IBM

Dr. Torsten Braun

European Networking Center

Heidelberg

IP next generation

Oktober 1996 - 1

IP Next Generation

Dr. Torsten Braun
IBM European Networking Center
Vangerowstr. 18, D-69115 Heidelberg

Tel.: 06221/59-4352, Fax: 06221/59-3300
Email: braun@heidelbg.ibm.com

Internet Aktuell
Offenbach, 25. November 1996

IBM

Dr. Torsten Braun

European Networking Center

Heidelberg

IP next generation

Oktober 1996 - 2

© IBM Deutschland 1996

Inhalt

IBM

Dr. Torsten Braun

European Networking Center

Heidelberg

Problemstellung

Adressierungsproblem wegen der nach der Jahrtausendwende nicht mehr ausreichenden Anzahl von IP-Adressen:

IP-Adreßraum wird zwischen den Jahren 2000 und 2010 nicht mehr ausreichen.

- 1992: Beginn des IPng (IP next generation) Projekts zur Findung eines Nachfolgers für die aktuelle IP Version 4
- 1994: Entscheidung für SIPP (Simple Internet Protocol Plus)
- 1995: Internet Draft “Internet Protocol, Version 6 (IPv6) Specification“ wird “proposed standard” (9/95), Veröffentlichung als RFC1883 (12/95)

IBM

Dr. Torsten Braun

European Networking Center

Heidelberg

IPv6-Kennzeichen I

- erweiterte Adressierungsmöglichkeiten
  - 128 bit - Adressen (6.65 · 10^{23} Adressen pro m^2 der Erde)
  - Hierarchieebenen (registry, provider, subscriber, subnet, interface)
  - Anycast-Adressen adressieren den “nächsten” Knoten einer Region
- neues Datenformat
  - vereinfachter, minimaler IP Header
  - bessere Unterstützung von neuen Optionen und Erweiterungen
- Dienstgütenunterstützung
  - Flow Labels
  - Prioritäten

Dr. Torsten Braun

European Networking Center

Heidelberg

IPv6-Kennzeichen II

- Multicast-Integration
  - vordefinierte Gruppen für Kontrollfunktionen
  - IGMP (Internet Group Management Protocol) in ICMP (Internet Control Message Protocol) integriert
  - spezielles Adreßformat für Multicast-Adressen
  - alle Router und Endsysteme Multicast-fähig
- automatische Systemkonfiguration
- Unterstützung mobiler Systeme
- Sicherheitsfunktionen
  - Verschlüsselung
  - Authentifizierung

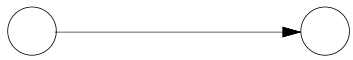
Dr. Torsten Braun

European Networking Center

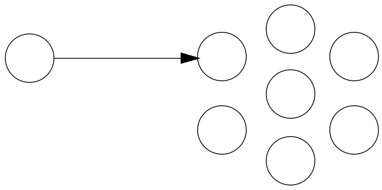
Heidelberg

Adreßtypen

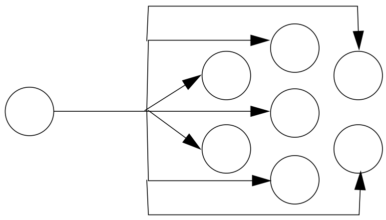
- Unicast -Adressen (1:1)



- Anycast-Adressen
  (1:nächster Knoten, Adressierung von Routern)



- Multicast-Adressen (1:n)



Dr. Torsten Braun

European Networking Center

Heidelberg

Unicast-Adressen

- provider-basiert

3 bit	n bit	m bit	o bit	p bit	125-m-n-o-p bit
010	Registry-ID	Provider-ID	Subscriber-ID	Subnetz-ID	Interface-ID

- geograpisch-basiert
- Link-lokal
  - für Konfigurationsphase oder Netze ohne Router
  - Präfix + Interface-ID (Nummer, MAC-Adresse)
- Standort-lokal
  - für nicht an das Internet angeschlossene IP-Netze
  - Präfix + Subnetz-ID + Interface-ID
- kompatibel (IPv4, IPX, NSAP)
  - IPv4-kompatible Adresse:
    Präfix (96 0-bits) + IPv4-Adresse (32 bits)

Dr. Torsten Braun

European Networking Center

Heidelberg

Multicast-Adressen

- Format:

8bit	4bit	4 bit	112 bit
11111111	flags	scope	Gruppen-ID

- flags: transiente/permanente Adresse
- Gültigkeit (scope):
  Knoten-, Link-, Standort-, Organisations-lokal
- reservierte Multicast-Adressen:
  - All Nodes (Knoten-, Link-lokal)
  - All Routers (Knoten-, Link-lokal)
  - DHCP-Server/Relay-Agent (Link-lokal)
  - Solicited-Node (Link-lokal)
    wird für jede Unicast- und Anycast-Adresse eines Knotens aus einem festgelegten 96-Bit-Präfix und den niederwertigsten 32 Bit der Unicast-/Anycast-Adresse gebildet

Dr. Torsten Braun

European Networking Center

Heidelberg

IPv4 Header

<table>
<tr><td>version</td><td>hdr len</td><td>prec</td><td>TOS</td><td colspan="2">total length</td></tr>
<tr><td colspan="4">identification</td><td>flags</td><td>fragment offset</td></tr>
<tr><td colspan="2">time to live</td><td colspan="2">protocol</td><td colspan="2">header checksum</td></tr>
<tr><td colspan="6">source address</td></tr>
<tr><td colspan="6">destination address</td></tr>
</table>

- 20 Bytes, 13 Felder
- Veränderungen
  - precedence -> priority
  - total length -> payload length
  - time to live -> hop limit
  - protocol -> next header

Dr. Torsten Braun

European Networking Center

Heidelberg

IPv6 Header

<table>
<tr><td>version</td><td>priority</td><td colspan="3">flow label</td></tr>
<tr><td colspan="3">payload length</td><td>next header</td><td>hop limit</td></tr>
<tr><td colspan="5">source address</td></tr>
<tr><td colspan="5">destination address</td></tr>
</table>

- 40 Bytes, 8 Felder

Dr. Torsten Braun
European Networking Center
Heidelberg

Header-Erweiterungen

Verkettung von Header-Erweiterungen
-> Flexibilität
-> einfache Einführung neuer Erweiterungen und Optionen

IPv6 Header next header = TCP	TCP Header+Daten

IPv6 Header next header = Routing	Routing Header next header = TCP	TCP Header+Daten

IPv6 Header next header = Routing	Routing Header next header = Fragment	Fragment Header next header = TCP	TCP Header+Daten (Fragment)

Dr. Torsten Braun
European Networking Center
Heidelberg

Reihenfolge der Header-Erweiterungen

IPv6 header	40 Bytes	next header field
Hop-by-hop options	variabel	
Destination options header	variabel	
Routing header	variabel	
Fragment header	8	
Authentication header	variabel	
Encapsulation security payload header	variabel	
Destination options header	variabel	
TCP header	20 (optionaler, variabler Teil)	
Anwendungsdaten	variabel	

Dr. Torsten Braun

European Networking Center

Heidelberg

IP next generation

Routing-Header

next header	routing type=0	hdr ext len	segments left
reserved	loose/strict bit mask		
address [0]			
address [1]			
...			

- Routing-Header enthält Liste von zu besuchenden Unicast- oder Anycast-Adressen
- vgl. Source-Routing-Option in IPv4

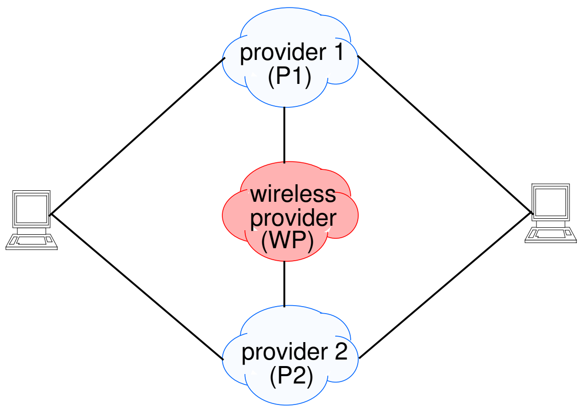
Dr. Torsten Braun

European Networking Center

Heidelberg

IP next generation

Anwendung von Routing Headern



- Fall1: kein Routing Header (H1, H2)
-> beliebiger Provider wird ausgewählt
- Fall 2: H1 sendet Daten für H2 über Provider 1 (H1, P1, H2) mit “strict” Routing
- Fall 3: H1 wird mobil, d.h. Anschluß an Provider WP (H1, WP, P1, H2)

