

Das Protokoll der Zukunft: IPv6

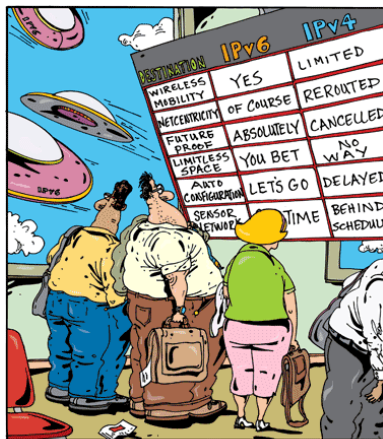
Ingo Ebel

Seminar Next Generation Internet, WS 2009/10

Gliederung

- 1 Einführung
 - Warum und Wofür eigentlich IPv6?
 - Aufbau
 - Autokonfiguration, ICMPv6 und Co
- 2 Sicherheit
 - Vorteile von IPv6
 - Nachteile von IPv6
- 3 IPv6 benutzen
 - Provider
 - Workshop
- 4 Zusammenfassung

Warum eigentlich mit IPv6 beschäftigen?



Suddenly, it dawned on Ronald that he needed to be on the right flight plan and IPv6 seemed to be just the ticket.

Gliederung

- 1 Einführung
 - Warum und Wofür eigentlich IPv6?
 - Aufbau
 - Autokonfiguration, ICMPv6 und Co
- 2 Sicherheit
 - Vorteile von IPv6
 - Nachteile von IPv6
- 3 IPv6 benutzen
 - Provider
 - Workshop
- 4 Zusammenfassung

Wichtige Neuerungen

- Quality of Service (QoS)
- Mobilitätsunterstützung (Mobile IP)
- Autokonfiguration
- native IPsec Unterstützung
- Erweiterbarkeit
- viele viele IP-Adressen
- Kleinere Routingtabellen

von IPv4 eingeholt?

- QoS, IPsec, Mobile IP, ...
- Mittlerweile auch alles in IPv4 vorhanden

2 Wichtige Gründe bleiben!

- genügend IP Adressen (+ endlich NAT loswerden)
- kleine Routingtabellen

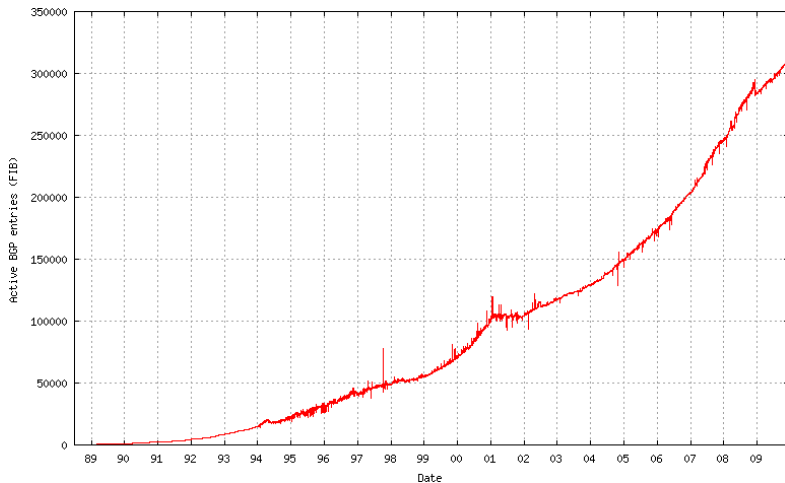
von IPv4 eingeholt?

- QoS, IPsec, Mobile IP, ...
- Mittlerweile auch alles in IPv4 vorhanden

2 Wichtige Gründe bleiben!

- genügend IP Adressen (+ endlich NAT loswerden)
- kleine Routingtabellen

BGP Routen



Stand 10.12.2009: 311635 / Quelle: <http://bgp.potaroo.net/as2.0/bgp-active.html>

Gliederung

- 1 Einführung
 - Warum und Wofür eigentlich IPv6?
 - **Aufbau**
 - Autokonfiguration, ICMPv6 und Co
- 2 Sicherheit
 - Vorteile von IPv6
 - Nachteile von IPv6
- 3 IPv6 benutzen
 - Provider
 - Workshop
- 4 Zusammenfassung

Aufbau der IP-Adressen

- IPv6 Adressen sind 128bit lang, es gibt also 2^{128} mögliche Adressen (vgl. IPv4: 32 Bit)
- $2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456$
- ca. 667 Billionen Adressen pro mm^2 Erdoberfläche.

