



Let's talk about it...



(IPv6 wartet schon eine Weile auf den Durchbruch..)

Let's talk about it...



(IPv6 wartet schon eine Weile auf den Durchbruch..)

Übersicht

- Geschichte
- Konzepte
- Adressaufbau und Arten
- IPv4 => IPv6
- Beispiele in der Praxis
- Adressvergabe bei IPv6
- Heute nicht:
 - ICMP6 Neighbor Discovery (ARP für IPv6)
 - Ethernet Protocol

Geschichte

- **IPv4**
 - Späte 1970
 - 4 Byte Adresse, z.B. 216.58.211.3 (ca. 4.3 Milliarden)
 - NAT - Network Address Translation
- **IPv5** (1970er, Internet Stream Protokoll)
- **IPv6**
 - Frühe 1990
 - 16 Bytes, z.B. 2001:a60:a07d:1:3113:1f13:d36f:9c53 (2^{128} ...)
 - End-zu-End Prinzip
- Übrigens: IP Header hat 4 Bit Feld (max. IPv8)

Adressverteiler



CIDR Notation

- Classless Inter-Domain Routing (CIDR)
- IPv4 hat Class A/B/C Netze... zu ungenau..

192.168.1.1	192.168.1.1/32	
192.168.1.x	192.168.1.0/24	Class C
192.168.x.y	192.168.0.0/16	Class B
10.x.y.z	10.0.0.0/8	Class A
192.168.[30/31].x	192.168.0.0/23	Class ?

Notation wird verwendet in Konfigurationsoberflächen,
Dokumentationen, Konsole..



~255 x Ipv4 /8 Blöcke

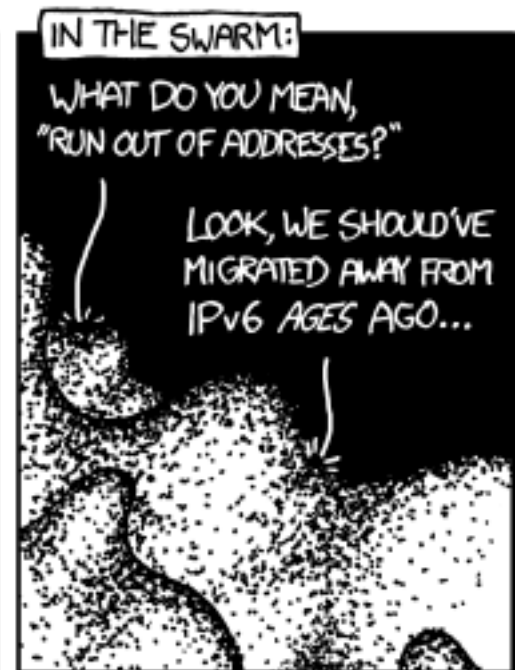
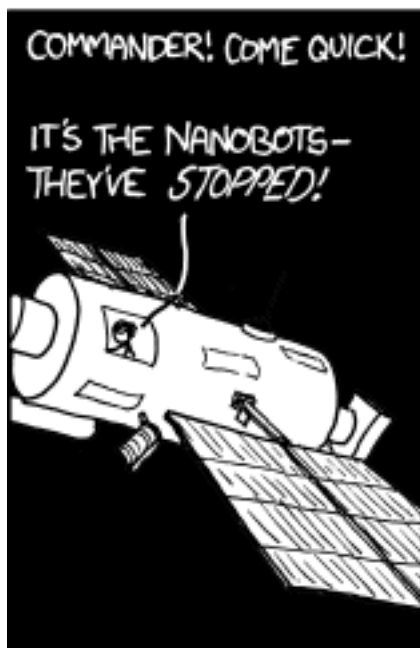
- Anfang 2011 letzter /8 Block von der RIPE verteilt
- Auktionen und “Recycling”
- Angeblich nur 20% genutzt
- Ungleicher Verteilung
 - 36.0.0.0/8 - Stanford University
 - IBM / Ford / ...
 - US DoD hat mehrere /8 Blöcke
 - Historische Verteilung

IPv4 Adressen sind aus..



IPv6 Adressen

- $2^{128} \approx 3.4 \cdot 10^{38} \Rightarrow$ Sehr Viele!



IPv6 Adressaufbau

- 16 Bytes (= 128 Bit)
- Hexadezimal. 00 (0) bis FF (255)
- 8x 2-Byte Blöcke getrennt mit Semicolon
- Schreibweise:
 - 2001:0DB8:0000:0000:0208:C7FF:FEC5:5E7A
 - 2001:0DB8:0:0:208:C7FF:FEC5:5E7A
 - 2001:0DB8::208:C7FF:FEC5:5E7A
- Groß/Kleinschreibung egal
- Abkürzungsregeln
 - Vorgestellte Nullen müssen nicht geschrieben werden
 - Eine (!) Folge von Nullen darf mit :: abgekürzt werden

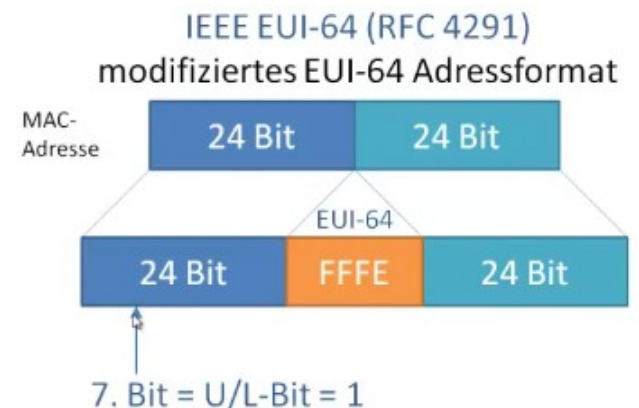
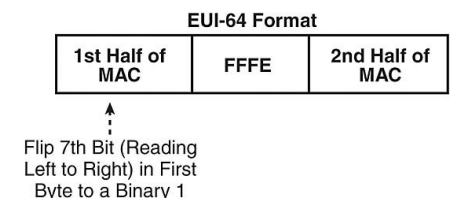
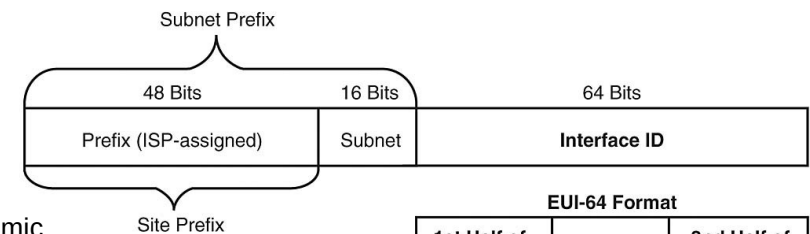


