SharkFest'22 EUROPE
Estoril, Portugal
Oct 31 - Nov 4

#sf22eu

IPv6 Crash Course

https://tinyurl.com/ipv6-crash-1
https://tinyurl.com/ipv6-crash-2

Johannes Weber
https://netsec.blog/

SharkFest'22 EUROPE
Estoril, Portugal
Oct 31 - Nov 4

#sf22eu

Hello!

I am Johannes Weber

I am here because I love #IPv6 ;)

You can find me at @webernetz

My blog at https://netsec.blog/

Agenda

- IPv6 addresses
- IPv6 address assignment
- link-layer address resolution
- ICMPv6 everywhere
- routing
- security

Some Questions

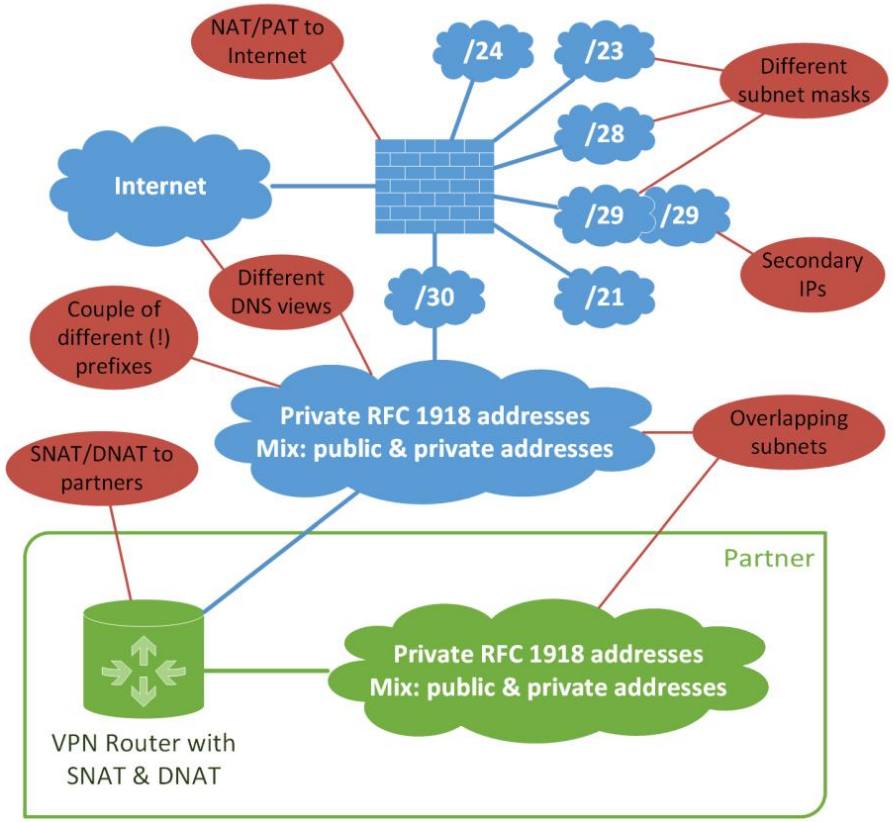
- Who is familiar with IPv6?
- Are you biased?

Are you biased?

Why IPv6?

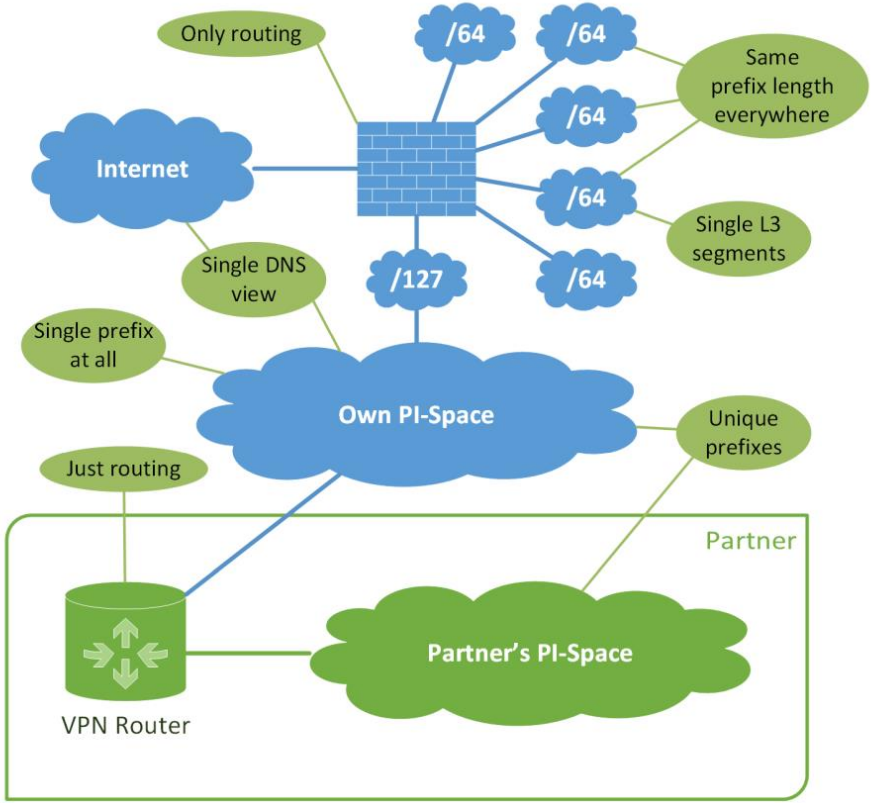
- IPv4 address space is exhausted
- IPv6 brings enough addresses ;)
  - every client is global addressable
  - subnets for everyone
- only layer 3 changes (almost)

Legacy IP



IPv6

! FIXED !

