
# IPv6 Essentials

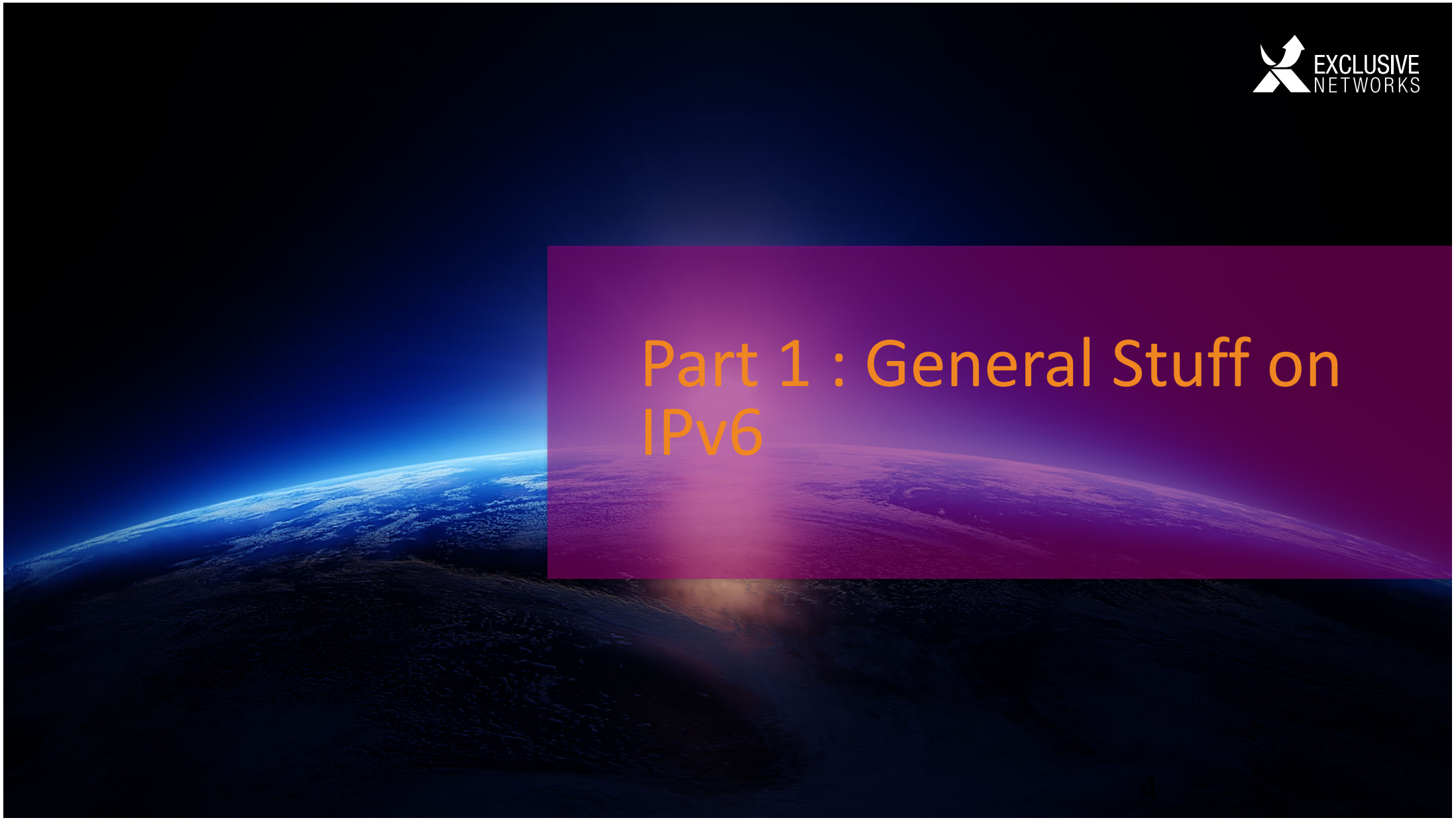
Thierry Van Steirteghem
Senior Presales Engineer & IPv6 Evangelist

# Who Am I

- Thierry Van Steirteghem
- Senior Presales Engineer
  - Infoblox
  - F5
  - Broadcom - Symantec
  - Thales - Gemalto HSM & DPoD
  - IPv6
- Professional Services
- Certified Trainer
  - Infoblox
  - F5
  - IPv6
- 10 years in Security
  - Twitter: @steirtet
  - Email: tvansteirteghem@Exclusive-Networks.be
  - Linked-in: www.linkedin.com/in/steirtet

