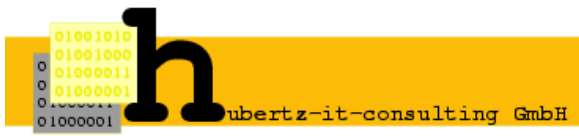
IPv6

– nur zum Spielen oder schon ausgereift?

Johannes Hubertz

hubertz-it-consulting GmbH

SoftwareFreedomDay Köln, 15. 9. 2012



IPv6 – zum Anfassen: Inhalt

Einleitung, Vorstellung

IPv6 – Fiktion, Hype oder nur Marketing?

Mythen und Märchen

IPv4 – Header – IPv6

IPv6 – genug Adressen, nie und nimmer NAT

IPv6 – next header – IPv6

ICMPv6 – Das Wichtigste

IPv6 Autokonfiguration

IPv6 Konfiguration in Linux und OpenBSD

IPv6 – Paketfilter

Quellen und Lesetipps

Vorstellung: hubertz-it-consulting GmbH

Erkenntnisse aus dem Berufsleben

Bellovin and Cheswick: Firewalls and Internet Security, 1994

Fazit: Keep it simple!

Oder mit Einstein: So einfach wie möglich, aber nicht einfacher!

Etwas Erfahrung war Voraussetzung

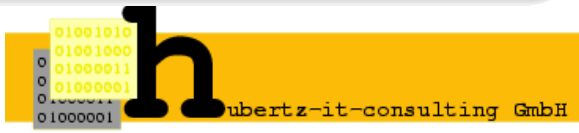
Gründung am 8. August 2005, Sitz in Köln

Geschäftsinhalt: Dienstleistungen im Umfeld der IT-Sicherheit

Logo: Johannes Hubertz Certificate Authority als ASCII-7Bitmuster

Diese paar Bits findet sich in einigen 10000 X.509 Anwenderzertifikaten in der Seriennummer wieder

Wir sind käuflich ;-)



IPv6 – nur Marketing?

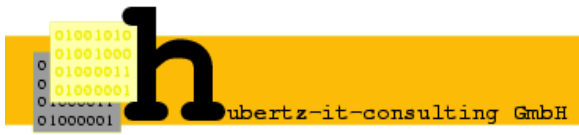
Haben Sie eine Idee,

wie **Ihr Mobiltelefon**

mit **Ihrem PC**

via bluetooth . . .

???



ewige Wahrheiten . . .

**Ich denke nie an die Zukunft,
sie kommt früh genug.**

Albert Einstein

Bald ist das Internet alle . . .

RIPE Community resolution: (27.October 2007)

„Growth and innovation on the Internet depends on the continued availability of IP address space.

The remaining pool of unallocated IPv4 address space is likely to be fully allocated within two to four years. IPv6 provides the necessary address space for future growth.

We therefore need to facilitate the wider deployment of IPv6 addresses.“

RIPE $\Leftrightarrow$ Réseaux IP Européens

Es wird ernst . . .

RIPE Community statement: (7. May 2010)

„The RIPE community supports all efforts to assist in the deployment of IPv6, especially in developing countries.

However, we note concerns being expressed within the ITU by a few members, most recently in the ITU IPv6 Group, that the current address management system is inadequate.

The RIPE community mandates the RIPE NCC to work with the ITU IPv6 Group, individual ITU members, and the community to clearly identify these concerns and to find ways to address them within the current IP address management system.“

ITU $\Leftrightarrow$ International Telecommunication Union

Februar 2011: IANA vergibt letzte /8-Blöcke an RIRs

IPv6 – Fiktion, Hype, Marketing, oder was?

IPv6 ist schon betagt:

Start in der Mitte der 90er Jahre

IPv6 ist reine Technik:

weit mehr als 200 RFCs spezifizieren IPv6

IPv6 ist notwendig:

IPv4 wird knapp (Feb. 2011: Es ist schon alle!)

IPv6 existiert:

IPv6 ist fertig, funktioniert schon bestens und bald omnipräsent

ewige Wahrheiten . . .

Menschen mit einer neuen Idee gelten solange als Spinner,
bis sich die Sache durchgesetzt hat.

Mark Twain

Mythen und Märchen

Die schlechte Nachricht

IPv6 ist genauso unsicher wie IPv4

really!

Die gute Nachricht

IPv6 ist genauso sicher wie IPv4

really!

ICMPv6 ist böse

ICMPv6 ist essentieller Bestandteil von IPv6.

ICMPv6 komplett zu filtern (wie es bei IPv4 oft üblich war), ist gleichbedeutend mit IPv6 ausschalten. Es funktioniert nicht.

IPsec ist schon drin!

IPsec wurde zuerst auf IPv6 spezifiziert

Jede IPv6-Implementierung sollte auch IPsec realisieren. Jedoch:
Zur Nutzung braucht man Schüsselverteilung,
z. B. IKEv1 oder IKEv2 oder proprietär, Preshared Keys oder X.509-Zertifikate
KnowHow-trächtige Konfigurationen sind gefragt,
Kompatibilität unter Herstellern,

. . . nix ändert sich, was reg ich mich auf . . . ;-)

Wir brauchen nur eine

PKI!