Aufbau der IP-Adressen

- IPv6 Adressen sind 128bit lang, es gibt also 2^{128} mögliche Adressen (vgl. IPv4: 32 Bit)
- $2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456$
- ca. 667 Billionen Adressen pro mm^2 Erdoberfläche.

Aufbau der IP-Adressen

- IPv6 Adressen sind 128bit lang, es gibt also 2^{128} mögliche Adressen (vgl. IPv4: 32 Bit)
- $2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456$
- ca. 667 Billionen Adressen pro mm^2 Erdoberfläche.

Notation

Hexadezimal, 8 Blöcken à 16 Bit (2 Bytes), per Doppelpunkt getrennt

- 2001:0db8:85a3:08d3:0000:0000:0170:7a44

Führende Nullen können weggelassen werden:

- 2001:db8:85a3:8d3:0:0:170:7a44

aufeinander folgende Blöcke, deren Wert 0 beträgt, dürfen ausgelassen und durch zwei Doppelpunkte ersetzt werden

- 2001:db8:85a3:8d3::170:7a44

aber die geht nur einmal!

- 2001:db8:0:0:1:0:0:7a44 lässt sich **nicht** zusammenfassen nach 2001:db8::1::7a44

Notation

Hexadezimal, 8 Blöcken à 16 Bit (2 Bytes), per Doppelpunkt getrennt

- 2001:0db8:85a3:08d3:0000:0000:0170:7a44

Führende Nullen können weggelassen werden:

- 2001:db8:85a3:8d3:0:0:170:7a44

aufeinander folgende Blöcke, deren Wert 0 beträgt, dürfen ausgelassen und durch zwei Doppelpunkte ersetzt werden

- 2001:db8:85a3:8d3::170:7a44

aber die geht nur einmal!

- 2001:db8:0:0:1:0:0:7a44 lässt sich **nicht** zusammenfassen nach 2001:db8::1::7a44

Notation

Hexadezimal, 8 Blöcken à 16 Bit (2 Bytes), per Doppelpunkt getrennt

- 2001:0db8:85a3:08d3:0000:0000:0170:7a44

Führende Nullen können weggelassen werden:

- 2001:db8:85a3:8d3:0:0:170:7a44

aufeinander folgende Blöcke, deren Wert 0 beträgt, dürfen ausgelassen und durch zwei Doppelpunkte ersetzt werden

- 2001:db8:85a3:8d3::170:7a44

aber die geht nur einmal!

- 2001:db8:0:0:1:0:0:7a44 lässt sich **nicht** zusammenfassen nach 2001:db8::1::7a44

Arten der Adressierung

- Unicast
 - global
 - link-local
 - site-local (veraltet)
 - unique-local (löst site-local ab)
- Anycast
- Multicast
- pro Interface mehrere Adressen:
 - immer 1x link-local
 - immer ein oder mehrere Multicast Adressen
 - kann mehrere globale Adressen haben

Arten der Adressierung

- Unicast
 - global
 - link-local
 - site-local (veraltet)
 - unique-local (löst site-local ab)
- Anycast
- Multicast

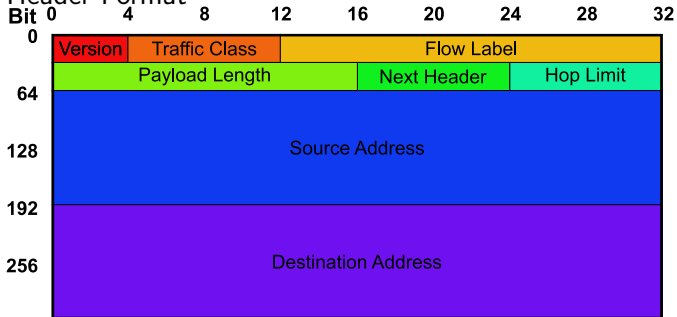
- pro Interface mehrere Adressen:
 - immer 1x link-local
 - immer ein oder mehrere Multicast Adressen
 - kann mehrere globale Adressen haben