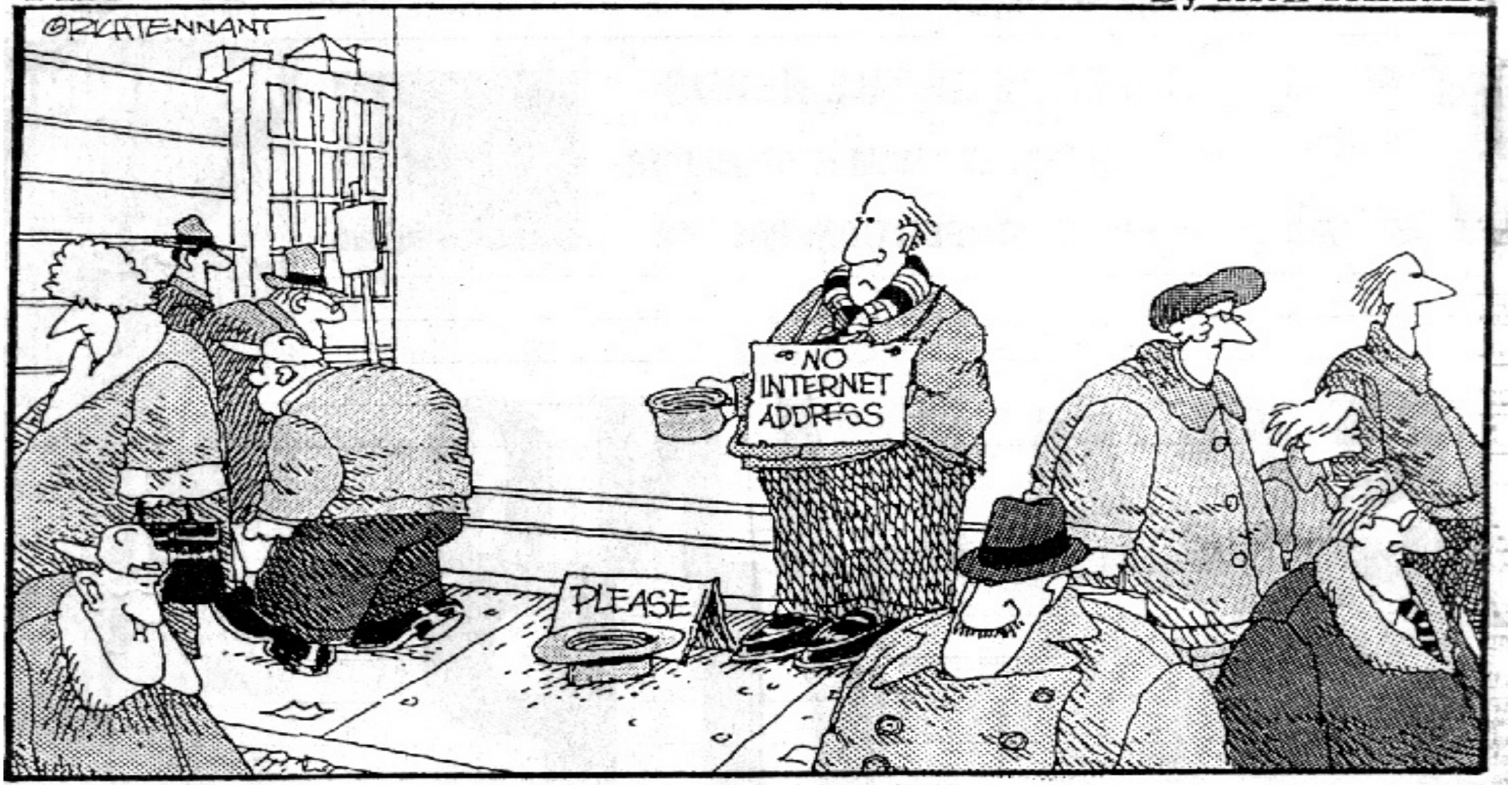
# Remark

- This slide desk is based on the information gven during the ipv6 meetup at 29 april 2020
- This slide desk is part of an IPv6 basic training given by the author
- Not slides from the training are available in this pdf
- The content is available on the IPv6 council website
- Questions can be sent to ipv6 council or to the author - thierry@vansteirteghem.eu


EXCLUSIVE
NETWORKS
Part 1 : General Stuff on IPv6

# The 5th Wave

By Rich Tennant



# IPv6 <> IPv4

| Feature | IPv4 | IPv6 |
|---|---|---|
| Number of bits (bytes) | 32 (4) | 128 (16) |
| Expressed form | Dotted-decimal | Colon-hexadecimal |
| Variable-length subnets | Yes | No |
| Public addresses | Yes | Yes (global addresses) |
| Private addresses | Yes (RFC 1918 addresses) | Yes (unique local addresses) |
| Autoconfigured addresses for the local link | Yes (APIPA) | Yes (link-local addresses) |
| Support for address classes | Yes, but deprecated by CIDR | No |
| Broadcast addresses | Yes | Multicast used instead |
| Subnet mask | Required | Implicit 64-bit address prefix length for addresses assigned to interfaces |

# The next IP version

- What will be the next version

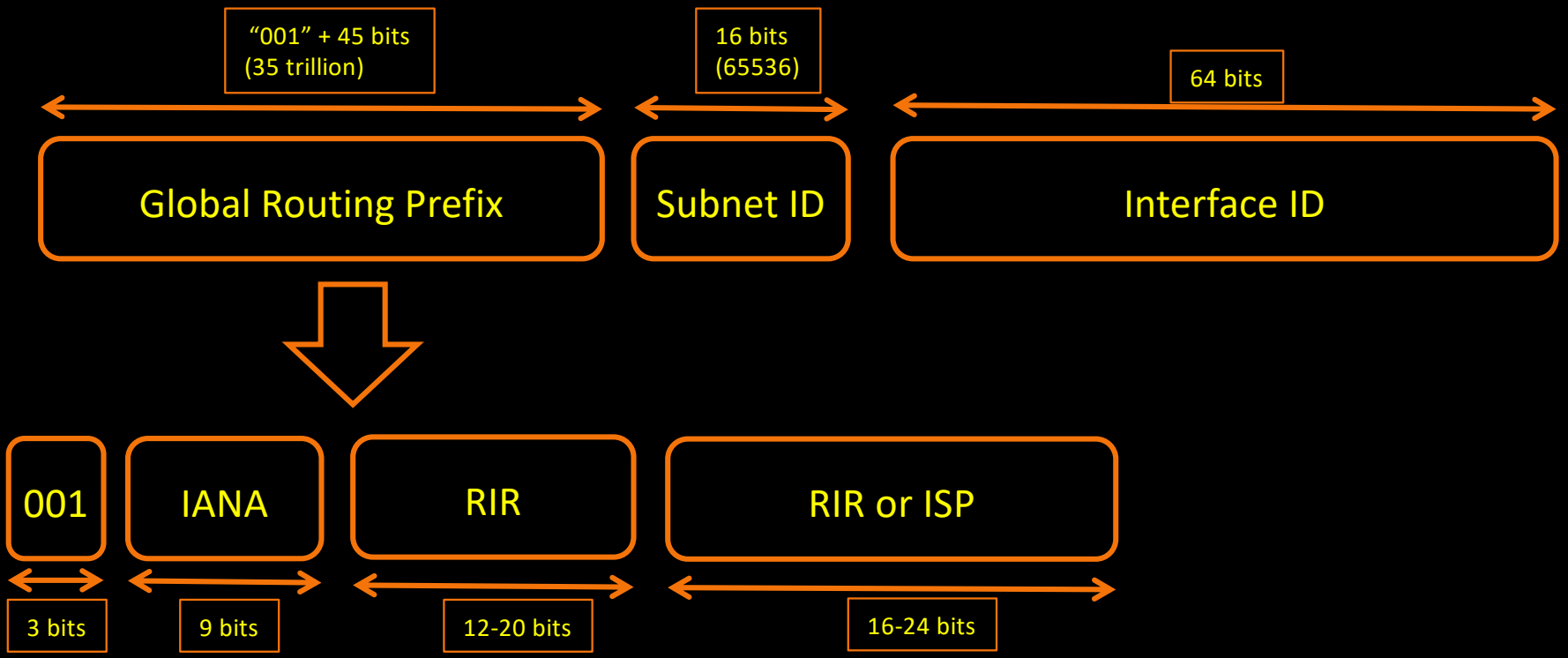

EXCLUSIVE
NETWORKS
Part 2 : IPv6 Address Assignment – DHCPv6

# IPv4 <> IPv6

| IP version | IPv4 | IPv6 |
|---|---|---|
| Deployed | 1981 | 1999 |
| Address Size | 32-bit number | 128-bit number |
| Address Format | Dotted Decimal Notation: 192.0.2.76 | Hexadecimal Notation: 2001:0DB8:0234:AB00: 0123:4567:8901:ABCD |
| Number of Addresses | $2^{32}$ = 4,294,967,296 | $2^{128}$ = 340,282,366,920,938,463, 463,374,607,431,768,211,456 |
| Examples of Prefix Notation | 192.0.2.0/24<br>10/8<br>(a "/8" block = 1/256$^{th}$ of total IPv4 address space = $2^{24}$ = 16,777,216 addresses) | 2001:0DB8:0234::/48<br>2A00:0000::/12 |