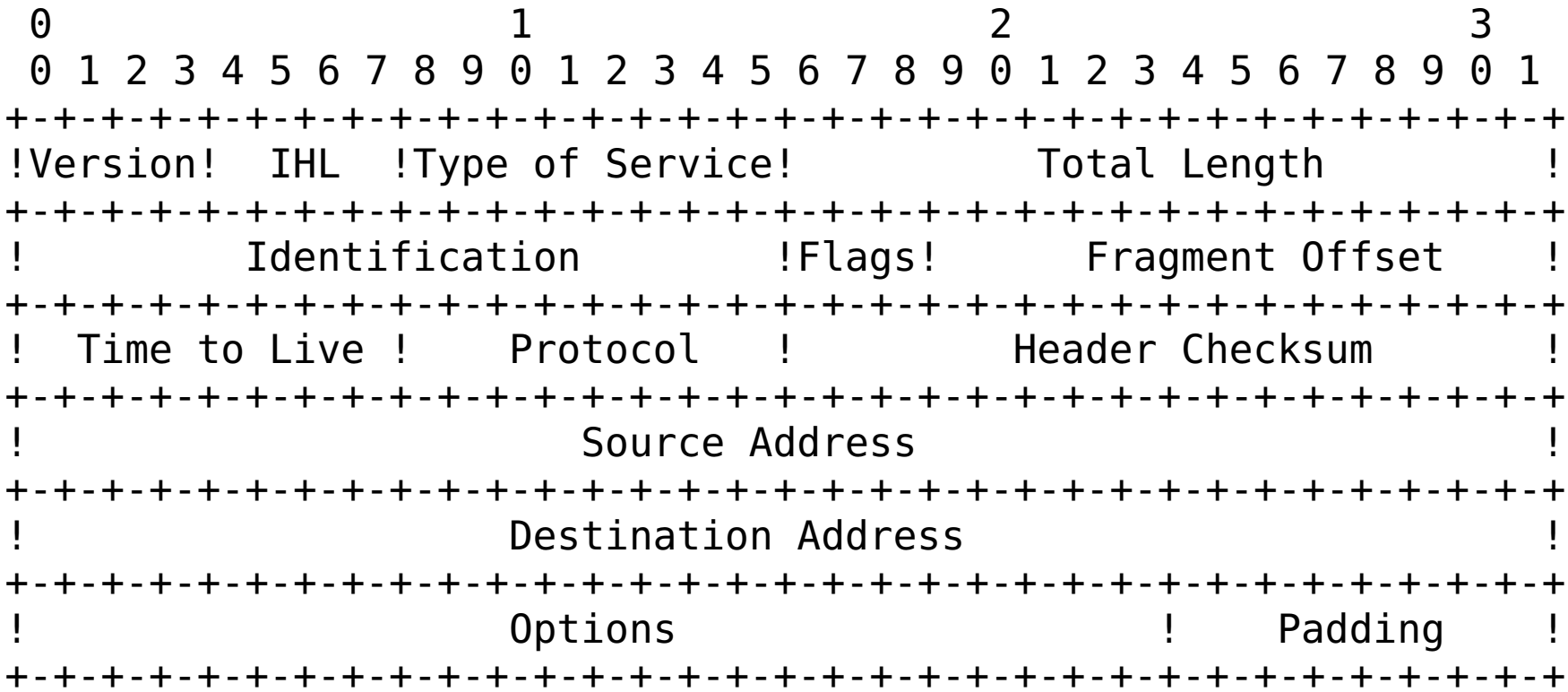
Dann ist die Welt ja in Ordnung.

IPv4 – IPv6

unvergleichbar, oder?

