Dr. Torsten Braun

European Networking Center

Heidelberg

© IBM Deutschland 1996

IP Next Generation

Dr. Torsten Braun

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

Meet The Experts
Internet - Technik und Anwendung

8. Oktober 1996

IBM European Networking Center

Dr. Torsten Braun

European Networking Center

Heidelberg

© IBM Deutschland 1996

Inhalt

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

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 Deutschland 1996

IBM

Dr. Torsten Braun

European Networking Center

Heidelberg

IPng/IPv6-Kennzeichen I

- 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
- neues Datenformat
  - vereinfachter, minimaler IP Header
  - bessere Unterstützung von neuen Optionen und Erweiterungen
- Dienstgütenunterstützung
  - Flow Labels
  - Prioritäten

© IBM Deutschland 1996

IBM

Dr. Torsten Braun

European Networking Center

Heidelberg

IPng/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 und Authentifizierung)

© IBM Deutschland 1996

IBM

Dr. Torsten Braun

European Networking Center

Heidelberg

Adreßtypen

- Unicast-Adressen (1:1)
  - 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 isolierte IP-Netze)
  - Standort-lokal (für nicht an das Internet angeschlossene IP-Netze)
  - kompatibel (IPv4, IPX, NSAP)
- Anycast-Adressen (1:nächster Knoten, Adressierung von Routern)
- Multicast-Adressen (1:n)

© IBM Deutschland 1996

IBM

Dr. Torsten Braun

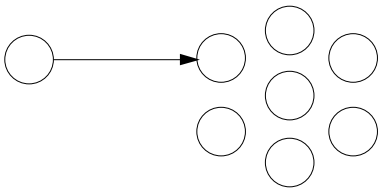
European Networking Center

Heidelberg

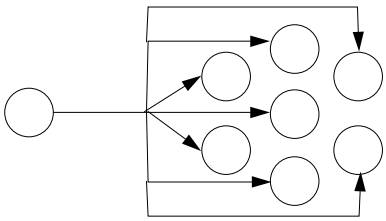
Addreßtypen II

- unicast

- anycast



- multicast



© IBM Deutschland 1996

IBM

Dr. Torsten Braun

European Networking Center

Heidelberg

Unicast-Adressen

Adreßtyp	Präfix	Anteil am Adreßraum
reserviert (z.B. für Loopback-, IPv4-kompatible Adressen)	00000000	1/256
NSAP-Adressen	0000001	1/128
IPX-Adressen	0000010	1/128
Provider-basierte Unicast-Adressen	010	1/8
Geographisch-basierte Unicast-Adressen	100	1/8
Link-lokale Unicast-Adressen	11111110 10	1/1024
Standort-lokale Unicast-Adressen	11111110 11	1/1024

- Link-lokale Adressen: Präfix + lokale ID (Nummer, MAC-Adresse)
- IPv4-kompatible Adresse: Präfix (96 0-bits) + IPv4-Adresse (32 bits)
- Standort-lokale Adresse: Präfix + Subnetz-ID + Interface-ID

© IBM Deutschland 1996

IBM

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

© IBM Deutschland 1996

IBM

Dr. Torsten Braun

European Networking Center

Heidelberg

IPv4 Header

version	hdr len	prec	TOS	total length
identification			flags	fragment offset
time to live		protocol		header checksum
source address				
destination address				