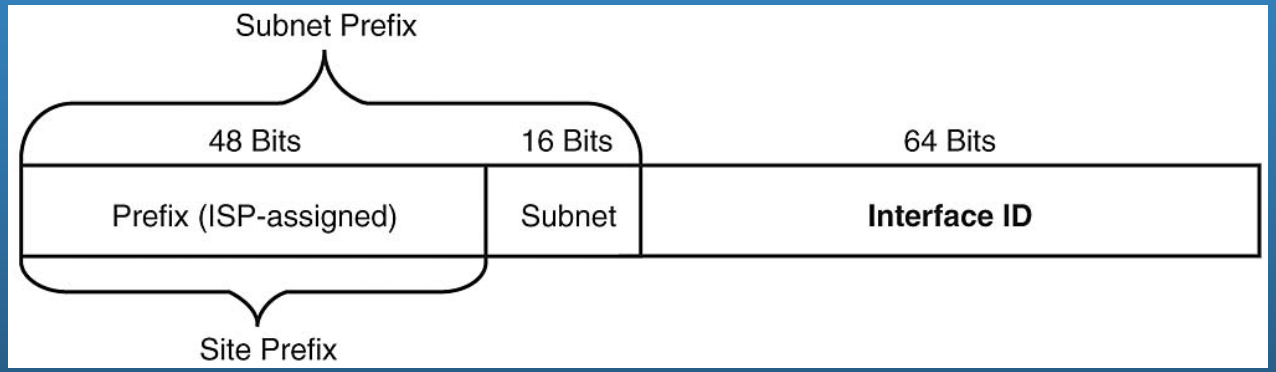


IPv6 Addresses

IPv6 Addresses

- 128 bits long, hexadecimal, 8 groups called „hextets“
  `2001:0db8:0000:0000:cafe:0000:1200:f1b2`
- Two address abbreviations:
  `2001:db8::cafe:0:1200:f1b2`
- Notation: address/prefix-length:
  `2001:db8::/32`

IPv6 Addresses



- Subnets are ALWAYS /64
- Sites almost /48
- → 16 bits for local subnetting = 65.536 subnets
- LIRs get /32

Image Source: https://images.techhive.com/images/idge/imported/article/nww/2007/08/17fig07-100299183-orig.jpg

IPv6 Addresses

- Link-Local, LL: `fe80::/64`
- Global Unicast, GUA: `2000::/3`
- Every node gets 1x link-local + couple of GUAs

- Default Route: `::/0`
- Documentation Prefix: `2001:db8::/32`

IPv6 Addresses

- Lazy IPv6 people use:
- IPv6 Buddy
- https://www.ipv6buddy.com/
- 25 $ + shipping

IPv6 Address Assignment

Manual:

```
iface eth0 inet6 static
    address 2001:db8:0:110::11
    netmask 64
    gateway 2001:db8:0:110::1
    dns-nameservers 2001:db8::53
    dns-search weberlab.de
```

Stateful DHCPv6:

- Similar to IPv4 DORA
- SOLICIT, ADVERTISE, REQUEST, REPLY
- Requires DHCPv6 server
- Log of DUID = DHCP Unique Identifier

IPv6 Address Assignment

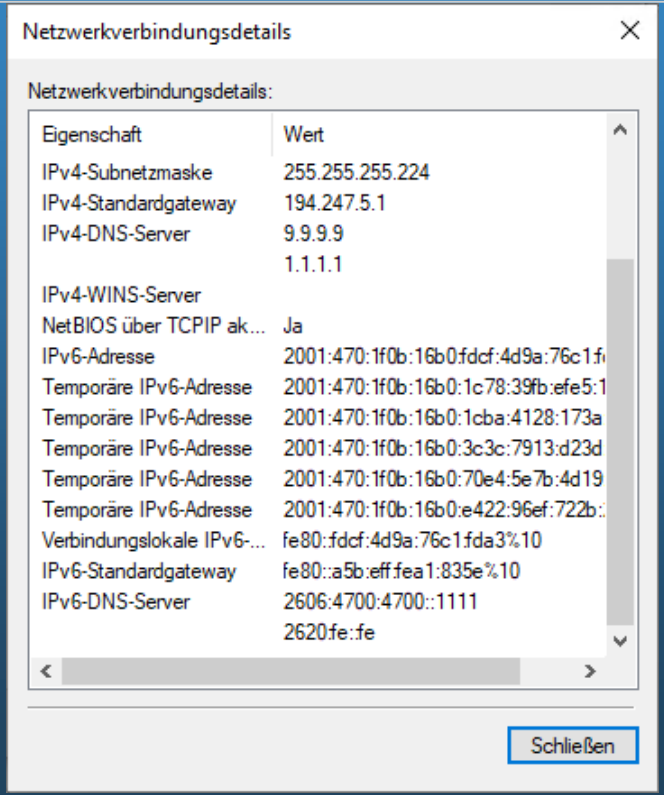
SLAAC: Stateless Address Autoconfiguration

- Router sends Router Advertisement RA with /64 prefix (periodically + when a clients requests through an RS)
- Client generates interface-ID, IID
  - ~~based on MAC address, EUI-64~~
  - OR stable opaque
  - and [optional] temporary (privacy extensions)
- Client sends duplicate address detection, DAD
- Client installs default route
- Recursive DNS server through RA or stateless DHCPv6

IPv6 Address Assignment

Example: Windows 10

- 1x SLAAC stable opaque
- 5x SLAAC temporary
- 1x Link-Local
- Default Gateway via link-local
- 2x DNS-Server



IPv6 Address Assignment

- Router Advertisement
  - prefix as /64
  - flags, flags, flags
  - lifetimes
- [optional]
  - link-layer address
  - recursive DNS server

```
Internet Control Message Protocol v6
    Type: Router Advertisement (134)
    Code: 0
    Checksum: 0x1553 [correct]
    [Checksum Status: Good]
    Cur hop limit: 255
    Flags: 0x48, Other configuration, Prf (Default Router Preference): High
        0... .... = Managed address configuration: Not set
        .1.. .... = Other configuration: Set
        ..0. .... = Home Agent: Not set
        ...0 1... = Prf (Default Router Preference): High (1)
        .... .0.. = Proxy: Not set
        .... ..0. = Reserved: 0
    Router lifetime (s): 1800
    Reachable time (ms): 30000
    Retrans timer (ms): 1000
    ICMPv6 Option (Prefix information : 2003:50:aa10:4243::/64)
        Type: Prefix information (3)
        Length: 4 (32 bytes)
        Prefix Length: 64
        Flag: 0xc0, On-link flag(L), Autonomous address-configuration flag(A)
        Valid Lifetime: 604800
        Preferred Lifetime: 86400
        Reserved
        Prefix: 2003:50:aa10:4243::
    ICMPv6 Option (MTU : 1492)
```

Link-Layer Address Resolution

Link-Layer Address Resolution

- = ARP in IPv4
- Client A sends Neighbor Solicitation NS to the „solicited-node multicast address“ `ff02::1:ffxx:xxxx`
- Client B responds with Neighbor Advertisement NA (unicast)
- Both embed link-layer addresses

Tracefiles

- https://tinyurl.com/ipv6-crash-1
- https://tinyurl.com/ipv6-crash-2

Wireshark Display Filters

Photo by Raychan on Unsplash

SharkFest'22 EUROPE
Estoril, Portugal
Oct 31 - Nov 4

1st Basic IPv4-IPv6 Messages - Knoppix Telekom.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmpv6 Expression...

