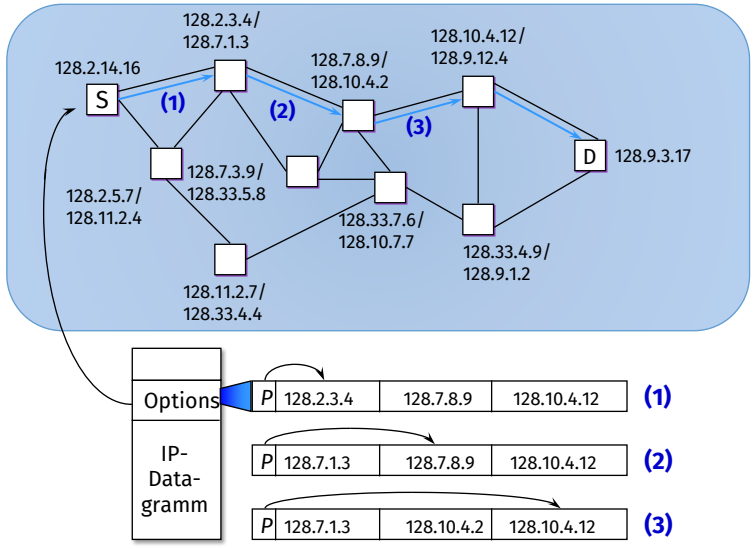
Strict Source Routing

- Kompletter Pfad mit allen Routern im Options-Feld

Loose Source Routing

- Nur eine Teilmenge der Router im Options-Feld
- Weitere Router zwischen den angegebenen über herkömmliches Routing bestimmt
- Mittels einer zusätzlichen „Route Recording“-Option Aufzeichnung des kompletten Pfads

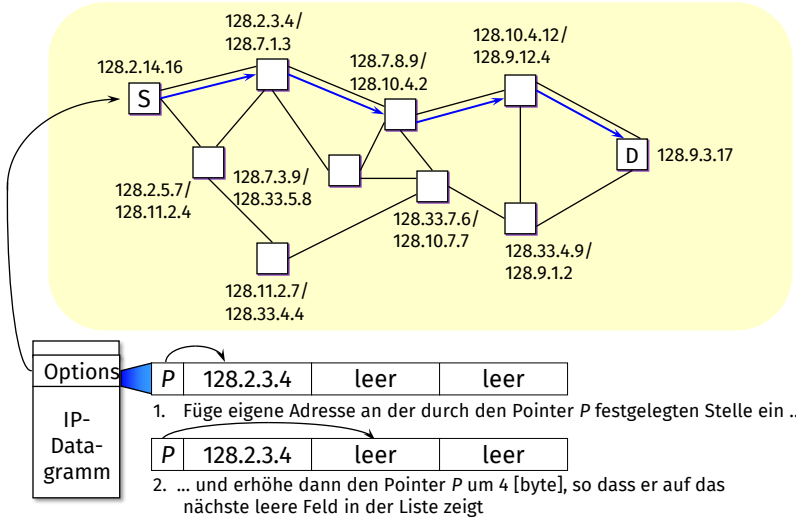
IP-Dienste: Source Routing – Beispiel



44

IPv4-Dienste: Route Recording

Im Datagramm wird der durchlaufene Weg festgehalten



1. Füge eigene Adresse an der durch den Pointer *P* festgelegten Stelle ein …
2. … und erhöhe dann den Pointer *P* um 4 [byte], so dass er auf das nächste leere Feld in der Liste zeigt

45

IPv4-Dienste: Zeitstempel

Einfügen eines **Zeitstempels** im Optionsfeld, der den Zeitpunkt charakterisiert, zu dem das Paket vom Router bearbeitet wurde

- Aussagen über die Belastung der Netzwerke
- Abschätzen der Effizienz der benutzten Routing-Algorithmen

4 bit langes **Flag** im Optionsfeld:

- Flag-Wert = 0: Nur Zeitstempel aufzeichnen, keine Adressen
- Flag-Wert = 1: Sowohl Zeitstempel als auch Adressen (*Route Recording*) aufzeichnen
- Flag-Wert = 3: Die Adressen sind vom Sender vorgegeben (*Source Routing*), die adressierten Router tragen nur ihren Zeitstempel ein

IPv4-Dienste: Segmentierung und Reassemblierung

Unterschiedliche Netzwerktechniken mit unterschiedlich langen maximale Paketlängen (*Maximum Transmission Unit*, MTU)

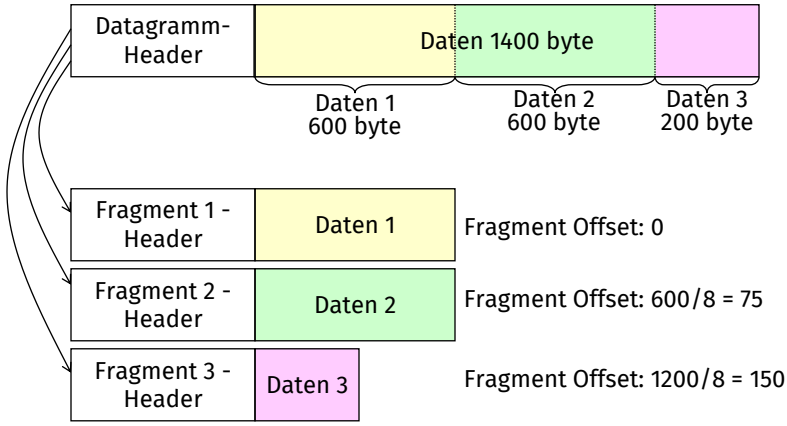
→ Segmentierung und Reassemblierung notwendig

- Beispiel Ethernet: 1.500 byte Nutzdaten

Notwendige Informationen im IP-Header:

- *Flags im IP Header*
  - Bit 0: reserviert
  - Bit 1: 0 = darf fragmentiert werden
    1 = darf nicht fragmentiert werden
  - Bit 2: 0 = letztes Fragment
    1 = es folgen weitere Fragmente
- *Fragment Offset*
  - Definiert die Stelle, an der das Fragment in die Original-PDU eingesetzt werden muss (in der Einheit 8 byte)

IPv4-Dienste: Segmentierung und Reassemblierung – Beispiel



Zusammenfassung zu IPv4

Die Vermittlungsschicht im Internet ist nicht nur IP!