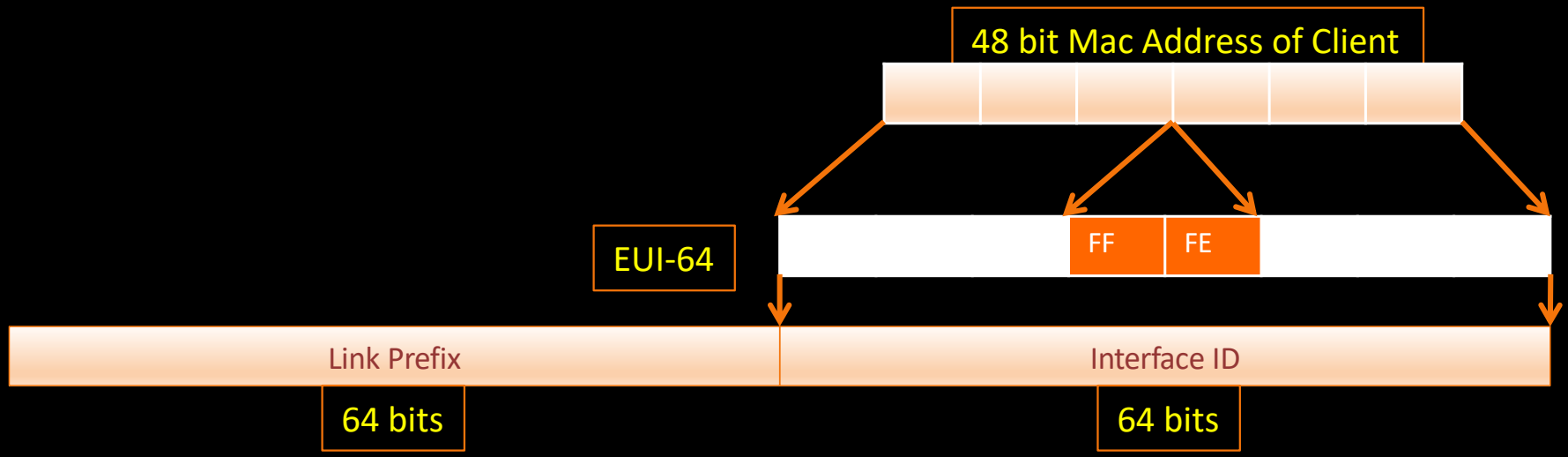

My ::/32 is bigger than your /32
No place like ::1
cafe::c0ff:ee

# Structure of a Global Unicast IPv6 address



# IPv6 Stateless Address Autoconfiguration

- SLAAC
- Neighbor Discovery ICMPv6 messages
- Host get IPv6 address
  - Host asks to receive IPv6 prefix
  - Host creates IPv6 address (privacy enabled?)



# SLAAC

- No manual configuration
- Stateless and Statefull DHCPv6
- DNS added via RFC6106

# IPv6 Addresses

- compare with IPv4

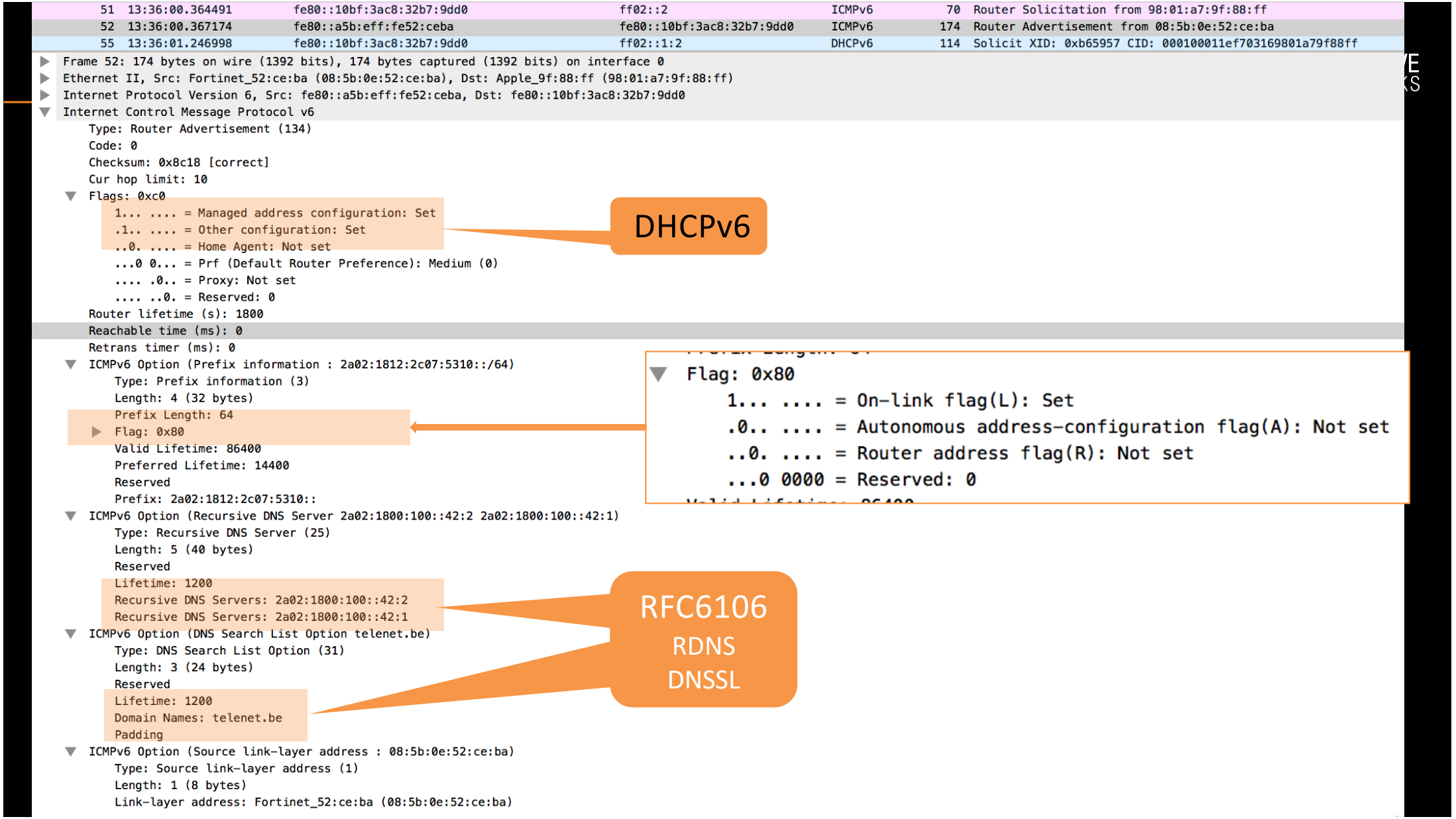
| Type | IPv6 | IPv6 Scope | IPv4 |
|---|---|---|---|
| Unspecified | ::/128 | | 0.0.0.0 |
| Loopback | ::1/128 | host | 127.0.0.1 |
| Unique Local Address | fc00::/7 | global | RFC 1918 |
| Private Administration | fd00::/8 | global | RFC 1918 |
| Link-Local Address | fe80::/10 | link | 169.254/16 |
| Documentation | 2001:db8::/32 | | 192.0.2/24 |
| Global Unicast | 2000::/3 | global | |
| Multicast | ff00::/8 | variable | 224/4 |
| 6to4 | 2002::/16 | global | |
| Teredo | 2001:0000:/32 | global | |

