Dr. Torsten Braun

braun@heidelbg.ibm.com

IBM European Networking Center
Heidelberg

Online ’96, 5./6.2.-9.2.1996 Hamburg

IPng: Das Internet-Protokoll der nächsten Generation

Dr. Torsten Braun

braun@heidelbg.ibm.com

IBM European Networking Center
Vangerowstr. 18
D-69115 Heidelberg

Dr. Torsten Braun

braun@heidelbg.ibm.com

IBM European Networking Center
Heidelberg

Überblick

- Problemstellung
- Internet Protocol Version 6
  - Adressierung
  - Paketformat
  - Segmentieren und Reassemblieren
  - Dienstgütenunterstützung (Prioritäten, Flow-Konzept)
- Automatische Systemkonfiguration
  - Neighbor Discovery
  - Dynamic Host Configuration Protocol
- Sicherheitsaspekte
  - Authentifizierung
  - Verschlüsselung
- Mobilitätsunterstützung
- Übergangsstrategien
- Ausblick

/u/braun/trans/online/online_f.doc; created on October 17, 1995; last modified on January 16, 1996

Dr. Torsten Braun

braun@heidelbg.ibm.com

IBM 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 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” (18.9.95), Veröffentlichung als RFC1883

/u/braun/trans/online/online_f.doc; created on October 17, 1995; last modified on January 16, 1996

Dr. Torsten Braun

braun@heidelbg.ibm.com

IBM European Networking Center
Heidelberg

IPng/IPv6-Kennzeichen

- erweiterte Adressierungsmöglichkeiten
  - 128 bit - Adressen ($6.65 \cdot 10^{23}$ Adressen pro m^2 der Erde)
  - Hierarchieebenen (registry, provider, subscriber, subnet, interface)
  - Anycast-Adressen adressieren den “nächsten” Knoten einer Region
- vereinfachter, minimaler IP Header
- bessere Unterstützung von neuen Optionen und Erweiterungen
- Dienstgütenunterstützung
  - Flow Labels
  - Prioritäten
- Multicast-Integration
  - vordefinierte Gruppen für Kontrollfunktionen
  - IGMP (Internet Group Management Protocol) in ICMP (Internet Control Message Protocol) integriert
  - spezielles Adreßformat für Multicast-Adressen
- automatische Systemkonfiguration
- Unterstützung mobiler Systeme
- Sicherheitsfunktionen (Verschlüsselung und Authentifizierung)

Dr. Torsten Braun

braun@heidelbg.ibm.com

IBM European Networking Center
Heidelberg

Adreßtypen

- Unicast-Adressen (1:1)
  - provider-basiert
  - geograpisch-basiert
  - Link-lokal
  - Standort-lokal
  - kompatibel (IPv4, IPX, NSAP)
- Anycast-Adressen (1:nächster Knoten)
- Multicast-Adressen (1:n)

Adreßtyp	Präfix	Anteil am Adresraum
reserviert (z.B. für Loopback-, IPv4-kompatible Adressen)	0000 0000	1/256
NSAP-Adressen	0000 001	1/128
IPX-Adressen	0000 010	1/128
Provider-basierte Unicast-Adressen	010	1/8
Geographisch-basierte Unicast-Adressen	100	1/8
Link-lokale Unicast-Adressen	1111 1110 10	1/1024
Standort-lokale Unicast-Adressen	1111 1110 11	1/1024

/u/braun/trans/online/online_f.doc; created on October 17, 1995; last modified on January 16, 1996

Dr. Torsten Braun

braun@heidelbg.ibm.com

IBM European Networking Center
Heidelberg

Adreßformate

Provider-basierte Unicast-Adressen

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

Multicast-Adressen

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

- flags: transiente/permanente Adresse
- scope: Knoten-, Link-, Standort-, Organisations-lokale Gültigkeit
- reservierte Multicast-Adressen:
    - All Nodes (Knoten-, Link-lokal)
    - All Routers (Knoten-, Link-lokal)
    - DHCP-Server/Relay-Agent (Link-lokal)
    - Solicited-Node (Link-lokal, für jede Unicast- und Anycast-Adresse eines Knotens)

/u/braun/trans/online/online_f.doc; created on October 17, 1995; last modified on January 16, 1996