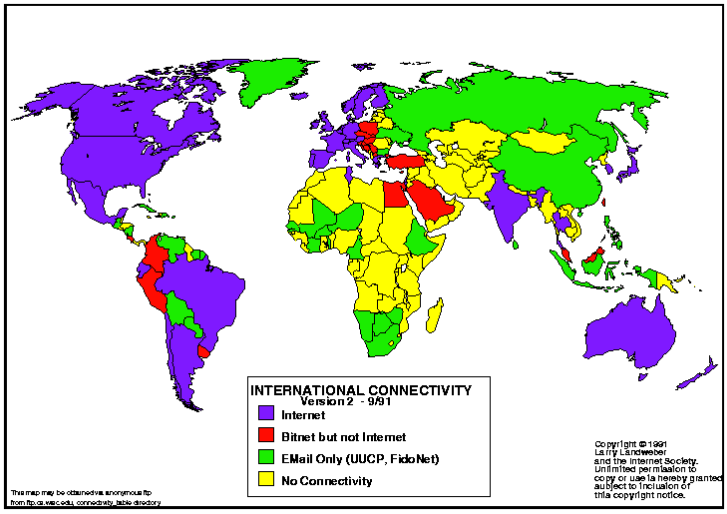
Die Adressierung mittels IPv4 ist schon an die physikalische Grenze gestoßen

- Neues Adressierungsschema notwendig
  → längere Adressen
- Konsequenz: Tiefer gehende Änderung von IP
  → Inkompatibilität

Neuentwicklung: **IPv6**

Entwicklung der globalen Vernetzung

Stand 1991

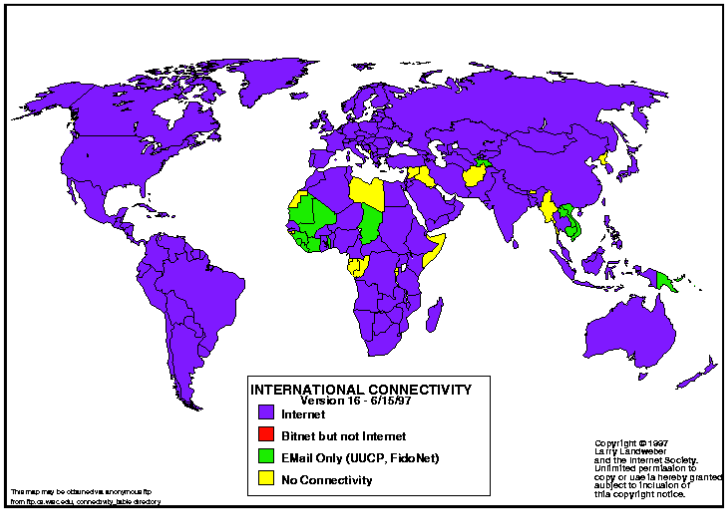


Wintersemester 2020/21 DIE INTERNET-PROTOKOLLWELT - 2. IP 50

50

Entwicklung der globalen Vernetzung

Stand 1997



Wintersemester 2020/21 DIE INTERNET-PROTOKOLLWELT - 2. IP 51

51

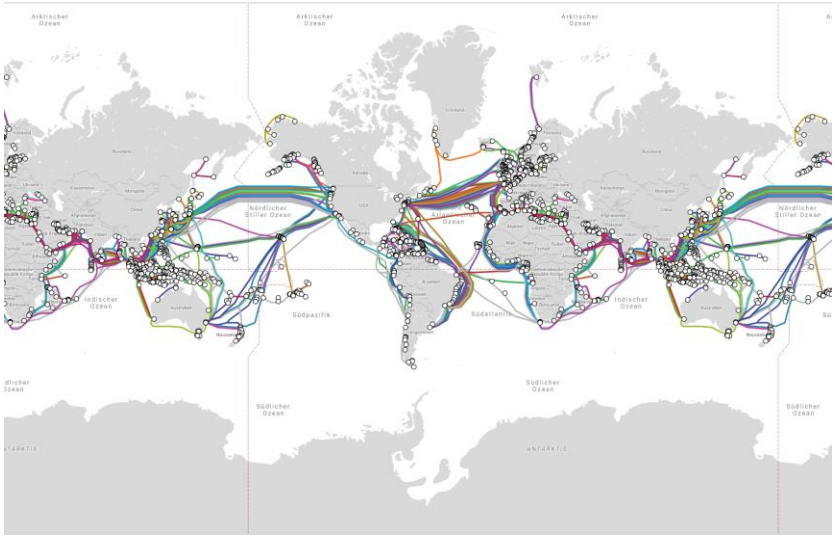
Internet-Backbone

www.submarinecablemap.com

abgerufen im August 2019

Wintersemester 2020/21

Umgang mit Adressknappheit bei IPv4?



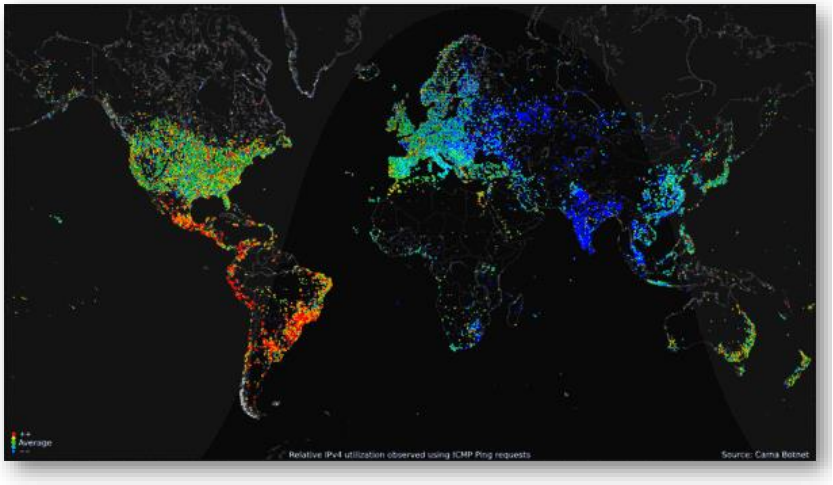
52

Internetnutzer

https://www.youtube.com/watch?v=5GQq_qMxai0

Oktober 2016

Wintersemester 2020/21



53

Gründe für Adressknappheit in IPv4

32 bit Länge → 2^{32} = 4.294.967.296 Adressen

Aber:

- Routing im Backbone anhand der Netz-ID
- Anzahl der Adressen je Netz
  - bei Klasse A: 2^{24} = 16.777.216 Adressen
  - bei Klasse B: 2^{16} = 65.536 Adressen
  - bei Klasse C: 2^{8} = 256 Adressen
- Adressen eines Netzes nur in diesem Netz verwendbar!

