RIPE NCC

RIPE NETWORK COORDINATION CENTRE

Introduction to IPv6 - II

Building your IPv6 network

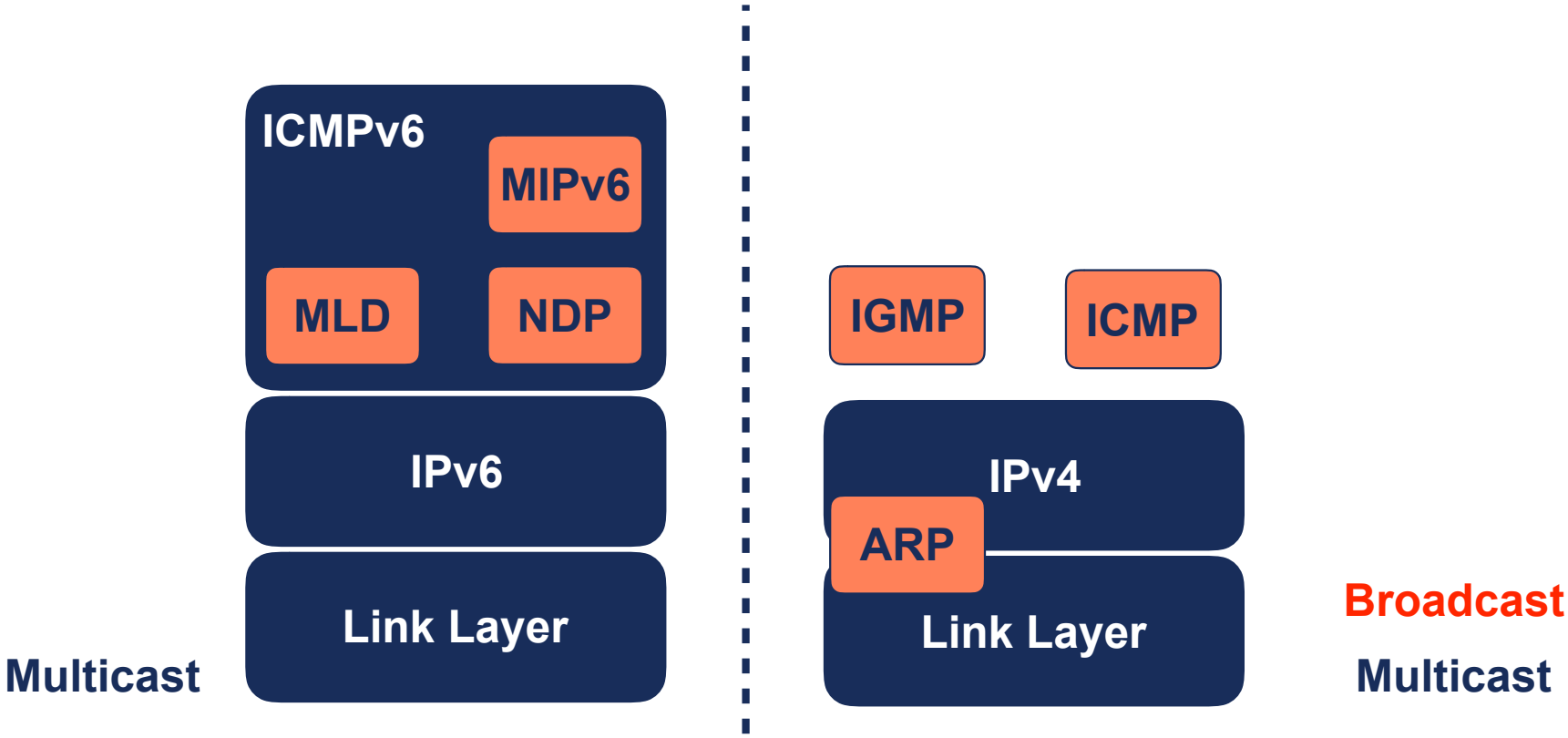
Alvaro Vives | 27 June 2017 | Workshop on Open Source Solutions for the IoT

Contents

- IPv6 Protocols and Autoconfiguration
  - ICMPv6
  - Path MTU Discovery (PMTU-D)
  - NDP
  - Autoconfiguration: DHCPv6 vs. SLAAC
- Use of IP on WSN/IoT
- Connecting our IPv6 Network to the Internet

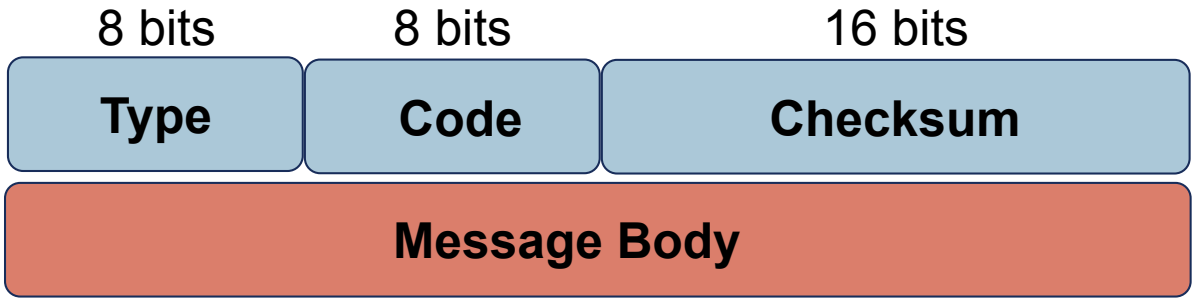
IPv6 Protocols: ICMPv6 (1)

- ICMPv6 fundamental part of IPv6



IPv6 Protocols: ICMPv6 (2)

- It's used for several things, both:
  - Locally on the LAN: **NDP, MLD**
  - On the Internet: Fragmentation, detect other errors
- You should be careful when filtering
- Two type of messages:
  - **Error**: Destination unreachable, packet too big, time exceeded, parameter problem (type = 0 … 127)
  - **Informative**: echo request, echo reply (type = 128 … 255)



IPv6 Protocols: ICMPv6 (3)

ICMPv6 **Error** Messages

- **Destination Unreachable** (type = 1, parameter = 0)
  - No route to destination (code = 0)
  - Communication with destination administratively prohibited (code = 1)
  - Beyond scope of source address (code = 2)
  - Address Unreachable (code = 3)
  - Port Unreachable (code = 4)
  - Source address failed ingress/egress policy (code = 5)
  - Reject route to destination (code = 6)
- **Packet Too Big** (type = 2, code = 0, parameter = next hop MTU)
- **Time Exceeded** (type = 3, parameter = 0)
  - Hop Limit Exceeded in Transit (code = 0)
  - Fragment Reassembly Time Exceeded (code = 1)
- **Parameter Problem** (type = 4, parameter = offset to error)
  - Erroneous Header Field (code = 0)
  - Unrecognised Next Header Type (code = 1)
  - Unrecognised IPv6 Option (code = 2)

