A Whirlwind Tour of IPv6

Differences and common features of IPv4 and IPv6

Agenda

- Reasons for IPv6
- Address schemas: IPv4 vs. IPv6
  - SLAAC: EUI-64 vs. Privacy Extension
- Link-local addresses
- Private addresses (ULA)
- Global addresses (GUA)
- Prefix Delegation
- Self-hosted Services for the Internet
  - „Dual Stack“ vs. „DS-Lite“
  - IPv4 ←→ IPv6 Gateway Technologies
- End-to-End Connectivity
  - No more NAT! / MTU discovery
  - Implications for Dynamic DNS / local firewalls

Reasons for IPv6

- **IPv4 address exhaustion**
  - IPv4: 4 Bytes = 4 * 8 Bit = 32 Bit
  - example: `192.168.148.200`
- **Larger address space**
  - IPv6: 8 Words = 8 * 16 Bit = 128 Bit
  - example: `2001:16b8:2a60:6ef0:e922:304a:fec5:d131`
- Stateless address autoconfiguration (SLAAC)
  - automatic vs. static address assignments
- Simplified processing by routers
  - fixed size headers (with optional extension headers)
- Multicasting
  - instead of Broadcasting
- Ipsec VPN protocol
  - also implemented for IPv4

Address schemas: IPv4 vs. IPv6

- IPv4 addresses (32 bits)
  - 4 decimal numbers: **0 – 255**
  - separated by 3 dots: **.**
  - network + host part = 32 bits
- Mostly only one address for each interface
- CIDR notation:
  - 192.168.178.1/24
    - 24 bits for network: 192.168.178.0
    - 8 bits for host address: **.1**
  - 10.11.22.33/16
    - 16 bits for network: 10.11.0.0
    - 16 bits for host address: **.22.33**
  - 127.0.0.1/8
    - 8 bits for network: 127.0.0.0
    - 24 bits for host address: **.0.0.1**

- IPv6 addresses (128 bits)
  - 8 hexadecimal fields: **0 – ffff**
  - separated by 7 colons: **:**
  - network part = 64 bits
  - host part = 64 bits
- Usually more than one address for each interface
- Special notations:
  - Leading zeros **0** may be dropped
  - Adjacent fields with all zeros can be written with double colons **::** (allowed only one time)
- CIDR notation is also possible:

2001:16b8:2ab0:f000:f0ee:37ff:fe8c:5e73/64

  - network: 2001:16b8:2ab0:f000::/64
  - host: ::f0ee:37ff:fe8c:5e73/128

Host address: EUI-64 vs. Privacy Extension

- IPv4 addresses are either statically or dynamically assigned (via DHCP4).
- IPv6 addresses are either statically or self assigned (via router adver-tisements). DHCP6 is not often used.
- SLAAC addresses are either hardware derived (EUI-64) or deterministically generated.
- See "`/etc/dhcpcd.conf`":

```
# Generate SLAAC address using the
Hardware Address of the interface
#slaac hwaddr
# OR generate Stable Private IPv6
Addresses based from the DUID
slaac private
```

- From MAC (48 bits) to EUI-64:
  1. `f2:ee:37:8c:5e:73`
  2. `f2ee:3700:008c:5e73`
     xor
     `0200:00ff:fe00:0000`
  3. `f0ee:37ff:fe8c:5e73`
- From EUI-64 (64 bits) to MAC:
  1. `f0ee:37ff:fe8c:5e73`
     xor
     `0200:00ff:fe00:0000`
  2. `f2ee:3700:008c:5e73`
  3. `f2:ee:37:8c:5e:73`
- Private host address:
  - middle part is **not** `ff:fe` !
  - `e267:f3d3:f6cb:6611`

Special addresses: IPv4 vs. IPv6

- IPv4 localhost / loopback addr.
  - 127.0.0.1/8
- IPv4 default route
  - 0.0.0.0/0
- IPv4 link-local addresses

  Avahi / APIPA / Bonjour / zeroconf:
  - network: 169.254.0.0/16
- IPv4 documentation networks
  - 192.0.2.0/24
  - 198.51.100.0/24
  - 203.0.113.0/24
  - 233.252.0.0/24

- IPv6 localhost / loopback addr.
  - ::1/128
- IPv6 default route
  - ::/0
- IPv6 link-local addresses
  - network: fe80::/10
  - fe80::f0ee:37ff:fe8c:5e73/64
- IPv6 documentation network
  - 2001:db8::/32