→ Viele Adressen bleiben ungenutzt!

CIDR: Classless Inter-Domain Routing [RFC 4632]

Beispiel für „Verschnitt“ von IPv4-Adressen:

- Kleinbetrieb mit 100 Endgeräten → Klasse C Adresse
- 254 Adressen zugewiesen → 154 ungenutzte Adressen

Idee von *Classless Inter-Domain Routing*, CIDR:

- Ersetzen der festen Klassen durch Netzwerk-Präfixe variabler Länge von 13 bis 27 bit
- Beispiel: 129.24.12.0/14: Die ersten 14 Bits der IP-Adresse → Netzwerk-Identifikation
- Einsatz in Verbindung mit hierarchischem Routing:
  - Backbone-Router, z. B. an Transatlantik-Link, betrachtet nur z. B. die ersten 13 Bits:
    - kleine Routing-Tabellen
    - wenig Rechenaufwand
  - Router eines angeschlossenen Providers z. B. die ersten 15 Bits
  - Router in einem Firmennetz mit 128 Hosts betrachtet 25 Bits

NAT: Network Address Translation [RFC 3022]

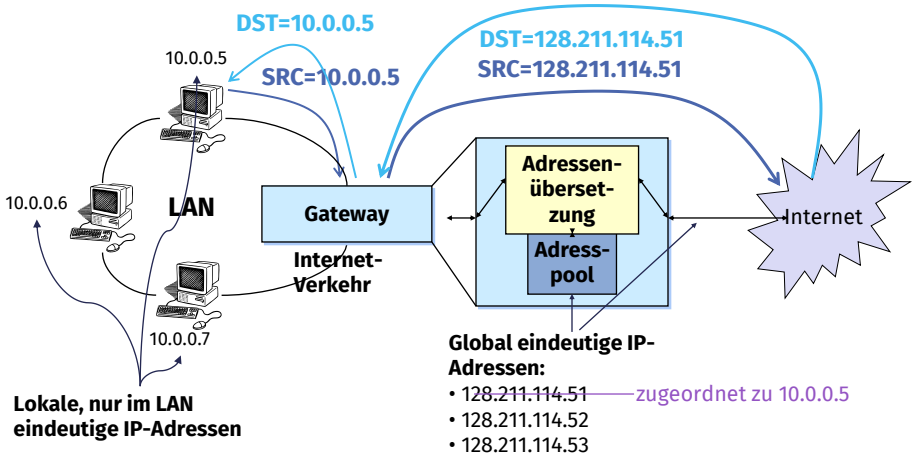
Problem:

- Adressen müssen auch beim Einsatz von CIDR global eindeutig sein

Idee:

- In einem Firmennetz brauchen nur die Rechner eine global eindeutige Adresse, die aktuell Verbindungen aus dem Firmennetz heraus aufbauen
- Temporäre Vergabe der global eindeutigen Adresse: *Network Address Translation*, NAT
- Verwaltung eines Adressenpools z. B. durch Gateway

NAT: Ablauf



Erweiterung Network Address Port Translation (NAPT) [RFC 3235]

Mehr lokale Endgeräte als globale Adressen (z. B. DSL-Anschluss)

- Bei gleichzeitigem Internetzugang aller Endgeräte zurückkommende Pakete nicht eindeutig einer lokalen IP-Adresse zuordenbar
- Weiteres Unterscheidungsmerkmal notwendig → Portnummer
- Abbildung
  (lokale IP-Adresse, ausgehende Portnummer) → (global IP-Adresse, freie Portnummer)

Damit flexible Anzahl von Endgeräten im lokalen Netz bei gleichbleibender Anzahl von globalen IP-Adressen

Theoretische maximale Anzahl von gleichzeitigen Kommunikationsvorgängen:
65.536 (2^{16}) je Transportschichtprotokoll

Motivation für eine „neue" Internet-Protokollsuite

Adressierungsprobleme

- IP-Adressraum nicht mehr ausreichend
- Class-B-Adressen sind erschöpft
- Übergangslösung helfen nur kurzfristig
- Keine hierarchische Adressierung
- Routing-Tabellen wachsen sehr schnell, daher ineffizientes Routing

Sicherheitsprobleme

Verstärkte Dienstgüteanforderungen durch Multimediaanwendungen

Geschichte von IPv6

1993	Call for Proposals für *IP next generation*, IPng	[RFC 1550]
1994	Vorschlag: *Simple Internet Protocol Plus*, SIPP als Kombination aus drei eingereichten Vorschlägen	
1995	Proposed Standard „*Internet Protocol Version 6*" erste prototypische Implementierungen → sanfte Migration erwünscht	[RFC 1883]
1996	Erstes IPv6-Backbone, 6Bone, erste Produkte am Markt erhältlich	
1998	IPv6 zum Draft Standard erhoben	[RFC 2460]
2017	Überarbeitung des IPv6-Standards, Status: Internet-Standard	[RFC 8200]

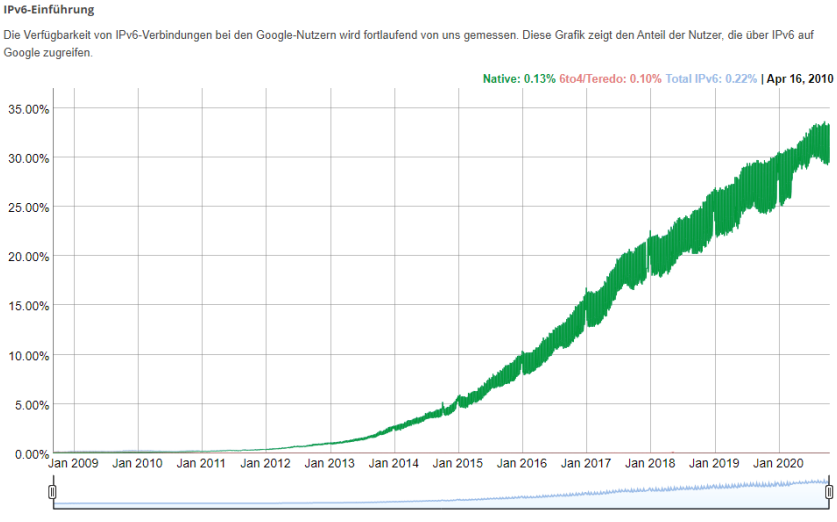
60

Anwendung von IPv6

http://www.google.de/ipv6/statistics.html

Oktober 2020:

Weniger als 35% der Zugriffe auf Google erfolgen mit IPv6



61

Eigenschaften von IPv6 im Überblick

Erweiterte Adressierungsmöglichkeiten

Neues IP-Paketkopfformat
- Einfachere Struktur
- Verbesserte Behandlung von Optionen

Multicast-Integration

Segmentierung nur Ende-zu-Ende

Autokonfiguration von IP-Systemen

Mobilitätsunterstützung

Sicherheitsvorkehrungen

Dienstgüteunterstützung für Multimedia

IPv6-Adresse [RFC 1924]

128 bit lange Adressen
- Theoretische Anzahl von Adressen: $3{,}4 \times 10^{38}$ Adressen
- Optimistische Abschätzung: 700×10^{21} pro m^2
- Pessimistische Abschätzung (RFC1715): 1.700 pro m^2

Neue Notation
- 8 durch Doppelpunkte getrennte 4-stellige Hexadezimalzahlen:
  5800:0000:0000:0000:0000:0000:0056:0078
- Reihen von Nullen können weggelassen werden:
  5800::56:78

IPv6-Adressen können Strukturinformation zur hierarchischen Lokalisierung beinhalten

IPv6-Adressen: aggregierbare Unicast-Adresse

Top-Level Aggregation, TLA
- große Internet Service Provider, ISP mit Transitnetzen, an denen andere ISPs angeschlossen sind

Next-Level Aggregation, NLA
- Organisationen auf einer niedrigeren Stufe
- Mehrere NLA-Ebenen möglich

Site-Level Aggregation, SLA
- Individuelle Adressierungs-hierarchie einer einzelnen Organisation

IPv6-Adressen: Spezielle Unicast-Adressen

Lokale Unicast-Adressen
- Link-lokal für Konfigurationszwecke oder IP-Netze ohne Router
- Standort-lokale für noch nicht an das Internet angeschlossene IP-Netze, einfach rekonfigurierbar

Kompatible Unicast-Adressen
- IPv4-kompatibel: Präfix (96 „0”-Bits) + IPv4-Adresse
- IPv4-mapped: Präfix (80 „0”-Bits + 16 „1”-Bits) + IPv4-Adresse
- IPX-kompatibel oder OSI-kompatibel

Unspezifizierte Adresse
- 0::0 (oder ::) beim Booten

Loopback-Adresse
- 0::1 (oder ::1) entspricht der IPv4-Adresse 127.0.0.1

IPv6-Adressen: Anycast

- Neuer Adresstyp in IPv6
- Teil des Unicast-Adressraums
- Adressierung einer ganzen Gruppe
  → der am wenigsten belastete / nächste / am besten erreichbare... IP-Knoten antwortet
- Eigener Eintrag in der Routing-Tabelle für jede Anycast-Adresse
- Anycast-Adressierung somit nur für Router relevant
- Anwendungsbeispiel: Verteilung eines Web-Servers auf mehrere physische Knoten

IPv6-Adressen: Multicast

- Alle Router und Endsysteme unterstützen Multicast
- Vordefinierte Multicast-Gruppen für Kontrollfunktionen
- IGMP in ICMPv6 integriert
- Die Multicastadresse enthält zusätzlich
  - *Flags* (Unterscheidung temporär/permanent)
  - *Scope* (Wirkungsgrad/Reichweite des Pakets)

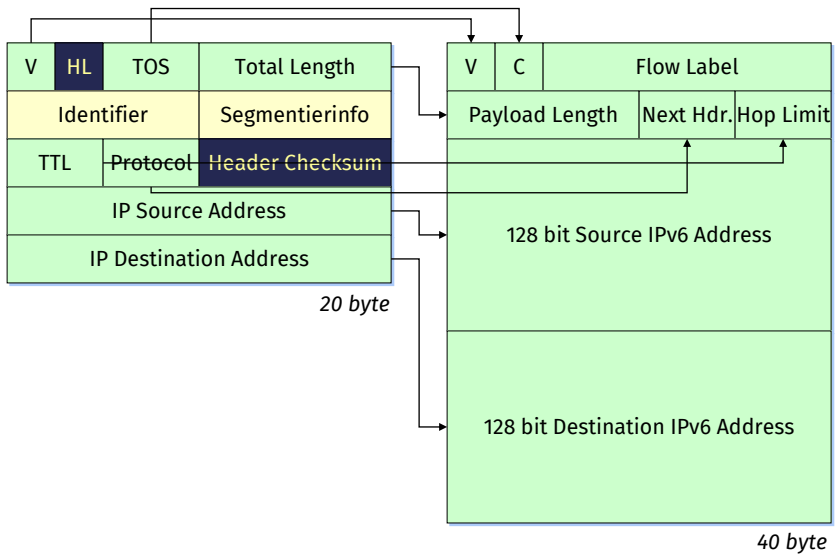
Vergleich der Adressierungsarten in IPv4 und IPv6

Adressierungs-art	*IPv4*	*IPv6*	*Verwendete Schnittstellen*	*Notwendige Auslieferungen*
Unicast	Obligatorisch	Obligatorisch	1	1
Multicast	Optional	Obligatorisch	Gruppe	Alle in der Gruppe
Broadcast	Obligatorisch	—	Alle	Alle
Anycast	—	Obligatorisch	Gruppe	1

68

Paketköpfe – Vergleich zwischen IPv4 und IPv6

V: Version
HL: Header Length
TOS: Type of Service
TTL: Time to Live
C: Class
■ : gelöscht
□ : verschoben



69

IPv6 - Erweiterungspaketköpfe

Verkettung von Erweiterungspaketköpfen (*Extension Headers*)