IBM

Dr. Torsten Braun

European Networking Center

Heidelberg

Segmentieren und Reassemblieren

- kein Segmentieren/Reassemblieren durch IPv6-Router
- Vermeiden von Segmentieren und Reassemblieren in den Routern erfordert Vorkehrungen in den Endsystemen
  - Segmentieren in den Endsystemen (Fragment Header)
  - Senden minimaler Link-MTUs
  - Path MTU Discovery
- Link-MTU = maximale Größe einer Übertragungseinheit (MTU: maximum transmission unit) auf einem Link
  - mindestens 576 Oktetts
  - kleinere Segmente (z.B. ATM-Zellen) erfordern Segmentier- und Reassemblierfunktionen auf Link-Ebene
- Path-MTU = Minimum aller Link-MTUs auf dem Pfad zwischen Quell- und Zielknoten

IBM

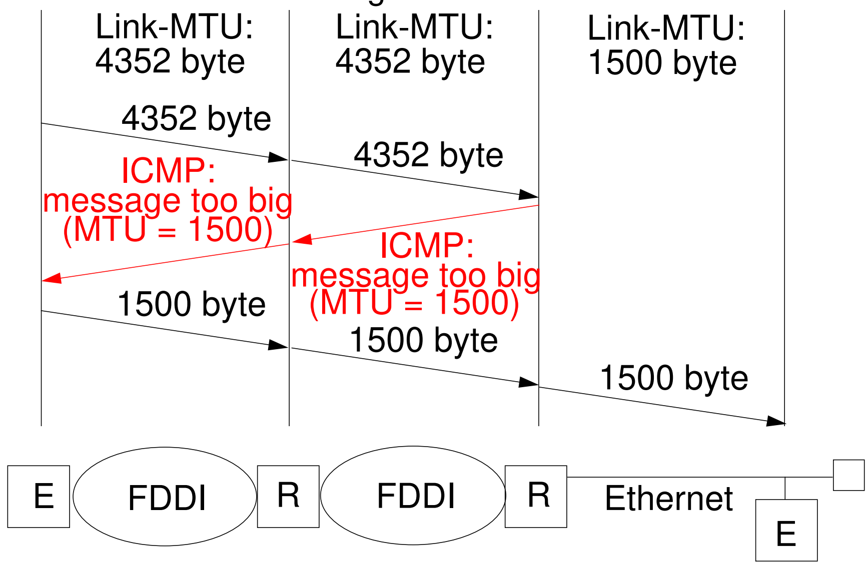
Dr. Torsten Braun

European Networking Center

Heidelberg

Path MTU Discovery

1. Senden der Pakete mit der Länge der Link-MTU
2. “packet too big”-ICMP-Nachrichten bei zu langen Paketen
3. Reduzieren der Paketlänge



IBM

Dr. Torsten Braun

European Networking Center

Heidelberg

Prioritäten

- 2 unabhängige Prioritätsbereiche:
  - Verkehrsarten mit Staukontrolle (z.B. TCP-Verkehr) Werte: 0-7 (s. Tabelle)
  - Verkehrsarten ohne Staukontrolle (z.B. Realzeitdaten-verkehr), Werte: 8-15 zur Anzeige einer Wegwerfpriorität

Wert	Verkehrsart
0	nicht näher charakterisierter Verkehr
1	Füllverkehr (z.B. news)
2	Datenverkehr ohne spezielle Behandlung (z.B. electronic mail)
3	reserviert
4	Datenverkehr mit spezieller Behandlung (z.B. ftp, NFS)
5	reserviert
6	interaktiver Verkehr (z.B. telnet, X)
7	Kontrollverkehr (z.B. Routing-Protokolle, ICMP)