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

© IBM Deutschland 1996

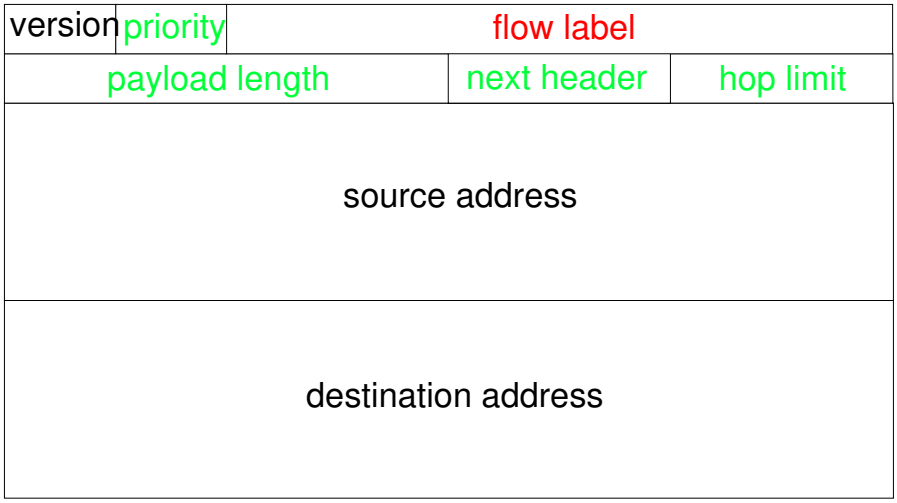
IBM

Dr. Torsten Braun

European Networking Center

Heidelberg

IPv6 Header



- 40 Bytes, 8 Felder

© IBM Deutschland 1996

IBM

Dr. Torsten Braun

European Networking Center

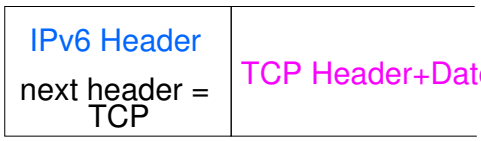
Heidelberg

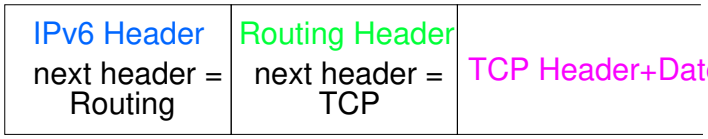
Header-Erweiterungen

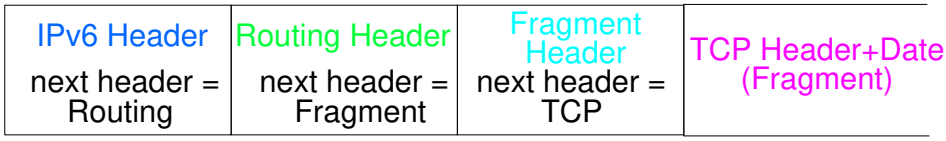
Verkettung von Header-Erweiterungen

-> Flexibilität

-> einfache Einführung neuer Erweiterungen und Optionen







© IBM Deutschland 1996

IBM

Dr. Torsten Braun

European Networking Center

Heidelberg

Reihenfolge der Header-Erweiterungen

- 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

© IBM Deutschland 1996

IBM

Dr. Torsten Braun

European Networking Center

Heidelberg

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).

© IBM Deutschland 1996

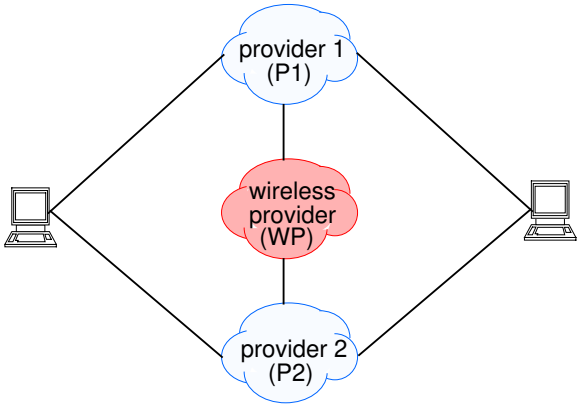
IBM

Dr. Torsten Braun

European Networking Center

Heidelberg

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
  -> H2 antwortet mit (H2, P1, H1)
- Fall 3: H1 wird mobil, d.h. Anschluß an Provider WP -> (H1, WP, P1, H2), (H2, P1, WP, H1)

© IBM Deutschland 1996

IBM

Dr. Torsten Braun

European Networking Center

Heidelberg

Jumbo-Payload-Option

- Paketlänge ist auf 65535 Bytes begrenzt
  (2 Byte für Längenangabe).
- Jumbo-Payload Length enthält 4-Byte lange Angabe der Paketlänge.
- Jumbo-Payload-Option ist Beispiel für Hop-by-Hop-Option.

next header	Hdr Ext Len	option type=194	opt data len=4
Jumbo Payload Length			

© IBM Deutschland 1996

IBM

Dr. Torsten Braun

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 Routern erfordert Vorkehrungen in den Endsystemen
  - Segmentierung in den Endsystemen (Fragment Header)
  - Senden minimaler Link-MTUs oder
  - Path MTU Discovery