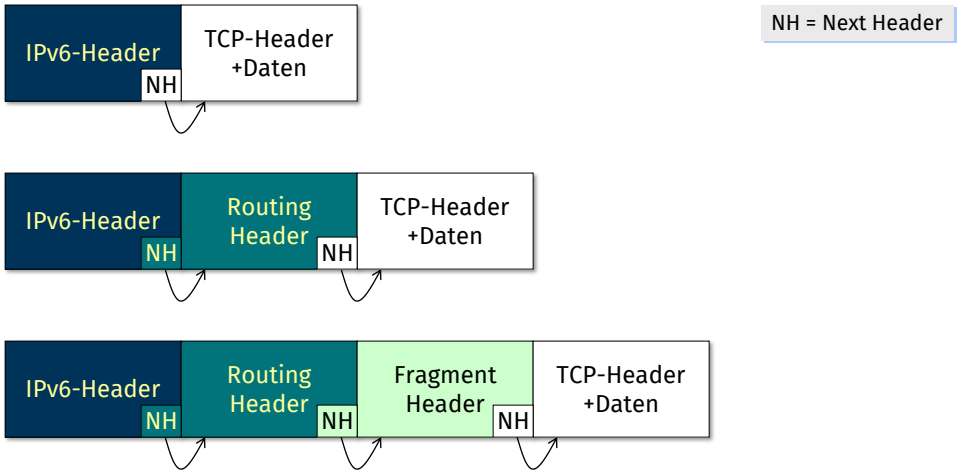
- Kleiner minimaler Paketkopf
- Je nach Anforderungen seitens der Anwendungen und/oder Eigenschaften der Netze Einfügen von Erweiterungspaketköpfen in bestimmter Reihenfolge
- Verkettung einer beliebigen Zahl von Erweiterungspaketköpfen
- Einfache Einführung neuer zukünftiger Erweiterungen und Optionen

Router muss nicht alle Erweiterungspaketköpfe bearbeiten

Aufgaben der Erweiterungspaketköpfe beispielsweise

- Sicherheitsüberprüfung
- Segmentierung
- Source Routing
- Netzmanagement

Beispiele für Erweiterungspaketköpfe

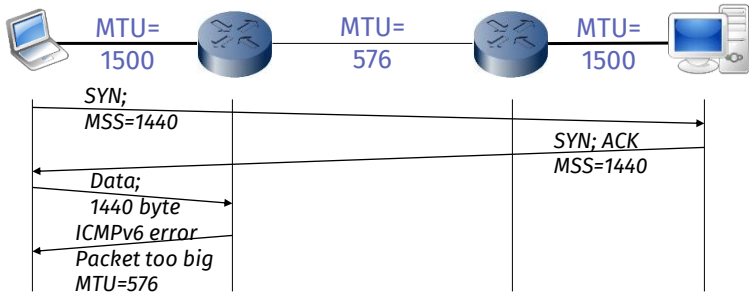


IPv6: Segmentierung

Nur der Sender kann segmentieren

Paket zu groß → Router senden eine ICMPv6-Nachricht „*packet too big*"

Feststellen der maximalen Paketgröße (*Maximum Transfer Unit* MTU) mittels Angabe im ICMPv6-Paket:



IPv6: automatische Adresskonfiguration

„Plug & Play"

- Beschaffung der eigenen IP-Adresse
- Erkennung doppelter IP-Adressen
- Adressauflösung
- Bestimmung von ortsabhängigen Parametern (Subnetz-ID, MTU, DNS-Server, ...)
- Erkennung von Routern
- Unterstützung mobiler Endgeräte

Prinzip der „Nachbarschaftserkennung" (*Neighbor Discovery*)

- Spezielle ICMP-Nachrichten:
  - Router Solicitation/Advertisement
  - Neighbour Solicitation/Advertisement

IPv6: Unterstützung mobiler Knoten

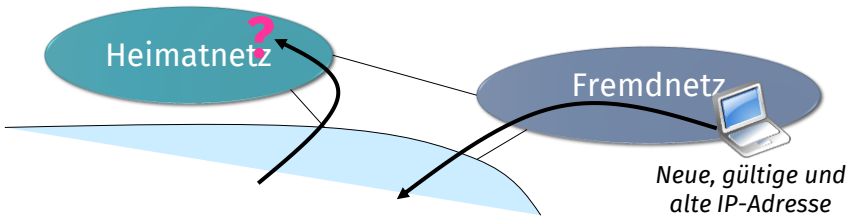
Mobile Rechner ohne Umkonfiguration ihrer IP-Adresse nicht in Fremdnetz betreibbar

Neue gültige IP-Adresse durch Autokonfiguration

Aber: alte IP-Adresse weiterhin gültig, damit sie erreichbar bleiben

Spezielle Architektur für das Weiterleiten von IP-Nachrichten notwendig

→ Spezielles Kapitel zu Internet und Mobilität



74

Allgemeine Sicherheitsziele

Merkformel für Sicherheitsziele:

Vertraulichkeit
- Geheimhaltung der Daten

Integrität
- Unversehrtheit der Daten

Authentizität
- Gesicherte Datenherkunft

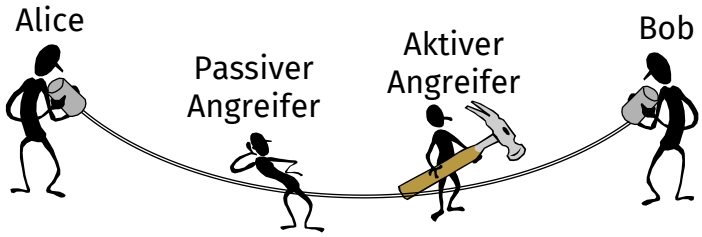
„CIA"
(Confidentiality)
(Integrity)
(Authenticity)

Zusätzliches wichtiges Ziel:

Verbindlichkeit (Non-Repudiability)
- Nichtabstreitbarkeit der Datenherkunft
- wichtig z. B. bei Verträgen

75

Einfaches Modell der Datenübertragung



Passiver Angreifer: kann nur abhören, nicht manipulieren
- Bedrohung für Vertraulichkeit

Aktiver Angreifer: kann abhören, ändern, löschen, duplizieren
- Bedrohung für Vertraulichkeit, Integrität, Authentizität

Bedrohungen

Abhören übertragener Daten

Modifizieren übertragener Daten
- Ändern, Löschen, Einfügen, Umsortieren von Datenblöcken