No.	UTC	Time Delta	Source	Destination	Protocol
1	2015-04-28 19:21:00,798805	0.000000	::	ff02::16	ICMPv6
2	2015-04-28 19:21:01,328798	0.529993	::	ff02::16	ICMPv6
3	2015-04-28 19:21:01,372142	0.043344	::	ff02::1:ff2d:3b8e	ICMPv6
6	2015-04-28 19:21:01,861868	0.489726	fe80::1	ff02::1	ICMPv6
7	2015-04-28 19:21:02,375493	0.513625	fe80::221:6aff:fe2d:3b8e	ff02::16	ICMPv6
8	2015-04-28 19:21:02,375527	0.000034	fe80::221:6aff:fe2d:3b8e	ff02::2	ICMPv6
9	2015-04-28 19:21:02,376324	0.000797	fe80::221:6aff:fe2d:3b8e	ff02::2	ICMPv6
10	2015-04-28 19:21:02,384950	0.008626	fe80::1	fe80::221:6aff:fe2d:3b8e	ICMPv6
11	2015-04-28 19:21:02,384997	0.000047	fe80::221:6aff:fe2d:3b8e	fe80::1	ICMPv6
12	2015-04-28 19:21:02,386441	0.001444	fe80::1	ff02::1	ICMPv6
15	2015-04-28 19:21:03,255455	0.869014	fe80::221:6aff:fe2d:3b8e	ff02::16	ICMPv6
16	2015-04-28 19:21:03,305456	0.050001	fe80::221:6aff:fe2d:3b8e	ff02::16	ICMPv6
20	2015-04-28 19:21:03,792359	0.486903	fe80::221:6aff:fe2d:3b8e	ff02::16	ICMPv6
21	2015-04-28 19:21:03,885708	0.093349	::	ff02::1:ff2d:3b8e	ICMPv6
22	2015-04-28 19:21:05,785862	1.900154	fe80::1	ff02::1	ICMPv6
23	2015-04-28 19:21:07,395690	1.609828	fe80::221:6aff:fe2d:3b8e	fe80::1	ICMPv6
24	2015-04-28 19:21:07,398964	0.003274	fe80::1	fe80::221:6aff:fe2d:3b8e	ICMPv6
25	2015-04-28 19:21:09,868895	2.469931	fe80::1	ff02::1	ICMPv6
28	2015-04-28 19:21:17,876504	8.007609	fe80::1	ff02::1	ICMPv6
29	2015-04-28 19:21:25,884348	8.007844	fe80::1	ff02::1	ICMPv6
32	2015-04-28 19:21:33,893857	8.009509	fe80::1	ff02::1	ICMPv6
43	2015-04-28 19:21:41,903559	8.009702	fe80::1	ff02::1	ICMPv6
45	2015-04-28 19:21:41,979658	0.076099	fe80::1	ff02::1	ICMPv6
46	2015-04-28 19:21:42,582381	0.602723	fe80::221:6aff:fe2d:3b8e	ff02::16	ICMPv6
47	2015-04-28 19:21:43,206127	0.623746	fe80::1	ff02::1	ICMPv6
52	2015-04-28 19:21:44,318127	1.112000	2003:50:aa10:4243:221:6aff:fe2d:3b8e	2a02:2e0:3fe:1001:302::	ICMPv6
53	2015-04-28 19:21:44,324504	0.006377	fe80::1	ff02::1:ff2d:3b8e	ICMPv6
54	2015-04-28 19:21:44,324536	0.000032	2003:50:aa10:4243:221:6aff:fe2d:3b8e	fe80::1	ICMPv6
55	2015-04-28 19:21:44,327662	0.003126	2a02:2e0:3fe:1001:302::	2003:50:aa10:4243:221:6aff:fe2d:3b8e	ICMPv6
58	2015-04-28 19:21:44,981772	0.654110	fe80::1	fe80::221:6aff:fe2d:3b8e	ICMPv6
59	2015-04-28 19:21:44,981808	0.000036	fe80::221:6aff:fe2d:3b8e	fe80::1	ICMPv6
60	2015-04-28 19:21:45,318191	0.336383	2003:50:aa10:4243:221:6aff:fe2d:3b8e	2a02:2e0:3fe:1001:302::	ICMPv6
61	2015-04-28 19:21:45,325679	0.007488	2a02:2e0:3fe:1001:302::	2003:50:aa10:4243:221:6aff:fe2d:3b8e	ICMPv6
66	2015-04-28 19:21:49,913260	4.587581	fe80::1	ff02::1	ICMPv6

1st Basic IPv4-IPv6 Messages - Knoppix Telekom.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmpv6 Expression...