IPv6 Konzepte

- Viele Adressen insgesamt und auch viele pro Interface
- Viele Subnetze in einem Netz normal (~ “DHCP” Server)
- End-zu-End Kommunikation
 - kein NAT nötig (War nie als Security-Feature gedacht)
 - Server am Heimanschluss
 - Direkte Kommunikation möglich ohne Server (Telefon/Chat?)
- Effizienter und eleganter, z.B. Anycast/Multicast statt Broadcast
- Automatische Konfiguration (Lokale und globale Adresse!)
- Keine Fragmentierung
 - “MTU detection”
- Kritikpunkte
 - Lange Adressen
 - DNS..?
 - Privatsphäre
 - Privacy Extensions..?

Viele Adressen...

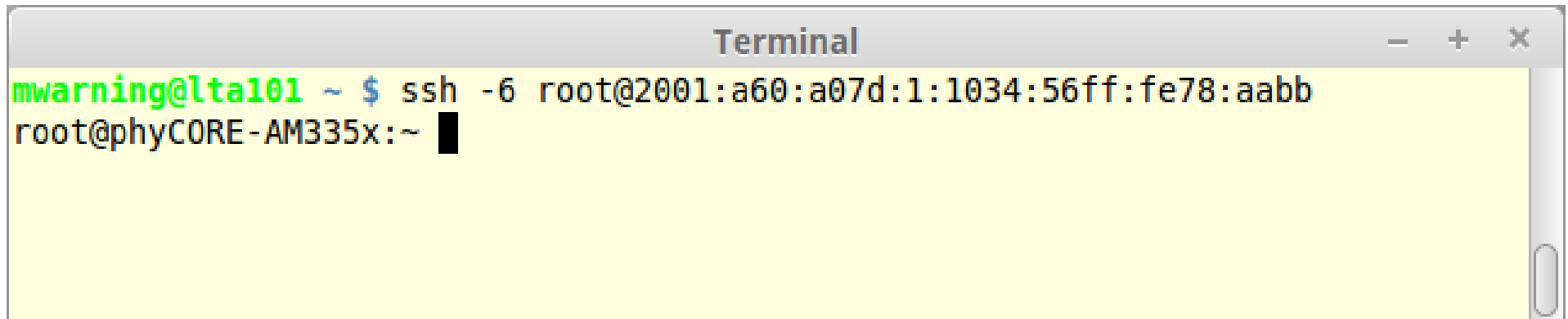
- mwarning@lta101 ~ \$ ip a
- 1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
 - link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
 - inet 127.0.0.1/8 scope host lo
 - valid_lft forever preferred_lft forever
 - inet6 ::1/128 scope host
 - valid_lft forever preferred_lft forever
- 2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
 - link/ether 34:e6:d7:4b:83:84 brd ff:ff:ff:ff:ff:ff
 - inet 192.168.31.93/23 brd 192.168.31.255 scope global eth0
 - valid_lft forever preferred_lft forever
 - inet6 2001:a60:a07d:1:3113:1f13:d36f:9c53/64 scope global temporary dynamic
 - valid_lft 562216sec preferred_lft 43216sec
 - inet6 2001:a60:a07d:1:5ddf:c27e:984a:e40a/64 scope global temporary deprecated dynamic
 - valid_lft 476418sec preferred_lft 0sec
 - inet6 2001:a60:a07d:1:ed6b:e5:2179:20db/64 scope global temporary deprecated dynamic
 - valid_lft 390620sec preferred_lft 0sec
 - inet6 2001:a60:a07d:1:a83d:b670:dd5b:1874/64 scope global temporary deprecated dynamic
 - valid_lft 304822sec preferred_lft 0sec
 - inet6 2001:a60:a07d:1:d5d8:e607:9e44:e778/64 scope global temporary deprecated dynamic
 - valid_lft 219025sec preferred_lft 0sec
 - inet6 2001:a60:a07d:1:c0e4:30f3:b104:1a17/64 scope global temporary deprecated dynamic
 - valid_lft 133227sec preferred_lft 0sec
 - inet6 2001:a60:a07d:1:bce6:925e:571a:33f7/64 scope global temporary deprecated dynamic
 - valid_lft 47430sec preferred_lft 0sec
 - inet6 2001:a60:a07d:1:36e6:d7ff:fe4b:8384/64 scope global dynamic
 - valid_lft 2591838sec preferred_lft 604638sec
 - inet6 fe80::36e6:d7ff:fe4b:8384/64 scope link
 - valid_lft forever preferred_lft forever



Blue'Log (1)