Path MTU Discovery (1)

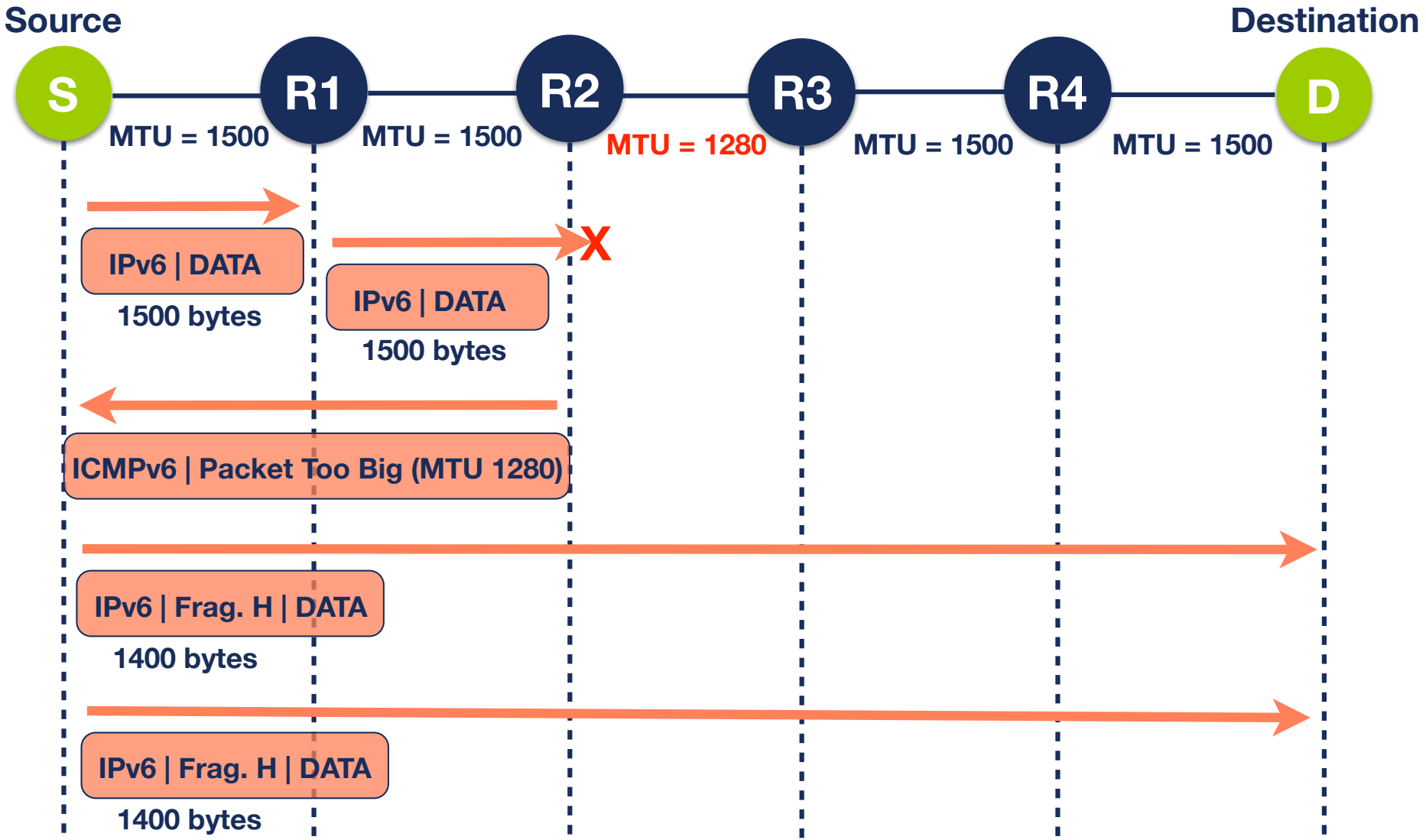
- MTU: Maximum Transmission Units
  - **Link MTU**: maximum number of bytes of IP packet
  - **Path MTU**: minimum link MTU from source to destination
- In IPv6 the minimum link MTU is 1280 bytes (v4 68 bytes)
- In IPv6 this is important because:
  - Fragmentation process changes: extension header
  - Encapsulation frequently used: overhead reduces available MTU

Path MTU Discovery (2)

- Path MTU Discovery sends packets bigger than 1280 bytes
  - For each destination, starts assuming MTU of first hop
  - If packet reaches a link MTU smaller than its size, ICMPv6 “packet too big” packet is sent to source, with info of link MTU (that MTU value is saved for that destination)
  - Eventually, saved MTU values are discarded to detect possible changes on the MTU values
- Constrained implementations: PMTU-D could be omitted, if detected that 1280 bytes packets could reach a destination

Path MTU Discovery (3)

- IPv6 fragmentation done in the source node



Autoconfiguration (1)

ICMPv6 **Informative** Messages

- Echo Request (type =128, code = 0)
- Echo Reply (type =129, code = 0)
- MLD (Multicast Listener Discovery) Messages:
  - Query, Report, Done (Like IGMP for IPv4)

- NDP Messages:
  - NS (Neighbor Solicitation)
  - NA (Neighbor Advertisement)
  - RS (Router Solicitation)
  - RA (Router Advertisement)
  - Redirect

Autoconfiguration (2)

- NDP: Neighbor Discovery Protocol
- Used for hosts-hosts and routers-hosts communication
- It offers several services on a LAN:
  - Discovery of routers, network prefixes, network parameters
  - Autoconfiguration
  - Address Resolution
  - DAD (Duplicate Address Detection)
  - NUD (Neighbor Unreachability Detection)
- It only uses 5 type of ICMPv6 packets:
  - NS, NA, RS, RA, Redirect