Private addresses (ULA): IPv4 vs. IPv6

- IPv4 private network A
  - 10.0.0.0/8
- IPv4 private network B
  - 172.16.0.0/12 → 16 networks
  - from 172.16.0.0/16
  - thru 172.31.0.0/16
- IPv4 private network C
  - 192.168.0.0/16 → 256 networks
  - from 192.168.0.0/24
  - thru 192.168.255.0/24
- IPv4 benchmark tests
  - 198.18.0.0/15
- IPv4 IETF protocols
  - 192.0.0.0/24 → RFC-6333
- IPv4 shared address space for carrier-grade NAT (CGNAT)
  - 100.64.0.0/10

- IPv6 network range reserved for **U**nique **L**ocal **A**ddresses within networks of private organizations
  - fc00::/7
- Usage in private IPv6 networks
  - **fd**00::/8 → 2^56 networks
  - from fd00:0000:0000:0000::/64
  - thru fdff:ffff:ffff:ffff::/64
- The 40 green bits are a global ID and should be chosen randomly:
  - fd**00:dead:beef**:cafe::/64
- The remaining 16 purple bits are a subnet ID and can be used to address 2^16 (= 65.536) subnets within an organization:
  - fd00:dead:beef:**cafe**::/64

Global Unicast Addresses (GUA)

- IPv6 network range reserved for **G**lobal **U**nicast **A**ddresses
  - `2000::/3` → 2^61 networks
  - from `2000:0000:0000:0000::/64`
  - thru `3fff:ffff:ffff:ffff::/64`
- Equivalent to **public IPv4** addresses

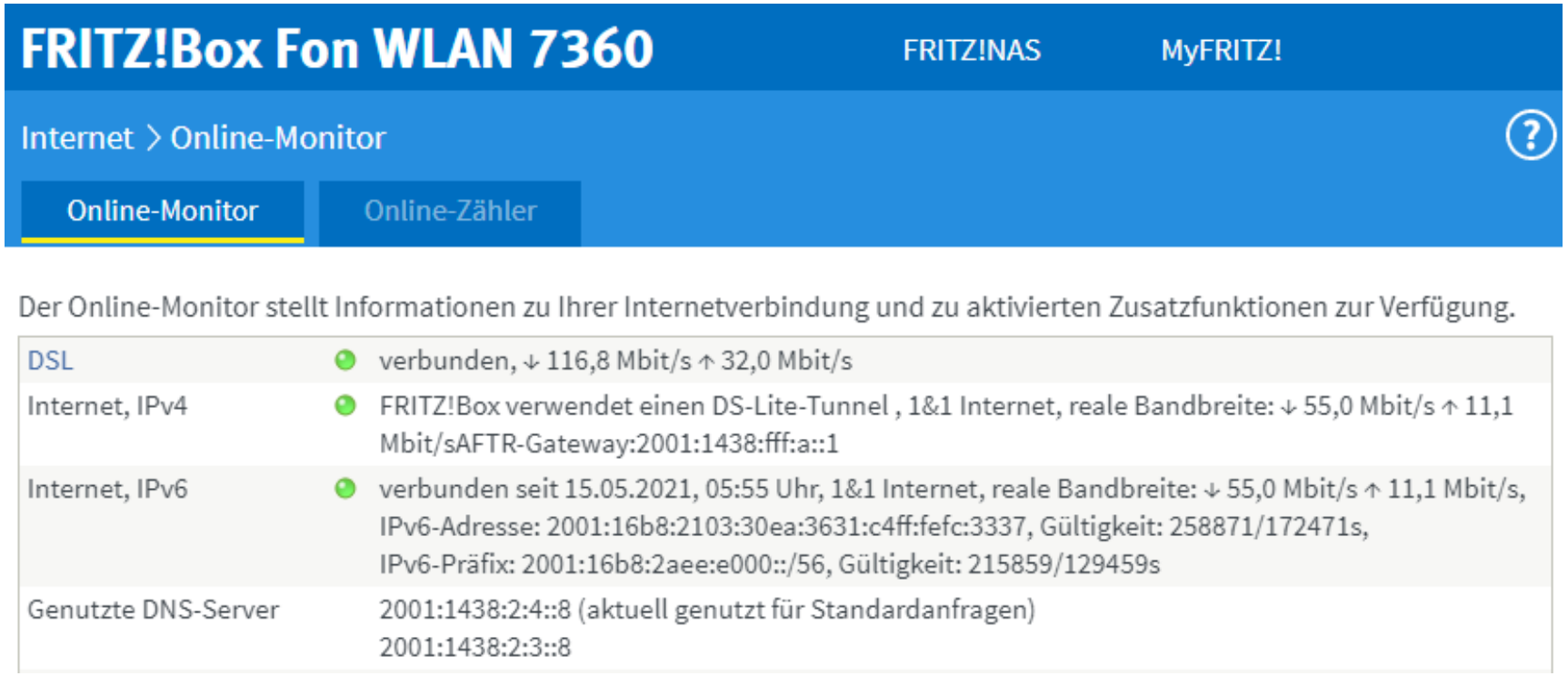
- Some subnet ranges have been reserved for special purposes
  - Teredo tunneling
    - `2001::/32` → `2001:0000::/32`
  - Documentation
    - `2001:db8::/32` → `2001:0db8::/32`
  - 6to4 tunneling
    - `2002::/16`
  - Benchmark tests
    - `2001:0002::/48` → `2001:0002:0000::/48`