No.	UTC	Time Delta	Source	Destination	Protocol
1	2015-04-28 19:21:00,798805	0.000000	::	ff02::16	ICMPv6
2	2015-04-28 19:21:01,328798	0.529993	::	ff02::16	ICMPv6
3	2015-04-28 19:21:01,372142	0.043344	::	ff02::1:ff2d:3b8e	ICMPv6
6	2015-04-28 19:21:01,861868	0.489726	fe80::1	ff02::1	ICMPv6
7	2015-04-28 19:21:02,375493	0.513625	fe80::221:6aff:fe2d:3b8e	ff02::16	ICMPv6
8	2015-04-28 19:21:02,375527	0.000034	fe80::221:6aff:fe2d:3b8e	ff02::2	ICMPv6
9	2015-04-28 19:21:02,376324	0.000797	fe80::221:6aff:fe2d:3b8e	ff02::2	ICMPv6
10	2015-04-28 19:21:02,384950	0.008626	fe80::1	fe80::221:6aff:fe2d:3b8e	ICMPv6
11	2015-04-28 19:21:02,384997	0.000047	fe80::221:6aff:fe2d:3b8e	fe80::1	ICMPv6
12	2015-04-28 19:21:02,386441	0.001444	fe80::1	ff02::1	ICMPv6
15	2015-04-28 19:21:03,255455	0.869014	fe80::221:6aff:fe2d:3b8e	ff02::16	ICMPv6
16	2015-04-28 19:21:03,305456	0.050001	fe80::221:6aff:fe2d:3b8e	ff02::16	ICMPv6
20	2015-04-28 19:21:03,792359	0.486903	fe80::221:6aff:fe2d:3b8e	ff02::16	ICMPv6
21	2015-04-28 19:21:03,885708	0.093349	::	ff02::1:ff2d:3b8e	ICMPv6
22	2015-04-28 19:21:05,785862	1.900154	fe80::1	ff02::1	ICMPv6
23	2015-04-28 19:21:07,395690	1.609828	fe80::221:6aff:fe2d:3b8e	fe80::1	ICMPv6
24	2015-04-28 19:21:07,398964	0.003274	fe80::1	fe80::221:6aff:fe2d:3b8e	ICMPv6
25	2015-04-28 19:21:09,868895	2.469931	fe80::1	ff02::1	ICMPv6
28	2015-04-28 19:21:17,876504	8.007609	fe80::1	ff02::1	ICMPv6
29	2015-04-28 19:21:25,884348	8.007844	fe80::1	ff02::1	ICMPv6
32	2015-04-28 19:21:33,893857	8.009509	fe80::1	ff02::1	ICMPv6
43	2015-04-28 19:21:41,903559	8.009702	fe80::1	ff02::1	ICMPv6
45	2015-04-28 19:21:41,979658	0.076099	fe80::1	ff02::1	ICMPv6
46	2015-04-28 19:21:42,582381	0.602723	fe80::221:6aff:fe2d:3b8e	ff02::16	ICMPv6
47	2015-04-28 19:21:43,206127	0.623746	fe80::1	ff02::1	ICMPv6
52	2015-04-28 19:21:44,318127	1.112000	2003:50:aa10:4243:221:6aff:fe2d:3b8e	2a02:2e0:3fe:1001:302::	ICMPv6
53	2015-04-28 19:21:44,324504	0.006377	fe80::1	ff02::1:ff2d:3b8e	ICMPv6
54	2015-04-28 19:21:44,324536	0.000032	2003:50:aa10:4243:221:6aff:fe2d:3b8e	fe80::1	ICMPv6
55	2015-04-28 19:21:44,327662	0.003126	2a02:2e0:3fe:1001:302::	2003:50:aa10:4243:221:6aff:fe2d:3b8e	ICMPv6
58	2015-04-28 19:21:44,981772	0.654110	fe80::1	fe80::221:6aff:fe2d:3b8e	ICMPv6
59	2015-04-28 19:21:44,981808	0.000036	fe80::221:6aff:fe2d:3b8e	fe80::1	ICMPv6
60	2015-04-28 19:21:45,318191	0.336383	2003:50:aa10:4243:221:6aff:fe2d:3b8e	2a02:2e0:3fe:1001:302::	ICMPv6
61	2015-04-28 19:21:45,325679	0.007488	2a02:2e0:3fe:1001:302::	2003:50:aa10:4243:221:6aff:fe2d:3b8e	ICMPv6
66	2015-04-28 19:21:49,913260	4.587581	fe80::1	ff02::1	ICMPv6

Wireshark Display Filters

- Problem: Everything is within ICMPv6
- Some (MLD) are not of interest at all!

Wireshark · Coloring Rules Default

Name	Filter
IPv6 MLD Zeugs	icmpv6.type in { 130, 131, 132, 143 }
ICMPv6 DAD	icmpv6.type eq 135 && ipv6.src eq ::
ICMPv6 NS/NA	icmpv6.type in { 135, 136 }
ICMPv6 RS/RA	icmpv6.type in { 133, 134 }
Bad TCP	tcp.analysis.flags && !tcp.analysis.window_update

Wireshark

- 1st Basic IPv4-IPv6 Messages - Knoppix Telekom.pcapng
  - Router Solicitation #8
  - Router Advertisement #12 (with O-flag)
  - Stateless DHCPv6 #13 & 14
  - Duplicate Address Detection #21
  - Neighbor Solicitation #53
  - Neighbor Advertisement #54 (echo-reply from router)
  - Ping #52 & 55

Wireshark

- 2nd IPv6-UpperLayers-FINAL.pcap
  → Nothing to see here ;)
  - DNS [hint: communication ≠ requested RR]
  - Ping
  - SNMP
  - HTTP/HTTPS
  - IMAP
  - SMTP with STARTTLS
  - SSH

A little routing, please

Static Routing

Virtual Router - default

- Router Settings
- **Static Routes**
- Redistribution Profile
- RIP
- OSPF
- OSPFv3
- BGP
- Multicast

IPv4 | **IPv6**

2 items

NAME	DESTINATION	INTERFACE	Next Hop TYPE	Next Hop VALUE	ADMIN DISTANCE	METRIC	ROUTE TABLE
default	::/0	ethernet1/2	ipv6-address	2001:470:1f0b:319::1	default	10	unicast
fg2_v6	2001:470:1f0b:16b0::/64	tunnel.1			default	10	unicast

Destination	Gateway IP	Interface	Status
IPv4 9			
IPv6 3			
::/0	::	HE	Enabled
2001:db8::/64	2001:470:1f0b:16b0::1234	internal	Enabled
2001:470:7250::/64	::	pa	Enabled