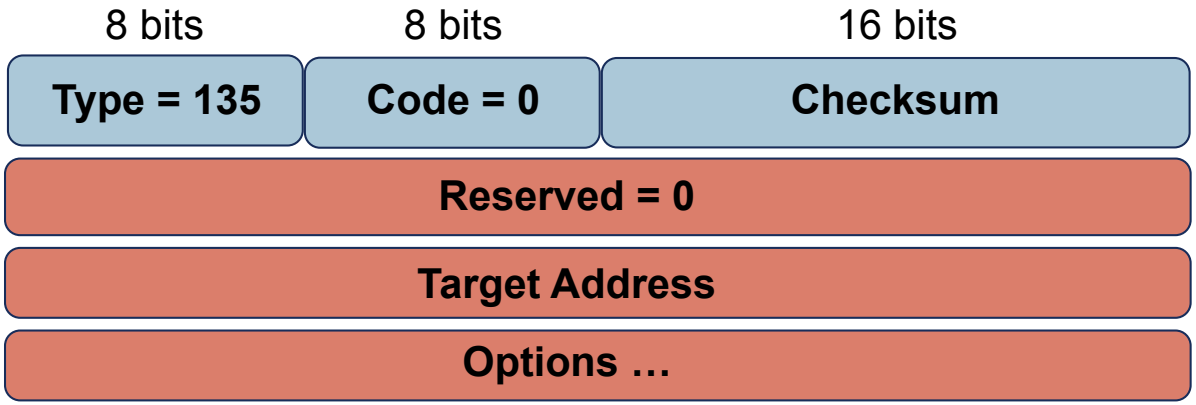
NS / NA

- A Host will send NS:
  1. To determine the MAC address associated with an IPv6 address: Dest. Addr. Multicast Solicited Node (Address Resolution = ARP IPv4)
  2. To check reachability: Dest. Addr. Unicast

- A Host will send NA:
  1. Answer to NS
  2. To quickly send new information (Unsolicited)

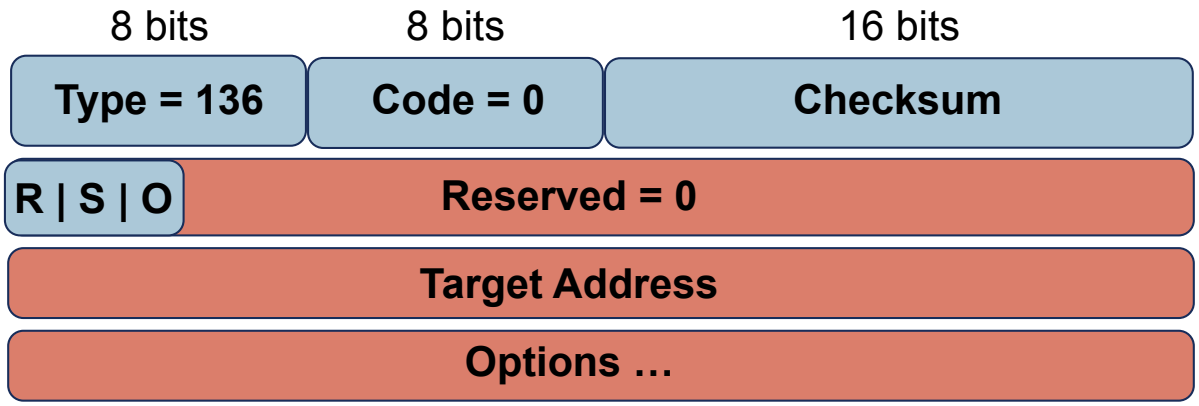
Neighbor Solicitation Format

- NS to determine MAC. Own MAC address is sent



- Target Address: IPv6 address that generated the request. Could not be a multicast address.
- Possible Options: Source Link-Layer Address

Neighbor Advertisement Format



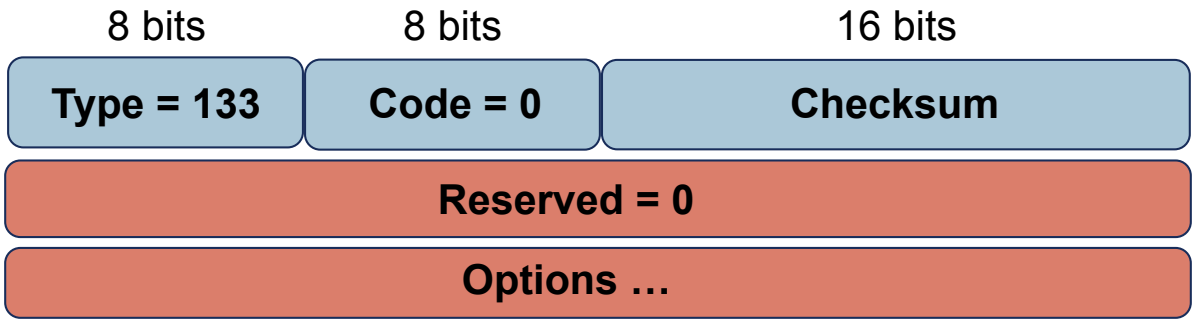
- Flags:
  - **R: Router Flag**=1 sending node is a router
  - **S: Solicited Flag**=1 sent as an answer to a NS
  - **O: Override Flag**=1 indicating caches should be updated
- Target Address (can't be a multicast address):
  - Solicited NAs = "Target Address" of NS
  - Unsolicited NA: IP address which MAC address has changed
- Possible Options: Target Link-Layer Address (MAC of Tx)

RS / RA

- A Host will send RS
  1. When bring up an interface: Dest. Addr = Well known multicast address of all routers

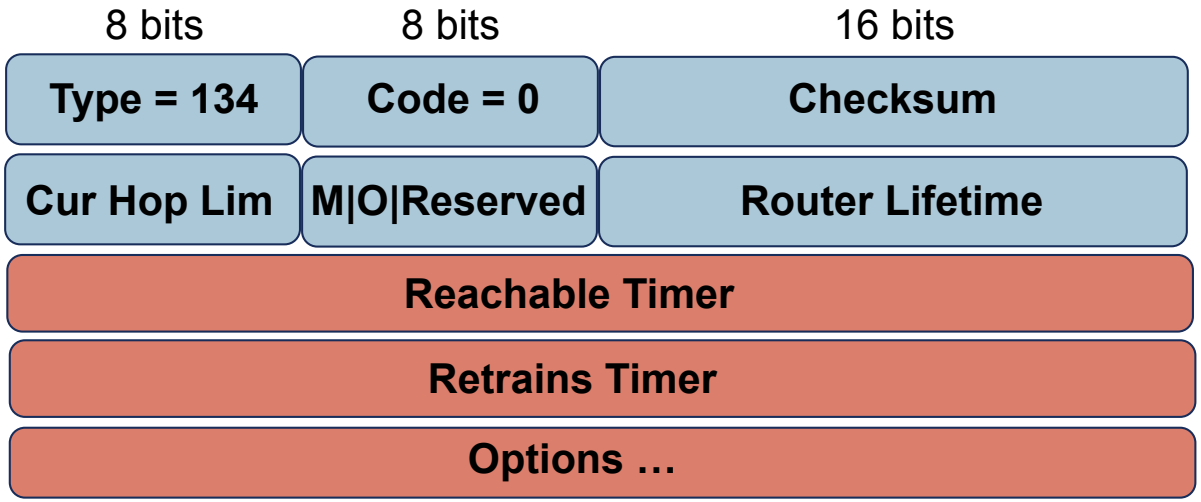
- A Router will send RA:
  1. As an answer to RS
  2. Periodically to inform about network parameters