Reservierte Bereiche

- :: nicht spezifizierte Adresse
- ::1 loopback
- FE80::/10 link-local
- FF00::/8 multicast
- FF01::1 multicast, alle Hosts
- FF01::2 multicast, alle Router
- FF05::3 multicast, alle DHCP-Server
- FC00::/8 Unique Local Adressen (zentral verwaltet)
- FD00::/8 Unique Local Adressen
- 2000::/3 globale Unicast Adressen
- 2001:DB8::/32 für Dokumentation

Aufbau der Pakete

Header-Format



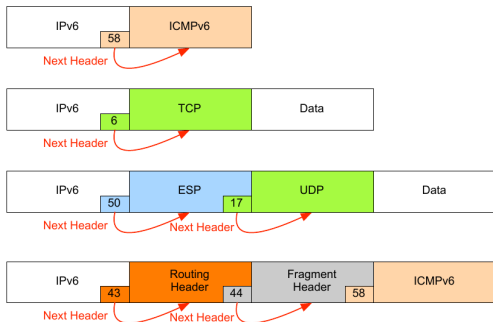
Quelle: Wikipedia (http://de.wikipedia.org/wiki/Datei:IPv6_header_rv1.svg)

Aufbau der Pakete (II)

- Vorteile gegen über IPv4:
 - IPv6-Header immer gleich lang -> Routing-Performance
 - im IPv4 Header viele Optionen ungenutzt
 - keine Checksum -> machen höhere Schichten
 - Fragmentierung wird besser gelöst (mit Path Maximum Transmission Unit Discovery)
 - Erweiterungs Header möglich (NextHeader)

NextHeader

- flexibler Mechanismus für die Erweiterung des Protokolls um zusätzliche Funktionalitäten
- Beispiele: Routing Header, Hop-By-Hop, Encapsulating Security Payload (ESP), Fragment Header, Authentication Header (AH)



Gliederung

- 1 Einführung
 - Warum und Wofür eigentlich IPv6?
 - Aufbau
 - Autokonfiguration, ICMPv6 und Co
- 2 Sicherheit
 - Vorteile von IPv6
 - Nachteile von IPv6
- 3 IPv6 benutzen
 - Provider
 - Workshop
- 4 Zusammenfassung

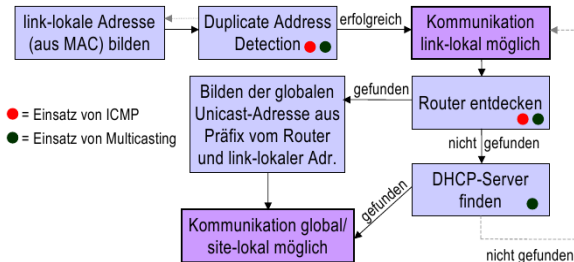
Autokonfiguration I

Ein Host kann vollautomatisch eine Internetverbindung herstellen.
ICPMv6 spielt eine zentrale Rolle.

- Stateless Address (Auto)Configuration
- für Hosts, nicht für Router
- Host weißt sich link-lokale Adresse meist aus der MAC-Adresse des Interfaces erzeugt
- Duplicate Address Detectionen
 - Neighbour Soliciting Message (ICMPv6 Typ 135) wird verschickt um Einzigartigkeit der konfigurierten Adresse zu überprüfen
 - Normal keine Antwort. Adresse kann genommen werden.
 - Oder Neighbour Advertising Message (ICMPv6 Typ 136) - Adresse belegt, neuer Versuch

Autokonfiguration II

- Host fragt via Multicast alle Router nach weiteren Präfixen (Router Solicitation - ICMPv6 Typ 133)
- für jeden empfangene Präfix wird eine weitere Interface Adresse hinzugefügt
- es wird weiter auf Router Announcements (ICMPv6 Typ 134) gehört



Quelle: http://m2w2.de/articles/IPv6_public.pdf

DHCPv6

- Trotz Autokonfiguration DHCP gibt es weiterhin
- Stateful Address Configuration
- Wird für die Zuweisung von DNS-Servern oder anderen »optionalen« Werten wie NTP gebraucht
- Automatisches Eintragen in DNS
- läuft auf anderen Ports wie DHCPv4. Server/Relay: 547 / UDP - Client: 546 / UDP