Global Unicast Addresses (GUA)

- Real IPv6 addresses of German ISPs assigned to Fritz!Box CPEs
  - Telekom (1+1)
    - Duew-V3: `2003:00e5:57ff:063f:cece:1eff:fefe:c367`
  - Versatel (1+1)
    - Lu-F2: `2001:16b8:2102:cc22:0a96:d7ff:feea:f30c`
    - Lu-F48: `2001:16b8:2103:30ea:3631:c4ff:fefc:3337`
  - Kabel Deutschland (Vodafone)
    - Lu-E12: `2a02:810c:0000:0011:89d2:f887:71ac:7a5f`

Prefix Delegation

- Besides an IPv6 address, the CPE device also gets an IPv6 subnet range assigned, that can be further sub netted and delegated to internal devices of the customer's network.
- Prefix `2001:16b8:2aee:e000::/56` can be sub netted into 256 x `/64` networks or 16 x `/60` networks or anything in between.



Prefix-Delegation (ISP to CPE)

- Versatel (1+1)
  - CPE address: 2001:16b8:2103:30ea:3631:c4ff:fefc:3337
  - deleg. Prefix: 2001:16b8:2aee:e000::/**56**
  - AFTR Gw: 2001:1438:fff:a::1

  - CPE address: 2001:16b8:2102:cc22:0a96:d7ff:feea:f30c
  - deleg. Prefix: 2001:16b8:2ad1:af00::/**56**
  - AFTR Gw: 2001:1438:fff:a::1

- Telekom (1+1)
  - CPE address: 2003:00e5:57ff:063f:cece:1eff:fefe:c367
  - deleg. Prefix: 2003:00e5:5705:de00::/**56**

- Kabel Deutschland (Vodafone)
  - CPE address: 2a02:810c:0000:0011:89d2:f887:71ac:7a5f
  - deleg. Prefix: 2a02:810c:0880:7ac0::/**62**
  - AFTR Gw: 2a02:8100:c0:407::b:1:af72

Prefix-Delegation (Fritz!Box to OPNsense)

- Telekom (1+1)
  - CPE address: 2003:e5:57ff:063f:cece:1eff:fefe:c367
  - ISP Prefix: 2003:e5:5705:de00::/**56**
  - OPNsense1:
    - WAN: 2003:e5:5705:de00:5054:ff:fe36:0810
    - Prefix: 2003:e5:5705:dee0::/*60*
    - LAN: 2003:e5:5705:dee1:5054:ff:fe08:1036
  - OPNsense2:
    - WAN: 2003:e5:5705:de00:e45f:13ff:fe97:34c3
    - Prefix: 2003:e5:5705:def0::/*60*
    - LAN: 2003:e5:5705:def0:445e:24ff:feae:d18b

- Versatel (1+1)
  - CPE address: 2001:16b8:2103:30ea:3631:c4ff:fefc:3337
  - ISP Prefix: 2001:16b8:2aee:e000::/**56**
  - OPNsense3:
    - WAN: 2001:16b8:2aee:e000:0c0a:84ff:fe47:e4c7
    - Prefix: 2001:16b8:2aee:e0f0::/*60*
    - LAN: 2001:16b8:2aee:e0f0:a80d:f9ff:febc:21f7

Self-hosted Services for the Classic Internet

- Classic service hosting:
  - An application listens on a port of a server for incoming requests.
  - The server has a (fixed) publicly reachable IPv4 address.
  - This IPv4 address is usually assigned a permanent DNS A-record.
  - Other ports on the server are protected by a local firewall.