Dr. Torsten Braun

braun@heidelbg.ibm.com

IBM 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>

precedence -> priority

total length -> payload length

time to live -> hop limit

protocol -> next header

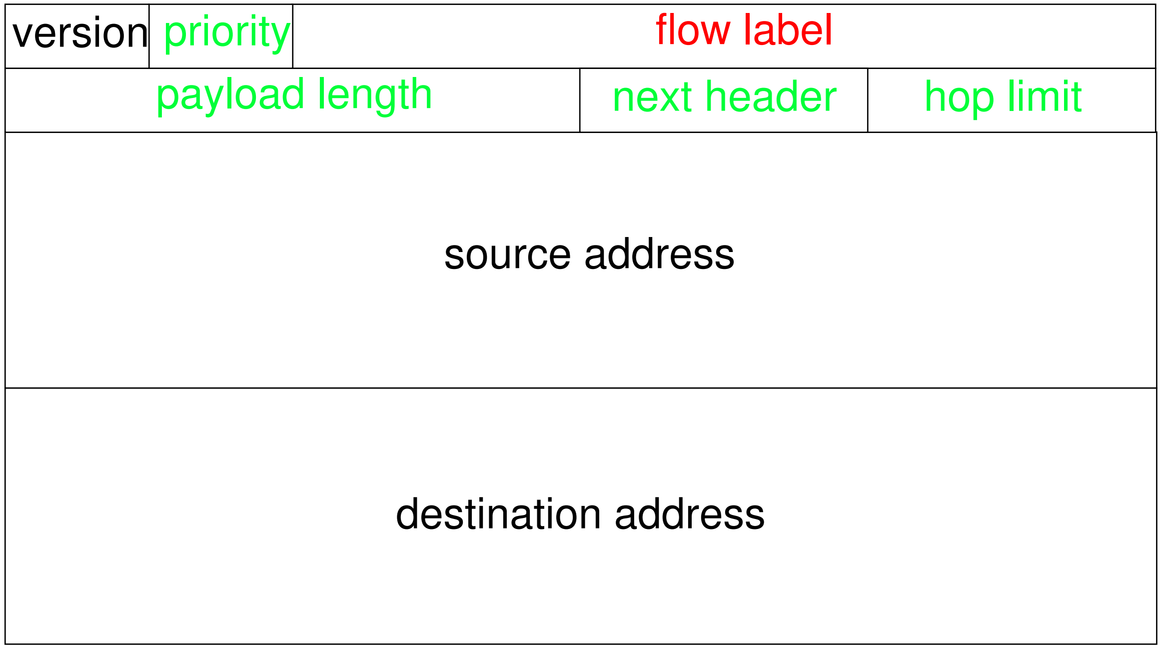
/u/braun/trans/online/online_f.doc; created on October 17, 1995; last modified on January 16, 1996

Dr. Torsten Braun

braun@heidelbg.ibm.com

IBM European Networking Center
Heidelberg

IPv6 Header



Dr. Torsten Braun

braun@heidelbg.ibm.com

IBM European Networking Center
Heidelberg

Header-Erweiterungen

IPv6 Header	TCP Header+Daten
next header = TCP	

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

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

- Hop-by-hop-Optionen
- Ziel-Optionen zur Verarbeitung im ersten durch die IPv6-Zieladresse gekennzeichneten Zielknoten und in den im Routing-Header angegebenen Knoten
- Routing-Header
- Fragment-Header
- Authentifizierungs-Header
- Verschlüsselungs-Header
- Ziel-Optionen zur Verarbeitung im endgültigen Zielknoten

IPng

Dr. Torsten Braun

braun@heidelbg.ibm.com

IBM European Networking Center
Heidelberg

Routing-Header

next header	routing type	num addrs	next addr
reserved	loose/strict bit mask		
address [0]			
address [1]			
...			

Routing-Header enthält Liste von zu besuchenden Unicast- oder Anycast-Adressen

/u/braun/trans/online/online_f.doc; created on October 17, 1995; last modified on January 16, 1996

Dr. Torsten Braun

braun@heidelbg.ibm.com

IBM European Networking Center
Heidelberg

Segmentieren und Reassemblieren

Link-MTU

maximale Größe einer Übertragungseinheit
(MTU: maximum transmission unit) auf einem Link

Path-MTU

Minimum aller Link-MTUs auf dem Pfad zwischen Quell- und Zielknoten

- kein Segmentieren/Reassemblieren durch IPv6-Router
- Link-MTU mindestens 576 Oktetts
- kleinere Segmente (z.B. ATM-Zellen) erfordern Segmentier- und Reassemblierfunktionen auf Link-Ebene
- Vermeiden von Segmentieren und Reassemblieren in den Endsystemen durch
    - Senden minimaler Link-MTUs oder
    - Path MTU Discovery