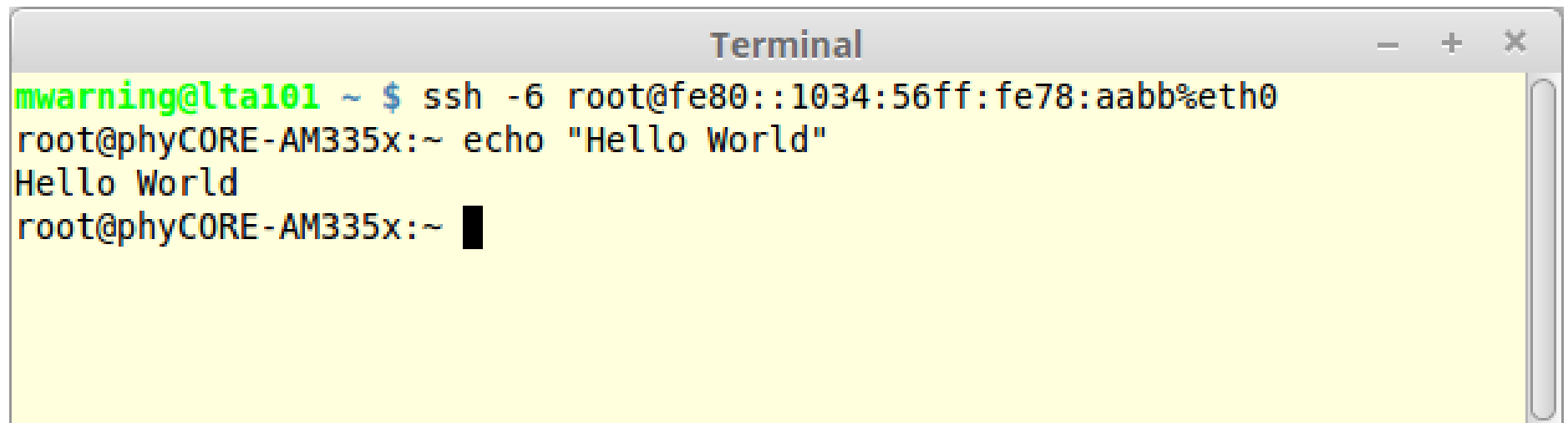
```
Terminal
root@phyCORE-AM335x:~ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: can0: <NOARP,UP,LOWER_UP,ECHO> mtu 16 qdisc pfifo_fast state UNKNOWN qlen 10
    link/can
    inet 127.42.23.179/24 scope host can0
        valid_lft forever preferred_lft forever
3: can1: <NOARP,UP,LOWER_UP,ECHO> mtu 16 qdisc pfifo_fast state UNKNOWN qlen 10
    link/can
    inet 127.42.23.179/24 scope host can1
        valid_lft forever preferred_lft forever
4: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 12:34:56:78:aa:bb brd ff:ff:ff:ff:ff:ff
    inet 192.168.30.219/23 brd 192.168.31.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 2001:a60:a07d:1:1034:56ff:fe78:aabb/64 scope global dynamic
        valid_lft 2591980sec preferred_lft 604780sec
    inet6 fe80::1034:56ff:fe78:aabb/64 scope link
        valid_lft forever preferred_lft forever
5: sit0@NONE: <NOARP> mtu 1480 qdisc noop state DOWN qlen 1
    link/sit 0.0.0.0 brd 0.0.0.0
root@phyCORE-AM335x:~
```

Blue'Log (2)



A terminal window titled "Terminal" with standard window controls (minimize, maximize, close). The background is yellow. The text shows a user named "mwarning" at a host "lta101" running an SSH command to connect to a remote host. The command is "ssh -6 root@2001:a60:a07d:1:1034:56ff:fe78:aabb". The prompt then changes to "root@phyCORE-AM335x:~" followed by a black cursor block.

```
Terminal  
mwarning@lta101 ~ $ ssh -6 root@2001:a60:a07d:1:1034:56ff:fe78:aabb  
root@phyCORE-AM335x:~ █
```

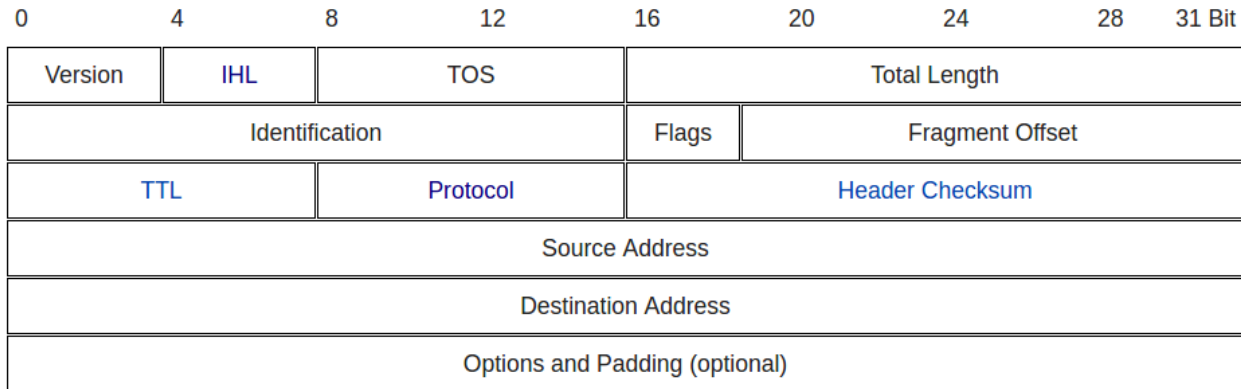


A terminal window titled "Terminal" with standard window controls (minimize, maximize, close). The background is yellow. The text shows a user named "mwarning" at a host "lta101" running an SSH command to connect to a remote host. The command is "ssh -6 root@fe80::1034:56ff:fe78:aabb%eth0". The prompt then changes to "root@phyCORE-AM335x:~" and the user enters the command "echo 'Hello World'". The output "Hello World" is displayed, and the prompt returns to "root@phyCORE-AM335x:~" followed by a black cursor block.

```
Terminal  
mwarning@lta101 ~ $ ssh -6 root@fe80::1034:56ff:fe78:aabb%eth0  
root@phyCORE-AM335x:~ echo "Hello World"  
Hello World  
root@phyCORE-AM335x:~ █
```