IBM

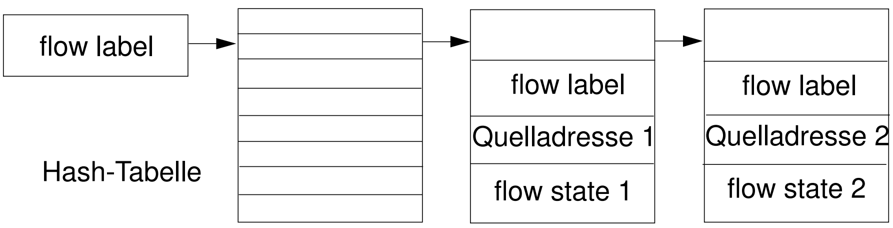
Dr. Torsten Braun

European Networking Center

Heidelberg

IPv6 Flows

- Flow = “a sequence of packets for which the source desires non-default or real-time service”
- Eindeutige Kennzeichnung von Datenflüssen zwischen Endsystemen durch Quelladresse und zufälligen Flow Label (-> Hashing)



- Beispiele für flow state
  - nächster Knoten
  - Information über zu unterstützende Dienstgüte des Flows

Dr. Torsten Braun

European Networking Center

Heidelberg

Flow Behandlung

- Spezielle Verarbeitung der Pakete eines Flows
  - Dienstgütenunterstützung
  - Mitteilung der Art der Behandlung über
    - spezielle Paket-Optionen (z.B. hop-by-hop-Optionen) oder
    - Ressourcenreservierungsprotokolle (z.B. RSVP)
- Vereinfachte Paketverarbeitung
  - Ergebnisse werden durch vollständige Verarbeitung des 1. Paket eines Flows berechnet und für folgende Pakete verwendet
  - Pakete eines Flows müssen gleiche Formate besitzen
  - Flow Labels sind 6 Sekunden gültig, danach Ergebnisauffrischung

Dr. Torsten Braun

European Networking Center

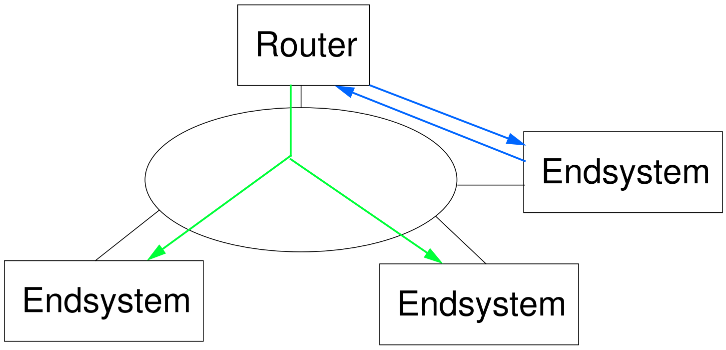
Heidelberg

Neighbor Discovery Funktionen I

- **Router Solicitation**: Aufforderung an All-Routers-Multicast-Adresse Router Advertisement-Pakete zu senden
- **Router Advertisement**: periodisch an All-Nodes-Multicast-Adresse oder an Quelle der Aufforderung gesendetes Paket mit Präfix-Werten, Link- und Internet-spezifischen Informationen, Anzeige zustandslose/-behaftete Konfiguration etc.
- Funktionen
  - Erkennung angeschlossener Router
  - Erkennung Link-lokaler Präfix-Werte sowie Link-lokaler und Internet-spezifischer Parameter wie z.B. MTU-Größe und max. Hop-Limit
  - zustandslose automatische Adreßkonfiguration (Kombination von Präfix-Werten und Link-lokaler Unicast-Adresse)
  - Bestimmung des nächsten Knotens durch Präfix-Vergleich

Plug-and-Play

- IPv4: Konfiguration der Endsysteme mit verschiedenen IP-Parametern (IP-Adresse, Subnetz-Maske, Default-Gateway)
- IPv6: Router teilt Parameter periodisch mit (Router Advertisement an alle Endsysteme) oder Endsystem fordert diese explizit an (Router Solicitation an fest-definierte Router-Multicast-Adresse)
- Endsystem verwendet in der Initialisierungsphase Link-lokale Adresse bestehend aus festem Präfix und Interface-ID (z.B. MAC-Adresse)