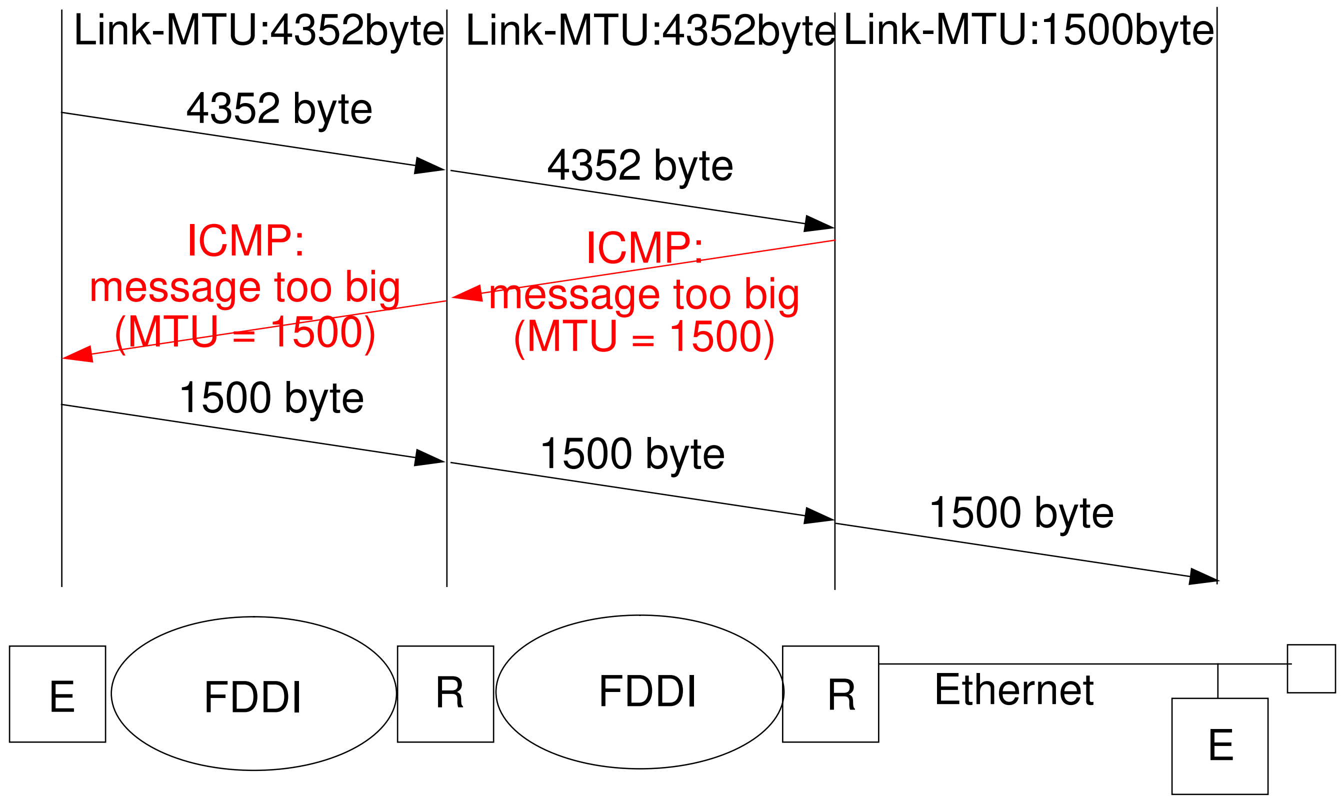
Dr. Torsten Braun

braun@heidelbg.ibm.com

IBM 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



/u/braun/trans/online/online_f.doc; created on October 17, 1995; last modified on January 16, 1996

Dr. Torsten Braun

braun@heidelbg.ibm.com

IBM 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. Realzeitdatenverkehr)
  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)