OSPFv3 for IPv6

- own protocol for IPv6

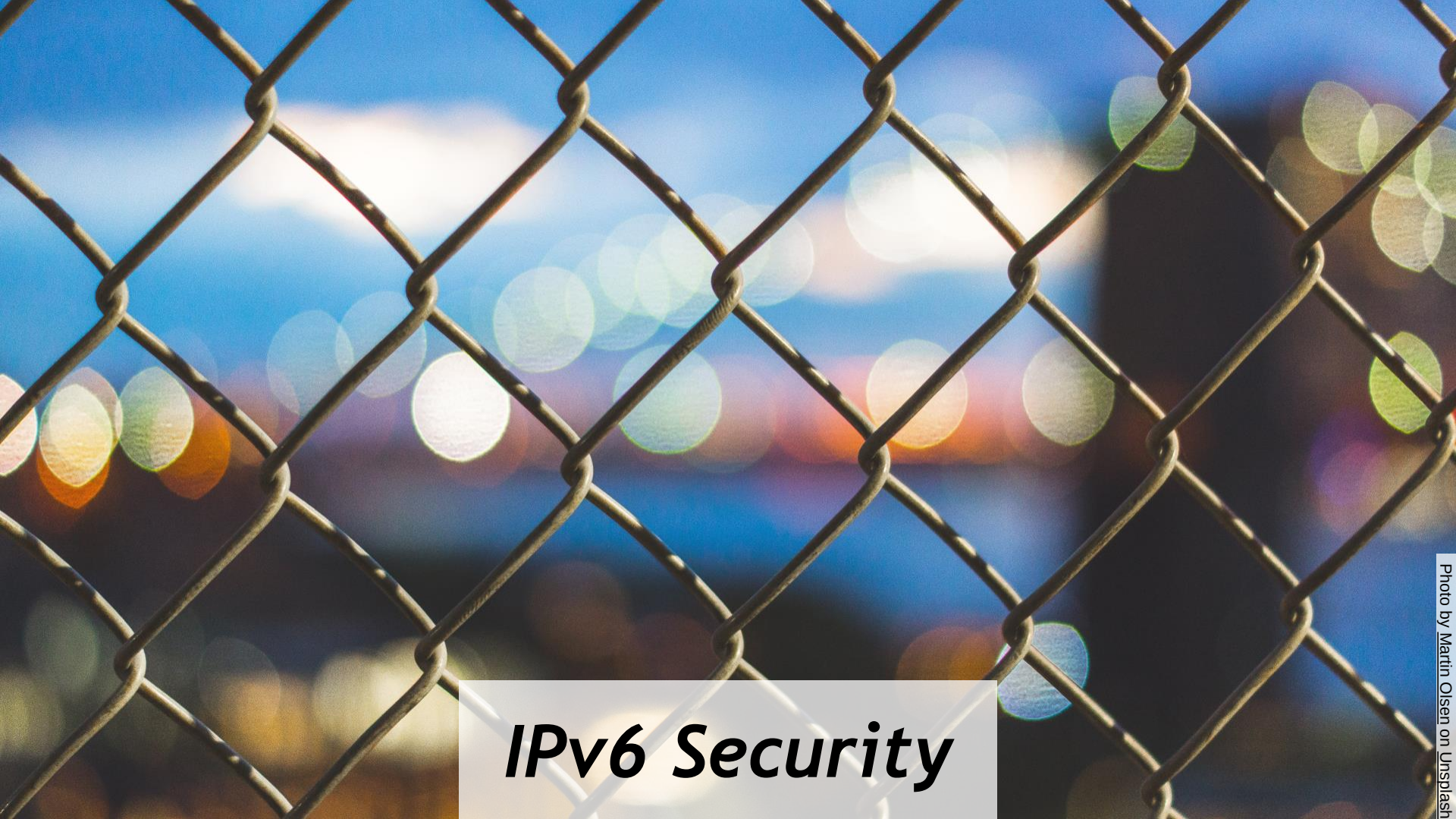
```
interface TenGigabitEthernet0/0
 ipv6 address 2003:51:6012:101::5/64
 ipv6 ospf 17 area 0.0.0.0
!
ipv6 router ospf 17
 router-id 172.16.1.5
```

MP-BGP

- one BGP process for both IPs
- neighbors either v4 or v6
- best practice:
  - v4 neighbors for v4 networks
  - v6 neighbors for v6 networks

MP-BGP

```
router bgp 64496
 neighbor 2001:DB8:0:F::3 remote-as 64496
 neighbor 198.51.100.47 remote-as 7028
 !
 address-family ipv4
  network 192.0.2.0 mask 255.255.255.0
  no neighbor 2001:DB8:0:F::3 activate
  neighbor 198.51.100.47 activate
 exit-address-family
 !
 address-family ipv6
  network 2001:DB8::/32
  neighbor 2001:DB8:0:F::3 activate
 exit-address-family
```