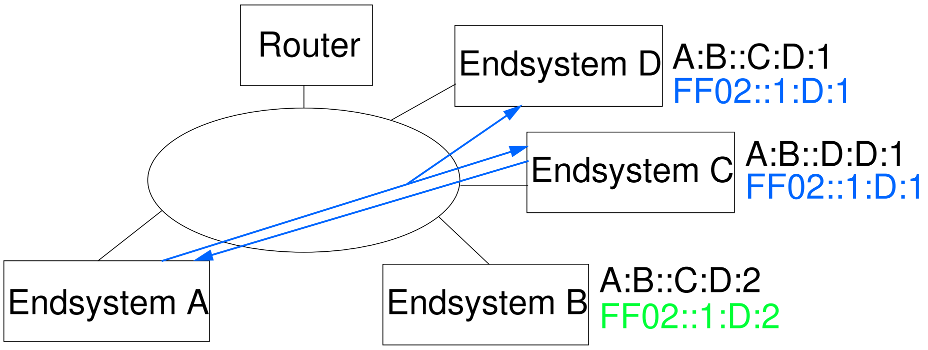


Neighbor Discovery Funktionen II

- **Neighbor Solicitation**: an Solicited-Nodes-Multicast-Adresse oder Unicast-Adresse gesendetes Paket
- **Neighbor Advertisement**: gezielte Antwort auf Neighbor-Solicitation-Paket oder Ankündigung einer Änderung der Link-Adresse an All-Nodes-Multicast-Adresse
- Funktionen
  - Erkennung von Adreßduplikaten durch entsprechende Antworten auf Neighbor-Solicitation-Pakete an die Solicited-Nodes-Multicast-Adresse
  - Erreichbarkeitsbestimmung
  - Adreßauflösung, d.h. Bestimmen der Link-Adresse bei bekannter IP-Adresse durch Senden eines Neighbor-Solicitation-Pakets an die Solicited-Nodes-Multicast-Adresse (vgl. Address Resolution Protocol, ARP)
- **Redirect**-Funktion, d.h. Mitteilen von günstigeren nächsten Knoten auf dem Weg zum Ziel

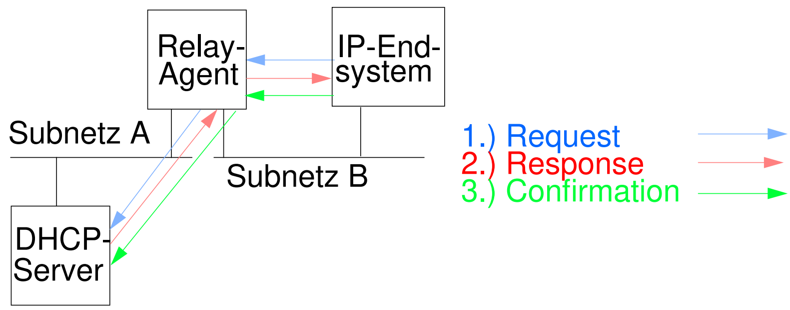
Broadcast-Vermeidung bei Adreßauflösung

- IPv4: Broadcast des ARP_Request, gesuchter Knoten antwortet mit ARP_Reply
- IPv6: Multicast des Neighbor Solicitation an kleine lokale Gruppe (Solicited-Nodes-Multicast-Adresse), Solicited Nodes-Multicast-Gruppe besitzt Mitglieder mit identischen niederwertigen 32 bits (meist 32 bits der MAC-Adresse)
- Gesuchter Knoten antwortet mit Neighbor Advertisement



Dynamic Host Configuration Protocol (DHCPv6)

- zustandsbehaftete Adreßkonfiguration (Client/Server-Konzept)
- Relay-Agenten vermitteln Nachrichten zwischen Client und DHCP-Server, falls kein DHCP-Server am lokalen Link



- Anforderung von IP-Adressen oder Host-Namen durch Request-Paket an Link-lokale DHCP-Server/Relay-Agenten-Multicast-Adresse -> Antwort im Response-Paket
- Begrenzte Gültigkeit von Adressen und Namen

IBM

Dr. Torsten Braun

European Networking Center

Heidelberg

Authentifizierung

- Überprüfung, ob der angegebene Sender das Paket auch tatsächlich gesendet hat
- Überprüfung, ob die gesendeten Daten manipuliert wurden
- Default-Algortihmus: Message Digest 5 (MD5)
  Berechnung einer 128-bit-Kennung im aus dem zu sendenden Paket und einem Schlüssel (-> authentication data)

next header	length	reserved
security parameter index (SPI)		
authentication data (n * 32 Bit)		

- SPI und Zieladresse identifizieren die etablierte Security-Assoziation
- Parameter der Security-Assoziation: Schlüssel, Algorithmus, Lebenszeit, Quelladresse, Sicherheitsstufe usw.