Dr. Torsten Braun

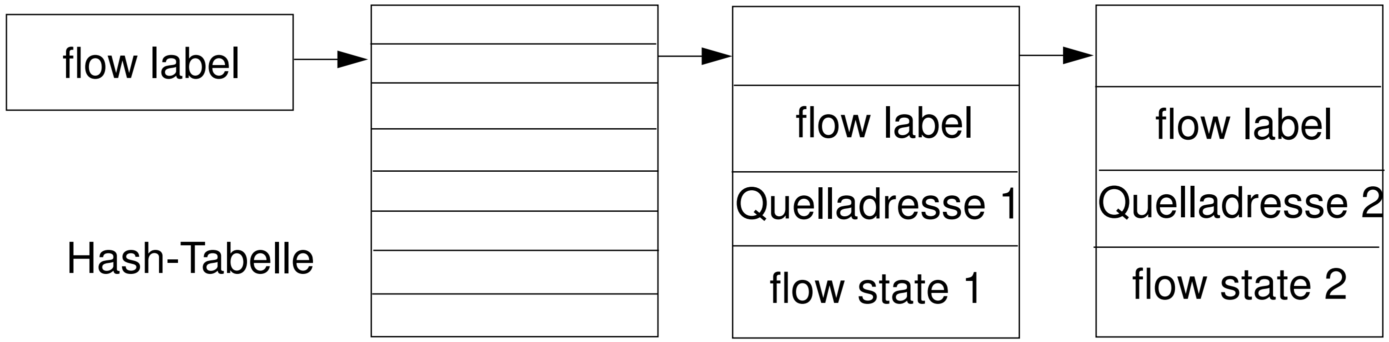
braun@heidelbg.ibm.com

IBM European Networking Center
Heidelberg

IPv6 Flows

"a sequence of packets for which the source desires non-default or real-time service"

Identifikation durch Quelladresse und zufälligen Flow Label (-> Hashing)



Spezielle Verarbeitung der Pakete eines Flows

- Unterstützung von Dienstgüten
  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

/u/braun/trans/online/online_f.doc; created on October 17, 1995; last modified on January 16, 1996

Dr. Torsten Braun

braun@heidelbg.ibm.com

IBM European Networking Center
Heidelberg

Neighbor Discovery Paketformate

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

Neighbor Solicitation

an Solicited-Hosts-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

Redirect

Informationen über einen besseren ersten Knoten für einen bestimmten Zielknoten

/u/braun/trans/online/online_f.doc; created on October 17, 1995; last modified on January 16, 1996

Dr. Torsten Braun

braun@heidelbg.ibm.com

IBM European Networking Center
Heidelberg

Neighbor Discovery Funktionen

Router Solicitation/Advertisement

- Erkennung der angeschlossenen Router
- Erkennung der Link-lokalen Präfix-Werte
- Bestimmung des nächsten Knotens durch Präfix-Vergleich
- Erkennung der Link-lokalen und der Internet-spezifischen Parameter (z.B. MTU-Größe und max. Hop-Limit)
- zustandslose automatische Adreßkonfiguration
  (Kombination von Präfix-Werten und Link-lokaler Unicast-Adresse)

Neighbor Solicitation/Advertisement

- Erkennung von Adreßduplikaten durch entsprechende Antworten auf Neighbor-Solicitation-Pakete an die Solicited-Node-Multicast-Adresse
- Erreichbarkeitsbestimmung
- Adreßauflösung
  Bestimmen einer Link-Adresse, falls nur die IP-Adresse bekannt ist (vgl. Address Resolution Protocol, ARP) durch Senden eines Neighbor-Solicitation-Pakets an die Solicited-Node-Multicast-Adresse

Redirect

- Redirect-Funktion zum Lernen von günstigeren nächsten Knoten auf dem Weg zum Ziel

/u/braun/trans/online/online_f.doc; created on October 17, 1995; last modified on January 16, 1996

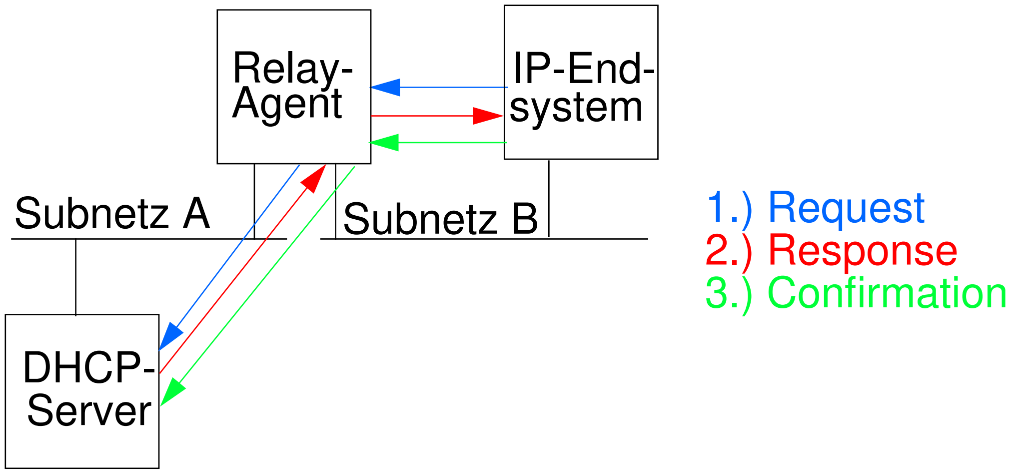
Dr. Torsten Braun

braun@heidelbg.ibm.com

IBM European Networking Center
Heidelberg

Dynamic Host Configuration Protocol (DHCPv6)

- zustandsbehaftete Adreßkonfiguration basierend auf Client/Server-Konzept
- Relay-Agenten vermitteln die Nachrichten zwischen Client und DVCP-Server, falls am lokalen Link kein DHCP-Server angeschlossen ist.