# RS example

EXCLUSIVE NETWORKS

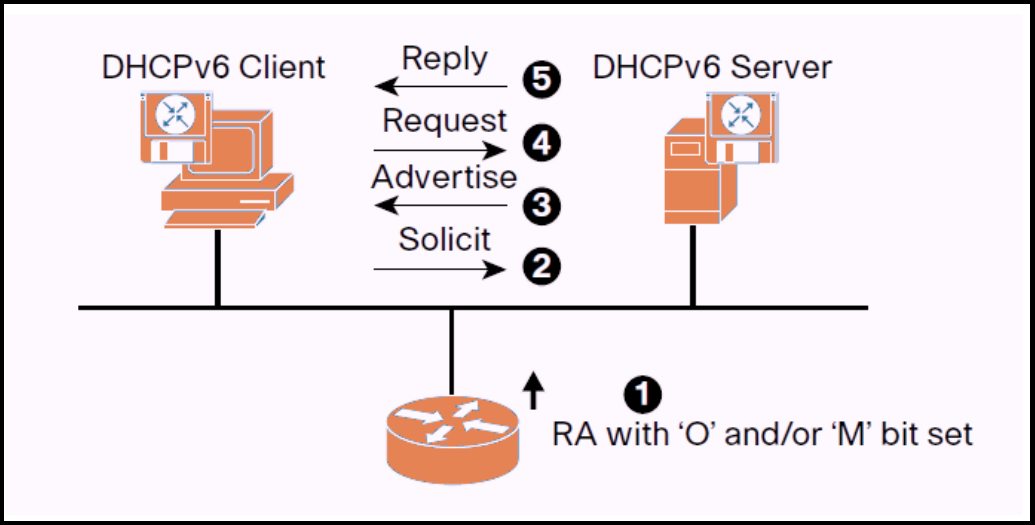
```
    26 13:35:55.919468 ::                      ff02::1:ffb7:9dd0    ICMPv6     86 Neighbor Solicitation for fe80::10bf:3ac8:32b7:9dd0
    27 13:35:55.920035 fe80::10bf:3ac8:32b7:9dd0 ff02::2            ICMPv6     62 Router Solicitation
    29 13:35:56.203566 fe80::10bf:3ac8:32b7:9dd0 ff02::16           ICMPv6    110 Multicast Listener Report Message v2
```

```
▶ Frame 27: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
▶ Ethernet II, Src: Apple_9f:88:ff (98:01:a7:9f:88:ff), Dst: IPv6mcast_02 (33:33:00:00:00:02)
▶ Internet Protocol Version 6, Src: fe80::10bf:3ac8:32b7:9dd0, Dst: ff02::2
▼ Internet Control Message Protocol v6
    Type: Router Solicitation (133)
    Code: 0
    Checksum: 0x6128 [correct]
    Reserved: 00000000
```


51 13:36:00.364491 fe80::10bf:3ac8:32b7:9dd0 ff02::2 ICMPv6 70 Router Solicitation from 98:01:a7:9f:88:ff
52 13:36:00.367174 fe80::a5b:eff:fe52:ceba fe80::10bf:3ac8:32b7:9dd0 ICMPv6 174 Router Advertisement from 08:5b:0e:52:ce:ba
55 13:36:01.246998 fe80::10bf:3ac8:32b7:9dd0 ff02::1:2 DHCPv6 114 Solicit XID: 0xb65957 CID: 000100011ef703169801a79f88ff
Frame 52: 174 bytes on wire (1392 bits), 174 bytes captured (1392 bits) on interface 0
Ethernet II, Src: Fortinet_52:ce:ba (08:5b:0e:52:ce:ba), Dst: Apple_9f:88:ff (98:01:a7:9f:88:ff)
Internet Protocol Version 6, Src: fe80::a5b:eff:fe52:ceba, Dst: fe80::10bf:3ac8:32b7:9dd0
Internet Control Message Protocol v6
Type: Router Advertisement (134)
Code: 0
Checksum: 0x8c18 [correct]
Cur hop limit: 10
Flags: 0xc0
1... .... = Managed address configuration: Set
.1.. .... = Other configuration: Set
..0. .... = Home Agent: Not set
...0 0... = Prf (Default Router Preference): Medium (0)
.... .0.. = Proxy: Not set
.... ..0. = Reserved: 0
Router lifetime (s): 1800
Reachable time (ms): 0
Retrans timer (ms): 0
ICMPv6 Option (Prefix information : 2a02:1812:2c07:5310::/64)
Type: Prefix information (3)
Length: 4 (32 bytes)
Prefix Length: 64
Flag: 0x80
Valid Lifetime: 86400
Preferred Lifetime: 14400
Reserved
Prefix: 2a02:1812:2c07:5310::
ICMPv6 Option (Recursive DNS Server 2a02:1800:100::42:2 2a02:1800:100::42:1)
Type: Recursive DNS Server (25)
Length: 5 (40 bytes)
Reserved
Lifetime: 1200
Recursive DNS Servers: 2a02:1800:100::42:2
Recursive DNS Servers: 2a02:1800:100::42:1
ICMPv6 Option (DNS Search List Option telenet.be)
Type: DNS Search List Option (31)
Length: 3 (24 bytes)
Reserved
Lifetime: 1200
Domain Names: telenet.be
Padding
ICMPv6 Option (Source link-layer address : 08:5b:0e:52:ce:ba)
Type: Source link-layer address (1)
Length: 1 (8 bytes)
Link-layer address: Fortinet_52:ce:ba (08:5b:0e:52:ce:ba)
DHCPv6
Flag: 0x80
1... .... = On-link flag(L): Set
.0.. .... = Autonomous address-configuration flag(A): Not set
..0. .... = Router address flag(R): Not set
...0 0000 = Reserved: 0
RFC6106
RDNS
DNSSL

# IPv6 Statefull address configuration

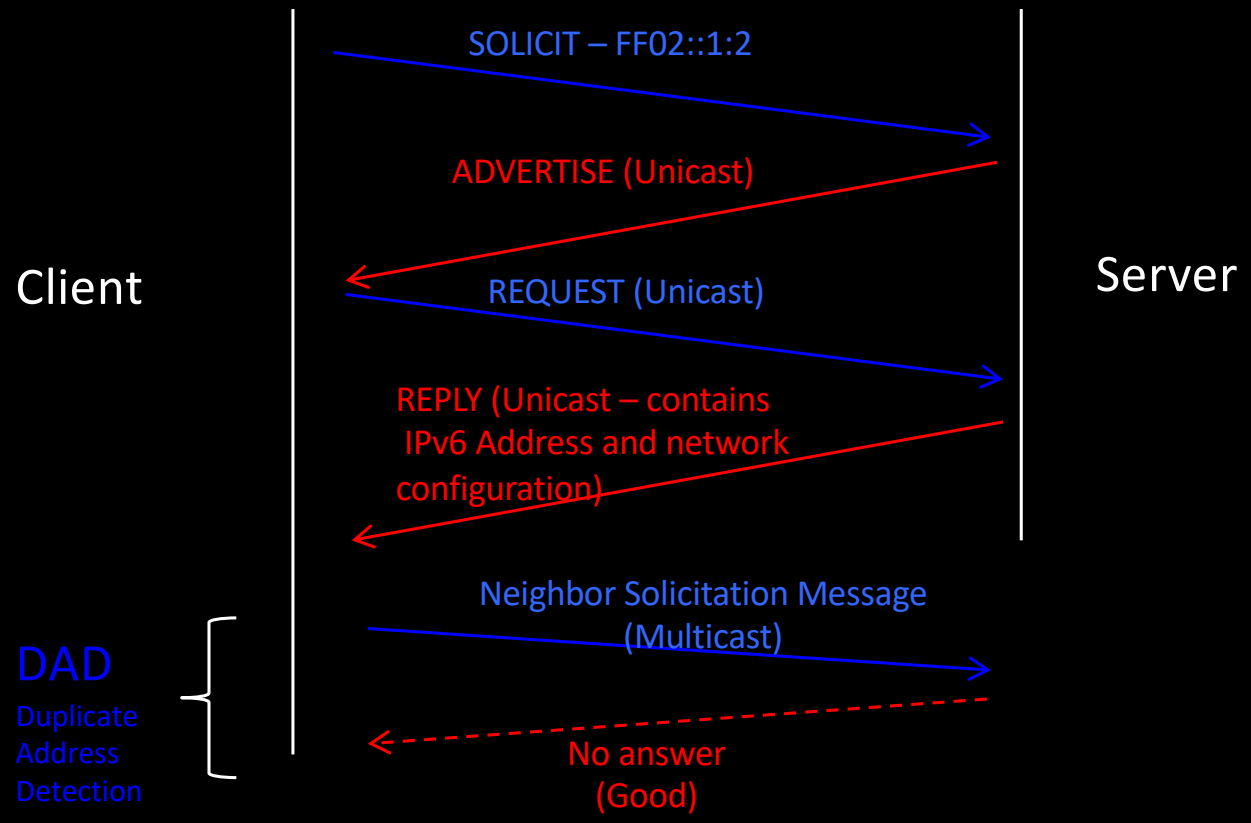
- DHCPv6
  - Used if router is not found
  - Used if Router Advertisement Message enables DHCPv6
- Manual configuration



