

IPv6

Next Generation Internet

markus.wichmann@hdm-stuttgart.de

Warum eine neue Version von IP?

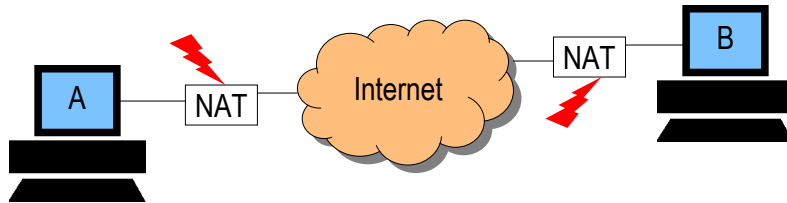
(1 von 4)

- Adressraum von IPv4 bald erschöpft
 - IPv4: „Nur“ 42 Milliarden theoretisch mögliche Adressen
 - Viele Nutzer teilen sich eine IP-Adresse (NAT)
 - Dynamische Adresszuweisung bei ISP-Dial-In
 - Bevölkerungswachstum: ~10 Mrd. Menschen im Jahr 2020
- Vorhersage: Erschöpfung des Adressraums ab 2005

Warum eine neue Version von IP?

(2 von 4)

- Viele Ende-zu-Ende-Dienste nicht uneingeschränkt möglich



Warum eine neue Version von IP?

(3 von 4)

- Wachsende Routing-Tabellen
 - Jede Class-A/B/C-Adresse erfordert Tabellen-Eintrag
 - IPv4 lässt hierarchisches Routing nicht zu
 - Performance-Einbußen
- Viele Felder des IPv4-Headers kaum/nie verwendet
 - Router werten diese Felder kaum (noch) aus
 - Auswerten kostet Zeit
 - Performance-Einbußen

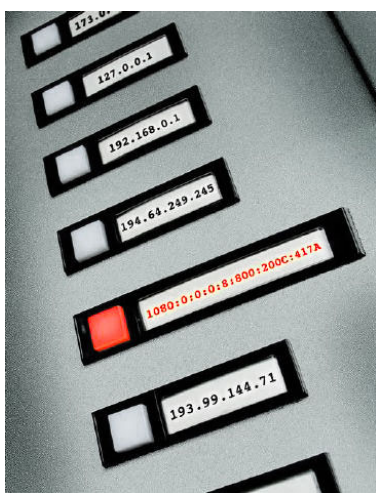
Warum eine neue Version von IP?

(4 von 4)

- Administrationskosten bei IPv4
 - Manuelle Konfiguration notwendig
 - in Endgeräten
 - und/oder in DHCP-Servern
 - Zunahme der Zahl mobiler Geräte verschärft dieses Problem

- Sicherheit der Daten in IPv4 auf Protokoll-Ebene
 - Authentizität und Verschlüsselung nicht ohne IPSec (zusätzliche, aufwändige Konfiguration)

Eure Vorstellungen von IPv6?

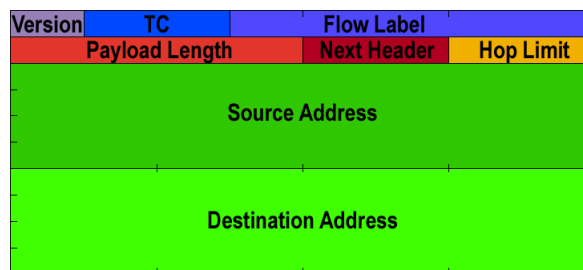


Anforderungen an IPv6

- Adressraum erweitern
- Leistung
 - Routing optimieren (v.a. in großen Netzen)
 - Effizienz auch in Netzen mit geringer Bandbreite sichern
- Administratoren bei Konfiguration unterstützen („Auto-Konfiguration“)
- Mechanismen zur Sicherheit von Daten integrieren
- Allmähliche Migration von IPv4 nach IPv6 ermöglichen

7

Der IPv6-Header

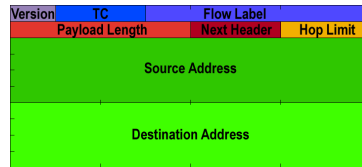


- Versionsfeld: gibt IP-Version an (binär 0110 = dezimal 6)
- TC = Traffic Classifier, dient der Priorisierung
- Flow Label für optimiertes Routing
- Payload Length: Länge der Nutzdaten
- Next Header gibt Typ des (optionalen) nachfolgenden Headers an
- Hop Limit entspricht ist ähnlich der Time-to-Live in IPv4