- Austausch von 3 Pakettypen:
  - Anforderung von IP-Adressen oder Host-Namen durch Request-Paket an die Link-lokale DHCP-Server/Relay-Agenten-Multicast-Gruppe
  - angeforderte Informationen in Response-Paket
  - Bestätigung durch Confirmation-Paket
- Adressen und Namen haben eine begrenzte Gültigkeit

/u/braun/trans/online/online_f.doc; created on October 17, 1995; last modified on January 16, 1996

Dr. Torsten Braun

braun@heidelbg.ibm.com

IBM European Networking Center
Heidelberg

Authentifizierung

- Überprüfung, ob der angegebene Sender das Paket auch tatsächlich gesendet hat
- Überprüfung, ob die gesendeten Daten manipuliert wurden
- Berechnung einer 128-bit-Kennung im Authentifizierungs-Header aus dem zu sendenden Paket und einem Schlüssel bei Verwendung des Default-Algorithmus Message Digest 5 (MD5)

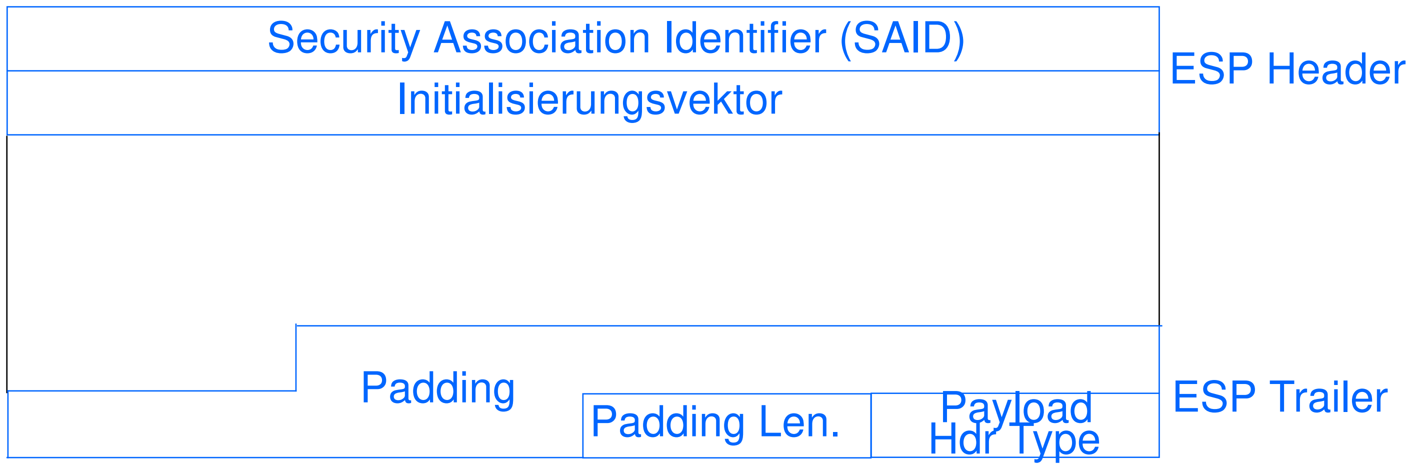
Dr. Torsten Braun

braun@heidelbg.ibm.com

IBM European Networking Center
Heidelberg

Verschlüsselung

- Paket wird für einen vertraulichen, abhörsicheren Datenaustausch verschlüsselt (DES-CBC als Default-Algorithmus)
  - 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
- Verschlüsselungsmöglichkeiten
  - Ende-zu-Ende mit Transport-Modus
  - Ende-zu-Security-Gateway mit Tunnel-Modus
  - Security-Gateway-zu-Security-Gateway mit Tunnel-Modus



ESP: encapsulating security payload

/u/braun/trans/online/online_f.doc; created on October 17, 1995; last modified on January 16, 1996