IP – header as defined in RFC 791 *as of September* 1981

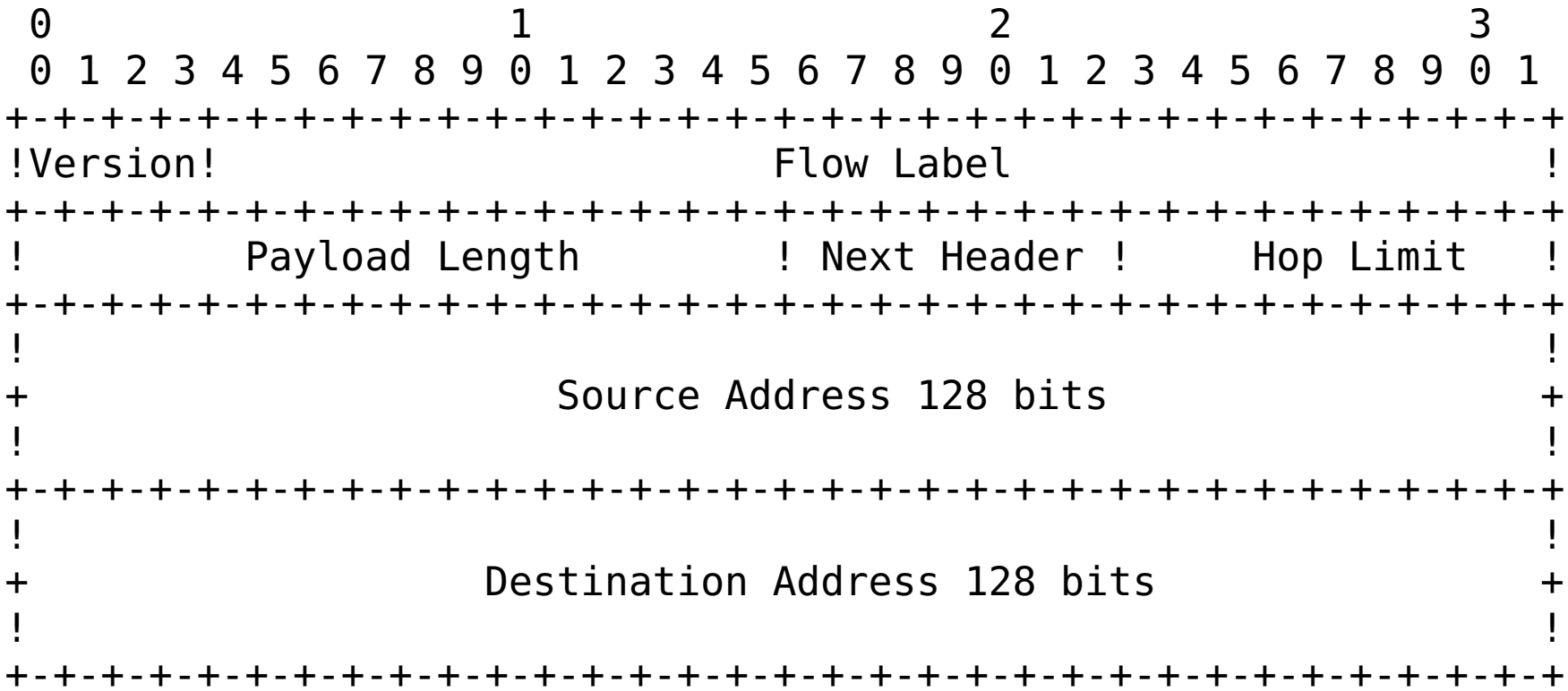
ASCII – ART



IPv6 – header as defined in RFC 2460

as of December 1998
obsoletes RFC 1883 (*December* 1995)

ASCII – ART



IPv6 – header explanations

Version	4 Bit	IP Version (==6)
Flowlabel	28 Bit	Zusatzinformationen für Router, z.B. für QOS
Payload Length	16 Bit	Länge des Paketes nach dem Header
Next Header	8 Bit	Welcher Header kommt danach?
Hop Limit	8 Bit	vgl. TTL bei IPv4
Source Address	128 Bit	
Destination Address	128 Bit	

IPv6 – address explained . . .

128 Bit are combined from:

bits number	**value** example	**meaning**
3	001_{bin} 111_{bin}	prefix global allocatable 2000::/3 multicasts et.al.
45	2001:db8::/32 2001:db8:beef::/48	global routing prefix documentation RIPE, ISP, customer friendly user test
16	0001_{hex} . . . $ffff_{hex}$	subnet ID second usable subnet /64 another $2^{16} - 3$ of /64 last usable /64
64	216:d3ff:fea4:5174	Interface ID a LapTop's ethernet interface ID

Es gibt keine Broadcasts mehr!

Adressen – Kleinigkeiten!

IPv6 – Adresseigenschaften

IPv6 Adressen sind 128 bit lang, d.h. $IP \in \{1..2^{128}\}$

$2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456_{dez}$

Das entspricht 665 Milliarden Adressen pro mm^2 Erdoberfläche

Hexadezimale Schreibweise, je 2 Bytes durch einen ‘:‘ getrennt.

Beispiel: `2001:db8:beef:4711::1` ‘::‘ $\Leftrightarrow$ fehlende 0-Bytes

‘::‘ Nur einmal in einer Adresse!

`2001:db8:beef::/48` $\Leftrightarrow$ 65.536 /64 Netze (prefix wie bei IPv4)

IPv6 – Scope (Reichweite)

link-local

Jedes Interface hat `1..n` link-local Adresse(n) aus `fe80::/10`

site-local deprecated!