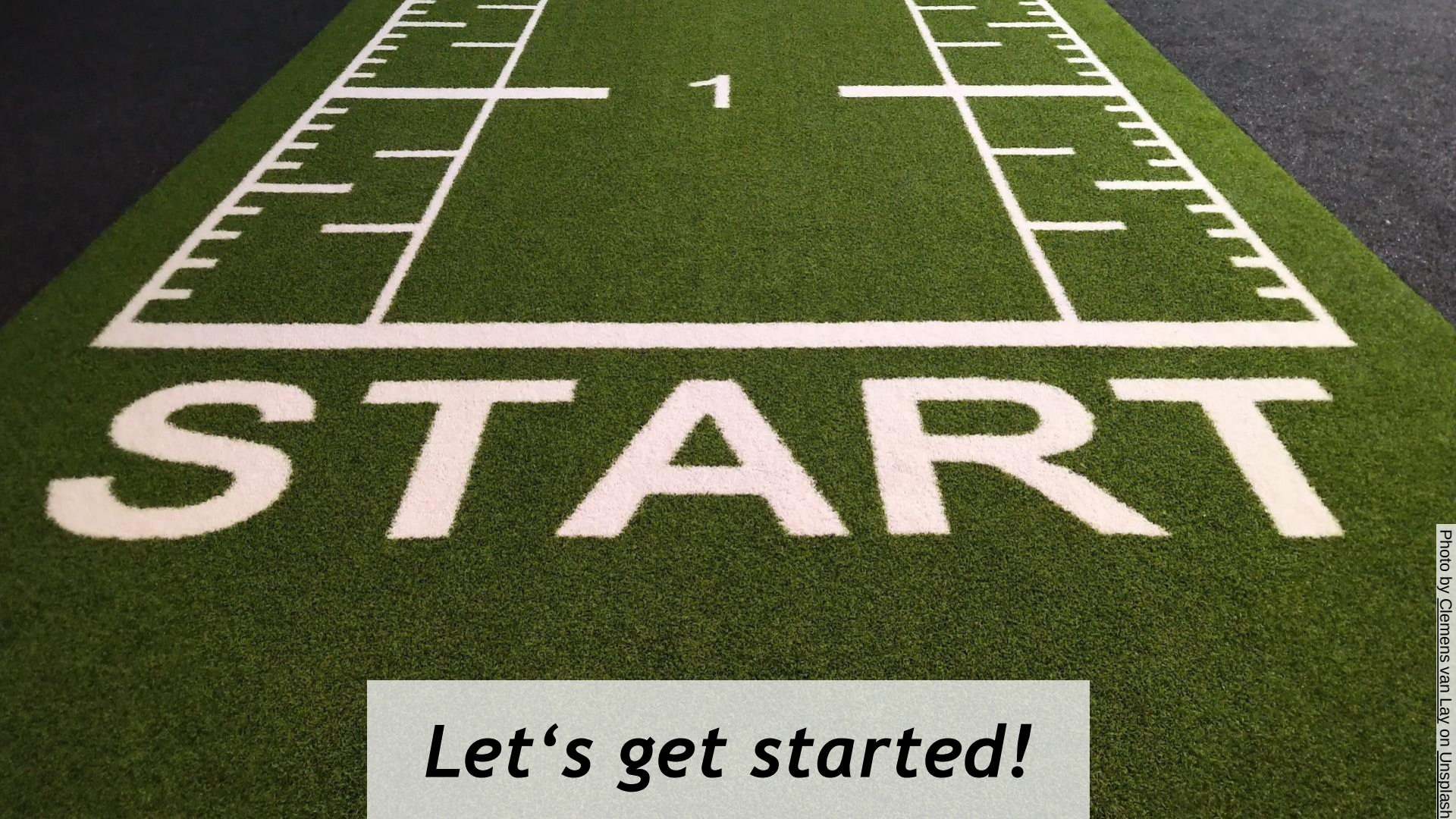


IPv6 Security

Photo by Martin Olsen on Unsplash

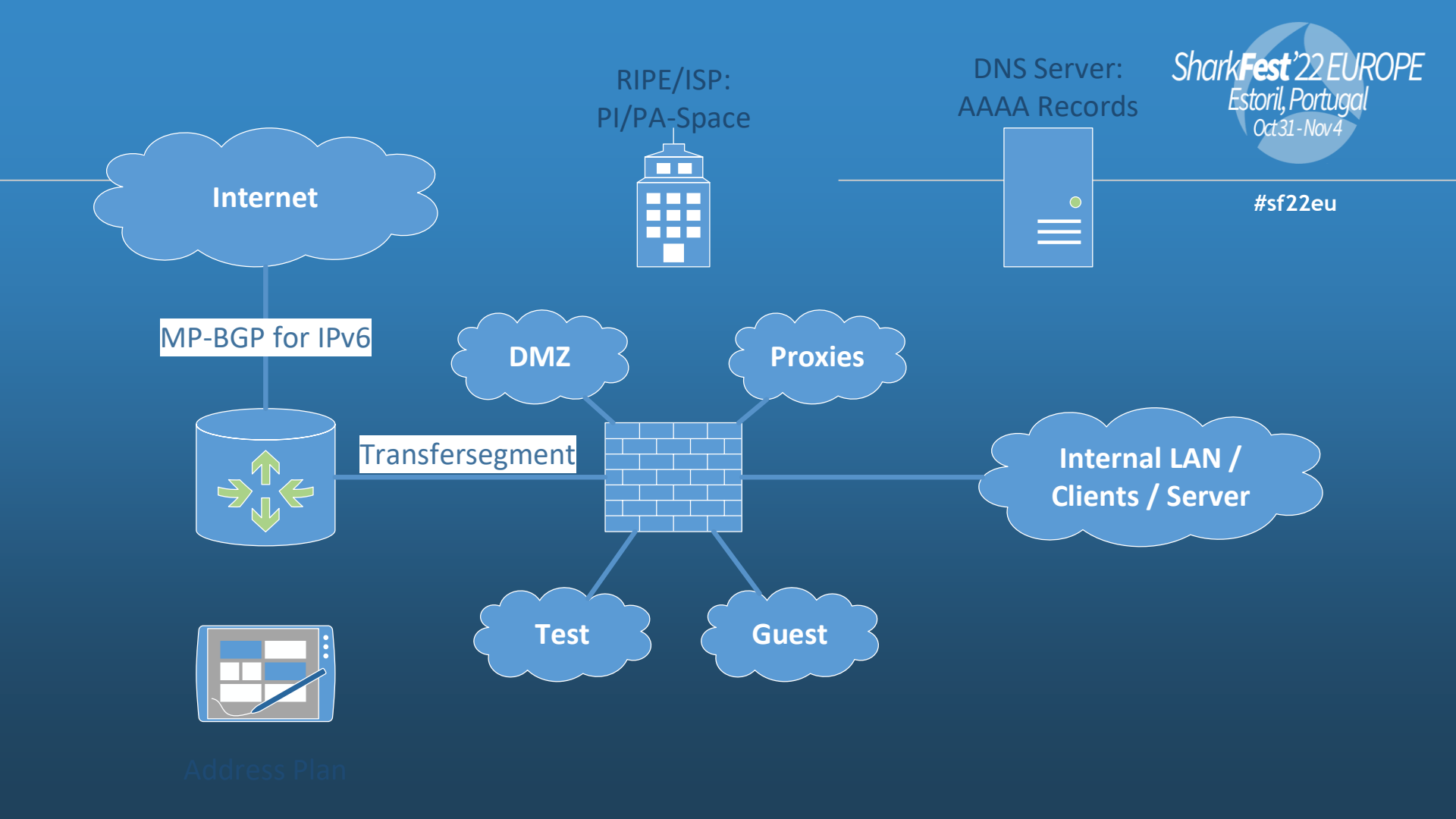
IPv6 Security

- TL;DR: same security level than legacy IP
- BUT:
  - different attack (names) → different countermeasures
  - dual-stack everywhere → doubled workload
  - admins are less experienced → human error
  - products are not feature complete



Let‘s get started!

Photo by Clemens van Lay on Unsplash


RIPE/ISP:
PI/PA-Space
DNS Server:
AAAA Records
SharkFest'22 EUROPE
Estoril, Portugal
Oct 31 - Nov 4
#sf22eu
Internet
MP-BGP for IPv6
DMZ
Proxies
Transfersegment
Internal LAN /
Clients / Server
Test
Guest
Address Plan