- Self-hosted services:
  - An application listens on a port of a server for incoming requests.
  - The server has a private IPv4 address and **cannot** be reached from the Internet.
  - The CPE device has a public IPv4 addresses that is often changing.
  - A Dynamic-DNS service can be used to announce this public address.
  - The CPE is doing masquerading (NAT and PAT), that is translation of addresses and ports from the internal ranges to the public address.
  - The CPE is acting as a firewall and can be used to forward requests from external ports to internal ports of the application server.
  - Other ports on the server are protected by the CPE and a local firewall.

Self-hosted Services for the New Internet

- “Classic” service hosting:
  - An application listens on a port of a server for incoming requests.
  - The server has a (fixed) publicly reachable IPv6 address.
  - This IPv6 address is usually assigned a permanent DNS AAAA-record.
  - Other ports on the server are protected by a local firewall.

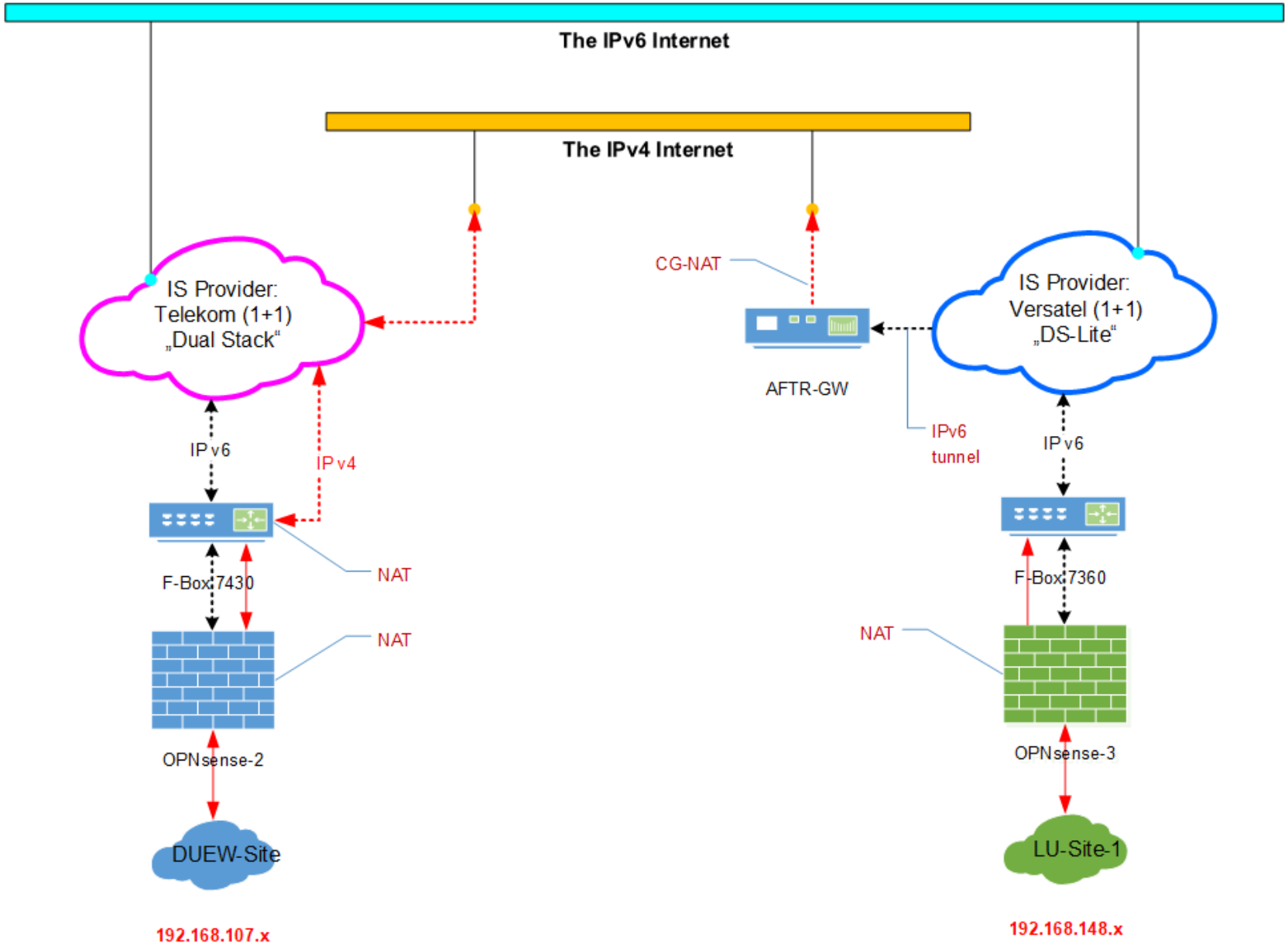
- Self-hosted services:
  - An application listens on a port of a server for incoming requests.
  - The CPE device has been delegated a public IPv6 address range that is often changing.
  - The CPE assigns a public IPv6 address from this range to the server.
  - The server **can** be reached via the IPv6 gateway from the Internet.
  - A DynDNS service can be used to announce the server’s IPv6 address.
  - The CPE is not doing any masquerading (neither NAT nor PAT).
  - The CPE is acting as a firewall and can be used to forward requests from external ports to internal ports of the application server.
  - Other ports on the server are protected by the CPE and a local firewall.