© IBM Deutschland 1996

IBM

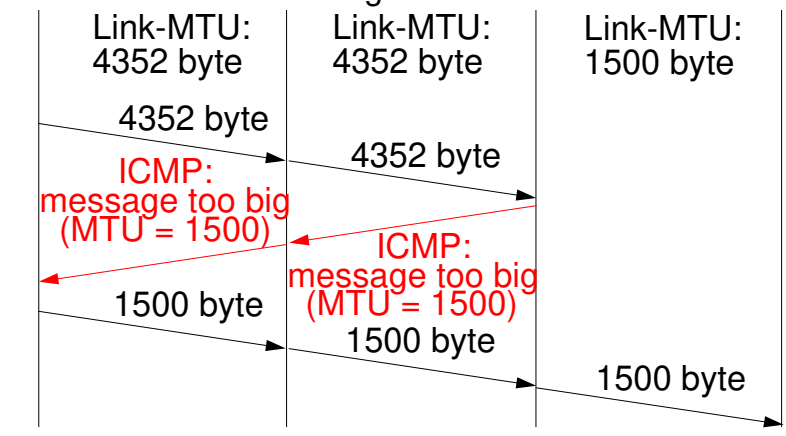
Dr. Torsten Braun

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 Deutschland 1996

IBM

Dr. Torsten Braun

European Networking Center

Heidelberg

Fragment-Header

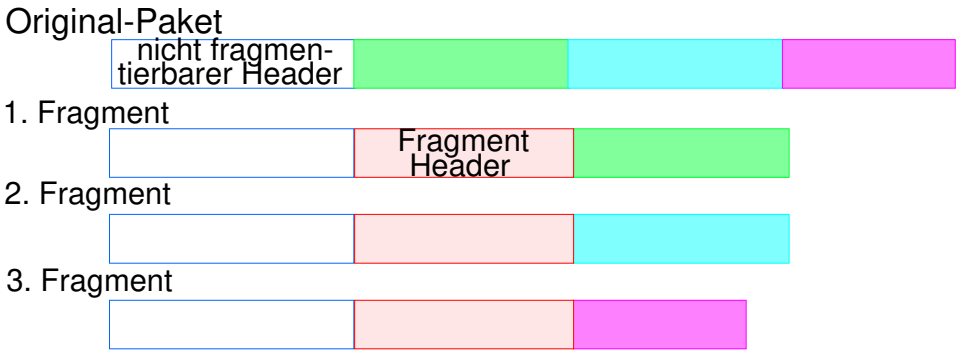
Fragment-Header erlaubt das Senden von Paketen, die größer als die Path-MTU sind.

next header	reserved	fragment offset	00M
Identification			

fragment offset: relative Position der Fragment-Daten im Original-Paket

M flag: more fragments (M=1)

identification: eindeutige Senderkennung des Pakets



© IBM Deutschland 1996

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 Deutschland 1996

IBM

Dr. Torsten Braun

European Networking Center

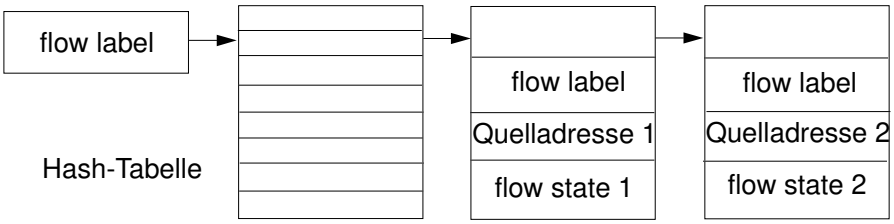
Heidelberg

IPv6 Flows

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

Kennzeichnung von Datenflüssen zwischen Endsystemen

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



© IBM Deutschland 1996

IBM

Dr. Torsten Braun

European Networking Center

Heidelberg

Flow Behandlung

- 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

© IBM Deutschland 1996

IBM

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

© IBM Deutschland 1996

IBM

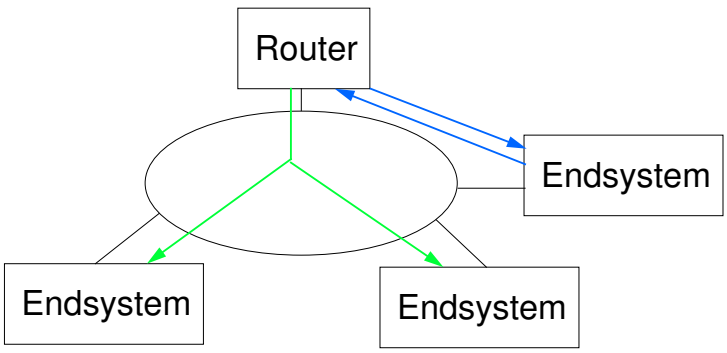
Dr. Torsten Braun

European Networking Center

Heidelberg

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 Endsyst.) 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)