DNS64 & NAT64

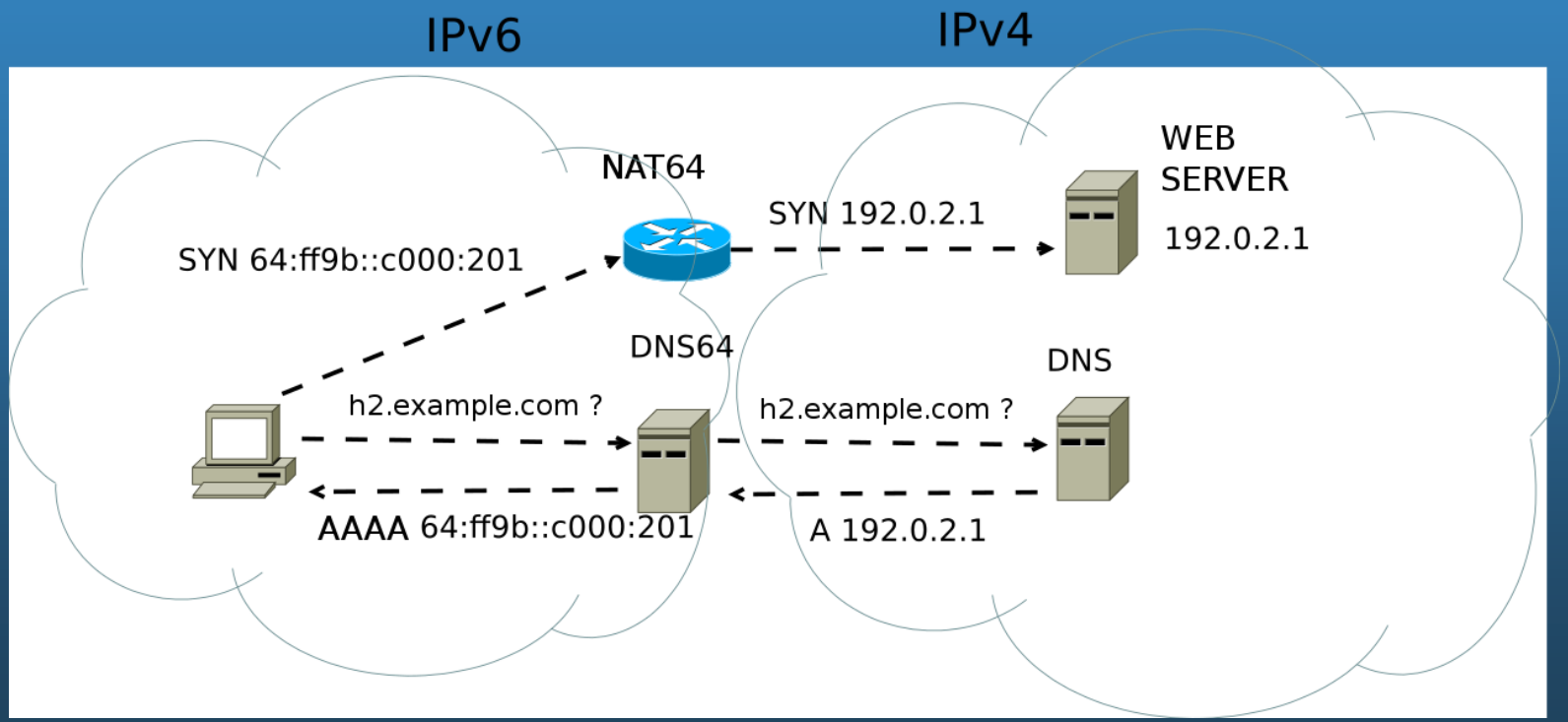


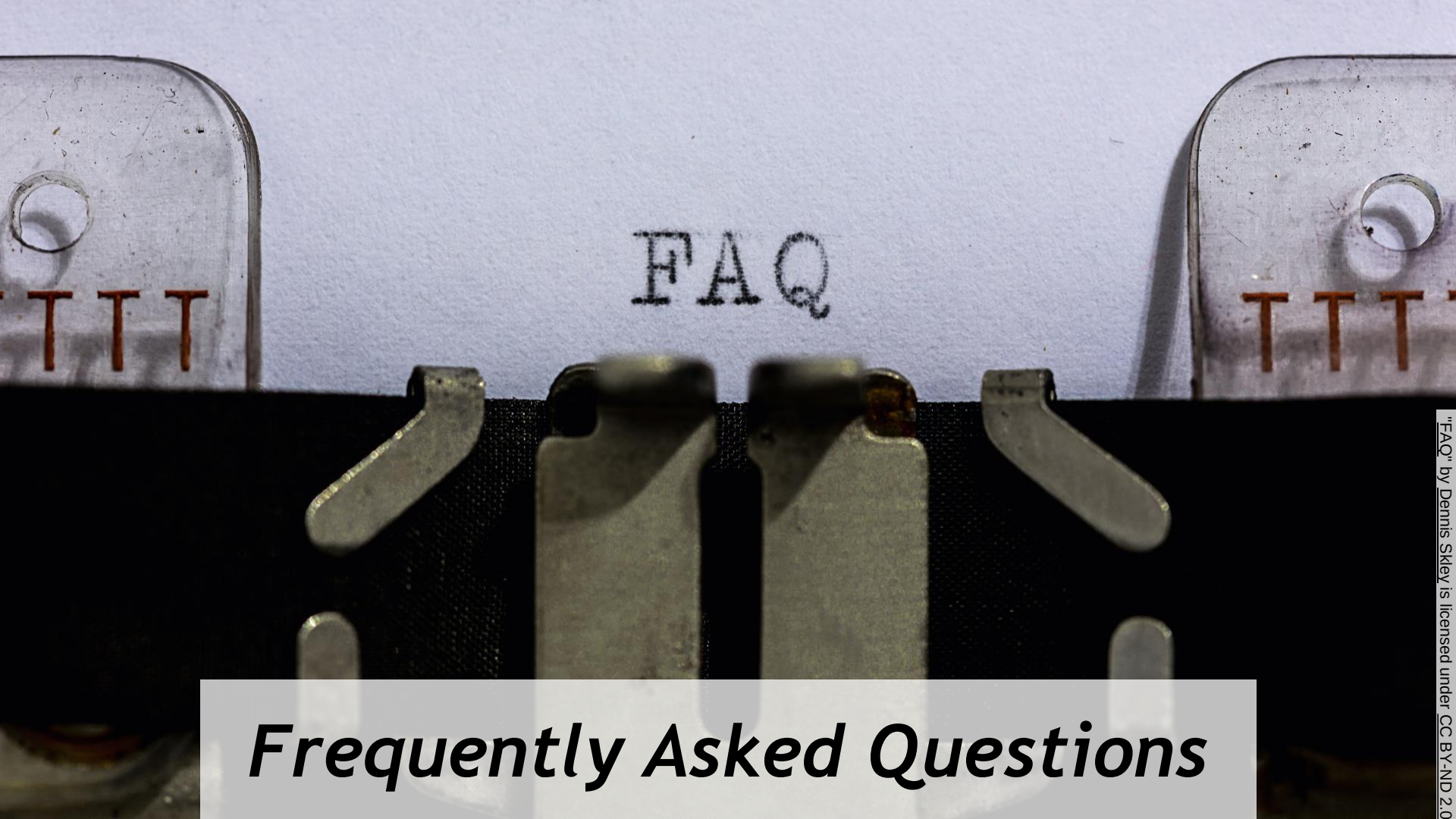
Image source: https://de.wikipedia.org/wiki/NAT64