Router Solicitation Format



- Possible Options: Source Link-Layer Address

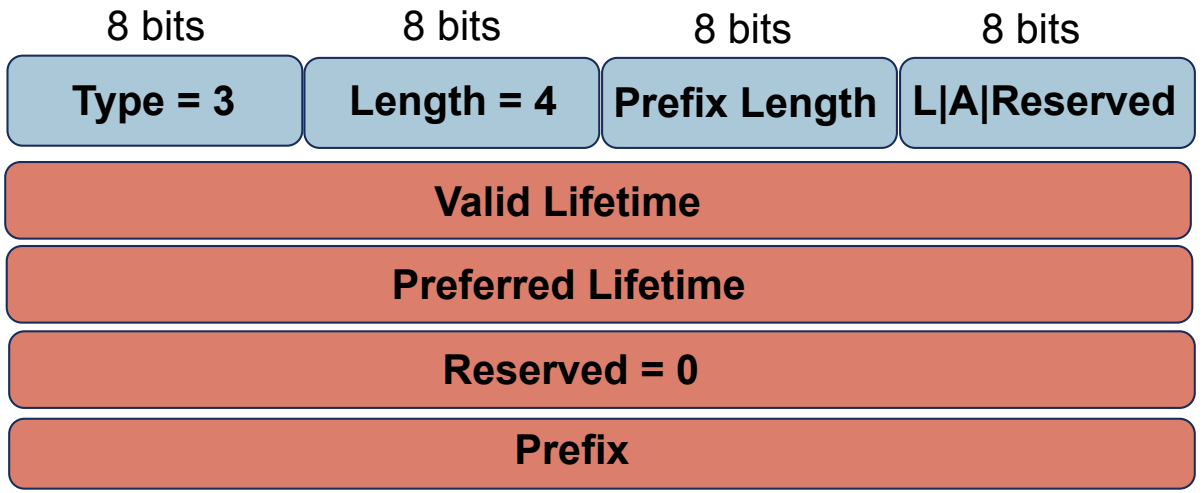
Router Advertisement Format (1)



- **Cur Hop Limit**: default value to be used as Hop Limit in IPv6 header for packets sent
- **M**: 1-bit "Managed address configuration" flag
- **O**: 1-bit "Other configuration" flag
- **Router Lifetime**: time the router could be used as default router
- **Reachable Time**: time node assumes a neighbour is reachable after having received a reachability confirmation (used in NUD)
- **Retrans Timer**: time (ms) between retransmitted NS (u in NUD, AR)
- **Possible Options**: Source LinkLayer Address, MTU, Prefix Information, RDNSS, Flags Expansion

Router Advertisement Format (2)

- Options: TLV (Type-Lenght-Value)
- Example: Prefix Information
  - **L**(1bit): **on-link flag**=1 indicates if prefix could be used for “on-link determination”
  - **A**(1bit): **autonomous address-configuration** flag=1 indicates if prefix could be used for stateless address autoconfiguration.
  - **Valid Lifetime**: Time in secs. Prefix is valid for on-link determination. Used for stateless address autoconfiguration as well.
  - **Preferred Lifetime**: Time in secs. that addresses generated with this prefix using SLAAC are in preferred state
  - **Prefix** (128 bits): IPv6 Address or prefix



Autoconfiguration (3)

- Autoconfiguration: automatically configure network parameters, not manually
- In IPv4 we only have DHCP
- In IPv6 there are more options

- Two scenarios: router or non-router
- Router:
  - Sends RAs -> M and O Flags -> four combinations
  - Hosts should look at M and O flags and then start to autoconfigure
  - M is about IPv6 address, O is about other parameters (DNS, etc.)
  - We have two “tools” SLAAC (0) and DHCPv6 (1)

Autoconfiguration (4)

- SLAAC vs. DHCPv6
- NOTE: Default gateway is learnt from the RA(s) (or manually)

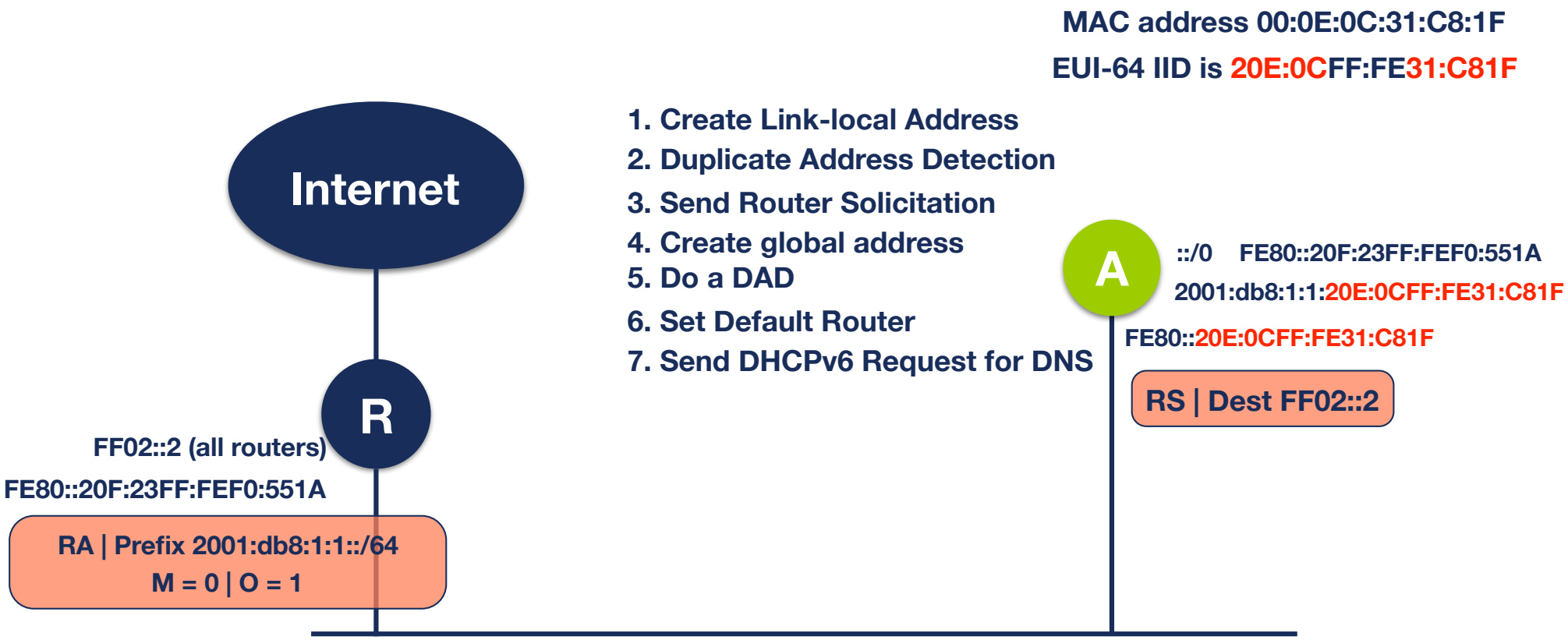
IP / Other	M	O	Comments
SLAAC / SLAAC	0	0	If dual-stack, could use IPv4 for DNS
SLAAC / DHCPv6	0	1	DHCPv6 Stateless
DHCPv6 / SLAAC	1	0	If dual-stack, could use IPv4 for DNS
DHCPv6 / DHCPv6	1	1	Gateway is learnt from RA