© IBM Deutschland 1996

IBM

Dr. Torsten Braun

European Networking Center

Heidelberg

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

© IBM Deutschland 1996

IBM

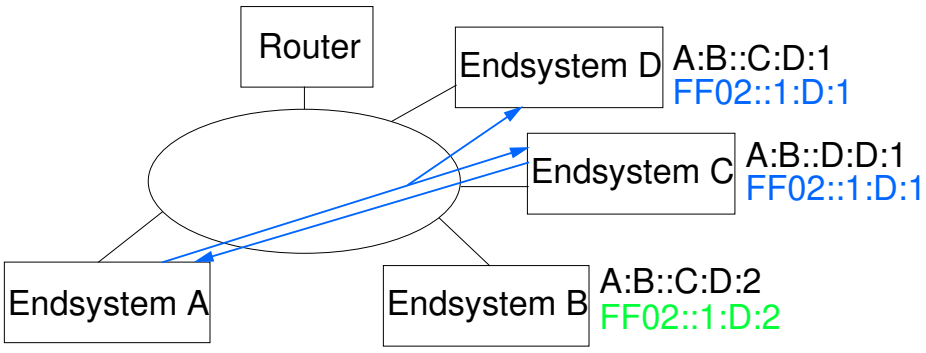
Dr. Torsten Braun

European Networking Center

Heidelberg

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



© IBM Deutschland 1996

IBM

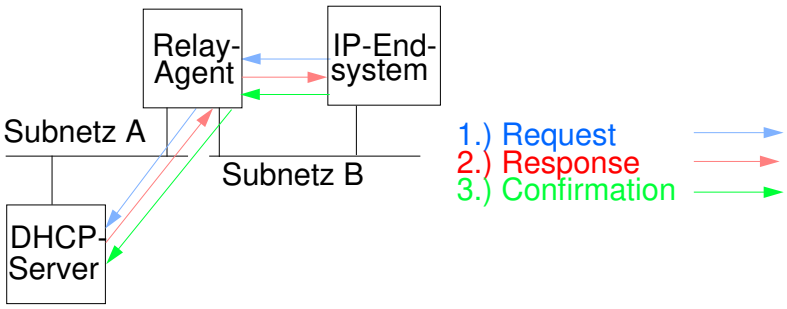
Dr. Torsten Braun

European Networking Center

Heidelberg

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 Deutschland 1996

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 identifiziert die etablierte Security-Assoziation

© IBM Deutschland 1996

IBM

Dr. Torsten Braun

European Networking Center

Heidelberg

Verschlüsselung

- Paket wird für vertraulichen, abhörsicheren Daten-austausch 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

ESP: encapsulating security payload

© IBM Deutschland 1996

IBM

Dr. Torsten Braun

European Networking Center

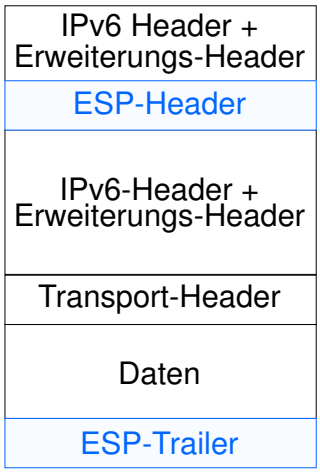
Heidelberg

Verschlüsselungsmöglichkeiten

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

Transport-Modus

Tunnel-Modus



© IBM Deutschland 1996

IBM

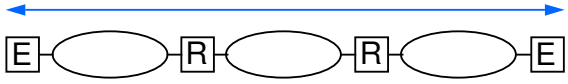
Dr. Torsten Braun

European Networking Center

Heidelberg

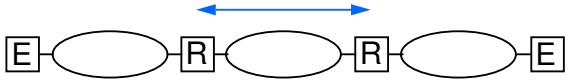
Anwendung von Verschlüsselung

- Ende-zu-Ende mit Transport-Modus



  z.B. f:ur vetraulichen 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 Deutschland 1996