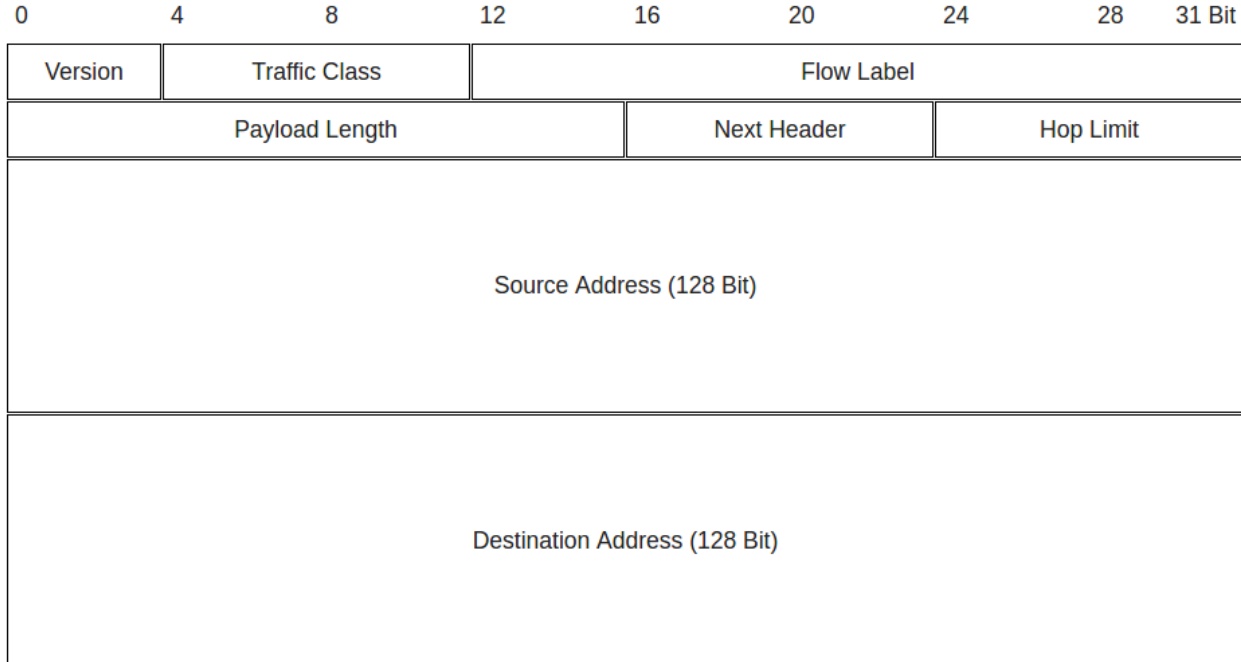

IP Header

IPv4



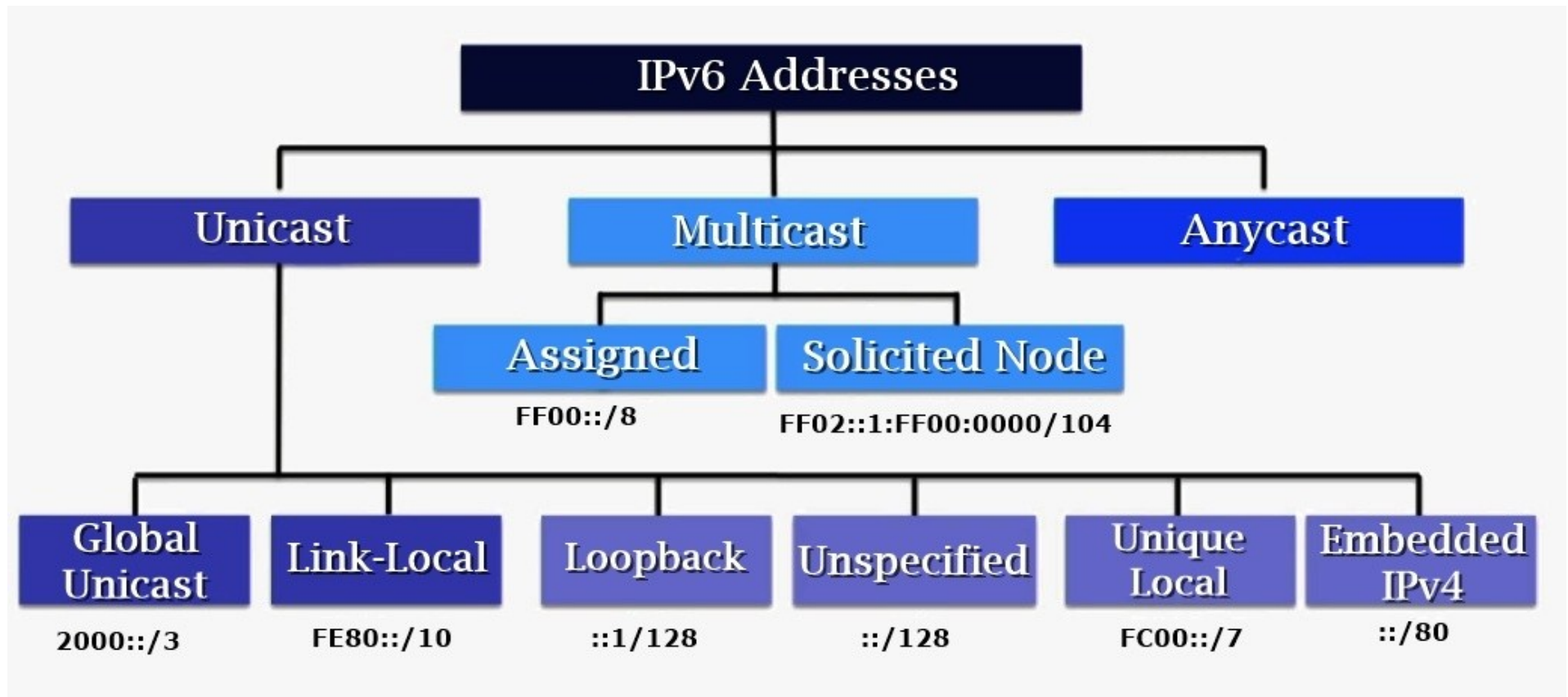
20+ Bytes

IPv6



40 Bytes

Adresstypen

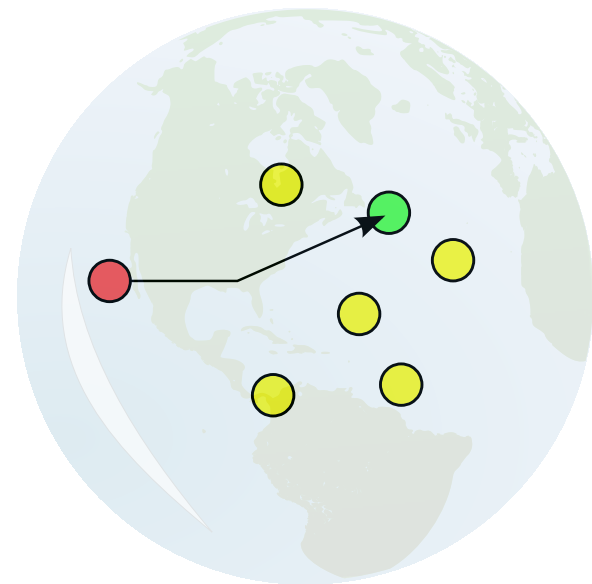
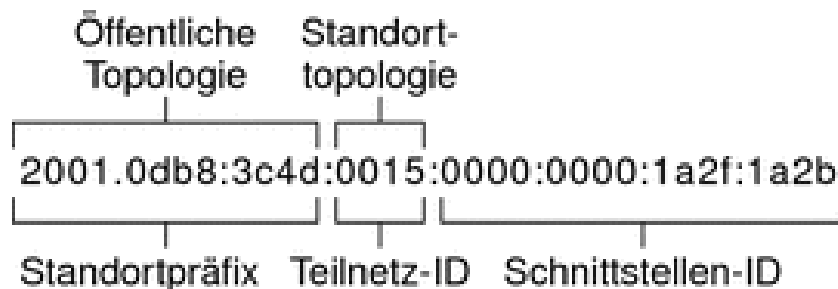


Paket-Quelle: Ist immer Unicastadresse

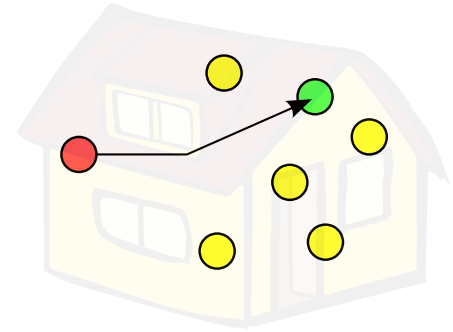
Paket-Ziel: Unicast-, Multicast- oder Anycast-Adresse

Global Unicast

- Unicast: Zieladresse ist ein Interface
- Global eindeutig
- 2000::/3
- Meteocontrol:
 - 2001::a60:a07d/48
 - 2001:a60:a07d:1/64



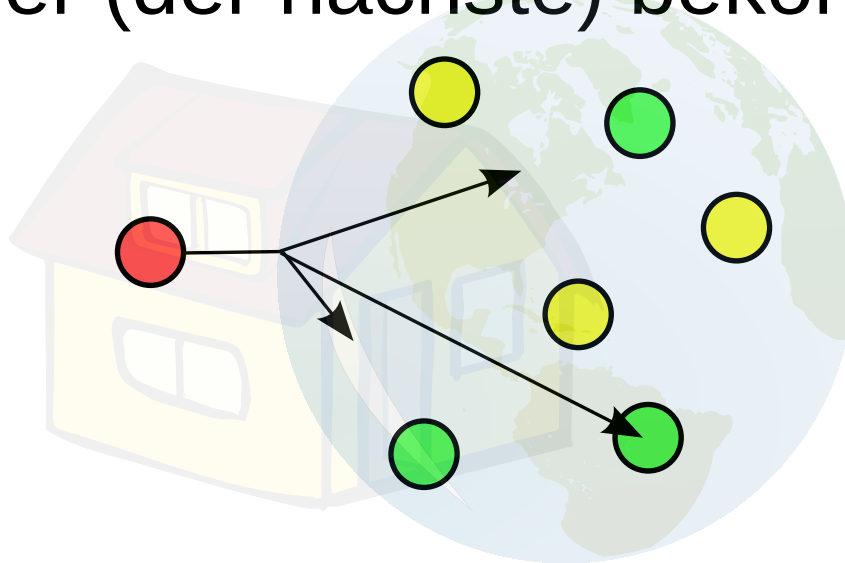
Link Local



- local unicast
- fe80::/10