Autoconfiguration (5)

- Host A attaches to a network with a Router

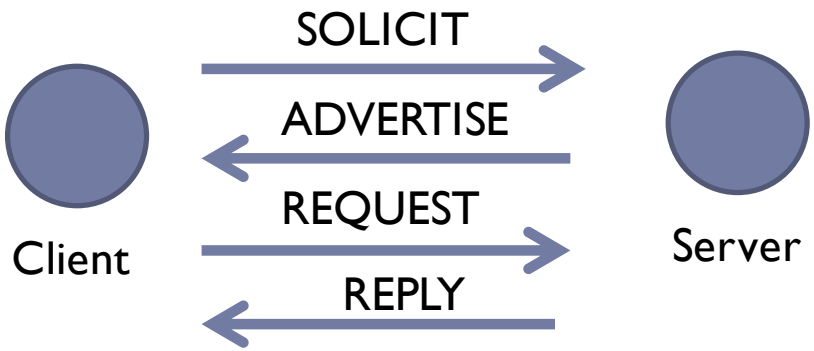
Autoconfiguration (6)

- In practice SLAAC for DNS is not yet available. Use IPv4 for DNS resolution (dual-stack) or DHCPv6 (O = 1)



DHCPv6 (1)

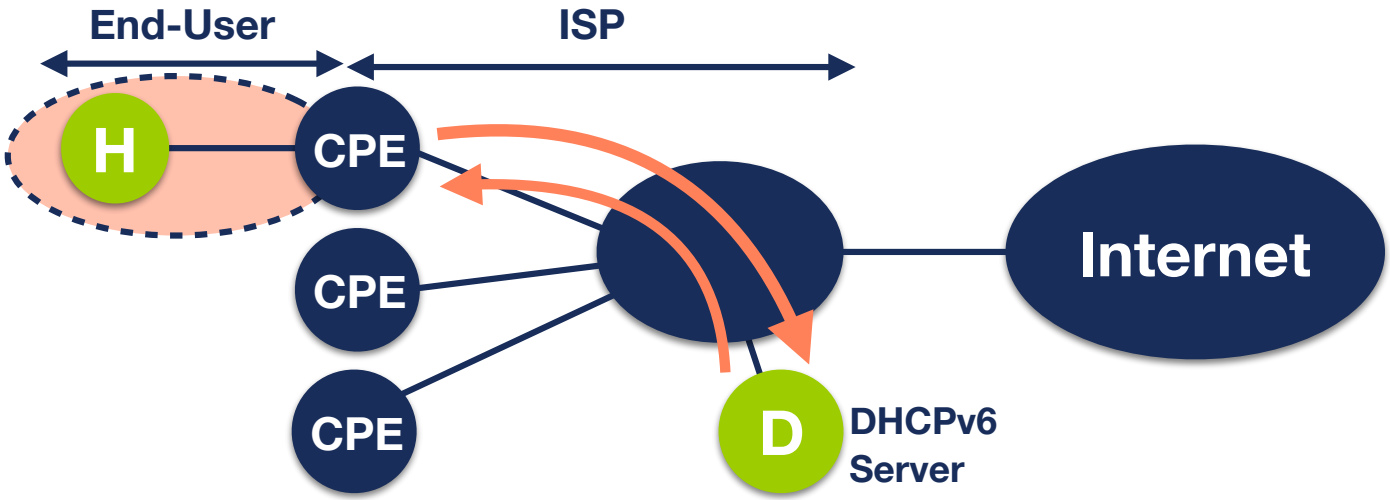
- DHCPv6 works as DHCPv4
  - Client-server
  - UDP
  - Use of relay



- DIFFERENCE: Does not provide default gateway
- Messages names change: SOLICIT, ADVERTISE, REQUEST,REPLY
- Servers/Relays listen on well-known multicast addresses (FF02::1:2)
- DHCPv6 stateless: only provides “other” info, not IP

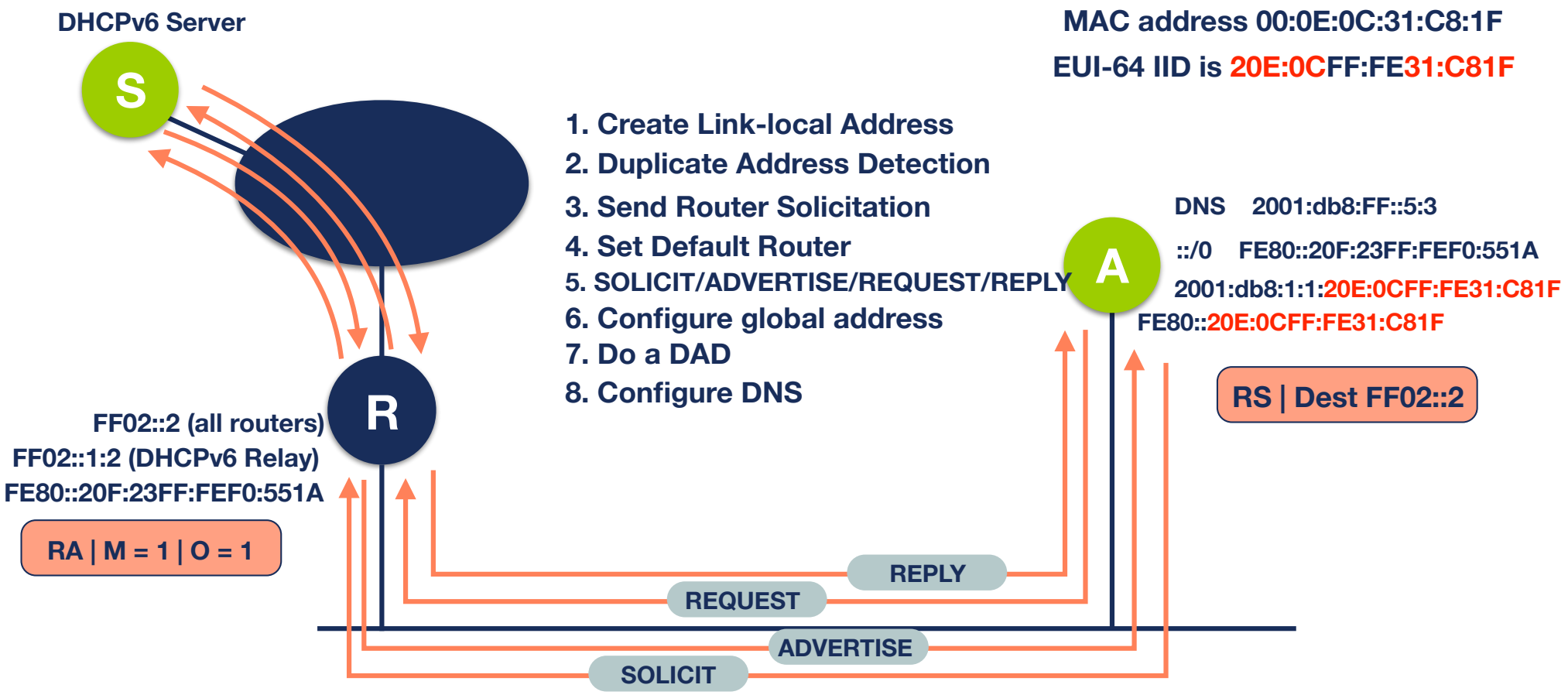
DHCPv6 (2)