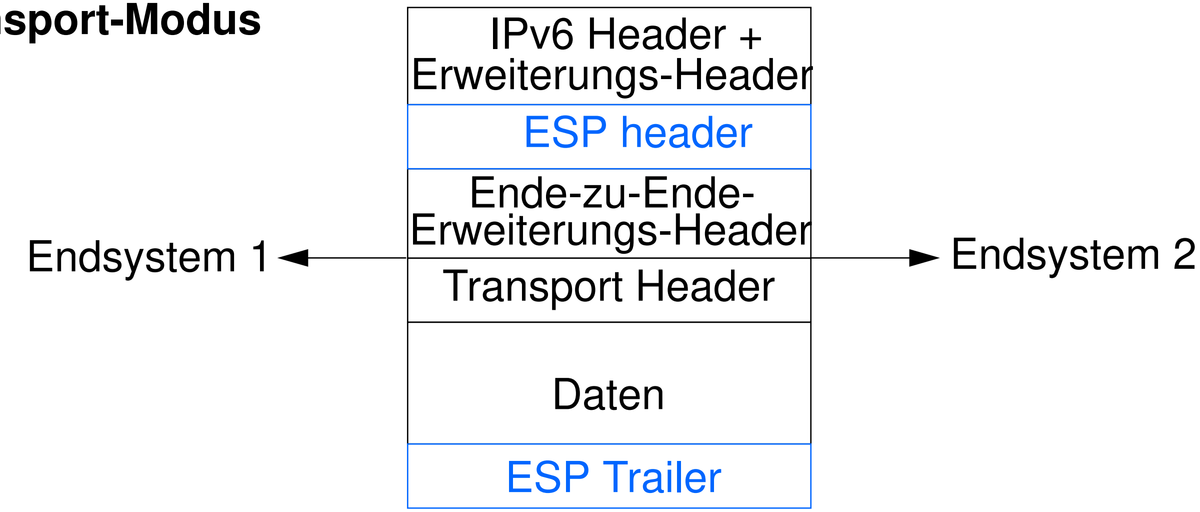
Dr. Torsten Braun

braun@heidelbg.ibm.com

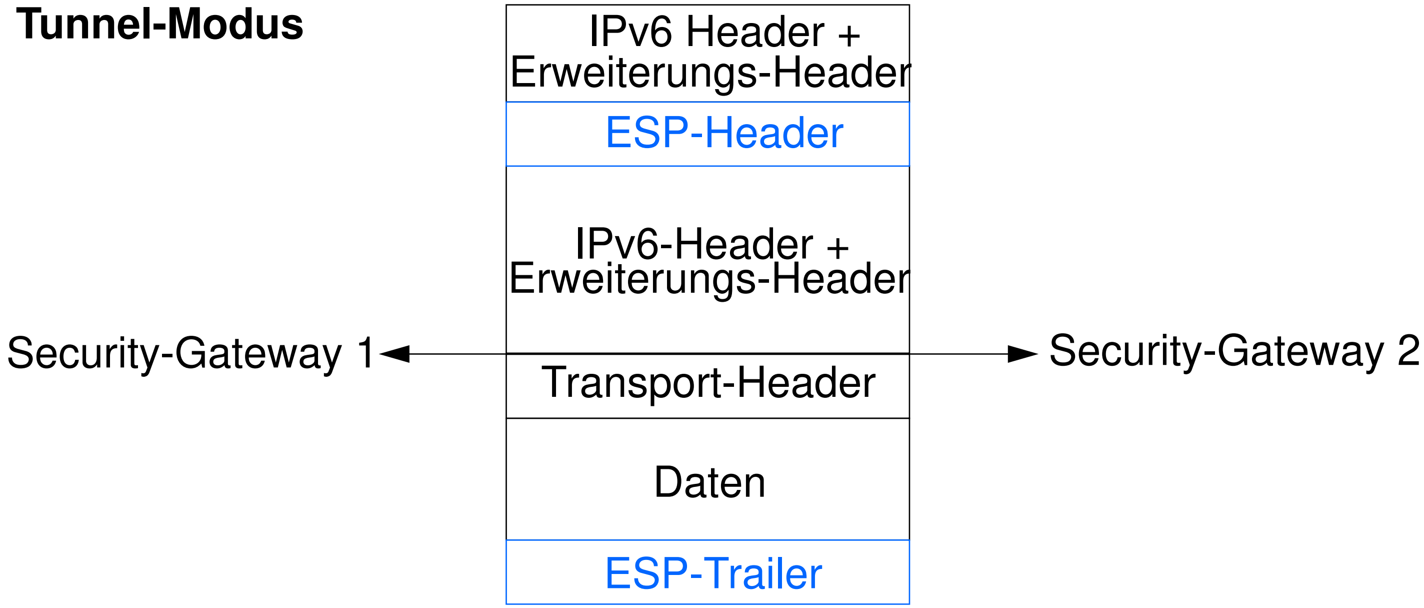
IBM European Networking Center
Heidelberg