Ein Interface hat `0..n` site-local Adressen aus `fc00::/8` oder `fd00::/8`

global

Ein Interface hat `0..n` globale Adressen aus `2000::/3`

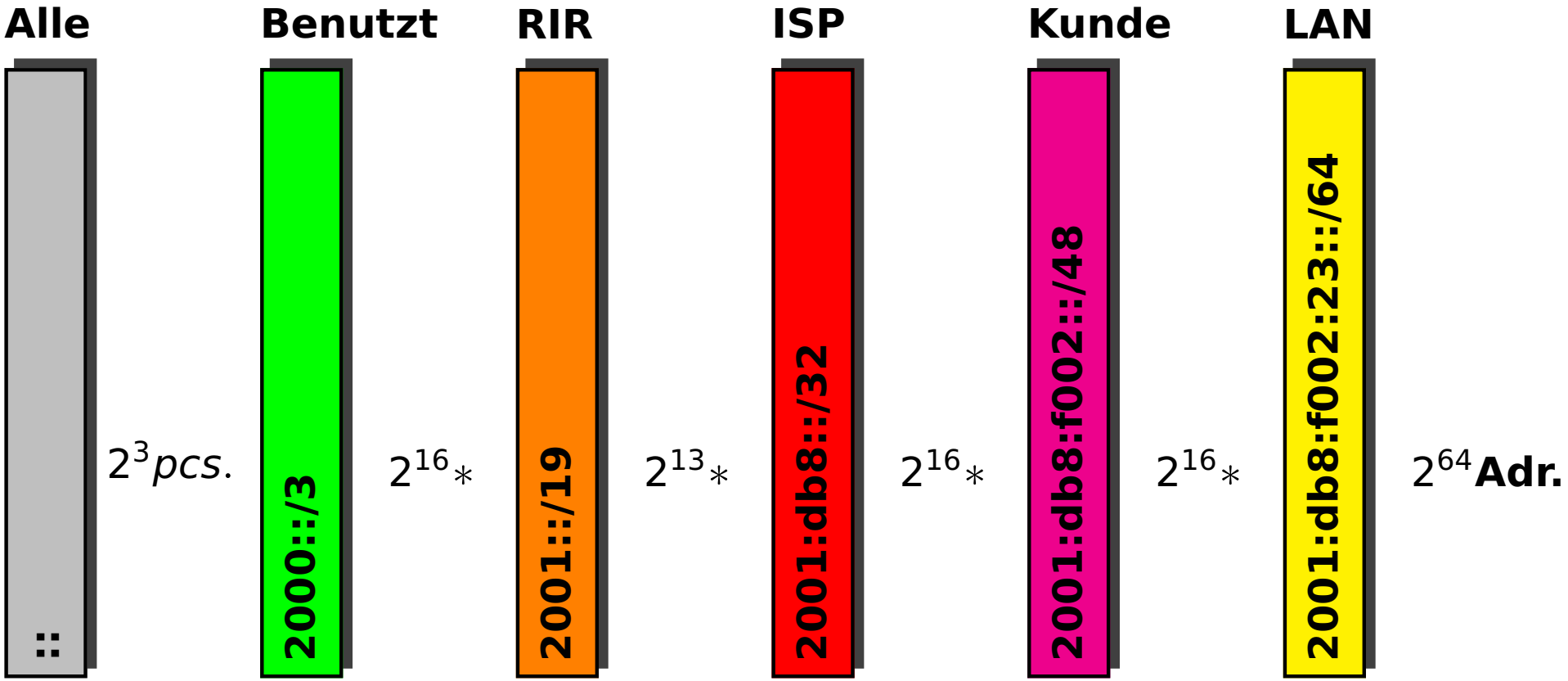
multicast

Ein Interface hat `0..n` Multicast Adressen aus `ff00::/8`

IPv6 – Besondere Adressen

::	nicht spezifizierte Adresse ⇔0:0:0:0:0:0:0:0
::1	loopback
fe80::/10	link-local
ff00::/8	multicast
ff01::1	multicast, all hosts
ff01::2	multicast, all routers
fc00::/8	Unique Local Adressen (zentral verwaltet)
fd00::/8	Unique Local Adressen
2000::/3	globale Unicast Adressen
2001:db8::/32	Prefix für Dokumentation

IPv6: Globale Verteilung



next header

Beliebig viele Header pro IP-Paket

IPv6 header: next header I

IPv6 header: next header field, 8 bits

- ähnlich dem Protokol-Feld im IPv4-Header, aber universeller
- Werte gleich, siehe auch `/etc/protocols`
- beliebig verkettbar
- RH Typ 0 und 2 bergen einige Sicherheitsrisiken
- RH Typ 0 ist „deprecated“ $\Rightarrow$, ist aber schon implementiert!(RFC 5095)
- RH Typ 2 ist essentieller Bestandteil von Mobile IPv6

Lösungsansätze gibt es, aber

- entweder kompliziert, z.B. im Firewalling
- oder noch nicht allgemein implementiert (RFC 5095)