Maskerade
- Vorspiegeln einer fremden Identität
- Versenden von Nachrichten mit falscher Quelladresse

Unerlaubter Zugriff auf Systeme
- Stichwort „Hacking"

Sabotage (*Denial of Service*)
- gezieltes Herbeiführen einer Überlastsituation
- „Abschießen" von Protokollinstanzen durch illegale Pakete

Angriffstechniken

- Anzapfen von Leitungen oder Funkstrecken
- Zwischenschalten (*man-in-the-middle attack*)
- Wiedereinspielen abgefangener Nachrichten (*replay attack*)
  (z. B. von Login-Nachrichten zwecks unerlaubtem Zugriff)
- gezieltes Verändern/Vertauschen von Bits oder Bitfolgen
  (ohne die Nachricht selbst entschlüsseln zu können)
- Brechen kryptographischer Algorithmen

Gegenmaßnahmen:

- keine selbstgestrickten kryptographischen Algorithmen verwenden,
  sondern nur bewährte und als sicher geltende Algorithmen!
- auf ausreichende Schlüssellänge achten
- Möglichkeiten zum Auswechseln von Algorithmen vorsehen

Sicherheitsdienste

Überwiegend mit kryptographischen Mechanismen:

- **Authentisierung**
  - von Datenpaketen (*data origin authentication*)
  - von Systemen/Benutzern (*entity authentication*)
- **Integritätssicherung** (*integrity protection*)
  - häufig kombiniert mit Datenpaket-Authentisierung
- **Verschlüsselung** (*encryption*)
- **Schlüsselaustausch** (*key exchange*)

Ohne kryptographische Mechanismen:

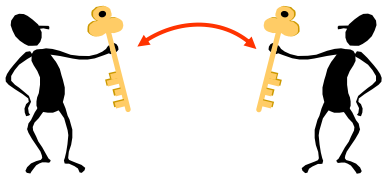
- **Zugriffskontrolle** (*access control*)
- **Einbruchserkennung** (*intrusion detection*)

Symmetrische Kryptographie

Instanzen besitzen gemeinsamen geheimen Schlüssel.

Vorteile:
- geringer Rechenaufwand
- kurze Schlüssel

Nachteile:
- Schlüsselaustausch schwierig
- keine Verbindlichkeit



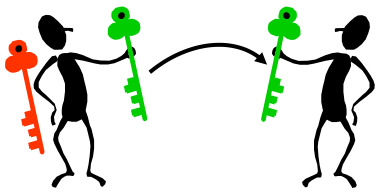
Asymmetrische Kryptographie

Engl. Public-Key-Kryptographie

Schlüsselpaar aus privatem und öffentlichem Schlüssel

Vorteile:
- öffentliche Schlüssel sind relativ leicht verteilbar
- Verbindlichkeit möglich

Nachteile:
- hoher Rechenaufwand
- längere Schlüssel



Hybride Systeme

In der Praxis: **Hybride Systeme**

- Zunächst:
  - Benutzer-Authentisierung und Austausch eines Sitzungsschlüssels (symmetrisch oder assymmetrisch)
- Danach:
  - Authentisierung/Verschlüsselung der Nutzdaten mit Sitzungsschlüssel (symmetrisch)
- Bei langen Sitzungen:
  - Gelegentliches Auswechseln des Sitzungsschlüssels (z. B. stündlich)

IPv6: Sicherheitsvorkehrungen

IPsec

- Sicherheit auch auf IP-Ebene
- Verschlüsselung
- Authentifizierung

Realisierung durch spezielle Erweiterungspaketköpfe

- *Authentication Header*
  - Überprüfung der Datenintegrität
  - Überprüfung der Senderidentität
- *Security Encapsulation Header*
  - Vertraulichkeit
  - Integrität und Authentizität

IPv6 und Multimedia

IPv6 ist für Multimediaströme vorbereitet

- **Flow Label**
  - Pakete mit gleichem Ziel bekommen identisches Label und können so gleichbehandelt werden
- **Priorität**
  - Einstufung der Pakete nach Dringlichkeit
  - Grobe Unterscheidung:
    - Non real time
    - Real time

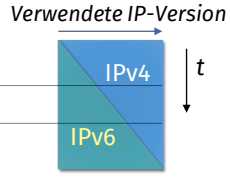
Spezielle Mechanismen in den Routern notwendig

Migration hin zu IPv6

Zurzeit überwiegende Kommunikation mit IPv4

Wie migriert man Millionen von Rechnern hin zu IPv6? [RFC 4213]

- Alle Rechner mit einem Schlag umstellen – nicht möglich
- Langsame, schrittweise Migration auf IPv6 mit zeitweise Co-Existenz beider Standards
- Verfahren
  - Tunneling
  - Dual Stack
  - Protokolltranslation

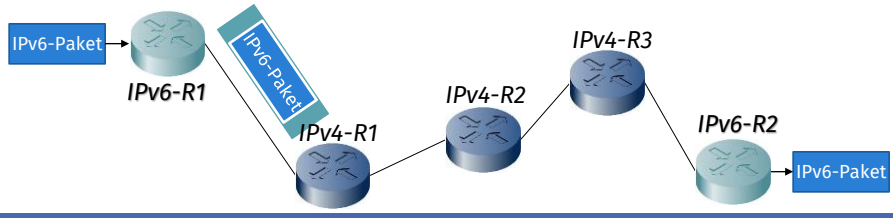


je nach Verbreitungsgrad optimal

Migrationsverfahren: Tunneling

IPv6-Pakete werden in speziellen Routern in IPv4-Pakete eingekapselt und wieder ausgepackt:

- Kommunikation nur zwischen solchen Tunnelendpunkten möglich
- Andere Router bemerken nichts von IPv6
- Automatisch (Zuweisung von IPv4-kompatiblen Adressen) oder konfigurierbar (fest konfigurierte Adressen für Tunnelendpunkte)



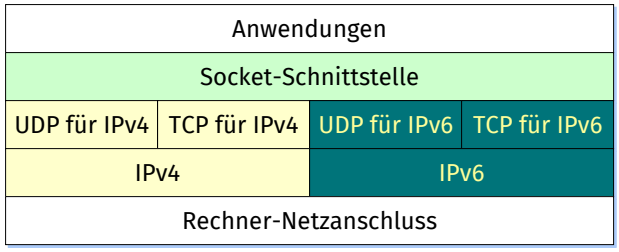
Migrationsverfahren: Dual Stack

Sowohl Endknoten als auch Router verfügen über zwei Protokollstacks: IPv4 und IPv6