- DHCPv6-PD (**Prefix Delegation**)
- In IPv6 no private IP + NAT. A GUA prefix is needed
- DHCPv6-PD allows scalable configuration of IPv6 prefixes in routers
- Same as for IP addresses: client-server, etc.
- Only changes the requested object: a prefix (IA-PD)
- Example: CPE connected to an ISP



DHCPv6 (3)

- Host A connected to network with Router and DHCPv6 relay
- M = O = 1



Use of IP on WSN/IoT (1)

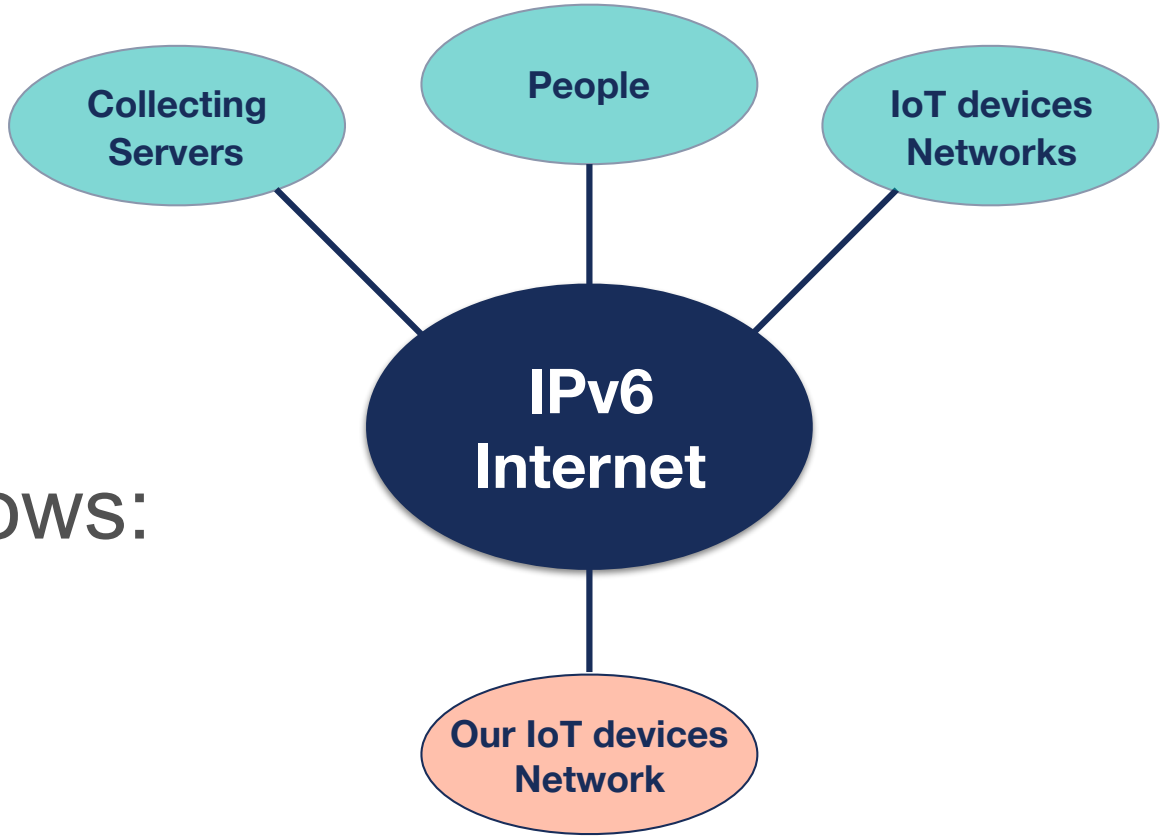
- IP has benefits for WSN/IoT:
  - Pervasive nature of IP allows use of existing infrastructure
  - IP-based technologies exist, are well-known, mature and widely available. Allowing easier and cheaper adoption, good interoperability and easier application layer development
  - Open/free specifications: easier understood by wider audience than proprietary solutions
  - Tools for IP networks already exist
  - IP devices can easily connect to IP networks. No need for protocol translation gateways or proxies

Use of IP on WSN/IoT (2)

- IPv6 in particular has benefits for WSN/IoT:
  - Gives huge amount of addresses
  - No (real) limit of hosts in a local link
  - Provides for easy network parameters autoconfiguration (SLAAC)
  - (Possible) end-to-end bi-directional communication
  - Could save battery:
    1. No NAT and keepalives
    2. No need to periodically pull information (PUSH model)

Connecting to IPv6 Internet (1)