IBM

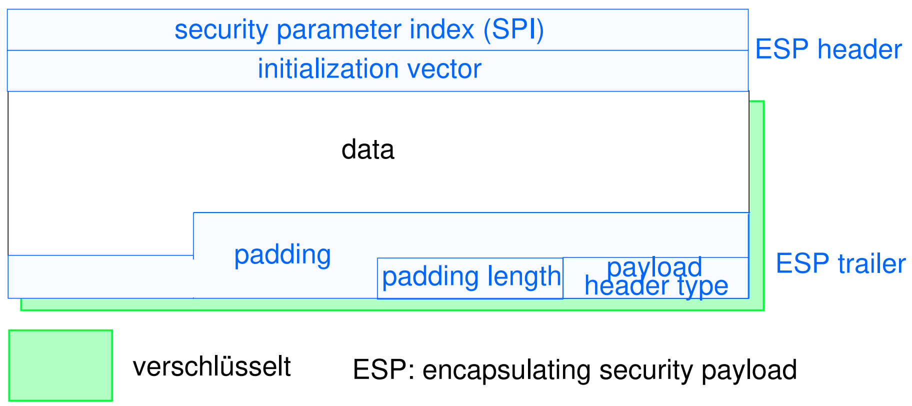
Dr. Torsten Braun

European Networking Center

Heidelberg

Verschlüsselung

- Paket wird für vertraulichen, abhörsicheren Datenaustausch verschlüsselt
- DES-CBC als Default-Algorithmus
- Initialisierungsvektor (n * 32 bit):
  Input für Verschlüsselungsalgorithmus
- Payload header type:
  Protokolltyp des Datenfelds (z.B. IP, TCP, UDP)



Dr. Torsten Braun

European Networking Center

Heidelberg

Verschlüsselungsmöglichkeiten

- Tunnel-Modus
  Einkapselung eines gesamten IP-Pakets mit neuem IP-Header
- Transport-Modus
  Ende-zu-Ende-Erweiterungs-Header und Transportprotokoll-Paket bilden Nutzlast des Verschlüsselungs-Pakets

Transport-Modus

IPv6 Header + Erweiterungs-Header
ESP-Header
Ende-zu-Ende-Erweiterungs-Header
Transport Header
Daten
ESP Trailer

Tunnel-Modus

IPv6 Header + Erweiterungs-Header
ESP-Header
IPv6-Header + Erweiterungs-Header
Transport-Header
Daten
ESP-Trailer

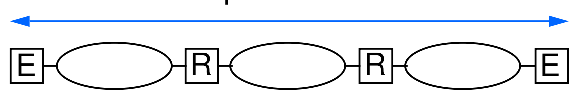
Dr. Torsten Braun

European Networking Center

Heidelberg

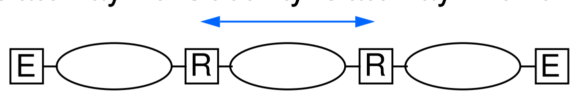
Anwendung von Verschlüsselung

- Ende-zu-Ende mit Transport-Modus



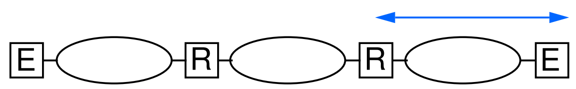
z.B. für vertraulichen Datenaustausch zwischen 2 Teilnehmern

- Security-Gateway-zu-Security-Gateway mit Tunnel-Modus



z.B. für Datenaustausch über unsichere Netze (Kopplung von Firmennetzen über das Internet)

- Ende-zu-Security-Gateway mit Tunnel-Modus



z.B. Verschlüsselung auf unsicherem Zugangsnetz (Zugriff über Funknetz auf Firmennetz)

IBM

Dr. Torsten Braun

European Networking Center

Heidelberg

Übergangsstrategien

- Auslaufen der IPv4-Adressen frühestens im Jahr 2000
- Betriebssysteme werden in Zyklen von ca. 3 Jahren gewechselt.
- IPv6-Implementierungen kommen 1996/1997 auf den Markt
- 2 Zyklen zum Übergang
- In der Übergangsphase sollen IPv4-Knoten und IPv6-Knoten miteinander kommunizieren können.
- Nach der Übergangsphase werden nur noch sehr wenige IPv4-Knoten betrieben.
- 2 Strategien werden derzeit als ausreichend betrachtet
  - doppelte Protokollstacks
  - IPv6 in IPv4 - Tunneling
- Header Translation ist nur notwendig, wenn alte IPv4-Knoten mit neuen (reinen) IPv6-Knoten kommunizieren wollen.