 - Der Rest wird gewürfelt oder mit MAC erzeugt
 - Darf mehrmals auf dem System vorkommen
 - z.B. für eth0 und eth1 identisch
 - Weil “Link Local”
- Jedes IPv6 fähige Interface hat mindestens eine (auch ohne “DHCP”)
- Darüber wird u.a. auch der “DHCP”-Server angesprochen.

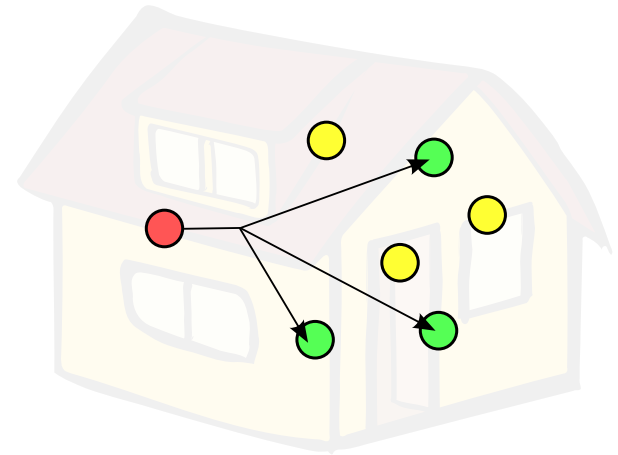
Anycast

- Nur ganz kurz das Konzept
- Wenn ihr z.B. 8.8.8.8 anpingt dann ist das nicht ein physikalischer Rechner in der USA oder so
 - Sondern einer von vielen
 - Jeder hat diese Adresse
- Irgendeiner (der nächste) bekommt die Pakete



Multicast

- Eine Adresse für die es mehrere Empfänger gibt
- Nur Lokal!