Alles bleibt anders

- ARP -> ICMPv6 Neighbor Discovery (ND)
- DNS statt A-Record AAAA-Record
- statt Internet Group Management Protocol (IGMP) -> Multicast Listener Discovery (MLD)
- statt RIP -> RIPv6
- statt OSPF -> OSPFv6

Gliederung

- 1 Einführung
 - Warum und Wofür eigentlich IPv6?
 - Aufbau
 - Autokonfiguration, ICMPv6 und Co
- 2 Sicherheit
 - Vorteile von IPv6
 - Nachteile von IPv6
- 3 IPv6 benutzen
 - Provider
 - Workshop
- 4 Zusammenfassung

alte Probleme ausgemerzt

- Von Anfang an sicher: eingebautes IPSec
- NAT fällt weg! Viel weniger Probleme. Auch ggf. Sicherheit da weniger bei Programmen implementiert werden muss.
- Subnetzgröße mindestens: 2^{64}
 - Angriffe durch Scannen unmöglich dauert ggf. Jahre bis Host gefunden wird.

Gliederung

- 1 Einführung
 - Warum und Wofür eigentlich IPv6?
 - Aufbau
 - Autokonfiguration, ICMPv6 und Co
- 2 Sicherheit
 - Vorteile von IPv6
 - Nachteile von IPv6
- 3 IPv6 benutzen
 - Provider
 - Workshop
- 4 Zusammenfassung

Problemfelder

Neue bzw. Andere Probleme

- Jedes Gerät kann sich am Netzwerk anmelden und erhält eine gültige Adresse
- Duplicate Address Detection kann für DOS-Attacks ausgenutzt werden
- Neue Wurmangriffsarten: vielleicht über Multicast schnell und leicht an alle Adressen kommen und/oder Verlagerung auf DNS
- Router Advertisements Nachrichten können gefälscht werden
- Anti-Spam-Blacklists stoßen an Grenzen - Nachteil von zu vielen IPs
- ICMPv6 sehr wichtig kann nicht einfach geblockt werden

Problemfelder

Neue bzw. Andere Probleme

- Jedes Gerät kann sich am Netzwerk anmelden und erhält eine gültige Adresse
- Duplicate Address Detection kann für DOS-Attacke ausgenutzt werden
- Neue Wurmangriffsarten: vielleicht über Multicast schnell und leicht an alle Adressen kommen und/oder Verlagerung auf DNS
- Router Advertisements Nachrichten können gefälscht werden
- Anti-Spam-Blacklists stoßen an Grenzen - Nachteil von zuvielen IPs
- ICMPv6 sehr wichtig kann nicht einfach geblockt werden

Problemfelder

Neue bzw. Andere Probleme

- Jedes Gerät kann sich am Netzwerk anmelden und erhält eine gültige Adresse
- Duplicate Address Detection kann für DOS-Attacke ausgenutzt werden
- Neue Wurmangriffsarten: vielleicht über Multicast schnell und leicht an alle Adressen kommen und/oder Verlagerung auf DNS
- Router Advertisements Nachrichten können gefälscht werden
- Anti-Spam-Blacklists stoßen an Grenzen - Nachteil von zuvielen IPs
- ICMPv6 sehr wichtig kann nicht einfach geblockt werden

Problemfelder

Neue bzw. Andere Probleme

- Jedes Gerät kann sich am Netzwerk anmelden und erhält eine gültige Adresse
- Duplicate Address Detection kann für DOS-Attacke ausgenutzt werden
- Neue Wurmangriffsarten: vielleicht über Multicast schnell und leicht an alle Adressen kommen und/oder Verlagerung auf DNS
- Router Advertisements Nachrichten können gefälscht werden
- Anti-Spam-Blacklists stoßen an Grenzen - Nachteil von zuvielen IPs
- ICMPv6 sehr wichtig kann nicht einfach geblockt werden

Problemfelder

Neue bzw. Andere Probleme

- Jedes Gerät kann sich am Netzwerk anmelden und erhält eine gültige Adresse
- Duplicate Address Detection kann für DOS-Attacke ausgenutzt werden
- Neue Wurmangriffsarten: vielleicht über Multicast schnell und leicht an alle Adressen kommen und/oder Verlagerung auf DNS
- Router Advertisements Nachrichten können gefälscht werden
- Anti-Spam-Blacklists stoßen an Grenzen - Nachteil von zuvielen IPs
- ICMPv6 sehr wichtig kann nicht einfach geblockt werden

Umgewöhnung

IPv6 ist nicht IPv4! Umgewöhnung notwendig!