IBM

Dr. Torsten Braun

European Networking Center

Heidelberg

© IBM Deutschland 1996

Doppelte Protokollstacks

- doppelte Stacks
  - UDP/IPv4 und UDP/IPv6
  - TCP/IPv4 und TCP/IPv6
- IPv6 als zusätzliche Protokollfamilie
- In der Übergangsphase haben alle IPv6-Knoten auch einen IPv4-Protokollstack

Applikation	
Sockets	
TCP für IPv4	TCP für IPv6
IPv4	IPv6
Netz	

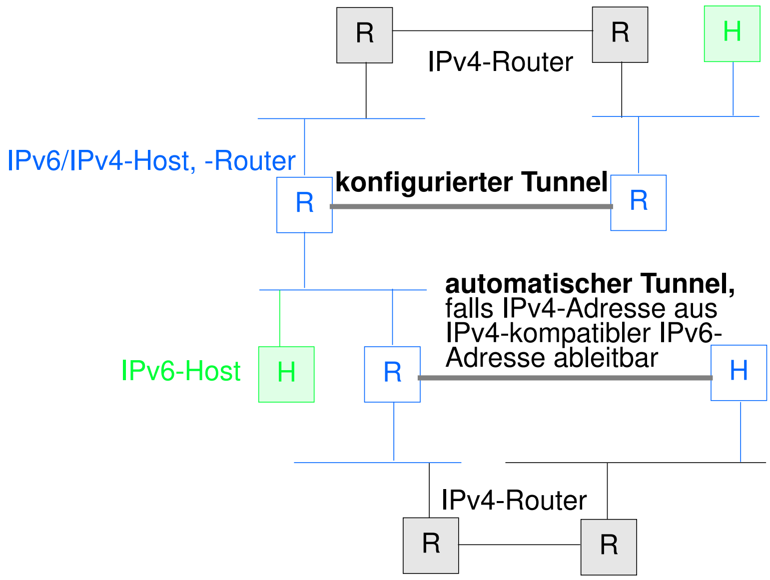
Dr. Torsten Braun

European Networking Center

Heidelberg

Tunnel-Technik

- Tunnel-Technik zur Überbrückung der IPv4-Welt
- IPv6-Paket wird in IPv4-Paket eingekapselt, IPv4-Adresse wird automatisch oder durch Konfiguration ermittelt



Dr. Torsten Braun

European Networking Center

Heidelberg

Auswirkungen auf andere Protokolle

- Änderung der Anwendungen wegen modifizierter Socket API erforderlich
- TCP
  - Modifizierter IP-Pseudo-Header erfordert Modifikation der Prüfsummenberechnung in UDP- und TCP-Implementierungen
  - TCP erlaubt derzeit keine Änderung der IP-Adresse während einer Verbindung
  - selektive Übertragungswiederholung ?
- Routing-Protokolle
  - Anpassungen an neues Adreßformat
- Domain Name System (DNS)
  - Unterstützung der IPv6-Adressen
  - dynamisches DNS

Referenzen

- http://playground.sun.com/ipng
- http://www.computermethods.com/ipng/IPng.htm
- http://www.ietf.cnri.reston.va.us/html.charters/ipngwg-charter.html
- http://www.iol.unh.edu/interop/ip/htmls/info1.html
- C. Huitema: IPv6 The New Internet Protocol, Prentice Hall, 1996
- T. Braun: Die Internet-Protokollfamilie der nächsten Generation, “Praxis der Informationsverarbeitung und Kommunikation” (PIK), 2/1996
- W. Stallings: IPv6: The New Internet Protocol, IEEE Communications Magazine, July 1996, pp. 96-108
- R. Hinden: IP Next Generation Overview, Communications of the ACM, June 1996, pp. 61-71