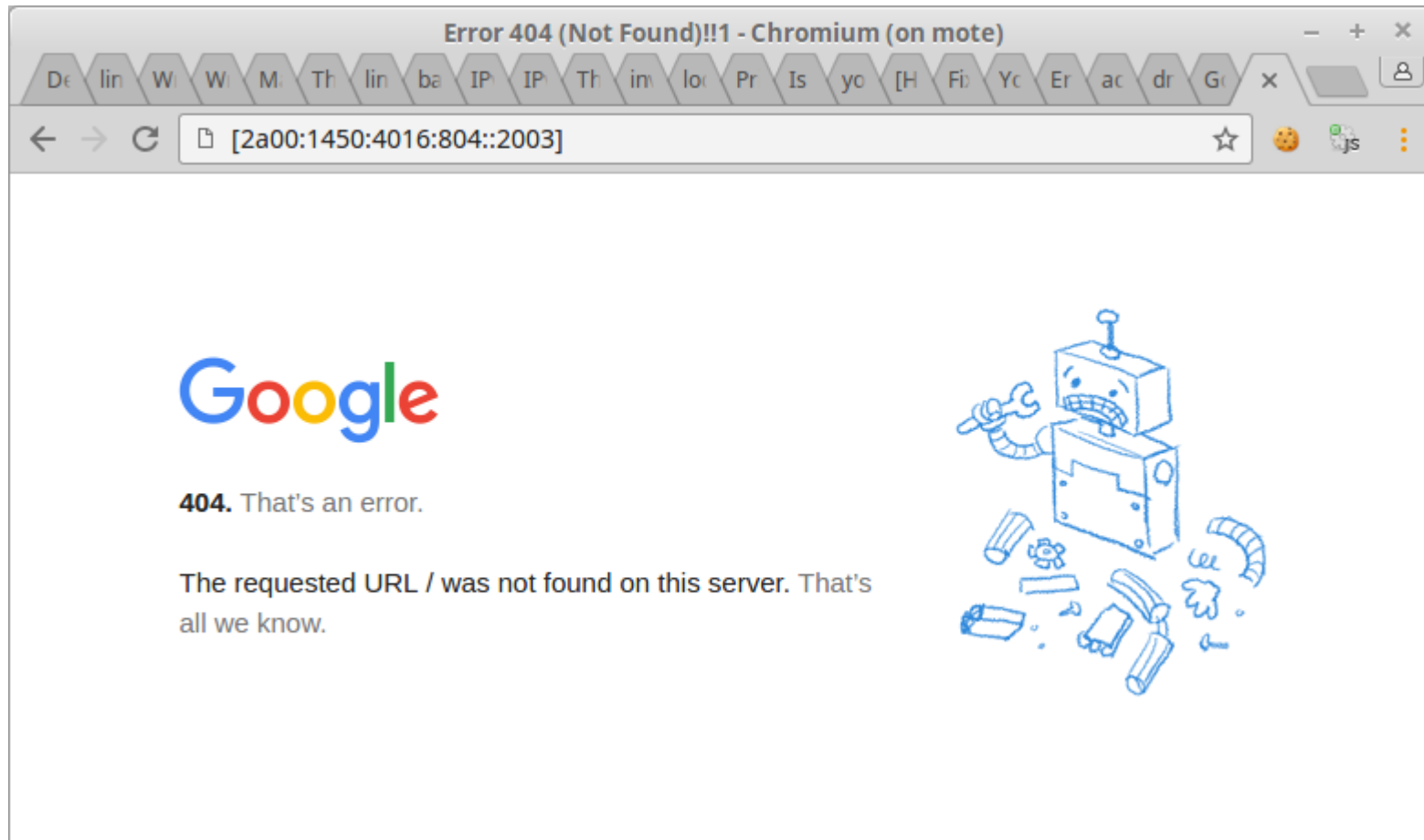


IPv4 => IPv6

192.168.0.0/16, 10.0.0.0/8	fc00::/7 (Unqiue Local Address)
0.0.0.0/32	::/128
127.0.0.1/8	::1/128
8.8.8.8	2001:4860:4860::8888
169.254.0.0/16	fe80::/64 (Link Local Address)
DHCPv4	DHCPv6 / SLAAC
ARP	NDP (Neighbor Discovery Protocol)

```
mwarning@lta101 ~ $ ping6 2001:4860:4860::8888
PING 2001:4860:4860::8888(2001:4860:4860::8888) 56 data bytes
64 bytes from 2001:4860:4860::8888: icmp_seq=1 ttl=59 time=3.38 ms
64 bytes from 2001:4860:4860::8888: icmp_seq=2 ttl=59 time=3.34 ms
```


Hallo Google?!



(Mit Port geht's kommt das Gleiche: "http://[2a00:1450:4016:804::2003]:80")

Aber Hey! – Google meldet sicher immerhin xD

[RIPE Database \(Whois\)](#)[Website](#)

Search IP Address or ASN



Your IP address is 2001:a60:a07d:1:3113:1f13:d36f:9c53

[Login](#)[Manage IPs and ASNs](#)

IPv4, IPv6 and ASNs
LIR Portal
RIPE Database
Resource Transfers and Mergers

[Analyse](#)

RIPE NCC Statistics
RIPEstat
RIPE Atlas
Raw Datasets

[Participate](#)