„Dual Stack“ vs. „DS-Lite“

- Technically, the IPv4 and IPv6 Internets are disjoint networks, that are not compatible with each other.
- Thus, a network client that wants to access services in both worlds needs addresses and network connectivity to both IPv4 **and** IPv6.
- This can be accomplished by connecting to an ISP, that delivers a “dual stack” of public IPv4 **and** IPv6 addresses.
- But today, many ISPs are unable to give a public IPv4 address to the CPE device.
- See RFC-6333 for “DS-Lite”.

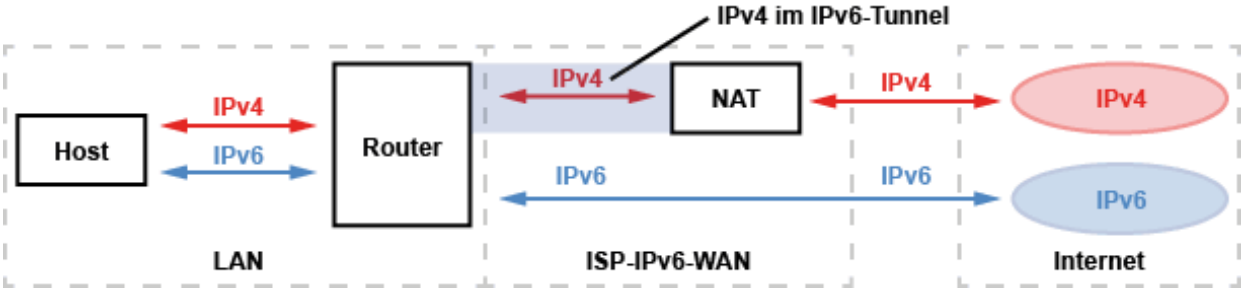
- So many of these ISPs are delivering only a *light* version of “dual stack” to the customer.
- With “DS-Lite”, the ISP creates an IPv6 tunnel between the CPE device and an AFTR gateway in it’s IPv6 network.
- The **AFTR** (Address Family Transition Router) is essentially a NAT device, that translates the tunneled IPv4 packets.
- Thus, the ISP needs a lot less public IPv4 addresses to service many customers.
- However, it is *impossible* for the customer to run any IPv4 based services in a “DS-Lite” network.

„Dual Stack“ vs. „DS-Lite“

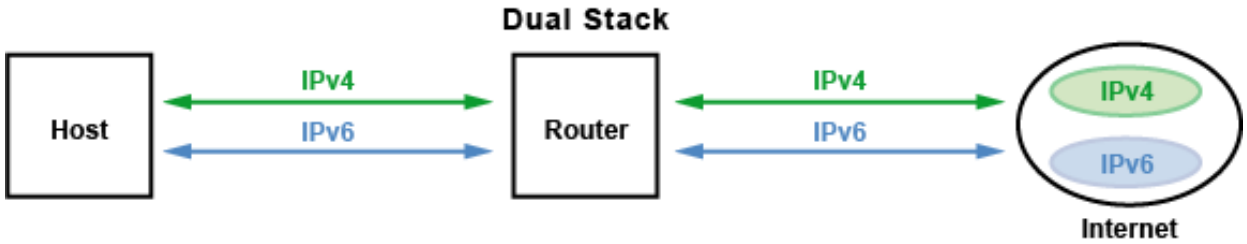


IPv4 ←→ IPv6 Transition Technologies

- Tunneling protocols (e.g. Teredo, 6in4, 6to4, 6over4, DS-Lite, AYIYA = Anything in Anything)