- Network Adress Translation (NAT) ist bei vielen Gefühlsmäßig wie eine Firewall. NAT ersetzt jedoch keine Firewall!
- Alle Dienste die gestartet sind evtl. ungeschützt im Netz
- mit Firewalls wie iptables (Linux) vertraut machen und konfigurieren
 - solange IPv6 und IPv4 parallel laufen doppelter Aufwand nötig
 - Fertiglösungen müssen nachziehen, oft wird IPv6-Traffic ungefiltert durchgelassen

Umgewöhnung

IPv6 ist nicht IPv4! Umgewöhnung notwendig!

- Network Adress Translation (NAT) ist bei vielen Gefühlsmäßig wie eine Firewall. NAT ersetzt jedoch keine Firewall!
- Alle Dienste die gestartet sind evtl. ungeschützt im Netz
- mit Firewalls wie iptables (Linux) vertraut machen und konfigurieren
 - solange IPv6 und IPv4 parallel laufen doppelter Aufwand nötig
 - Fertiglösungen müssen nachziehen, oft wird IPv6-Traffic ungefiltert durchgelassen

Gliederung

- 1 Einführung
 - Warum und Wofür eigentlich IPv6?
 - Aufbau
 - Autokonfiguration, ICMPv6 und Co
- 2 Sicherheit
 - Vorteile von IPv6
 - Nachteile von IPv6
- 3 **IPv6 benutzen**
 - **Provider**
 - Workshop
- 4 Zusammenfassung

Wie benutze ich IPv6 daheim?

Über einen Provider der IPv6 direkt anbietet:

| Provider | Zugang | URL |
|---------------|------------|---|
| d-hosting.de | T-DSL u.a. | http://www.d-hosting.de/ |
| RH-TEC | T-DSL u.a. | http://www.rh-tec.de/ |
| Titan DSL | T-DSL | http://www.ipv6-dialin.de/ |
| Tal.DE | T-DSL | http://www.tal.de/ |
| Spacenet AG | T-DSL u.a. | http://www.space.net/ |
| Speedpartner | T-DSL u.a. | http://www.speedpartner.de/ |
| IN-Berlin | T-DSL | http://www.in-dsl.de/ |
| IKS GmbH Jena | direkt | http://www.iks-jena.de/ |

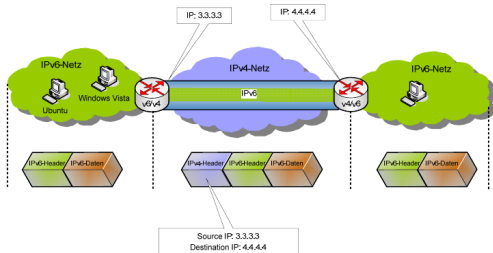
Oder auch M-Net in München direkt. <http://www.m-net.de/>

- Es gibt Gerüchte dass 1&1 und evtl. die Telekom im Jahr 2010 auch IPv6 nativ anbieten wollen.
- Rootserver Anbieter fangen auch an umzurüsten: Bei Strato kann jetzt IPv6 nativ genutzt werden.

Über einen Tunnel

Wenn kein natives IPv6 bereit steht, kann IPv6 über IPv4 getunnelt werden. Dafür gibt es auch verschiedene Anbieter so genannte Tunnel Broker z.B.:

- SixXS
 - arbeitet mit Punktesystem um Missbrauch vorzubeugen
 - <http://www.sixxs.net>, bietet Tunnel und Subnetze, auf der Seite gibt es auch viele Infos rund um IPv6



Quelle: https://www.mi.hdm-stuttgart.de/Downloads/Vorlesungsskripte/skripte/BACHELOR_Medieninformatik/Prak_Rechnernetze/v11-