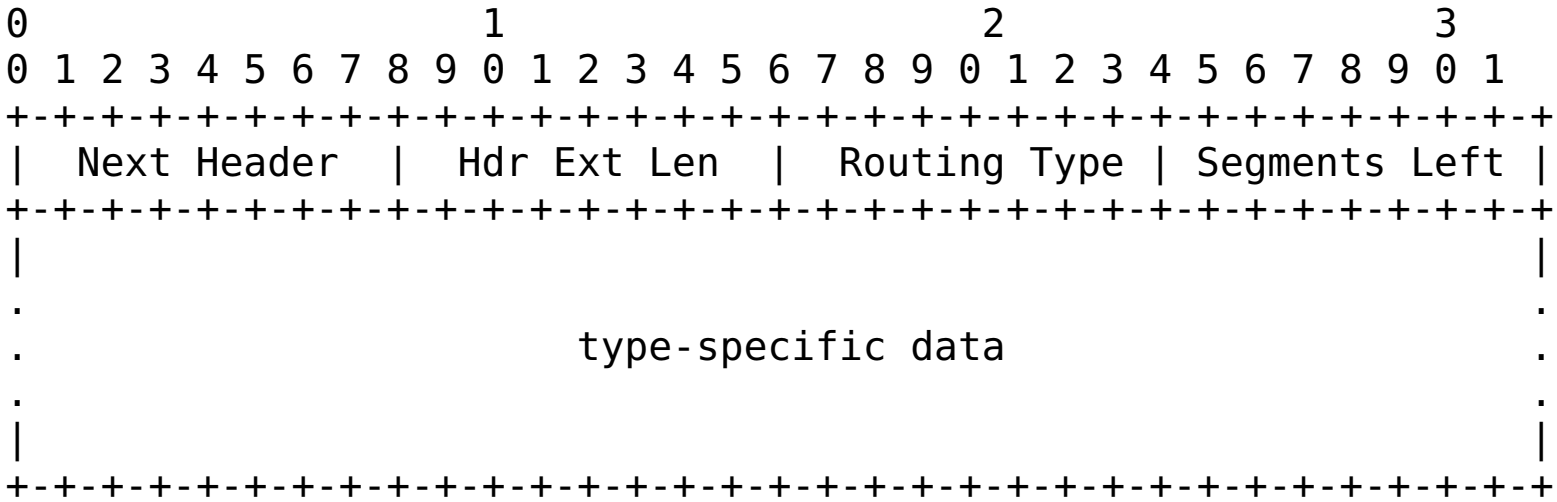
IPv6 header: next header II

Extension Header in der Basis-Spezifikation

value	**meaning**
0	hop by hop options header
43	routing header
44	fragmentation header
50	encapsulation payload header (RFC 2406)
51	authentication header (RFC 2402)
60	destination options header

IPv6 header: next header III

routing header *müssen* von jedem Host verarbeitet werden



routing header type 0

Enspricht dem (strict/loose) sourcerouting, für debug, ISP-spez.Routing, . . .

routing header type 2

Wird zwingend für Mobile-IPv6 benötigt

IPv6 header: next header IV

Verkettungen sind in beliebiger Länge möglich:

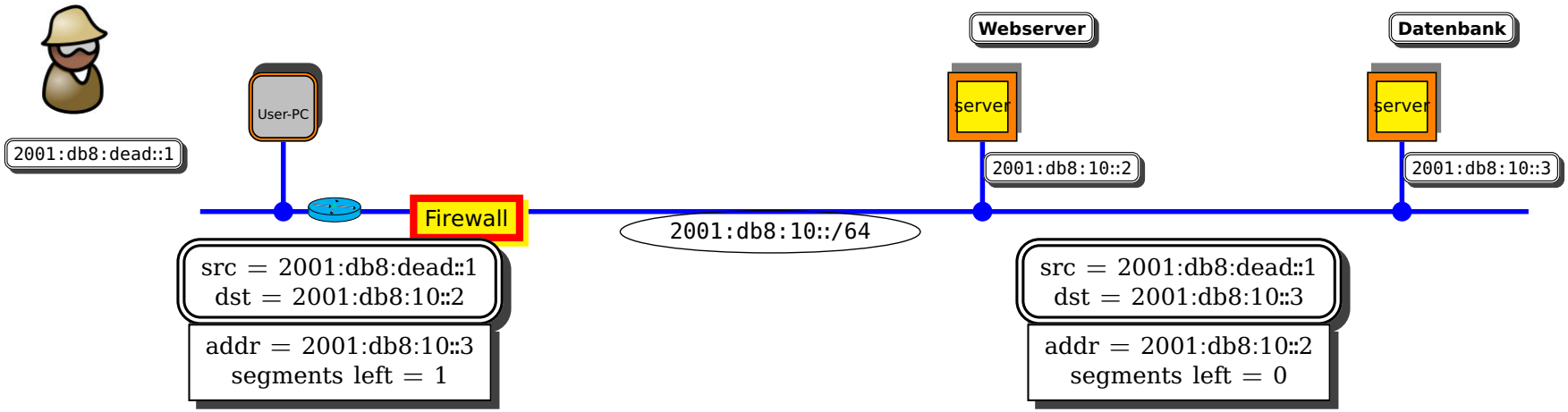
IPv6 header Next header = TCP value 6	TCP header and data		
IPv6 header Next header = Routing Value 43	Routing header Next header = TCP Value = 6	TCP header and data	
IPv6 header Next header = Routing Value 43	Routing header Next header = Fragment Value = 44	Fragment header Next header = TCP Value 6	TCP header and data

IPv6 header: next header V

Reihenfolge der extension header:

1	IPv6 Header
2	Hop-by-Hop Options Header
3	Destination Options Header für Router auf dem Pfad
4	Routing Header
5	Fragment Header
6	Authentication Header
7	Encapsulation Security Payload Header
8	Destination Options Header für den endgültigen Empfänger
9	Upper-Layer Header

IPv6 header: next header – malicious usage



Angreifer schickt ein Paket an die erreichbare Adresse ::2, dieser Host leitet es weiter an ::3, welcher durch Firewall strikt gefiltert wird.