- Parallel operation (e.g. Dual-Stack, CG-NAT)



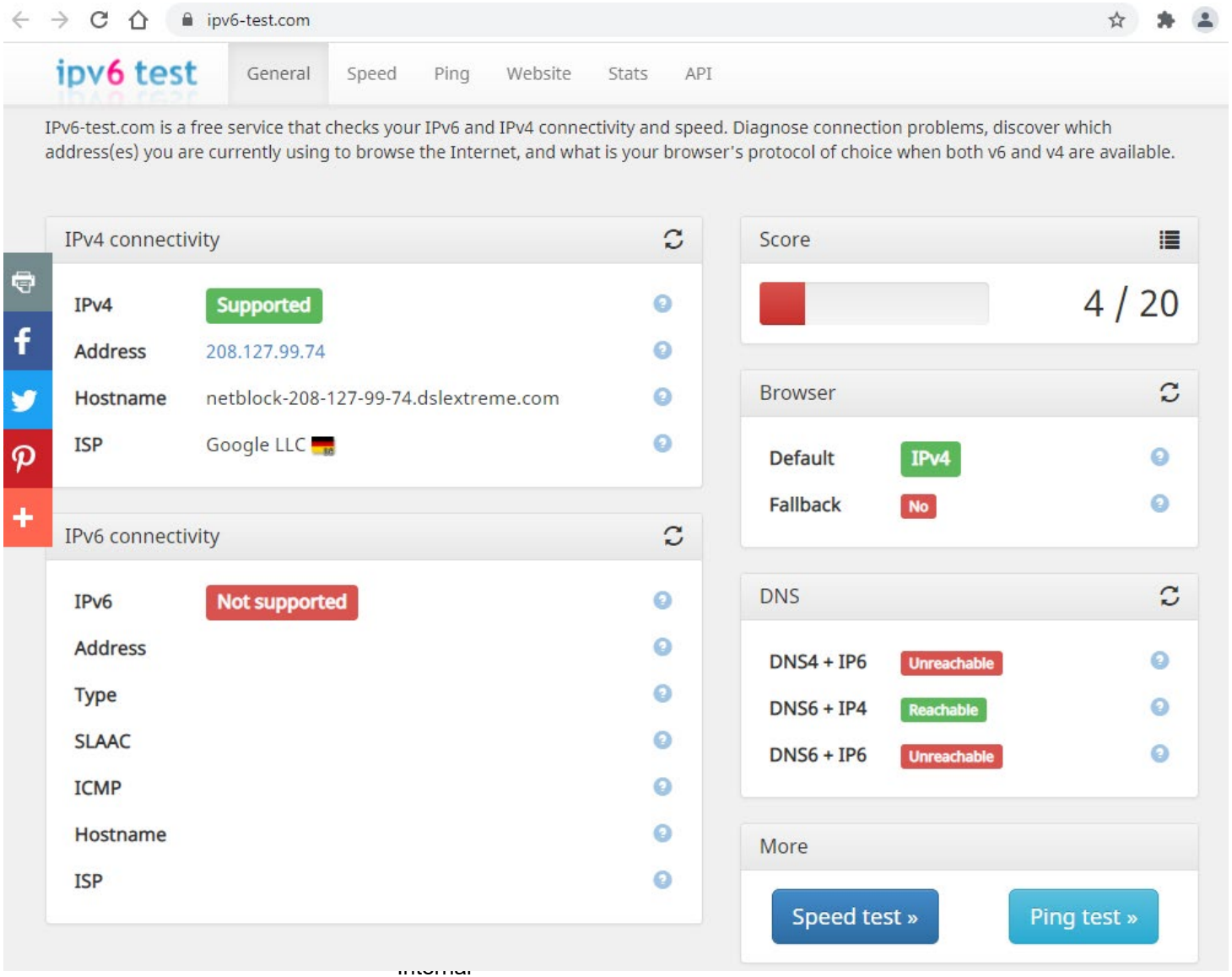
- Protokoll translation (e.g. NAT64 and DNS64)
  - See "IPv6-Workshop" (by Dan Lüdtke) – chapter 6.4 – pages 158 ff.

