RFC 6775 Extension

P.Thubert, E. Nordmark, S. Chakrabarti, C. Perkins

IETF 103

Bangkok

Unmet expectations

- Solicited node multicast requires highly scalable L2 multicast
  - IEEE does not provide it => turns everything into broadcast
  - IPv6 ND appears to work with broadcast on 802.1 fabrics up to some scale ~10K nodes
- IPv6 ND requires reliable and cheap broadcast
  - Radios do not provide that => conserving 802.1 properties over wireless is illusory
  - RFC 4862 cannot operate as designed on wireless
  - Address uniqueness is an unguaranteed side effect of entropy
- 802.11 expects proxy operation and broadcast domain separation
  - 802.11 provides a registration and proxy bridging at L2
  - Requires the same at L3, which does not exist
  - Implementations provide proprietary techniques based on snooping => widely imperfect

⇒ RFC 6775 solves the problem for DAD in one LL

⇒ This update enable establishing proxy services directly (ND for now), over a LLN, across multiple LLNs

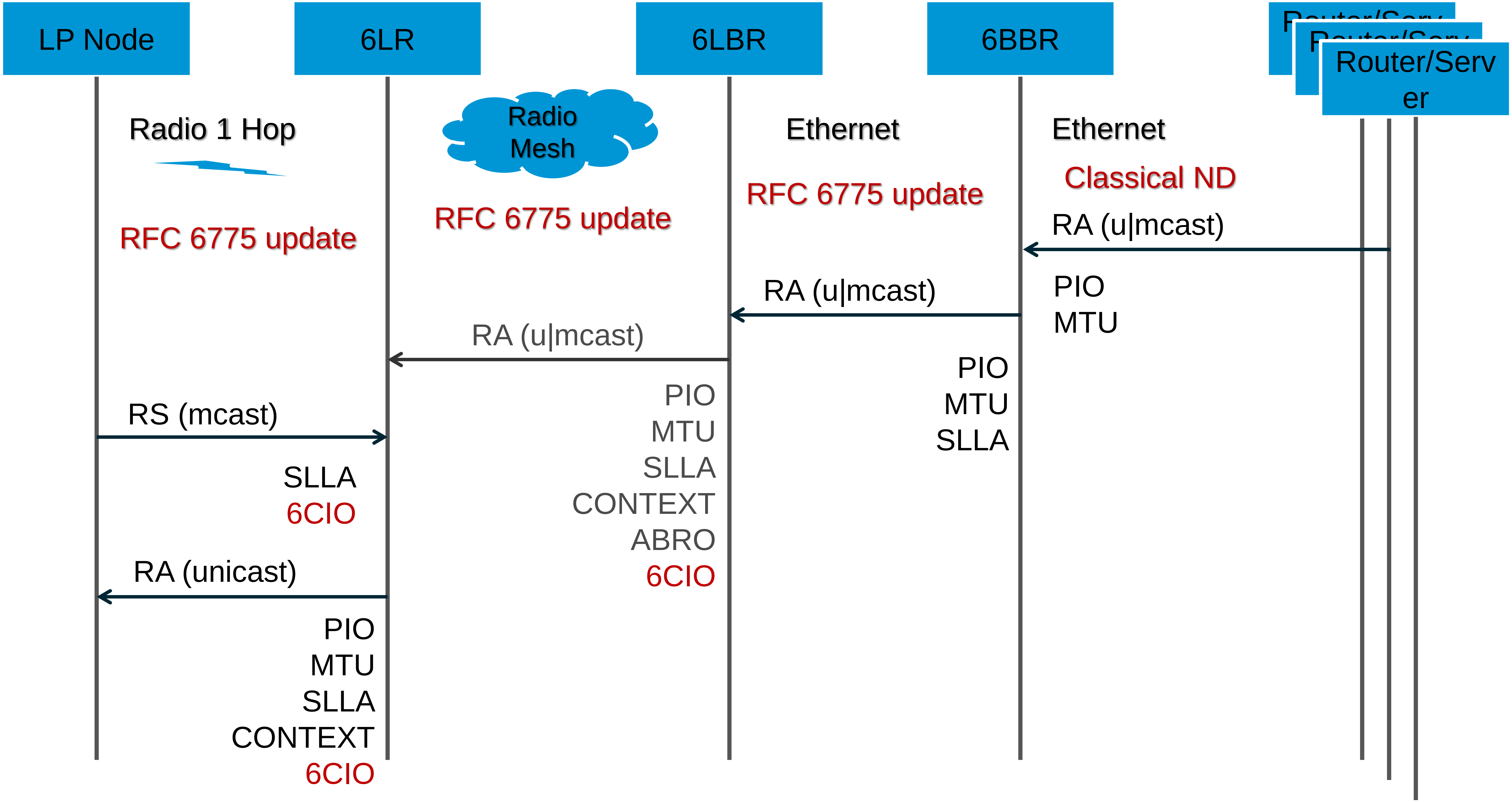
What are the 6LoWPAN ND extensions?