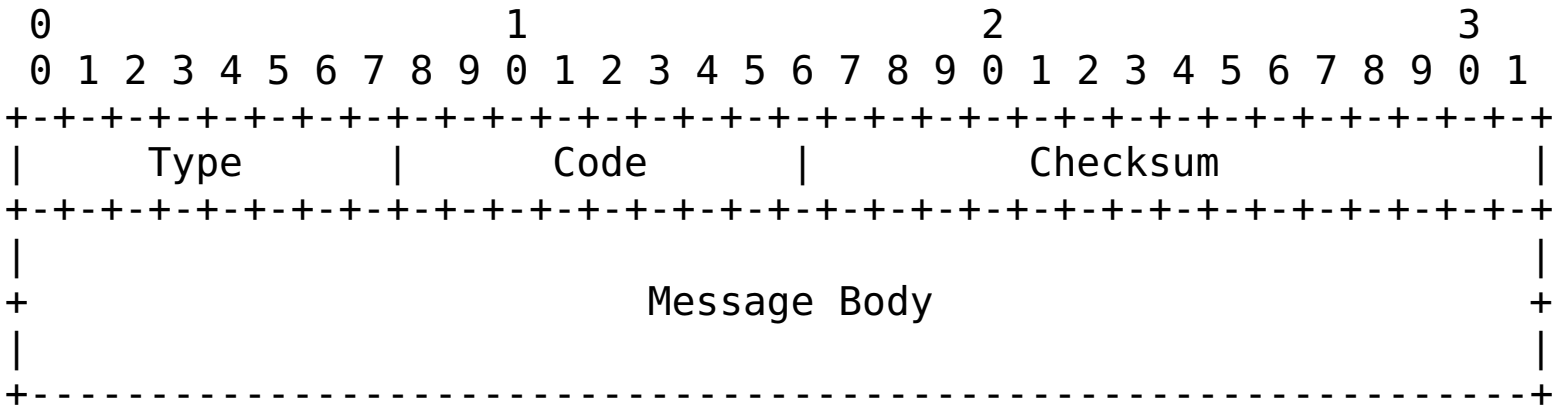
ICMPv6

internet control message protocol version 6

ICMPv6 – as defined in RFC 2463

ICMPv6

1.) nutzt multicasts: **ff00::0 ip6-mcastprefix**
2.) erkennt doppelte Adressen: **duplicate address detection (DAD)**
3.) ersetzt ARP vollständig: **neighbor discovery (ND)**
4.) kann automatisch Routen: **router discovery (RD)**



ICMPv6 ist essentieller Bestandteil der Ende-zu-Ende Kommunikation!
Daher: Filterung von ICMPv6 nur auf spezielle icmp-types möglich

ICMPv6 – as defined in RFC 2463

type	meaning
1	Destination Unreachable
2	Packet Too Big
3	Time Exceeded
4	Parameter Problem
128	Echo Request
129	Echo Reply
130	Group Membership Query
131	Group Membership Report
132	Group Membership Reduction
133	Router Solicitation
134	Router Advertisement
135	Neighbor Solicitation
136	Neighbor Advertisement
137	Redirect
138	Router Renumbering

DAD – duplicated address detection

duplicate address detection

DAD geschieht vor der Zuweisung der eigenen IPv6-Adresse, RFC 2462, December 1998: „Duplicate Address Detection is performed on unicast addresses prior to assigning them to an interface whose DupAddrDetectTransmits variable is greater than zero. Duplicate Address Detection MUST take place on all unicast addresses, regardless of whether they are obtained through stateful, stateless or manual configuration, with the exception of the following . . . “

1. Unicast, ICMP Typ 135, Absender ‘::‘ an die Zieladresse
2. Falls vorhanden, erfolgt eine Antwort an ff02::1
3. Falls nicht vorhanden, wird die Adresse gewählt

ND – neighbor detection

neigbour detection

ND ersetzt arp (address resolution protocol) RFC 2461, December 1998:
„Neighbor Solicitation: Sent by a node to determine the link-layer address of a neighbor, or to verify that a neighbor is still reachable via a cached link-layer address. Neighbor Solicitations are also used for Duplicate Address Detection.
Neighbor Advertisement: A response to a Neighbor Solicitation message. A node may also send unsolicited Neighbor Advertisements to announce a link-layer address change.

1. prefix ff02::1:ff00:0/104 und rechte 3 Oktetts der Ziel-IP $\rightarrow$ Multicast-Addresse
2. icmpv6 type 135 an diese Adresse
3. Zielhost antwortet mit icmpv6 type 136 oder timeout

IPv6 – autoconfiguration

automagically configuration of workstations. . .

IPv6 – fast alles kann automatisch geschehen . . .