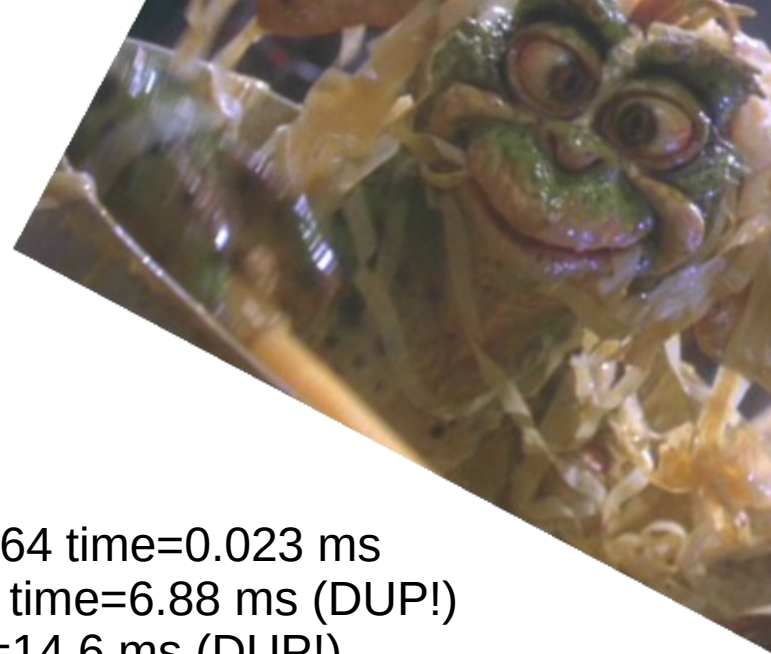
RIPE NCC Membership
RIPE Community
Policy Development Process
Internet Governance

[Get Support](#)[Contact Us](#)[Publications](#)[RIPE Documents](#)[About Us](#)[What We Do](#)

“Interessante” Adressen

ff02::1	All nodes on the local network segment
ff02::2	All routers on the local network segment
ff0x::101	Network Time Protocol (x beliebig)
::192.168.1.1	IPv4 address embedded in IPv6
fe80::1	Eigentlich nicht besonderes, aber schön kurz... Benötigt immer das Interface. Browser unterstützen das nicht :-)
...	Viele andere

Unfug :-)



```
root@vpn4:/home/mwarning# ping6 ff02::1%eth0
PING ff02::1%eth0(ff02::1) 56 data bytes
64 bytes from fe80::5254:ff:fe4f:adaf: icmp_seq=1 ttl=64 time=0.023 ms
64 bytes from fe80::22:eff:feff:c33: icmp_seq=1 ttl=64 time=6.88 ms (DUP!)
64 bytes from fe80::ff:fe00:1: icmp_seq=1 ttl=64 time=14.6 ms (DUP!)
64 bytes from fe80::7cb9:23ff:fe51:ad57: icmp_seq=1 ttl=64 time=16.1 ms (DUP!)
64 bytes from fe80::16:3cff:fe5d:b1c9: icmp_seq=1 ttl=64 time=18.8 ms (DUP!)
64 bytes from fe80::b048:7aff:fe99:a996: icmp_seq=1 ttl=64 time=19.7 ms
(DUP!)
64 bytes from fe80::90f6:52ff:fe4a:ff38: icmp_seq=1 ttl=64 time=21.9 ms (DUP!)
64 bytes from fe80::6470:2ff:fede:44a6: icmp_seq=1 ttl=64 time=22.0 ms (DUP!)
64 bytes from fe80::e894:f6ff:fe51:b364: icmp_seq=1 ttl=64 time=22.0 ms (DUP!)
64 bytes from fe80::a0f3:c1ff:feb3:c2e4: icmp_seq=1 ttl=64 time=23.0 ms (DUP!)
64 bytes from fe80::60e3:27ff:fec7:a150: icmp_seq=1 ttl=64 time=23.3 ms (DUP!)
64 bytes from fe80::14cc:20ff:fe6f:9fc6: icmp_seq=1 ttl=64 time=23.5 ms (DUP!)
64 bytes from fe80::c04a:ff:fe05:eb42: icmp_seq=1 ttl=64 time=23.5 ms (DUP!)
64 bytes from fe80::6872:51ff:fe3c:86a9: icmp_seq=1 ttl=64 time=23.7 ms (DUP!)
64 bytes from fe80::60e3:27ff:feed:d8ea: icmp_seq=1 ttl=64 time=23.8 ms
(DUP!)
64 bytes from fe80::98de:d0ff:fed3:d62e: icmp_seq=1 ttl=64 time=23.9 ms
(DUP!)
64 bytes from fe80::30b5:c2ff:fe80:f224: icmp_seq=1 ttl=64 time=23.9 ms (DUP!)
```

Autokonfiguration

- Wie bekomme ich IP-Adresse/Netz-Prefix/DNS-Server?
- Client unter Linux macht der Kernel (kein dhcpclient..)

- 1) Client gibt sich Link Local Adresse (fe80:: ...)
- 2) Client sendet Anfrage an multicast Adresse ff02::2 (alle Router)
"ICMPv6 Router Solicitation"
- 3) Router sendet an multicast Adresse ff02::1 (alle Geräte) IPv6 Prefix etc.
"ICMPv6 Router Advertisement"
- 4) Im Paket steht Prefix bzw. Wie die Einstellungen dynamisch geholt werden können:
 - 1) SLAAC (Prefix, Prefix-Länge, Gateway-Adresse)
 - 2) SLAAC with stateless DHCPv6 (Andere Infos, z.B. Domain/DNS Adresse über DHCPv6)
 - 3) Statefull DHCPv6 (Alles außer Gateway per DHCPv6 – vergleichbar mit DHCPv4)
- 5) Duplicate Address Detection (optional)

Privatssphäre mit IPv6

- Globale Adressen mit MAC Adresse?
- Privacy extensions!
 - Prefix mit zufälligen Bytes
 - Werden neu erstellt
 - Alte werden bei Nichtbenutzung entfernt
- Kein NAT => Firewall Regel (sollte default sein)
- Tentative (vorläufig), Preferred-valid (bervorzugt), Deprecated-valid (überholt)
 - Siehe IP Adressliste / zurückblättern..
- Cookies im Browser sind das Hauptproblem