End-to-End Connectivity

- With IPv6, all communication partners (e.g. clients and servers) are having end-to-end (E2E) connectivity.
  - There are usually no address translations (NAT or PAT) involved. Neither by gateways, nor by firewalls.
- During connection setup, the **M**aximum **T**ransfer **U**nit on the path between client and server is determined.
  - For PMTU discovery the ICMP6 protocol is used and required. Thus, ICMP6 ***must*** not be blocked by any firewalls.
  - The MTU size for IPv6 must be at least 1280 bytes.
- Due to the use of RA (**R**outer **A**dvertisement) and SLAAC (**S**tate**l**ess **A**ddress **A**uto**c**onfiguration) in customer networks the DHCP6 protocol is rarely used.
- In contrast to IPv4, the CPE does not do masquerading of IPv6 communication end points.
  - Thus, Dynamic DNS providers for IPv6 ***must*** learn the server's GUA.
    - Free DynDNS provider: "dynv6.com"
  - Host-based, local firewalls ***should*** be deployed on all servers.

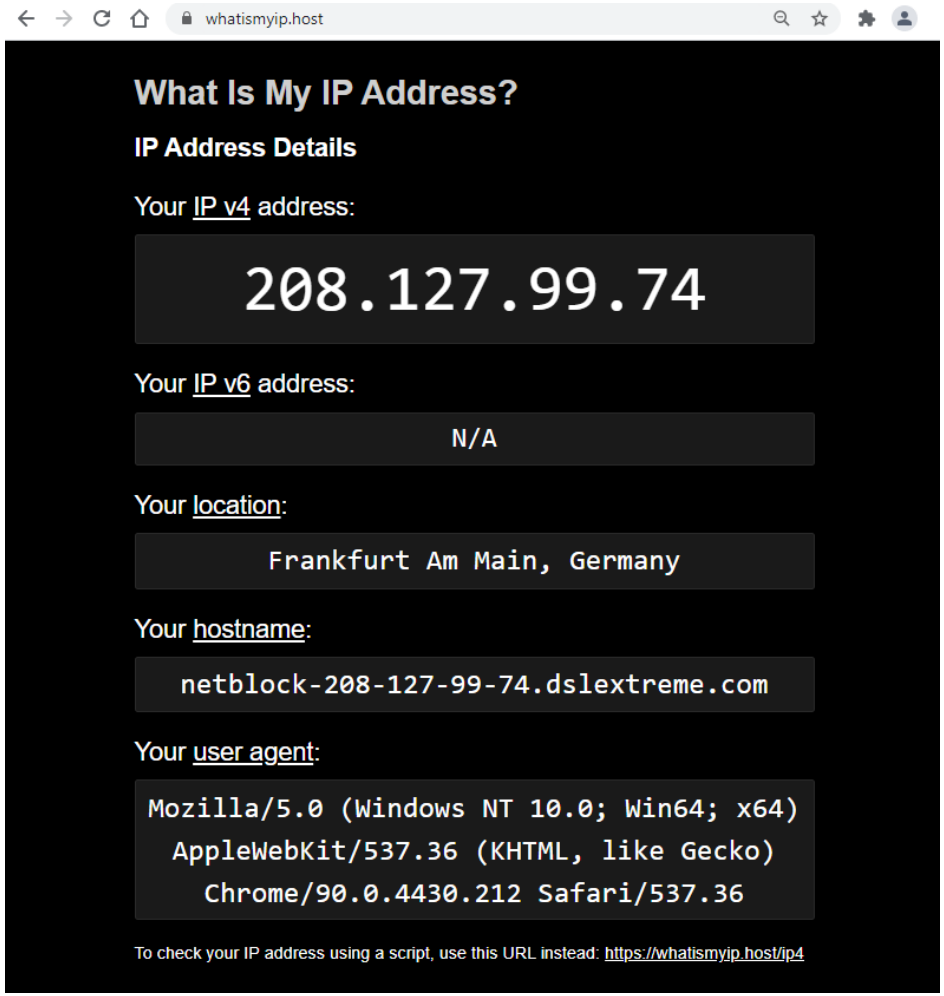
Testing IPv4 and IPv6 connectivity

ipv6-test.com

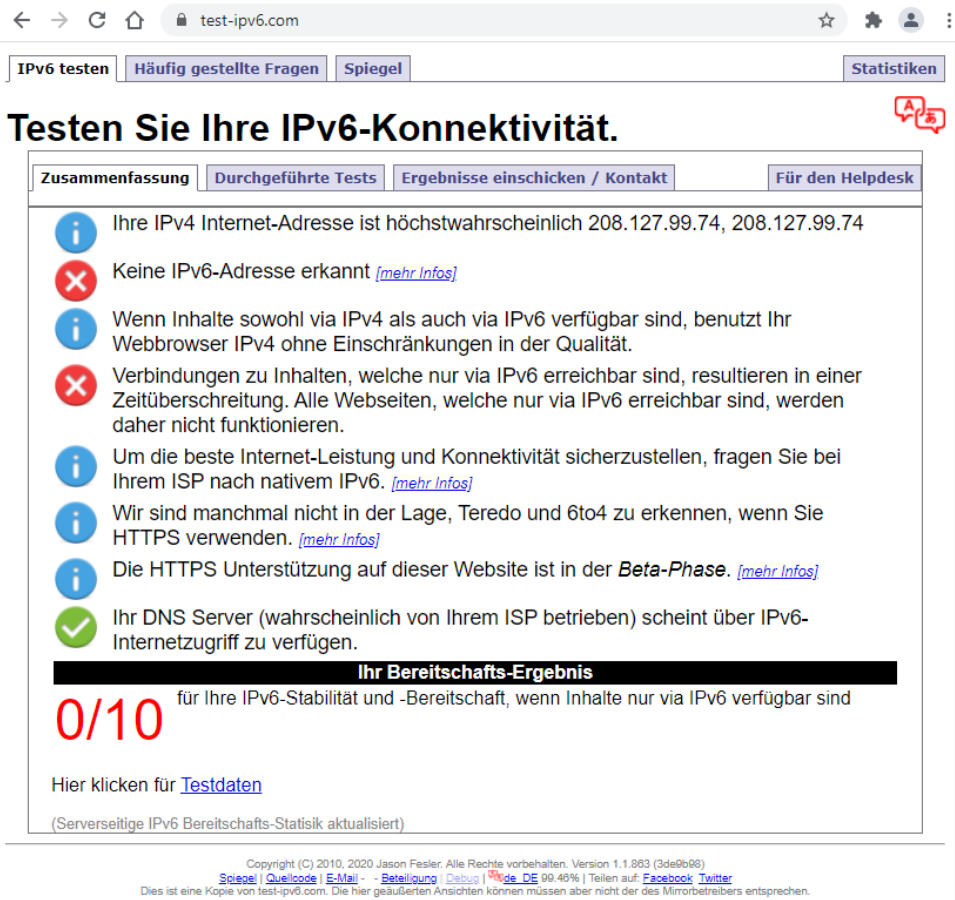


Testing IPv4 and IPv6 connectivity

whatismyip.host



test-ipv6.com



Testing IPv4 and IPv6 connectivity

heise.de

heise.de/netze/tools/meine-ip-adresse/

heise online) Tools) **Meine IP-Adresse**

Meine IP-Adresse