1. Interface-ID (MAC-Adresse) bestimmt link-local-Adresse $\rightarrow$ `fe00::/64`
2. DAD = duplicate address detection
3. RD = router detection
4. aktiver Host am LAN, erkennt Routing-Änderungen mit RD

Linux

interfaces – configuration

IPv6 Interface: Linux configuration

static:

```
tut:~# more /etc/network/interfaces
# The loopback network interface
auto lo
iface lo inet loopback
#
auto eth2
iface eth2 inet6 static
        pre-up /sbin/modprobe ipv6
        address 2001:db8:beef:fb00::1
        netmask 64
        post-up /sbin/ip route add 2001:db8:beef:fb00::/56 via 2001:db8:beef:fb00::2
        post-up echo "1" > /proc/sys/net/ipv6/conf/all/forwarding
```

autoconfiguration:

```
tut:~# more /etc/network/interfaces
# The loopback network interface
auto lo
iface lo inet loopback
# The primary network interface
allow-hotplug eth0
iface eth0 inet6 manual
        pre-up /sbin/ip link set dev eth0 up
        post-down /sbin/ip link set dev eth0 down
```

IPv6 Linux commands

`ip -6 address add nnn dev eth0 scope global`	IP-Adresse hinzufuegen
`ip -6 address del nnn dev eth0`	IP-Adresse wegnehmen
`ip -6 neigh show`	Nachbarschaft anzeigen
`ip -6 route show`	IPv6 Routen auflisten
`ip -6 route add target via nexthop dev eth0`	IPv6 Route hinzufuegen
`ip -6 route del target via nexthop dev eth0`	IPv6 Route wegnehmen

IPv6 Interface: OpenBSD configuration

static:

```
# cat hostname.sis0
inet 192.168.110.177 255.255.255.0 NONE
inet6 2001:db8:beef:2::10/64
#
# grep rtadvd rc.conf
rtadvd_flags=NO         # for normal use: list of interfaces
#
```

autoconfiguration:

```
# grep ip6 sysctl.conf
net.inet6.ip6.forwarding=0      # 1=Permit forwarding (routing) of IPv6 packets
#net.inet6.ip6.mforwarding=1    # 1=Permit forwarding (routing) of IPv6 multicast packets
#net.inet6.ip6.multipath=1      # 1=Enable IPv6 multipath routing
net.inet6.ip6.accept_rtadv=1    # 1=Permit IPv6 autoconf (forwarding must be 0)
#
```

IPv6 OpenBSD commands

ifconfig	**Alle Interfaces anzeigen [Mix aus L1,L2,L3]**
ndp -an	**Nachbarschaft anzeigen**
route -n show	**Routingtabelle anzeigen**

Client Autoconfiguration . . .

Server and clients view

IPv6 clients autoconfiguration (magic)

— Server —

radvd server-config-file[1] follows:

```
1 interface eth2 {
2    AdvSendAdvert on;
3    prefix 2001:db8:beef:fc00::/64    { };
4 };
```

rtadvd server-config-file[2] follows:

```
1 # cat /etc/rtadvd.conf
2 sis1: \
3         prefix: 2001:db8:beef::/48
4         prefix: 2001:db8:beef:0020::/64
5 #
```

Remark: radvd – router advertisement daemon

[1] Debian GNU/Linux: /etc/radvd.conf
[2] OpenBSD: /etc/rtadvd.conf

IPv6 clients autoconfiguration (magic)

— Server —

dibbler server-config-file[3] follows:

```
1  log-level 8
2  log-mode short
3  preference 0
4  iface "eth2" {
5   // also ranges can be defines, instead of exact values
6   t1 1800-2000
7   t2 2700-3000
8   prefered-lifetime 3600
9   valid-lifetime 7200
10  class {
11     pool 2001:db8:beef:fc00:0100:0000::/96
12  }
13  ta-class {
14     pool 2001:db8:beef:fc00:0200:0000::/96
15  }
16  pd-class {
17      pd-pool 2001:db8:beef:fc00:0300::/80
18      pd-length 96
19  }
20  option dns-server 2001:db8:beef:1::53
21  option domain hubertz.de
22  option vendor-spec 5678-0x0002aaaa
23  option ntp-server 2001:db8:beef:1::1
24  option time-zone  CET
25 }
```

Remark: dibbler-server is a portable implementation of the DHCPv6 server.

[3] Debian GNU/Linux: /etc/dibbler/server.conf

IPv6 client autoconfiguration (magic only)

— Client —

dibbler client-config-file[4] follows:

```
# 8 (Debug) is most verbose. 7 (Info) is usually the best option
log-level 7
# To perform stateless (i.e. options only) configuration, uncomment
# this line below and remove any "ia" keywords from interface definitions
#
# stateless
#
iface eth0 {
# ask for address
    ia
# ask for options
   option dns-server
   option domain
#   option ntp-server
#   option time-zone
#   option sip-server
#   option sip-domain
#   option nis-server
#   option nis-domain
#   option nis+-server
#   option nis+-domain
}
```

Remark: dibbler-client is a portable implementation of the DHCPv6 client.

[4] Debian GNU/Linux: /etc/dibbler/client.conf

Alle Clients sind konfiguriert,

Was nun?

Wir haben eine Firewall!

Da ist alles sicher.

?

NetFilter

ip6tables, pf – und wie?

NetFilter – linux 2.4, 2.6, . . .

altbewährte Technik mit 3 Standard-chains

- INPUT
- OUTPUT
- FORWARD
- userdefined chains

Ein Kommando für alles

man ip6tables

```
/sbin/ip6tables --help
```

/sbin/ip6tables – linux 2.4, 2.6, . . .

```
#
# /sbin/ip6tables --help

Usage: ip6tables -[AD] chain rule-specification [options]
       ip6tables -I chain [rulenum] rule-specification [options]
       ip6tables -R chain rulenum rule-specification [options]
       ip6tables -D chain rulenum [options]
       ip6tables -[LS] [chain [rulenum]] [options]
       ip6tables -[FZ] [chain] [options]
       ip6tables -[NX] chain
       ip6tables -E old-chain-name new-chain-name
       ip6tables -P chain target [options]
       ip6tables -h (print this help information)

. . .
```

Die man-page liest sich noch mühsamer!