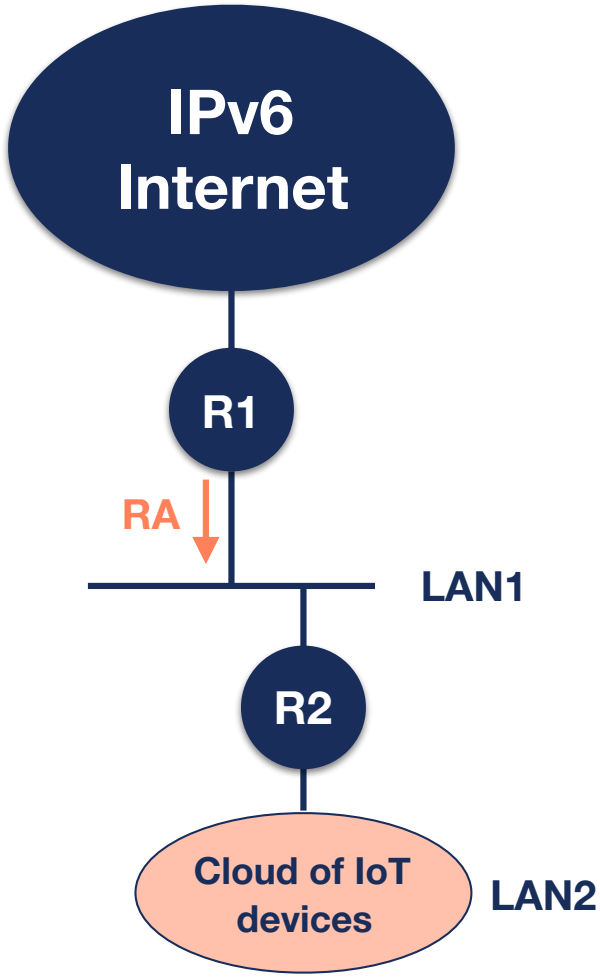
- Objective: Connect our network to the IPv6 Internet



- Bidirectional, allows:
  - Management
  - Control
  - Communication

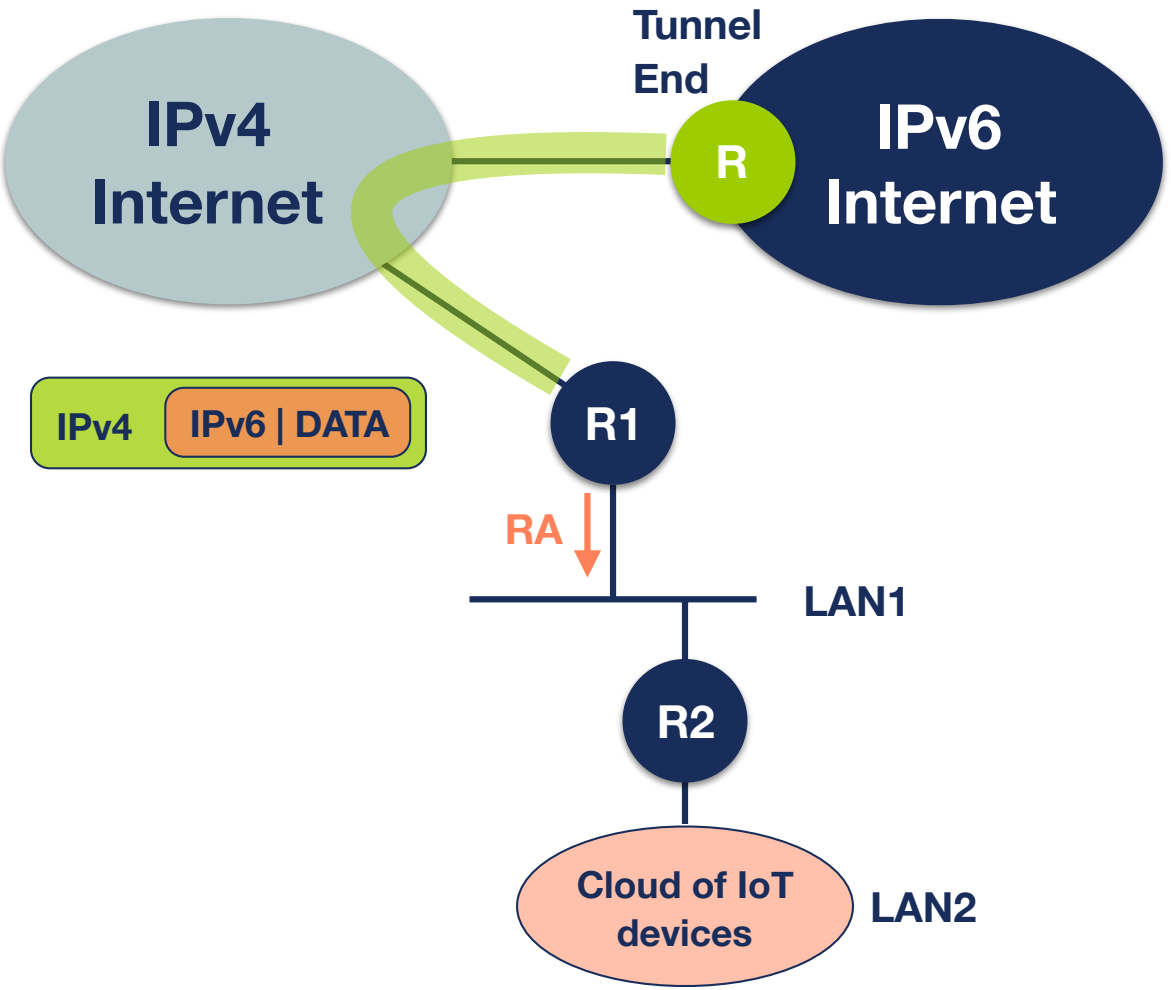
Connecting to IPv6 Internet (2)