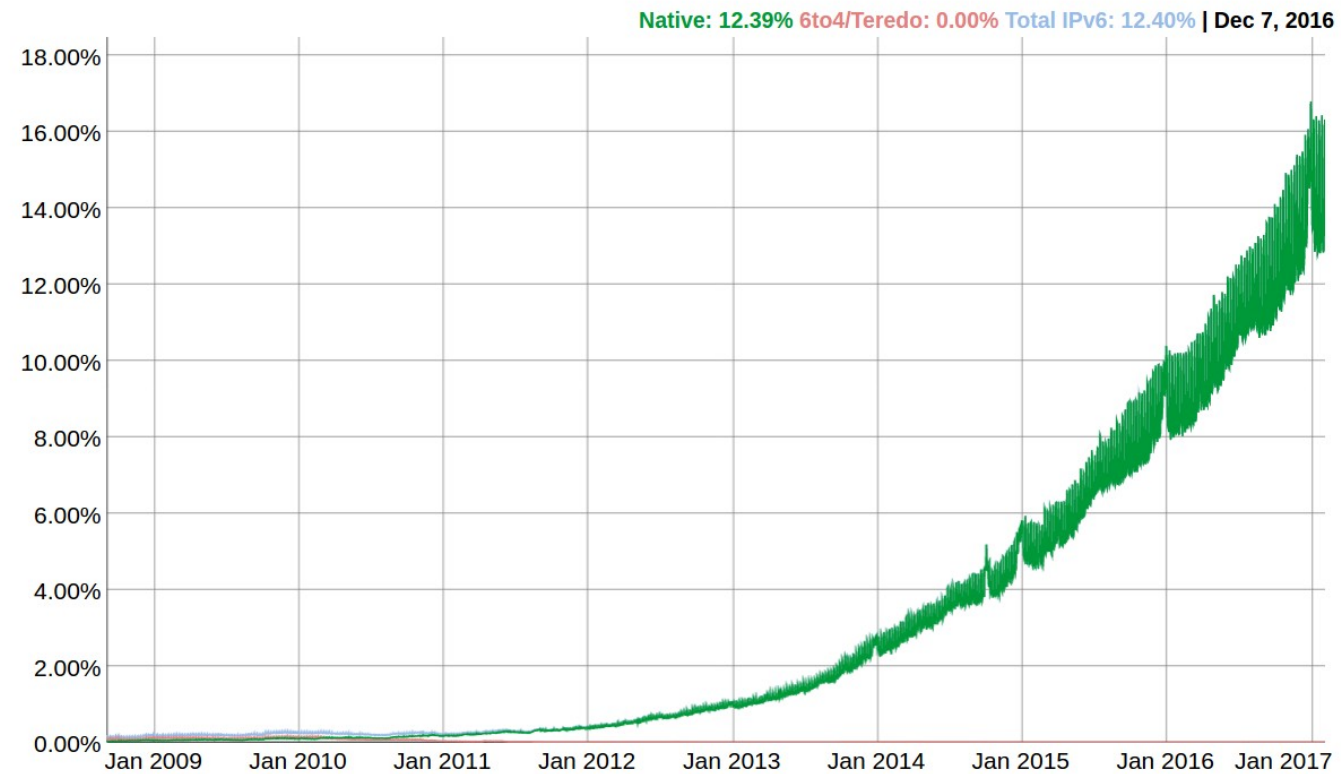


IPv6 Adoption



IPv6 Adoption

We are continuously measuring the availability of IPv6 connectivity among Google users. The graph shows the percentage of users that access Google over IPv6.



Übergangslösungen

- Dual-Stack: IPv4 and der Seite von IPv6
- Ein Interface hat beide Adresstypen
- IPv6 Tunnel Provider (IPv6 über IPv4 – uhhh.)
 - z.B. Hurricane Electric, Sixx
 - .. eigentlich nicht mehr nötig



Tips&Tricks

- Nur MAC? Keine IP-Adresse? Nachbarschaftsliste Fragen!

mwarning@lta101 ~ \$ ip -6 neighbor list

fe80::5a49:3bff:fe63:3d10 dev eth0 lladdr 58:49:3b:63:3d:10 router REACHABLE

2001:a60:a07d:1:250:56ff:fe92:5cfe dev eth0 lladdr 00:50:56:92:5c:fe STALE

fe80::205:b6ff:fe05:9114 dev eth0 lladdr 00:05:b6:05:91:14 router STALE

- Oder Link-Local Adresse selber bauen..

12:34:56:78:90:ab => fe:80:1034:56ff:fe78:90ab

(nicht ganz trivial und funktioniert nicht immer)

Tips und Tricks

- der bessere Teil -



Laptop A



Netzwerkkabel



Laptop B

Server/Router (darf nicht mitspielen) =>



SSH direkt ohne DHCP

File Edit View Search Terminal Help

```
[mwarning@xanax ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: wlp58s0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000
    link/ether aa:99:83:97:2c:e1 brd ff:ff:ff:ff:ff:ff
18: vboxnet0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 0a:00:27:00:00:00 brd ff:ff:ff:ff:ff:ff
35: enp0s20f0u2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:e0:8f:00:06:ac brd ff:ff:ff:ff:ff:ff
    inet6 fe80::f123:ecbf:873c:85f5/64 scope link
        valid_lft forever preferred_lft forever
[mwarning@xanax ~]$ ping -6 ff02::01 -I enp0s20f0u2
PING ff02::01(ff02::1) from fe80::f123:ecbf:873c:85f5%enp0s20f0u2 enp0s20f0u2: 56 data bytes
64 bytes from fe80::f123:ecbf:873c:85f5%enp0s20f0u2: icmp_seq=1 ttl=64 time=0.065 ms
64 bytes from fe80::f123:ecbf:873c:85f5%enp0s20f0u2: icmp_seq=2 ttl=64 time=0.065 ms
^C
--- ff02::01 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1019ms
rtt min/avg/max/mdev = 0.065/0.065/0.065/0.000 ms
[mwarning@xanax ~]$ ssh -6 fe80::f123:ecbf:873c:85f5%enp0s20f0u2
ssh: connect to host fe80::f123:ecbf:873c:85f5%enp0s20f0u2 port 22: Connection refused
[mwarning@xanax ~]$ ssh -6 ff02::01%enp0s20f0u2
ssh: connect to host ff02::01%enp0s20f0u2 port 22: Network is unreachable
[mwarning@xanax ~]$
```

Danke! - Fragen?