Der DNS-Rückgabewert entscheidet, welcher Stack verwendet wird

DNS muss also auch beide Protokolle unterstützen

IPv4-Adressen können so eingespart werden



Migrationsverfahren: Protokolltranslation

Übersetzung von IPv4-Pakete in IPv6-Pakete

Anwendungsschicht muss davon unabhängig bleiben

Beispiele:

- *Stateless IP/ICMP Translator*, SIIT
- *Network Address Translation – Protocol Translation*, NAT-PT
- *Socket-based IPv4/IPv6 Gateway*
- *Bump In The Stack*, BIS

IPv6 in der Praxis

Alle aktuellen Betriebssysteme IPv6-tauglich

Sehr viele Produkte unterstützen den neuen IP-Standard

Aber

- In der Regel wird IPv4 verwendet (Investitionsschutz)
- Ergänzungen zur IPv4-Welt ermöglichen weiterhin den Einsatz der alten Technik
- Anwendungen benötigen (noch) nicht die speziellen Eigenschaften von IPv6

IPv6 kommt immer noch vorrangig in speziellen Forschungsnetzen zum Einsatz

- *6bone* als IPv6-Backbone – mittlerweile abgeschaltet!
- *Internet2* als Entwicklungsplattform

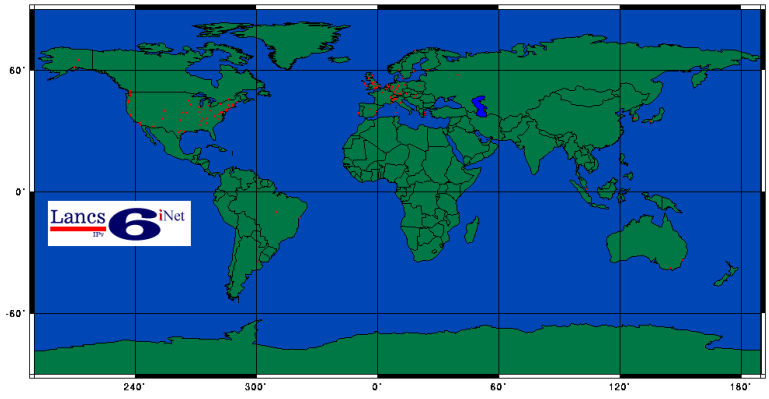
Das 6Bone

Weltweites IPv6-Testnetzwerk

→ Migrationsforschung

Verbindung der IPv6-Hauptknoten über konfigurierte IPv4-Tunnel

Gemäß RFC 3701 ging der vom 6Bone genutzte Adresspräfix am 6. Juni 2006 (06/06/06) zurück an die IANA, womit der Betrieb des 6bone offiziell beendet ist

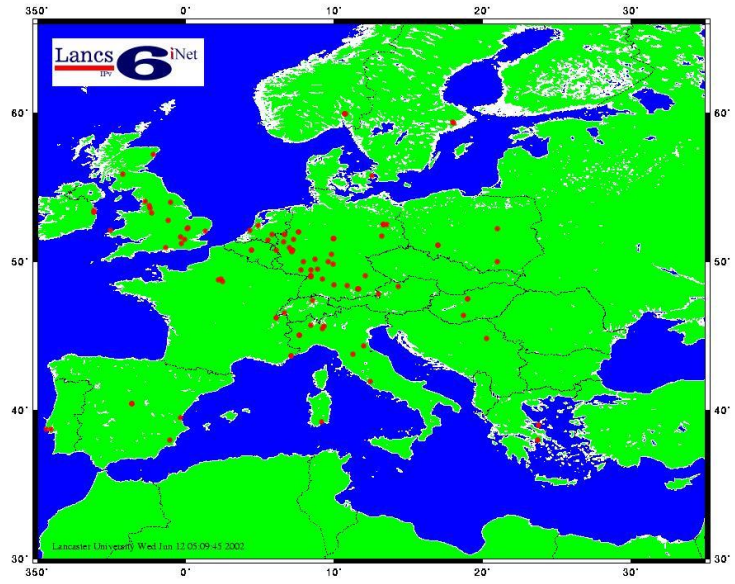


http://www.6bone.org/, Oktober 2016

90

6Bone in Europa

Published by Lancaster University
May 2002



91

Internet 2

Internet 2 (http://www.internet2.org/) Konsortium

- 180 Universitäten
- Industrie
- Regierung

für neue Netzanwendungen und -technologien

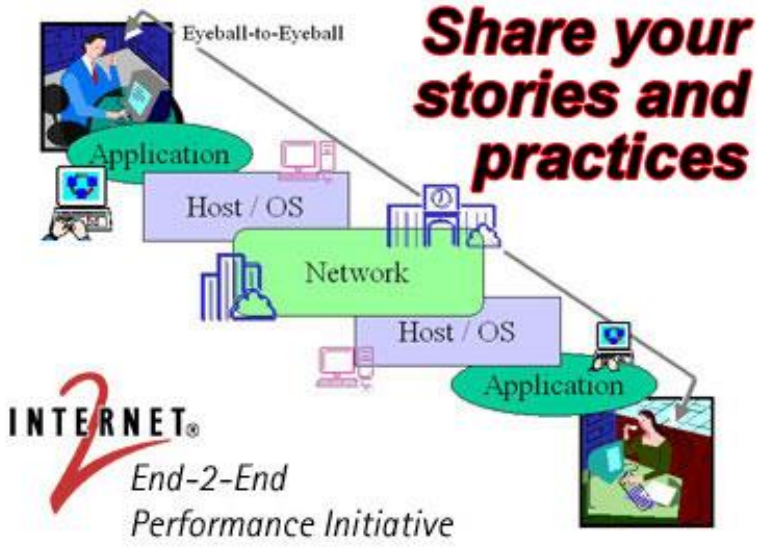
Working Groups:

- *Engineering* (IPv6, Multicast, QoS, Routing, Sicherheit…)
- *Middleware* (PKI, VidMid, MACE (*Middleware Architecture Committee for Education*)…)
- *Anwendungen* (Arts & Humanities, Digital Video, Health Sciences, Veterinary Medical, Voice over IP…)