Verschlüsselungsmöglichkeiten

Transport-Modus



Tunnel-Modus



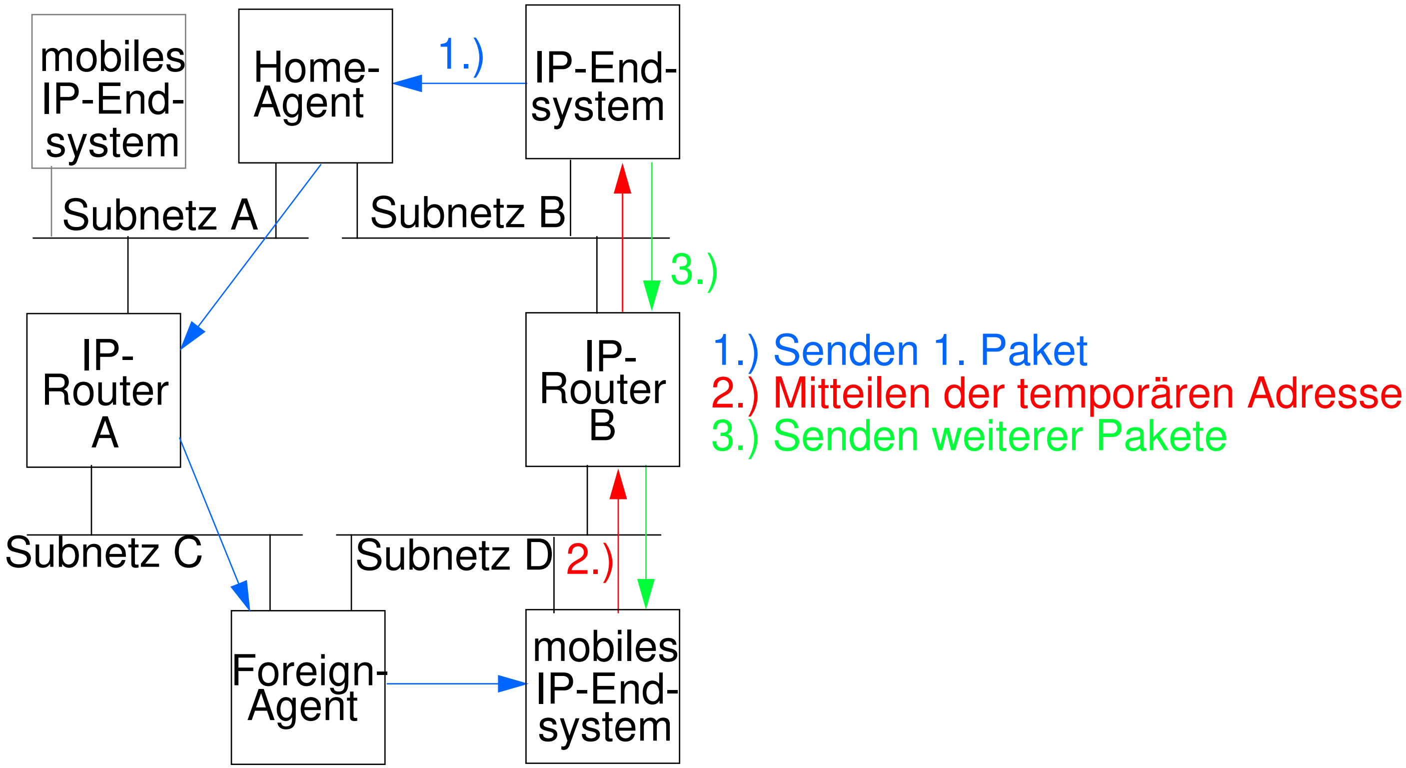
/u/braun/trans/online/online_f.doc; created on October 17, 1995; last modified on January 16, 1996

Dr. Torsten Braun

braun@heidelbg.ibm.com

IBM European Networking Center
Heidelberg

Mobilitätsunterstützung



Mitteilen der temporären Adresse über Optionen (2.)

Angabe von temporärer und permanenter Adresse im Routing-Header (3.)
=> keine IP-in-IP-Einkapselung wie bei IPv4

/u/braun/trans/online/online_f.doc; created on October 17, 1995; last modified on January 16, 1996