8

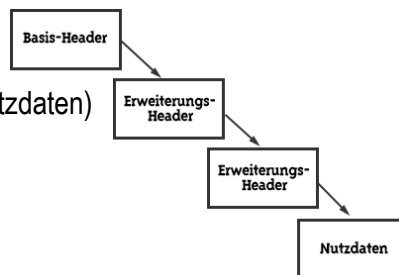
IPv6-Header vs. IPv4-Header

- IPv4 Internet Header Length entfällt
 - IPv6-Header immer gleich lang
 - Routing-Performance
- IPv4 Header-Prüfsumme entfällt (!)
 - Höhere Ebenen prüfen ausreichend
 - Performance
- Fragmentierungsmechanismen verlagert in Options-Header
 - Grund: Path-MTU-Discovery macht Fragmentierung quasi obsolet
- IPv4 „Protocol Type“ ersetzt durch IPv6 „Next Header“
- IPv6: „Payload Length“ umfasst nur Nutzdaten, nicht auch Header wie in IPv4



Erweiterungs-Header bei IPv6

- enthalten optionale Informationen
- stehen zwischen Basis-Header und Nutzlast
- können in beliebiger Anzahl vorkommen
- enthalten in Next-Header-Feld Informationen über Art des nachfolgenden Header (oder der Nutzdaten)
- Beispiele für Erweiterungs-Header:
 - Routing Header
 - Fragmentation Header
 - Authentication Header
 - Encapsulation Security Payload (ESP) Header



IPv6-Adressen: Darstellung

- 128 bits pro Adresse (IPv4: 32 bits)
- hexadezimale Notation in acht Oktetten
- Beispiel: 1080:0000:0000:0000:0008:0800:200C:417A
 - Kurzformen:
 - 1080:0:0:0:8:800:200C:417A
 - 1080::8:800:200C:417A
 - 0:0:0:BA98:7654:0:0:0 = ::BA98:7654:0:0:0 = 0:0:0:BA98:7654::
 - **::BA98:7654::** ist keine gültige Abkürzung

11

IPv6-Adressen: Prefixes

- Prefixnotation dient der Darstellung von Adressen in der beim Routing verwendeten Form
- IPv4: 192.168.10.0/24 bezeichnet das ganze Netz, dessen Adressen mit 192.168.10 beginnen
- IPv6: von FEDC:BA98:0000:0076:0000:1234:5678:9ABC sollen nur die ersten 64 bits berücksichtigt werden
→ FEDC:BA98:0:76::/64

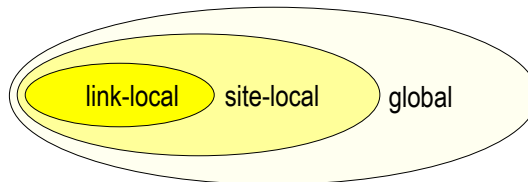
12

IPv6-Adressen: Typen

- Unicast: eindeutige Adresse eines einzigen Interfaces
- Multicast: alle Interfaces einer definierten Gruppe
 - Vermeiden der Übertragung identischer Daten beim Sender
- Anycast: das nächste Interface einer definierten Gruppe
 - mehrere Endgeräte haben gemeinsame Adresse
 - z.B. replizierte Webserver mit jeweils der selben IP-Adresse
 - z.B. praktisch für mobile Geräte: Nameserver werden zu einer Anycast-Gruppe zusammengefasst, DNS-Anfragen beantwortet der am schnellsten erreichbare DNS-Server
 - Server, die auf eine Anycast-Adresse hören, müssen diese den Routern ihres Subnetzes bekannt geben (via ICMP, siehe später)
- KEIN Broadcast mehr, abgelöst durch Multicast und Anycast

13

IPv6-Adressen: Unicast



- Geltungsbereich von Unicast-Adressen
 - global: weltweit gültig
 - site-local: gültig z.B. innerhalb eines Unternehmens (vergleichbar mit privaten Adressbereichen in IPv4)
 - link-local: gültig innerhalb eines Netzwerk-Segments
 - spielen große Rolle für automatische Adressvergabe, da direkt aus MAC der NIC gebildet (siehe später)

14

IPv6-Adressen: Einteilung Adressraum

Adresstyp	Binär-Prefix	v6-Notation
Global Unicast	001	2000::/3
Site-Local	1111111011	FEC0::/10
Link-Local	1111111010	FE80::/10
Multicast	11111111	FF00::/8
Loopback	000...1	::1/128

15

Globale Unicast-Adresse



- P=Prefix für globale Unicast-Adressen = 001
- TLA ID=Top Level Aggregator ID
 - z.B. ein ISP mit globalem Netz („Backbone-Provider“)
- res=reserviert für zukünftige Zwecke
- NLA ID=Next Level Aggregator ID
 - z.B. ein Provider
- SLA ID=Site Level Aggregator ID
 - z.B. kleinerer ISP oder Firmennetz
- Interface ID
 - entweder eine aus der MAC-Adresse der NIC abgeleitete Bit-Folge
 - oder eine zufällige oder vom Administrator zugewiesene Bit-Folge