Ihre Anfrage kommt von der IP-Adresse: **208.127.99.74**

Ihre Anfrage wurde von einem Proxy bearbeitet. Wahrscheinlich erscheint daher oben dessen Adresse. Der Proxy gibt als IP-Adresse Ihres PC **208.127.99.74** an.

kame.net

Nicht sicher | kame.net

The KAME project

1998.4 - 2006.3

Use IPv6 HTTP and you will watch the dancing kame

The KAME project was a joint effort of six companies in Japan to provide a free stack of IPv6, IPsec, and Mobile IPv6 for BSD variants.

Our products are available in:

- FreeBSD 4.0 and beyond
- OpenBSD 2.7 and beyond
- NetBSD 1.5 and beyond
- BSD/OS 4.2 and beyond

The project officially concluded in March 2006 (see press release from the WIDE project). Almost all of our implemented code has been merged to FreeBSD and NetBSD. The historical archive of the KAME repository is available at github.

Google

[Top] [Old info]

Ressources

- Wikipedia
  - IPv4
  - CG-NAT
  - Reserved IP addresses
  - IPv6
  - Link-local addresses
  - ULA
  - Private networks
- RFC documents of the IETF
- IPv6 docs for the pfSense firewall
- Free DynDNS service at “dynv6.com”

Ressources in German

- Excellent book by Dan Lüdtke: “IPv6 Workshop”
- “Elektronik-Kompendium.de” has lots of good content
- German Wikipedia
  - IPv4
  - IPv6
- AVM’s explanation of DS-Lite
- Heise‘s network tools
  - What is my IP?
  - IPv4
  - IPv6