92

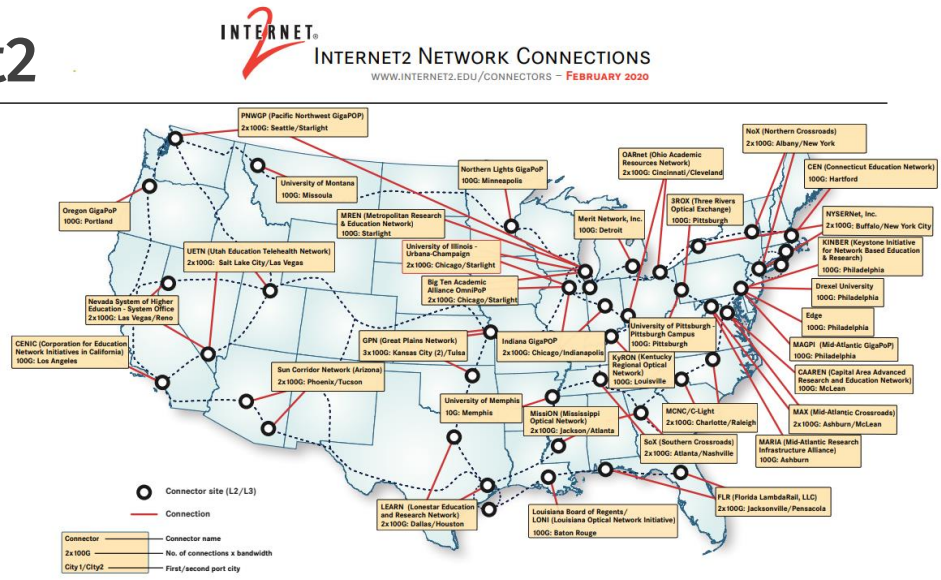
www.internet2.edu

Oktober 2016



93

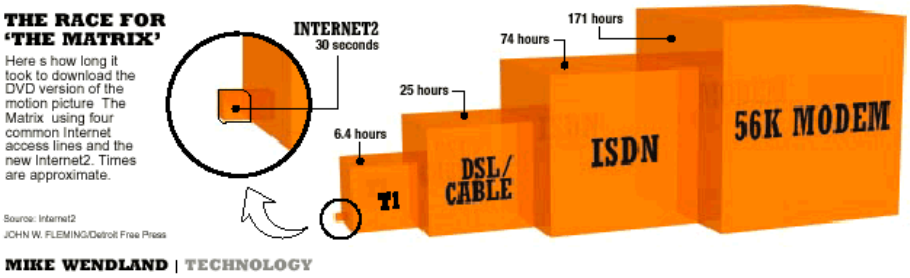
Internet2



www.internet2.edu

94

Download of “The Matrix” DVD (Comparison of the Internet2 Land Speed Record)



www.internet2.edu

95

Literatur

Comer, Douglas E. (2011): *TCP/IP - Studienausgabe. Konzepte, Protokolle, Architekturen*. Heidelberg: mitp.

Debes, Maik; Heubach, Michael; Seitz, Jochen; Tosse, Ralf (2007): *Digitale Sprach- und Datenkommunikation. Netze - Protokolle - Vermittlung*. München: Fachbuchverlag Leipzig im Carl Hanser Verlag.

Hagen, Silvia (2016): *IPv6. Grundlagen - Funktionalität - Integration*. 3., erweiterte und revidierte Ausgabe. Maur: Sunny Connection.

Jarzyna, Dirk (2013): *TCP-IP. Grundlagen, Adressierung, Subnetting*. 1. Auflage. Heidelberg, München, Landsberg, Frechen, Hamburg: mitp.

Kurose, James F.; Ross, Keith W. (2014): *Computernetzwerke. Der Top-Down-Ansatz*. 6., aktualisierte Auflage. Hallbergmoos: Pearson Studium (Pearson Studium - Informatik).

Perlman, Radia (2001): *Bridges, Router, Switches und Internetworking-Protokolle*. 2. Auflage. München, Boston [u.a.]: Addison-Wesley (Net.com).

Stallings, William (2014): *Data and Computer Communications*. 10th edition. Harlow, Essex, England: Pearson Education.

Stevens, W. Richard (2004): *TCP-IP. Der Klassiker: Protokollanalysen, Aufgaben und Lösungen*. 1. Auflage. Bonn: Hüthig.

Requests for Comments (RFC)

Postel, Jon (Hg.) (1981): *Internet Protocol*. Internet Engineering Task Force (IETF) (Request for Comments, 791).

Bradner, Scott; Mankin, Alison (1993): *IP: Next Generation (IPng) White Paper Solicitation*. Internet Engineering Task Force (IETF) (Request for Comments, 1550).

Huitema, Christian (1994): *The H Ratio for Address Assignment Efficiency*. Internet Engineering Task Force (IETF) (Request for Comments, 1715).

Elz, Robert (1996): *A Compact Representation of IPv6 Addresses*. Internet Engineering Task Force (IETF) (Request for Comments, 1924).

Srisuresh, Pyda; Egevang, Kjeld Borch (2001): *Traditional IP Network Address Translator (Traditional NAT)*. Internet Engineering Task Force (IETF) (Request for Comments, 3022).

Durnand, Alain; Huitema, Christian (2001): *The Host-Density Ratio for Address Assignment Efficiency: An Update on the H Ratio*. Internet Engineering Task Force (IETF) (Request for Comments, 3194).

Senie, Daniel (2002): *Network Address Translator (NAT)-Friendly Application Design Guidelines*. Internet Engineering Task Force (IETF) (Request for Comments, 3235).

Fink, Robert L.; Hinden, Robert M. (2004): *6bone (IPv6 Testing Address Allocation) Phaseout*. Internet Engineering Task Force (IETF) (Request for Comments, 3701).

Nordmark, Erik; Gilligan, Robert E. (2005): *Basic Transition Mechanisms for IPv6 Hosts and Routers*. Internet Engineering Task Force (IETF) (Request for Comments, 4213).

Fuller, Vince; Li, Tony (2006): *Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan*. Internet Engineering Task Force (IETF) (Request for Comments, 4632).

Deering, Stephen E.; Hinden, Robert M. (2017): *Internet Protocol, Version 6 (IPv6) Specification*. Internet Engineering Task Force (IETF) (Request for Comments, 8200).