16

Globale Unicast-Adresse: Beispiel

- Beispiel-Adresse: 3FFE:5C9:3:1D:200:B4FF:FE32:E6FF
 - 3FFE=0011 1111 1111 1110
 - Die ersten drei Bits sind 001 → globale Unicast-Adresse
 - Die nächsten 13 Bits sind (hex) 1FFE → TLA eines IPv6-Netzwerks
 - 5C9:3 sei die NLA ID der Telekom
 - 1D ist die SLA des Kunden (ein Unternehmen),
 - Host-Anteil ist 200:B4FF:FE32:E6FF

17

Vorteile der IPv6-Adressstruktur

P	TLA ID	res	NLA ID	SLA ID	Interface ID
---	--------	-----	--------	--------	--------------

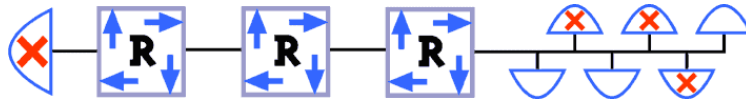
- Dezentrale Administration von Netzwerkadressen
 - IANA vergibt TLA IDs an tiefergelegene Instanzen
 - Diese vergeben NLA IDs an wiederum tiefergelegene
 - Diese wiederum vergeben die SLA IDs
- Diese Adress-Prefixes werden über Router propagiert
 - Router können (neue) Prefixes übermitteln
 - Wenn kein Router erreichbar dient definierte Abwandlung der MAC-Adresse der NIC zur Bildung einer link-lokalen IP-Adresse

18

Multicast-Adressen

(1 von 2)

- Zweck: Vermeiden von Verschwendung von Bandbreite
 - Punkt-zu-Mehrpunkt Datenfluss



- können unterschiedliche Geltungsbereiche haben, z.B.
 - link-lokal (z.B. alle Endgeräte am selben Link)
 - site-lokal (z.B. alle Router im Firmennetz)
 - global (z.B. „Kunden“ eines Streaming-Audio-Servers im Internet)

19

Multicast-Adressen

(2 von 2)

- Es gibt vordefinierte und benutzerdefinierte Multicast-Adressen
- Vordefinierte sind z.B.
 - alle Router
 - alle DHCP-Server
- An- und Abmeldung zu/von benutzerdefinierten Multicast-Quellen:
 - Host sendet Mitteilung (ICMPv6-Nachricht) an Router
 - Router passt seine internen Tabellen zur Multicast-Verteilung entsprechend an
 - Router meldet ggf. Wünsche des/der Hosts bei seinen hierarchisch höhenliegenden Routern an

20

Auto-Konfiguration

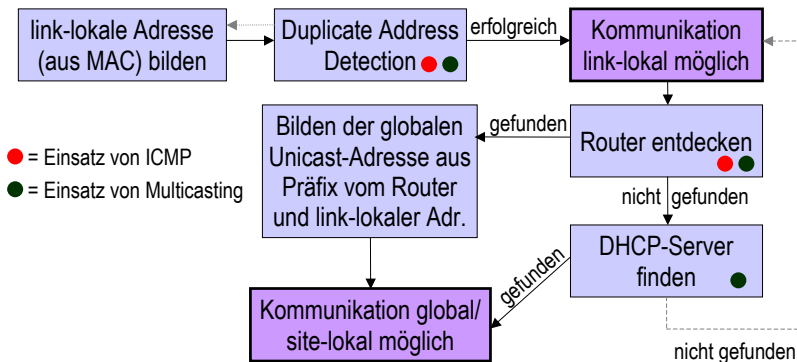
(1 von 2)

- Grundlage: ICMPv6 (Internet Control Message Protocol)
- Aufgaben von ICMP sind z.B.
 - „ping“ = echo request und echo reply (wie bei IPv4)
 - „Paket zu groß“ (Path MTU Discovery)
 - Anzeige einer Gruppen-Mitgliedschaft (Multicast)
 - Beenden einer Gruppen-Mitgliedschaft (Multicast)
 - Anfrage an Nachbarn (dazu gleich)
 - Anfrage an Router / Router-Bekanntmachung (dazu gleich)
- ICMP-Daten befinden sich im Datenteil des IP-Pakets

Auto-Konfiguration

(2 von 2)

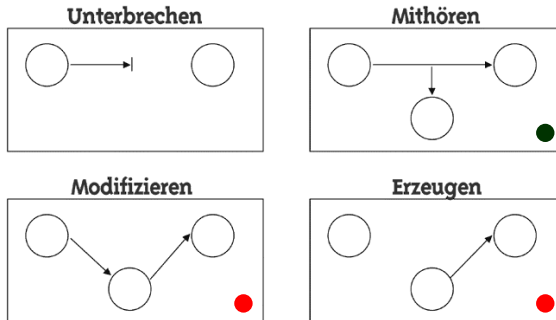
- wie bisher durch Einsatz von DHCP („stateful“)
- durch Einsatz von ICMP („stateless“)