What we've not talked about

Photo by You X Ventures on Unsplash

What we have not talked about

- header & extension headers (fragmentation)
- address planning
- renumbering, dynamic IPv6 prefixes, DHCPv6-PD, NPTv6
- migration techniques (Dual-Stack, DS-Lite)
- unsolved problems, implementations, bugs
- security & attacks
- comparison to IPv4, statistics



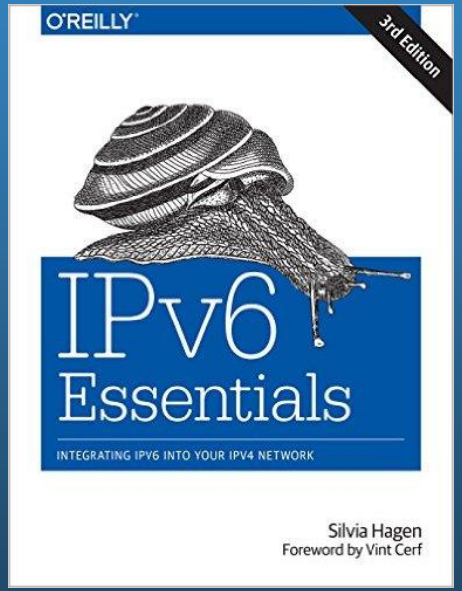
Frequently Asked Questions

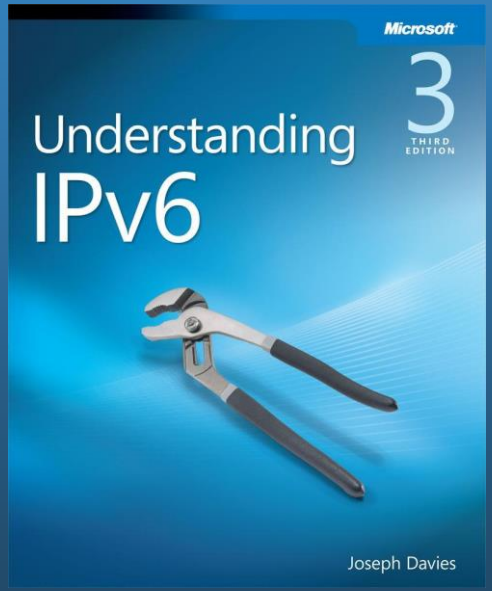
FAQs

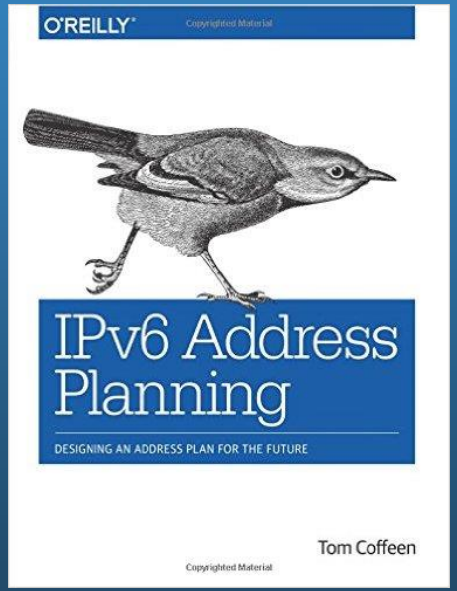
- Can I disable IPv6 completely?
  - Maybe partially through Windows GPOs, but what about your printers, cameras, access points, BYOD tablets/phones? And even if: It adds administative burdens when you're going to deploy IPv6 later on. → Hence: Don't disable IPv6 but deploy it!
- Can my security assessment tools scan my entire IPv6 prefix?
  - No. You need to provide IPv6 address lists to them in order to work properly.
- Can I use private IPv6 addresses (ULAs)?
  - You shouldn‘t. In any case: „The allocation of Global IDs is pseudo-random”!!!

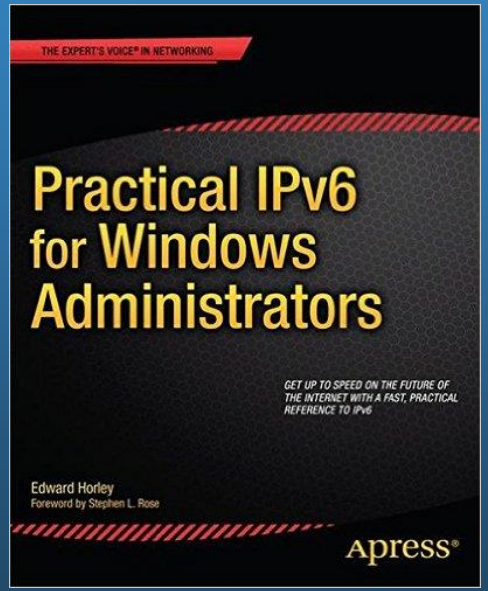
Literature

Literature


O'REILLY
3rd Edition
IPv6 Essentials
INTEGRATING IPV6 INTO YOUR IPV4 NETWORK
Silvia Hagen
Foreword by Vint Cerf


Microsoft
Understanding IPv6
3
THIRD EDITION
Joseph Davies


O'REILLY
IPv6 Address Planning
DESIGNING AN ADDRESS PLAN FOR THE FUTURE
Tom Coffeen


THE EXPERT'S VOICE® IN NETWORKING
Practical IPv6 for Windows Administrators
GET UP TO SPEED ON THE FUTURE OF THE INTERNET WITH A FAST, PRACTICAL REFERENCE TO IPv6
Edward Horley
Foreword by Stephen L. Rose
Apress®

Literature

- RFCs (8200, 4443, …)
- Podcast: IPv6 Buzz

- ipv6-ops Mailinglist
- ipv6hackers Mailinglist

- IPv6 Security Frequently Asked Questions (FAQ)
- Deploying IPv6 in Dropbox Edge Network
- APNIC - IPv6-only at Microsoft
- RIPE: Best Current Operational Practice for Operators: IPv6 prefix assignment for end-users - persistent vs non-persistent, and what size to choose

Thx!

- Questions? → johannes@webernetz.net || @webernetz