- Scenario 1: Native IPv6 and IPv6 Router



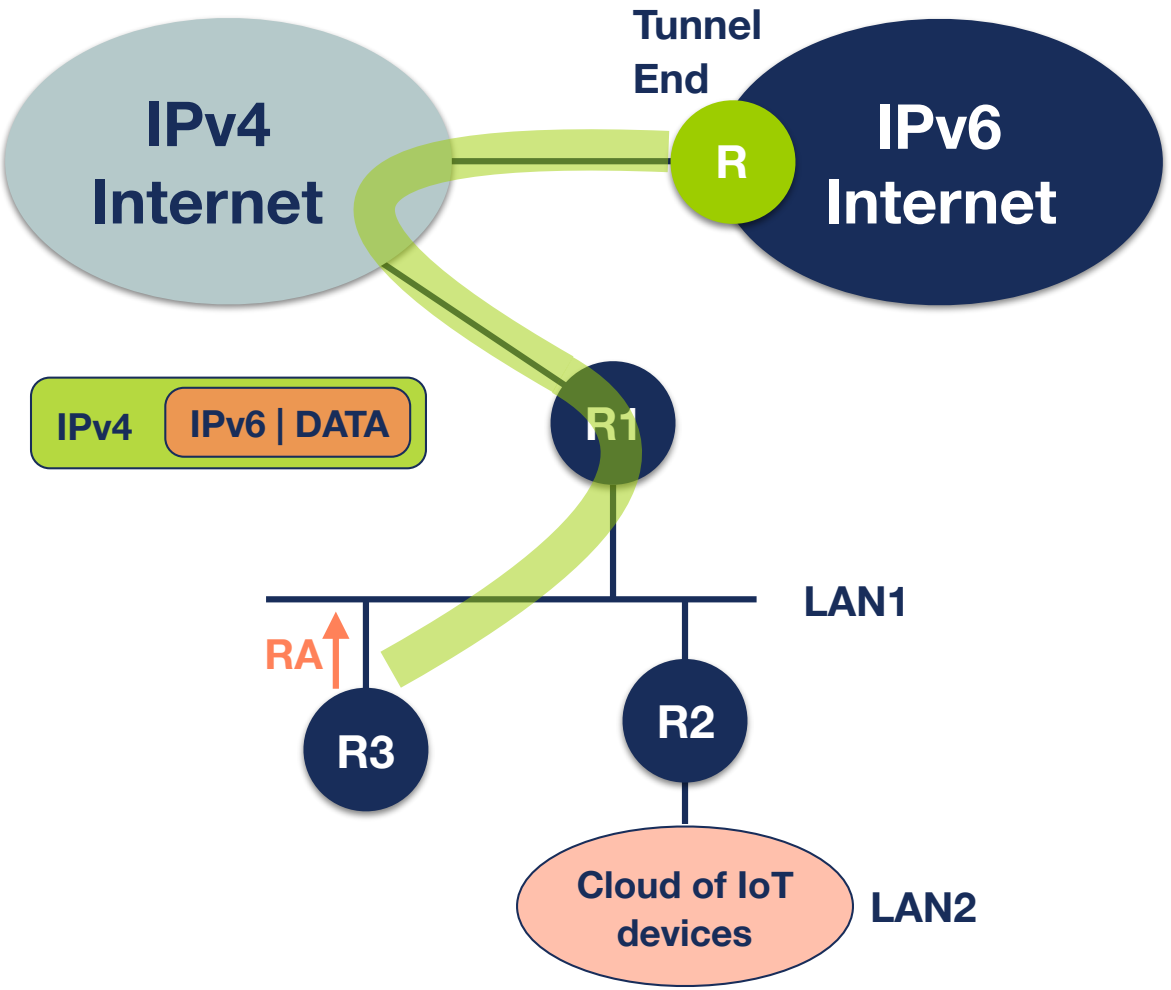
Connecting to IPv6 Internet (3)

- Scenario 2: Without native IPv6 and IPv6 Router



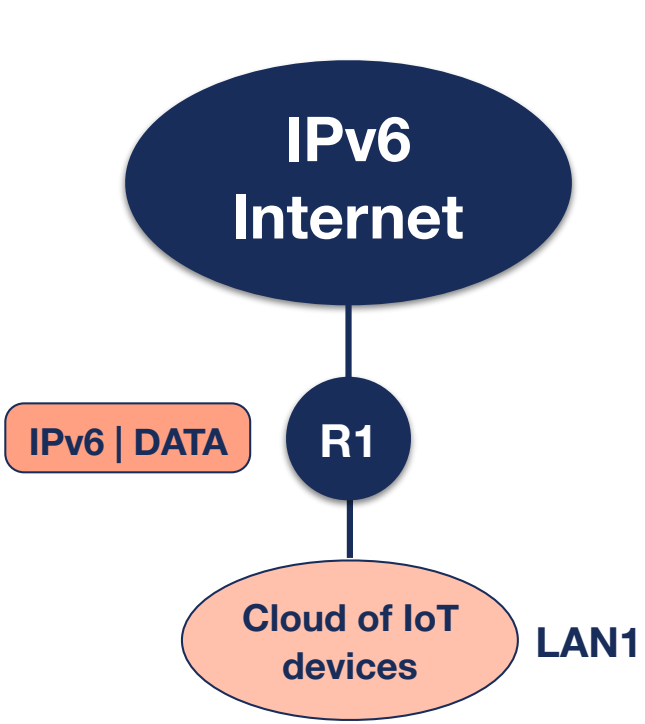
Connecting to IPv6 Internet (4)

- Scenario 3: Without native IPv6 or IPv6 Router

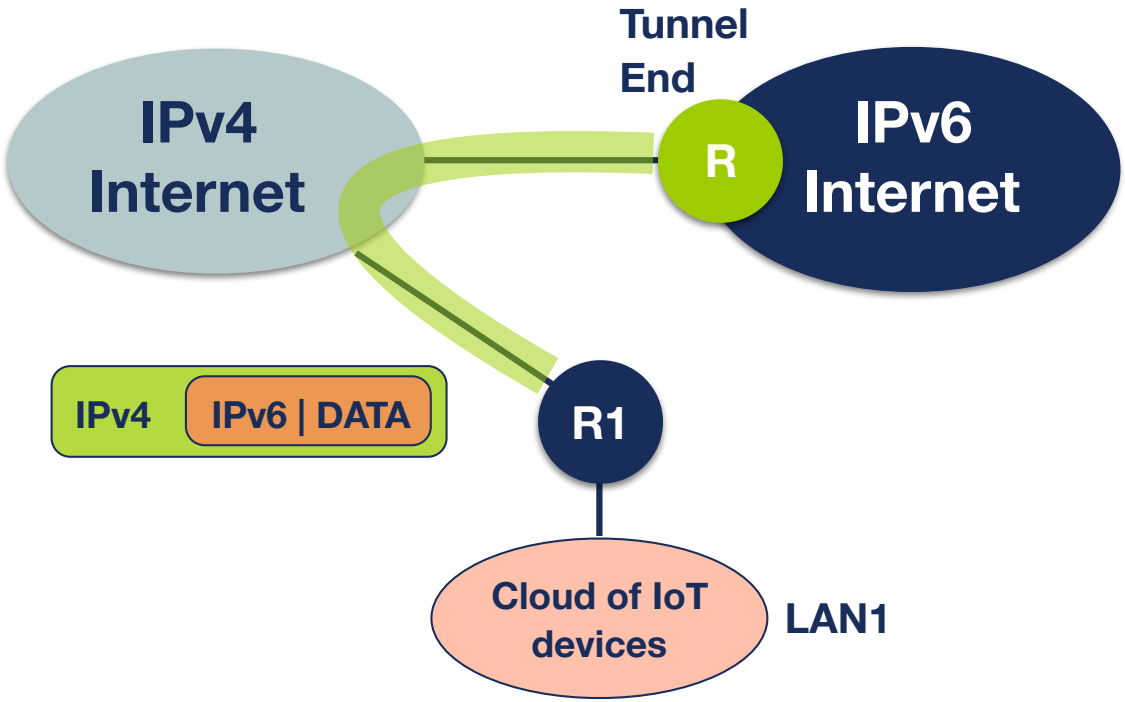


Connecting to IPv6 Internet (5)

- Simplified Scenarios



a) Native IPv6



b) Encapsulated IPv6

Questions

avives@ripe.net
@TrainingRIPENCC