Sicherheit mit IPv6

(1 von 3)

- Kurzer Rückblick auf mögliche Angriffsarten



- Verhindern durch Authentisierung
- Verhindern durch Verschlüsselung

23

Sicherheit mit IPv6

(2 von 3)

- basiert auf IPSec
- IPSec ist integraler Bestandteil von IPv6, optional bei IPv4
- nutzt in IPv6 die Erweiterungs-Header
 - Authentication Header (AH)
 - Encapsulated Security Payload Header (ESP)
- Anwendungen fordern sichere Kommunikation beim OS an

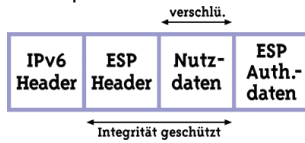
24

Sicherheit mit IPv6

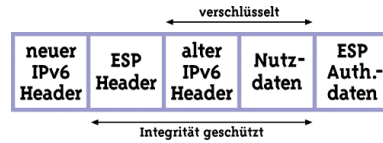
(3 von 3)

- ESP

Transport Mode

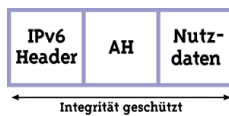


Tunnel Mode



- AH

Transport Mode



Tunnel Mode



25

Migration von IPv4 nach IPv6





Nicht so:



- sondern wird schrittweise erfolgen
- Dual-Stack-Hosts
 - beherrschen IPv4 und IPv6
 - Verwendung hängt von Gegenstelle ab
- Tunnelling
 - IPv6 wird in IPv4 eingepackt (6to4)
 - wird von Gateways/Routern erledigt

26

Systeme und IPv6

	Mac OS 9	nein
	Mac OS X vor 10.2	Do-it-yourself
	Mac OS X ab 10.2	eingebaut
	MS Windows 2000	für Entwickler
	MS Windows 9x/ME	Do-it-yourself (Trumpet IPv6)
	MS Windows XP	experimentell
	Linux ab Kernel 2.2	eingebaut
	OpenBSD ab V2.7	eingebaut
	FreeBSD ab V4.0	eingebaut
	NetBSD vor V1.5	Do-it-yourself
	NetBSD ab V1.5	eingebaut
	Sun Solaris 8	eingebaut
	IBM AIX ab V4.3	eingebaut
	IBM z/OS	eingebaut
	Router der Hersteller	Cisco, Hitachi, Nortel, Juniper, 6wind, IJ, Yamaha und andere

27

Ausblick

- Leidensdruck zum Umstieg fehlt
 - „Der Adressraum reicht uns doch noch“
 - „Multicast ist doch auch mit IPv4 möglich“
 - „Never change a running system“
- „Under Construction“
 - DHCPv6 z.B. noch im Entwurfszustand
- Echte „Geldspar-Features“ warten auf ihre Entdeckung
 - Auto-Konfiguration
 - Renumbering
- IP überall
 - Handies
 - mobile Kleinstgeräte (Beispiel: Lagerhaltung und Versand)
 - Geldscheine (?)

28

Fragen und Antworten

**Viel Spaß
beim Administrieren ☺**

Ressourcen

Christian Huitema: „IPv6“, Verlag Addison-Wesley

Hans-Peter Dittler: „IPv6“, dpunkt Verlag

Torsten Braun: „IPnG“, dpunkt Verlag

Felix von Leitner: „Das nächste Netz“, c't Ausgabe 16/2001, S.202, Verlag Heinz Heise

Friedhelm Hosenfeld: „Next Generation“, c't Ausgabe 11/1996, S.380, Verlag Heinz Heise

Prof. Roland Kiefer: Vorlesungen „Rechnernetze“, Hochschule der Medien, Stuttgart

Prof. Dr. Roland Schmitz: Vorlesung „Internet Security 1“, Hochschule der Medien, Stuttgart

Uwe Toenjes: „IPv6“, <http://www.ipv6-net.de/special/special2.html>

IETF.org: RFC 2461: „Neighbor Discovery Protocol“, <http://www.ietf.org/rfc/rfc2461.txt>

IETF.org: RFC 2529 „6over4“, <http://www.ietf.org/rfc/rfc2529.txt>

IETF.org: RFC 3056 „6to4“, <http://www.ietf.org/rfc/rfc3056.txt>

IETF.org: RFC 2894 „Router Renumbering“, <http://www.ietf.org/rfc/rfc2894.txt>

NGtrans Arbeitsgruppe der IETF: <http://www.ietf.org/html.charters/ngtrans-charter.html>

IPv6 Implementationen: <http://www.ipv6.org/impl/index.html>

Der 6bone: <http://www.6bone.net>