Tunnel II

- Hurricane Electric
 - <http://www.tunnelbroker.net/>
- Teredo
 - von Microsoft entwickelt, auch für Linux möglich (=Miredo)
 - nutzt UDP Port 3544
 - bei Windows 7 standardmäßig aktiviert!
- weitere siehe
http://en.wikipedia.org/wiki/List_of_IPv6_tunnel_brokers

Gliederung

- 1 Einführung
 - Warum und Wofür eigentlich IPv6?
 - Aufbau
 - Autokonfiguration, ICMPv6 und Co
- 2 Sicherheit
 - Vorteile von IPv6
 - Nachteile von IPv6
- 3 IPv6 benutzen
 - Provider
 - Workshop
- 4 Zusammenfassung

Hands on IPv6

Selbst etwas mit IPv6 »spielen«.

- Ich baue einen Tunnel ins IPv6-Netz auf (mit sixxs und aiccu)
- geht auf www.ipv6.bieringer.de, www.six.heise.de,
ipv6.google.com, www.deepspace6.net, blog.fefe.de
- nutzt ping6 und traceroute6
- viele Dienste wie SSH, Apache, Mailserver können schnell auf IPv6 konfiguriert werden

Teredo und Windows 7

- ist seit Windows XP SP 2 dabei
- bei XP und Vista nicht aktiviert
- seit Windows 7 standardmäßig aktiviert (bewusst machen!)
- ping -6 www.six.heise.de
- für Browser noch 2 Schritte (als richtiger Admin):
 - netsh interface ipv6 set address "LAN-Verbindung" 2001:db8::1/48
 - netsh interface ipv6 add route ::/0 9
- siehe auch [http://www.heise.de/netze/artikel/Einrichtung-
unter-Windows-223862.html](http://www.heise.de/netze/artikel/Einrichtung-unter-Windows-223862.html)

Zusammenfassung

- IPv6 ist anders als IPv4, löst aber einige Probleme
- Umdenken ist erforderlich, alle neuen Geräte können IPv6
- Sicherheit ist wichtig, daher praktische Erfahrungen sammeln

- Ausblick
 - IPv6 wird sich langsam durchsetzen
 - es bleibt spannend: neue Features, neue Implementierungen, neuer Hacking-Spaß

Vorsicht!

DOCTOR FUN

4 June 2003



Copyright © 2003 David Farley, d-farley@ibiblio.org
<http://ibiblio.org/Dave/drfun.html>

This cartoon is made available on the Internet for personal viewing only. Opinions expressed herein are solely those of the author.

The brave new world of IPv6

Weiterführende Literatur I

-  Anatol Badach, Erwin Hoffmann
Technik der IP-Netze
Hanser, 2007
-  Scott Hogg and Eric Vyncke
IPv6 Security.
Cisco Press, 2008
-  Benedikt Stockebrand
Eine Frage der Zeit
Heise IX (9):40–45, 2009.

Quellen

- http://inetcore.com/project/ipv4ec/index_de.html– IPv4 Counter
- http://www.zdnet.de/sicherheit_in_der_praxis_ipv6_mit_festen_adressen_so_nutzt_39001543-41522303-1.htm
- <http://www.deepspace6.net>– Anlaufstelle für alles was mit IPv6 zu tun hat (Linux HowTos etc)
- <http://www.heise.de/netze/artikel/Teredo-unter-Linux-und-Co-223864.html>– Teredo unter Linux und Windows
- <http://www.fefe.de/ct/ipv6.txt>
- <http://www.heise.de/netze/artikel/IPv6-Internetzugang-221479.html>
- <http://www.potaroo.net/tools/ipv4/index.html>– Statistiken über verfügbare IPv4-Adressen
- http://m2w2.de/articles/IPv6_public.pdf– Vortrag über IPv6 im Seminar NGI
- <http://bgp.potaroo.net/as2.0/bgp-active.html>– Aktive IPv4 BGB Routen
- <http://de.wikipedia.org/wiki/Ipv6>
- <http://blit.org/2009/zeitplan/events/5.de.html>
- <http://blit.org/2009/zeitplan/events/38.de.html>
- Bild IPv6 Flight Plan:
http://www.satnews.com/cgi-bin/display_story.cgi?number=1143127680

Schluss

Vielen Dank für die Aufmerksamkeit!

Fragen?

<http://blog.radiotux.de/tag/ipv6/>