Der Mensch ist faul und infolgedessen auch erfindungsreich . . .

Paketfilter I: Hier ist Handarbeit gefragt

Definitionen: Wer ist hier beteiligt?

#**Name**	**Adresse**	**Kommentar**
any	::/0	# Alle Welt
many	2000::/3	# erreichbare Welt
localhost	::1/128	#
srv	2001:db8:beef:2::10/128	# service
ns	2001:db8:beef:1::53/128	# 1.nameserver
ns	2001:db8:beef:3::23/128	# 2.nameserver
nc-dns	2001:4dd9:abcd:0:0:2:b351:f602/128	# NetCologne DNS
admin	2001:db8:beef:3:a00:27ff:fe67:4649/128	# administration
#admin	fe80::a00:27ff:fe67:4649/128	# administration

Paketfilter II: nochmals Handarbeit gefragt

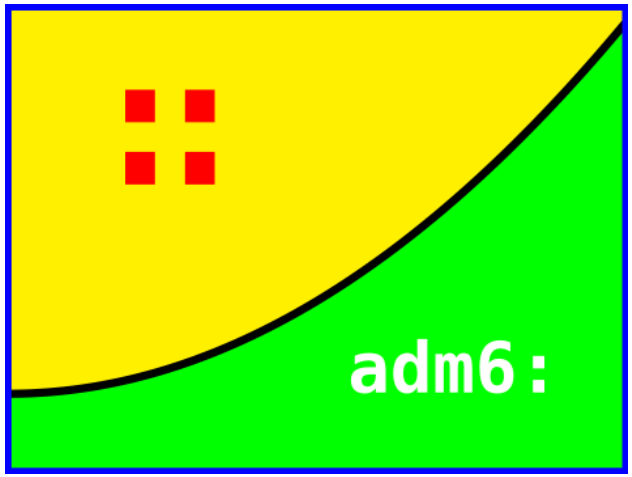
Regeln: Wer darf mit wem was?

#Source	Destination	protocol	port	action	Options	#Kommentar
admin	ns	tcp	22	accept	NOIF	
many	ns	udp	53	accept		
any	any	ip6	all	drop		# no def. log

Paketfilter III: Handarbeit ⇒ Automatik

adm6: Python generiert Filter für **Linux, OpenBSD, Win-XP, . . .**

http://evolvis.org/projects/adm6



git clone https://evolvis.org/anonscm/git/adm6/adm6.git

Lizenz: GNU General Public License version 3 or later

Quellen und Lesestoff

... only a few of more than 200 ...
RFC 2460 Internet Protocol, Version 6 (IPv6) Specification
RFC 2461 Neighbor Discovery for IP Version 6 (IPv6)
RFC 2462 IPv6 Stateless Address Autoconfiguration
RFC 2463 Internet Control Message Protocol for the Internet Protocol Version 6 (IPv6) Specification
RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
RFC 3315 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
RFC 3484 Default Address Selection for Internet Protocol version 6 (IPv6)
RFC 3756 IPv6 Neighbor Discovery (ND) Trust Models and Threats
RFC 3775 Mobility Support in IPv6
RFC 3971 SEcure Neighbor Discovery (SEND)
RFC 3972 Cryptographically Generated Addresses (CGA)
RFC 4429 Optimistic Duplicate Address Detection (DAD) for IPv6
RFC 4443 Internet Control Message Protocol for the Internet Protocol Version 6 (IPv6) Specification
RFC 4861 Neighbor Discovery for IPv6
RFC 4890 Recommendations for Filtering ICMPv6 Messages in Firewalls
RFC 5095 Deprecation of RH0

Linux:
http://www.bieringer.de/linux/IPv6/IPv6-HOWTO/IPv6-HOWTO.html
OpenVPN-tunnelbroker: http://blog.ghitr.com/index.php/archives/673
http://www.6net.org/publications/presentations/strauf-openvpn.pdf

Books:
IPv6 in Practice, Benedikt Stockebrand, Springer, ISBN 978-3-540-24524-7
IPv6, Sylvia Hagen, Sunny Edition, 2. Auflage, ISBN 978-3-9522842-2-2
Deploying IPv6 Networks, Ciprian Popoviciu et.al., Cisco Press, ISBN 1587052105

Tests:
http://freeworld.thc.org/thc-ipv6/
http://lg.he.net/

Security:
http://www.wecon.net/files/48/GUUG-RT_WEST2010-SvI.pdf
http://seanconvery.com/ipv6.html

Ich bedanke mich für Ihre Aufmerksamkeit

hubertz-it-consulting GmbH jederzeit zu Ihren Diensten

Ihre Sicherheit ist uns wichtig!

Frohes Schaffen

Johannes Hubertz

it-consulting _at_ hubertz dot de

powered by LaTeX 2ε
and PSTricks

hubertz-it-consulting GmbH