# DHCPv4 <> DHCPv6 messages

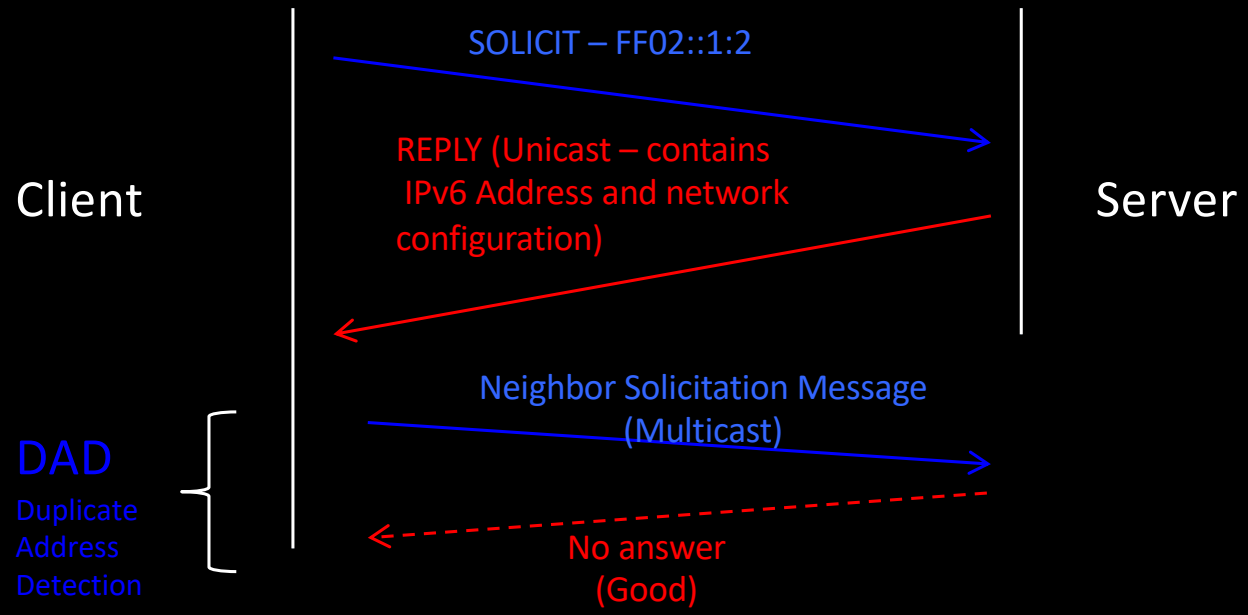
| DHCP (IPv4) | DHCPv6 |
|---|---|
| DHCPOFFER | ADVERTISE (2) |
| DHCPREQUEST | REQUEST (3), RENEW (5), REBIND (6) |
| DHCPACK/DHCPNAK | REPLY (7) |
| DHCPRELEASE | RELEASE (8) |
| DHCPINFORM | INFORMATION-REQUEST (11) |
| DHCPDECLINE | DECLINE (9) |
| -- | CONFIRM (4) |
| DHCPFORCERENEW | RECONFIGURE (10) |
| -- | RELAY-FORW (12), RELAY-REPLY (13) |

# DHCPv6 - Flow

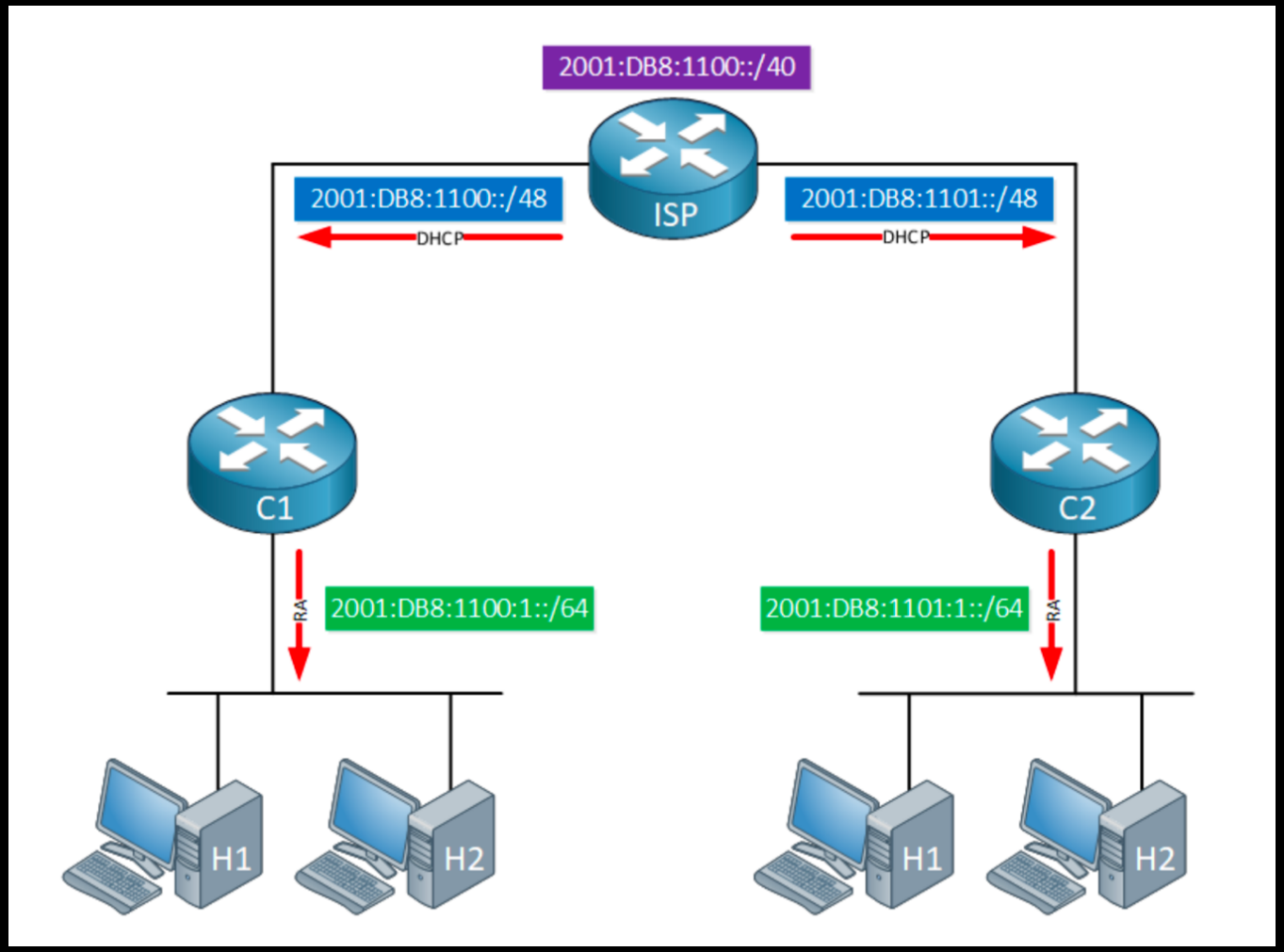

Client
Server
SOLICIT – FF02::1:2
ADVERTISE (Unicast)
REQUEST (Unicast)
REPLY (Unicast – contains IPv6 Address and network configuration)
Neighbor Solicitation Message (Multicast)
No answer (Good)
DAD
Duplicate Address Detection