Dr. Torsten Braun

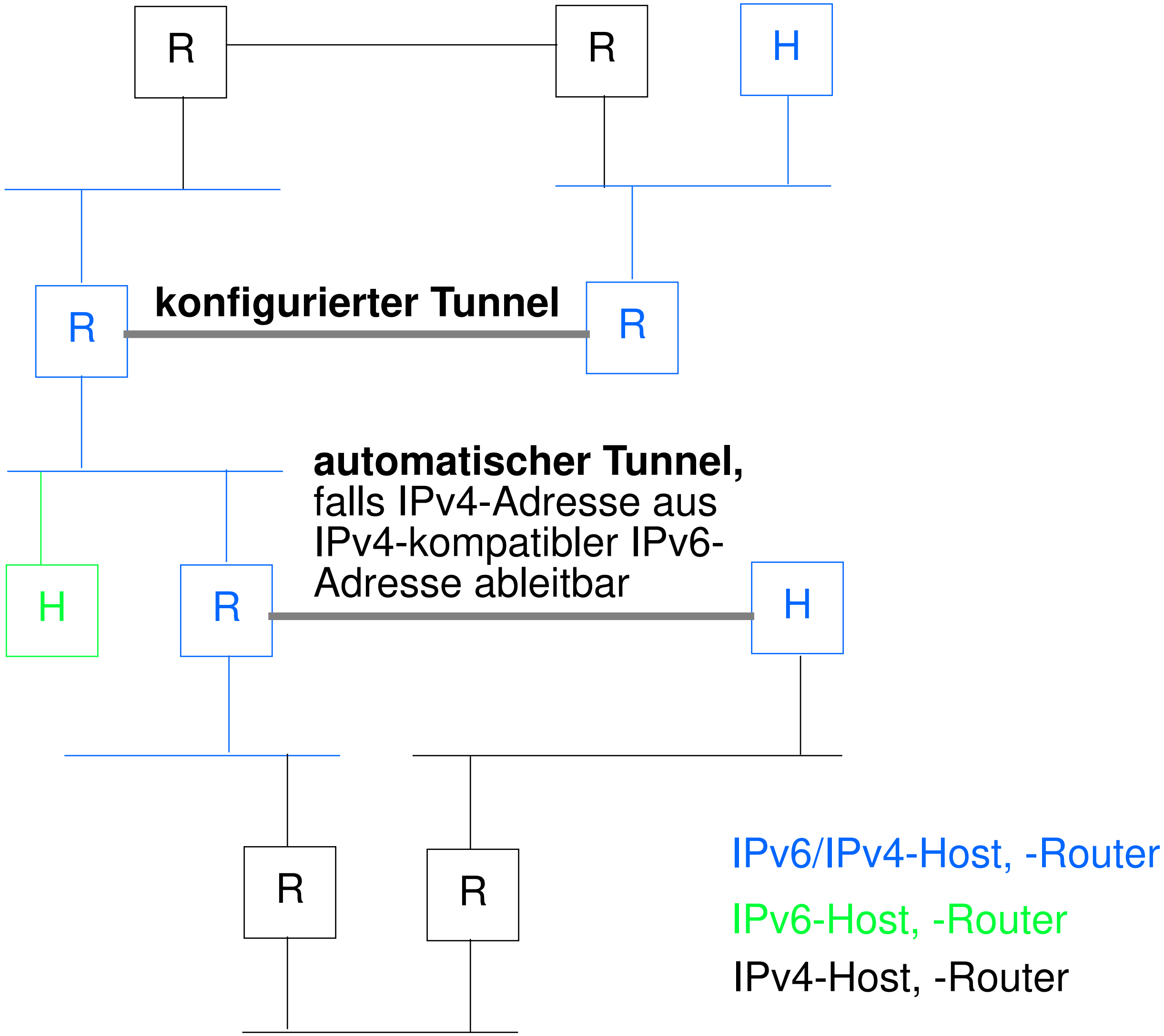
braun@heidelbg.ibm.com

IBM European Networking Center
Heidelberg

Übergangsstrategien

doppelte Stacks, d.h. UDP/IPv4 und UDP/IPv6 bzw. TCP/IPv4 und TCP/IPv6

Tunnel-Technik zur Überbrückung der IPv4-Welt



/u/braun/trans/online/online_f.doc; created on October 17, 1995; last modified on January 16, 1996

Dr. Torsten Braun

braun@heidelbg.ibm.com

IBM European Networking Center
Heidelberg

Ausblick

- Kontrollmechanismen basieren auf Multicast-Fähigkeit des Subnetzes: Notwendigkeit von IP-Multicast über ATM

  Problem:
  IP-Multicast basierend auf IGMP-Gruppenverwaltung ist auf “shared medium”-Subnetze ausgelegt.

  Lösung:
  Multicast Address Resolution Server (MARS) als Erweiterung des ATM ARP Servers nach RFC1577

- Änderung der Anwendungen wegen modifiziertem Socket API erforderlich

- TCPng ?
  - Erforderliche Modifikation der Prüfsummenberechnung in UDP- und TCP-Implementierungen wegen neu definierter IP-Pseudo-Header
  - TCP erlaubt derzeit keine Änderung der IP-Adresse während einer Verbindung
  - selektive Übertragungswiederholung