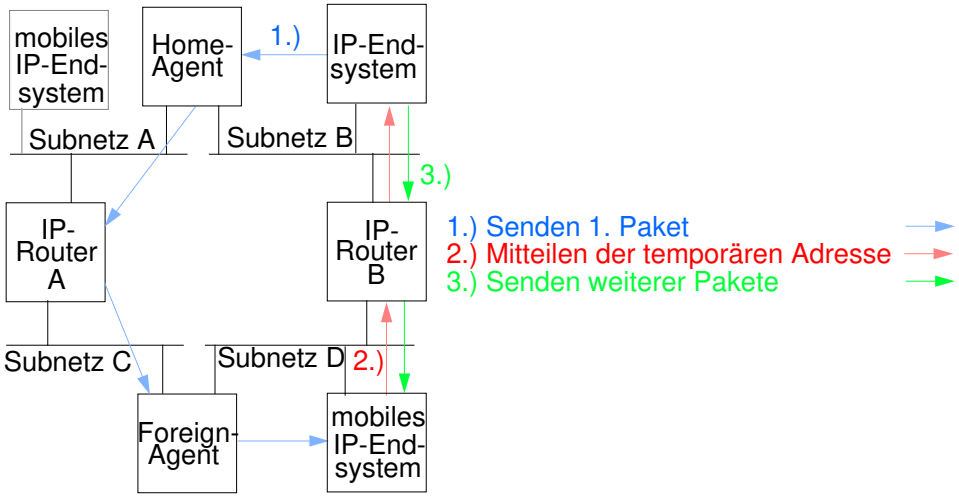
IBM

Dr. Torsten Braun

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

© IBM Deutschland 1996

IBM

Dr. Torsten Braun

European Networking Center

Heidelberg

Übergangsstrategien

- Auslaufen der IPv4-Adressen frühestens im Jahr 2000
- Betriebssysteme werdenin Zyklen von ca. 3 Jahren gewechselt
- IPv6-Implementierungen kommen 1996/1997 auf den Markt
- 2 Zyklen zum Übergang
- In der Übergangsphase sind IPv4-Knoten und IPv6-Knoten im Einsatz
- Beide Typen sollen 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 Deutschland 1996

IBM

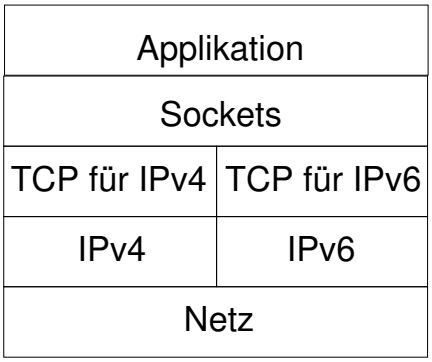
Dr. Torsten Braun

European Networking Center

Heidelberg

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



© IBM Deutschland 1996

IBM

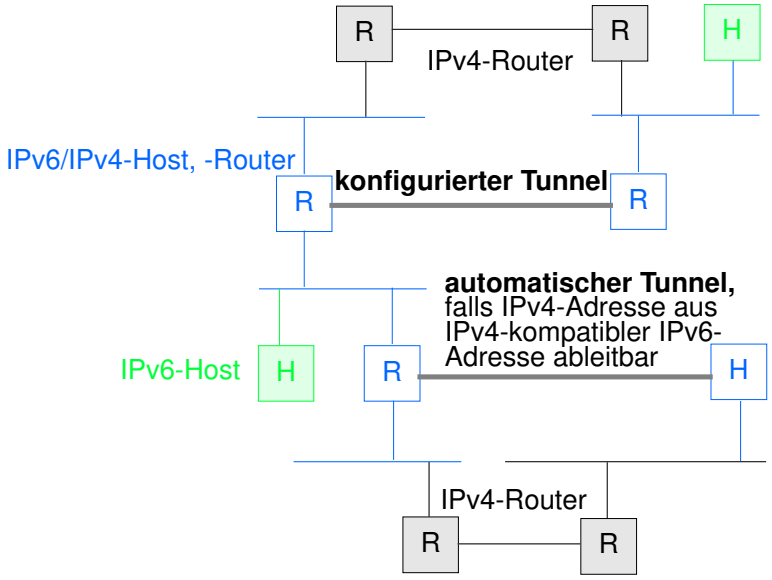
Dr. Torsten Braun

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



© IBM Deutschland 1996

IBM

Dr. Torsten Braun

European Networking Center

Heidelberg

IPv6 über ATM

- Problem:
  - Kontrollmechanismen (ND) basieren auf Multicast-Fähigkeit des Subnetzes
  - IP-Multicast basierend auf IGMP-Gruppenverwaltung ist auf “shared medium”-Subnetze ausgelegt.
- Lösungen in der Diskussion:
  - Multicast Address Resolution Server (MARS) als Erweiterung des ATM ARP Servers nach RFC1577
  - hierarchische Architektur von Neighbor Discovery Servern (NDS)
    NDS leitet ND-Nachrichten weiter
  - NHRP (NBMA Next Hop Resolution Protocol) für bestimmte ND-Funktionen (z.B. Adreßauflösung)

© IBM Deutschland 1996

IBM

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

© IBM Deutschland 1996

IBM

Dr. Torsten Braun

European Networking Center

Heidelberg

Literatur

- http://playground.sun.com/ipng
- 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

© IBM Deutschland 1996