# DHCPv6 – Rapid Commit

- Only when client and server commit to use rapid commit



# DHCPv6 Prefix Delegation



## DHCPv6

- Wireshark demo

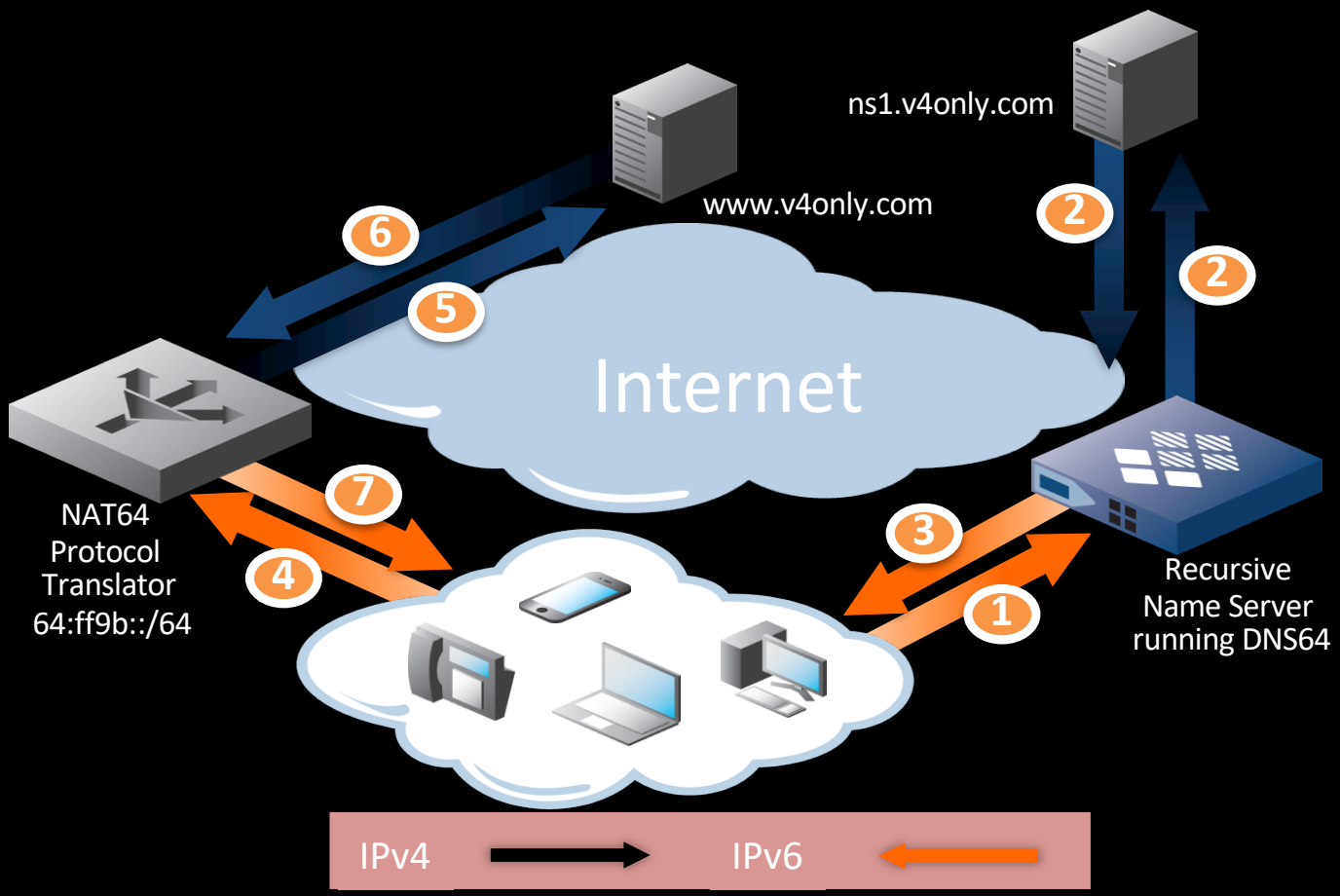

EXCLUSIVE
NETWORKS
Part 3 : NAT64 / DNS64

# Transition 3 : Translate

- NAT64/DNS64
  - Used when a IPv6 only subscriber wants to connect to IPv4 only network.
  - Both translators can be installed on the same or different devices

- Remark:
  - When using dual stack in windows:
  - windows client will first try to connect over IPv6 en then IPv4
  - In this case you do not need a translation

# DNS64




1. Client queries *www.v4only.com* AAAA to local recursive name server
2. Recursive name server queries name server for v4only.com and gets no AAAA response
3. Recursive name server synthesizes a IPv6 address to return to client – using /96 prefix
4. Client sends packet to synthesized IPv6 address which routes to the NAT64 protocol translator
5. NAT64 device translates packet to destination IPv4 address
6. IPv4 only web server returns the response over IPv4 to NAT64 device
7. NAT64 device converts the packet to IPv6 to return to the originating client

# DNS 64 Demo

- Differences in output between DNS64 enabled DNS responses and without


EXCLUSIVE
NETWORKS
Part 4 : IPv6
deployment

## Deployment

- IPv6 is not backward compatible with IPv4
- Not all platforms do support IPv6 (for free)
- Extra delays due to translation/tunneling

- Security is important
  - IPv6 and firewalls
  - IPSec and authentication are included

- Advantages
  - No NAT
  - No Broadcast

# Deployment scenarios

- Train your staff
  - IPv6 Essentials training
- Follow your suppliers and ask for info
  - Check applications and hardware for IPv6
  - Is IPv6 an extra license or is it included?
  - Network management tools : support for IPv6?
- Review all SLA's : is support for IPv6 included?
- Is your ISP ready to support native IPv6 connectivity

# IPv6 address concept

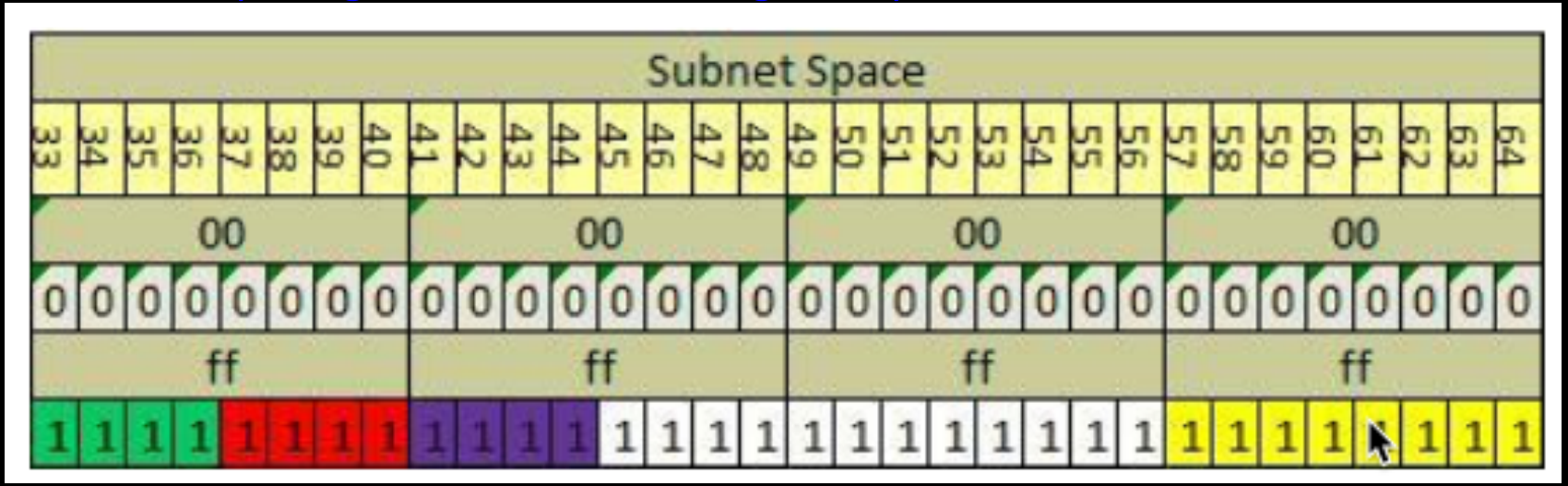
- Should take following into consideration:
  - Use of address types (ULA, GUA,..)
  - Prefix aggregation
  - Use of address mechanisms (DHCPv6, SLAAC, IPAM)
  - Security Aspects
  - Operational aspects
  - Growth

# Interface IDs

- Interface ID, 64 bit, with following formats
  - EUI-64
  - Manual
  - Random Changing (Privacy)
  - Random Stable (RFC 7217)
  - DHCPv6 static

# IPv6 Address planning

- Example
- Arrange per nibble
- $2^4$ = 16 options, $2^{12}$ = 4096 options, $2^8$ = 256 Options
- https://labs.ripe.net/Members/steffann/preparing-an-ipv6-addressing-plan
- https://www.ripe.net/support/training/material/IPv6-for-LIRs-Training-Course/Preparing-an-IPv6-Addressing-Plan.pdf



## IPv6 Requirements

- IPv6 RFC 6434 : IPv6 Node Requirements, 2011
- USGv6
- RIPE 554 - **Requirements for IPv6 in ICT Equipment**
  - > https://www.ripe.net/publications/docs/ripe-554
  - > **Best Current Practice template to develop tender documents containing IPv6 requirements**

## General recommendations

- Make sure you get the optimal prefix (preferably PI space)
- Minimize the number of prefix lengths (summarize routing)
- Reserve space for infrastructure
- Structure at nibble boundaries when possible
- Define addressing rules for all scopes
- Evaluate IPAM tools
- When starting new  networking projects, include IPv6


EXCLUSIVE
NETWORKS
Part 5 : IPv6 Security Basics

# Issues

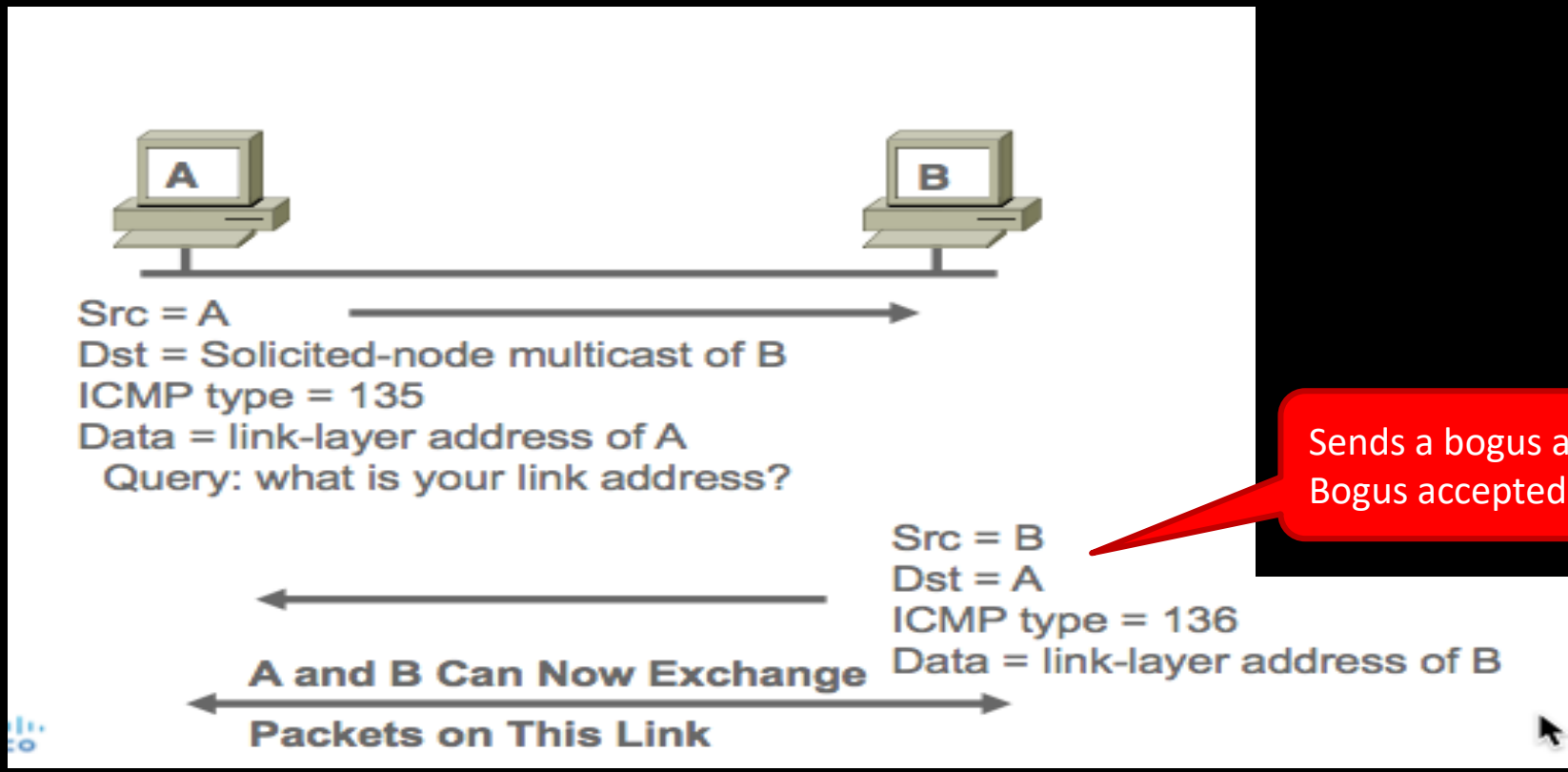
- Need for IPAM – IPv6 address Management
- Security
  - Firewall configurations
  - IDS Systems
- Management of AAAA records in DNS

- Protect RA
  - Microsoft clients' CPU can rise to 100%
  - http://www.networkworld.com/news/2011/050311-microsoft-juniper-ipv6.html?page=1
  - Make use of RA-Guard (see RFC 6105)
  - Example: https://www.youtube.com/watch?v=TfsfNWHCKK0

## Address Reconnaissance Myth

- Due to the large address space, It is not possible to scan all the hosts in a network ($2^{64}$ addresses)
- Check “ping6 ff02::1”

# Neighbor Solicitation




Sends a bogus answer.
Bogus accepted by client

# Mitigation

- ARP spoofing becomes ND spoofing

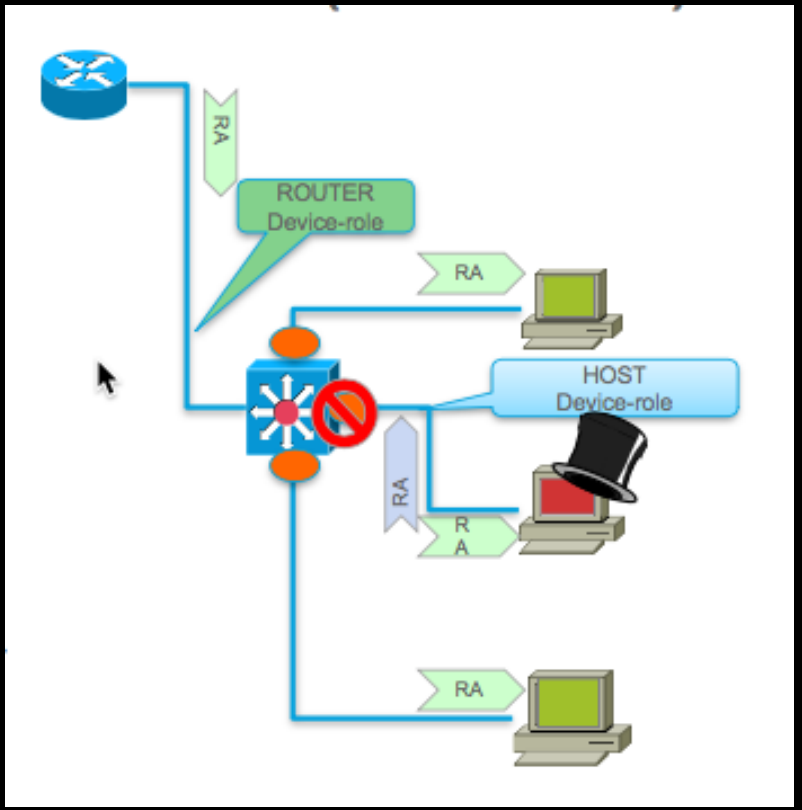
- **GOOD NEWS** : First-Hop-Security for IPv6 is available (cisco FHS)
  - Port ACL & RA Guard
  - NDP & DHCP snooping
  - Source Guard, Destination Guard
- **(kind of) GOOD NEWS** : Secure Neighbor Discovery
  - SeND = NDP + crypto
  - Available in IOS
  - But not in Windows 7, 2008, 2012 and 8, Mac OS/X, iOS, Android

# Mitigation (2)

- Other **GOOD NEWS** :
  - Private VLAN works with IPv6
  - Port security works with IPv6
  - IEEE 801.X works with IPv6 (except downloadable ACL)

# Example : RA Guard

- Port ACL
  - > Blocks all ICMPv6 RA from hosts
- RA GUARD
  - > Not always implemented, check documentation of network



# IPv6 security

- IPv6 addresses
  - IPv6 subnets are /64 (minimum)
  - Host randomly select and IPv6 address from tis subnet


  - Higher : Vendor specific : known or guessable (google)
  - FFFE defined
  - Lower: MAC address dependent from client
  - MAC addresses can be consecutive

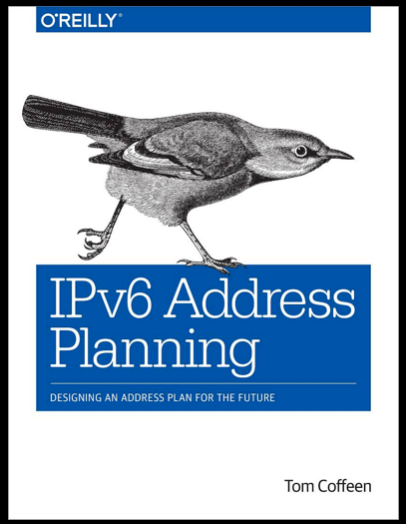
## Do I have IPv6 in my network

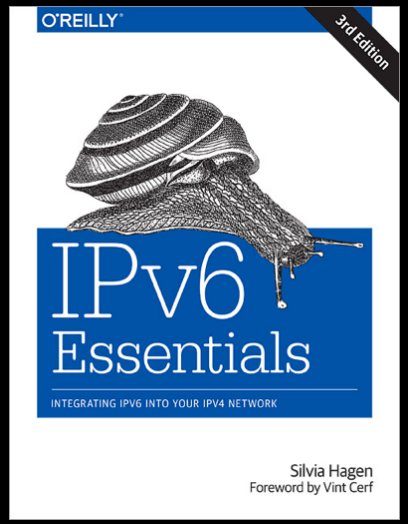
- DHCPv6
- Look in Netflow records
  - Protocol 41: IPv6 over IPv4 tunnels
  - Destination IPv4: 192.88.99.1 (6to4 anycast server)
  - UDP 3544: pubic part of Teredo
  - ICMPv6 packets (RA)
  - Check DNS query for ISATAP
- **Your IPv4-Only network can be vulnerable for IPv6 attacks NOW**

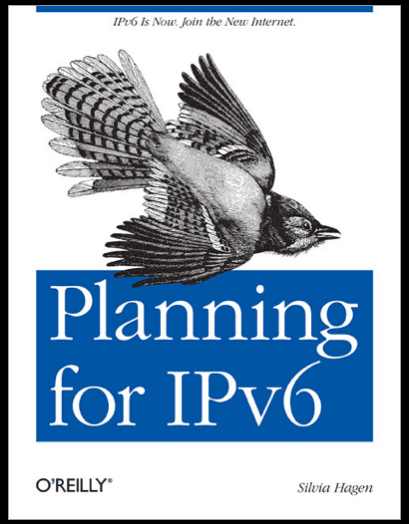
# Extra tools

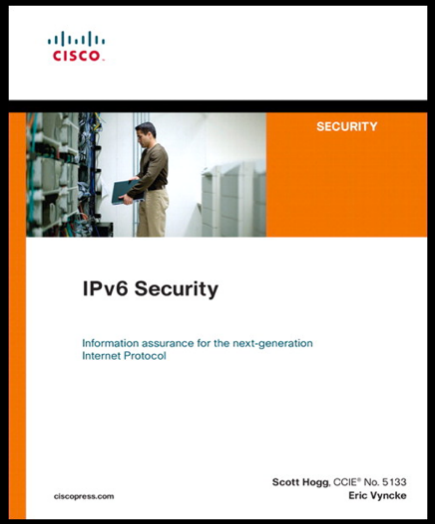
- https://www.si6networks.com
- https://www.si6networks.com/tools/ipv6toolkit/index.html

# Recommended IPv6 readings




- https://tools.ietf.org/html/draft-ietf-opsec-v6-11 (operational security Considerations for IPv6 networks)
- https://tools.ietf.org/html/rfc6434 (IPv6 Node Requirements)

# Questions

# Thanks for your attention