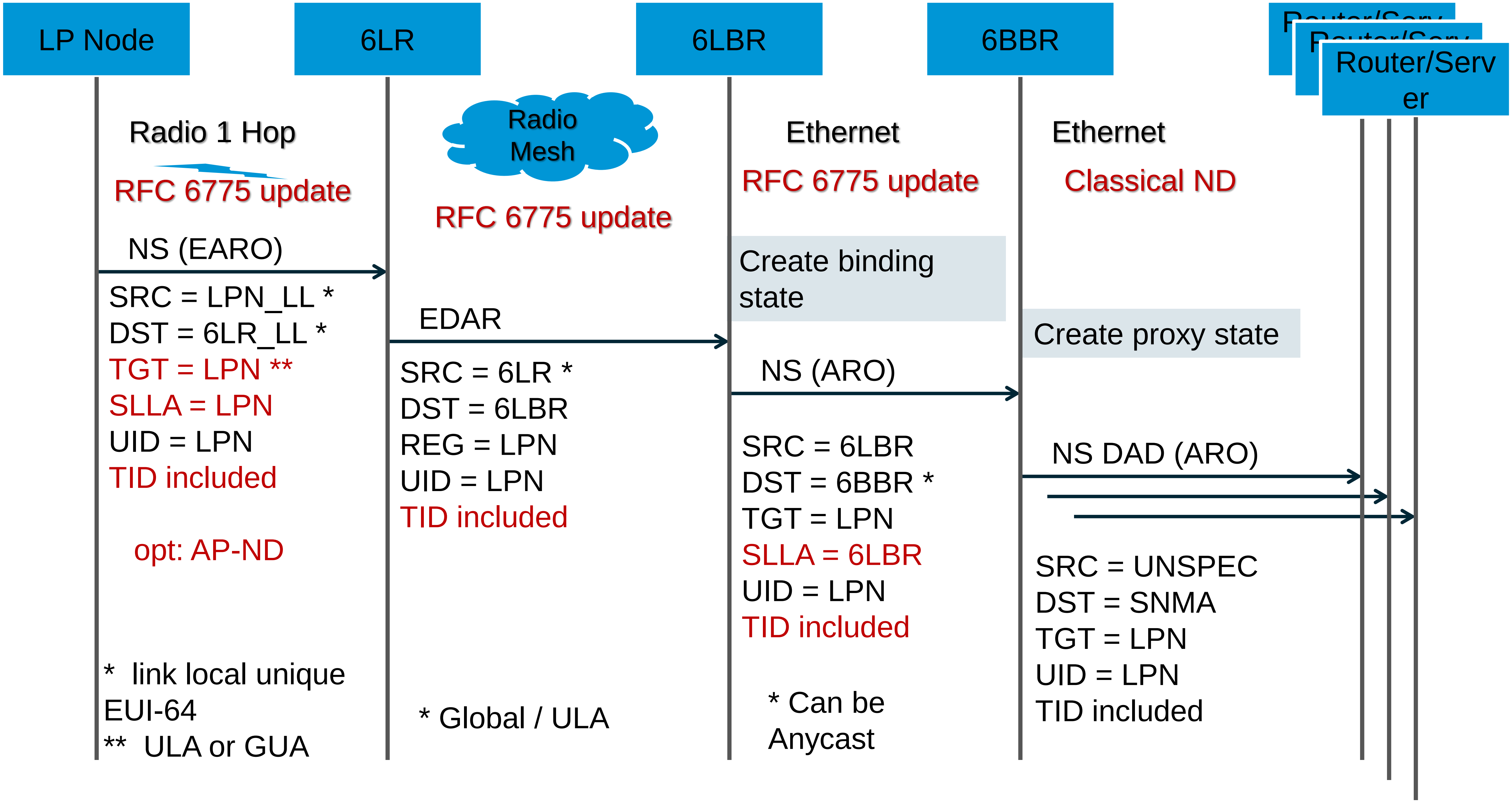
Provide for draft-thubert-6lo-rfc6775-update-reqs

- draft-ietf-6lo-rfc6775-update
  - Simplifies the protocol (no DAR/DAC for LL, no secondary NC)
  - Enables proxy registration
- draft-ietf-6lo-ap-nd
  - Protects addresses against theft (Crypto ID in registration)
- draft-ietf-6lo-backbone-router
  - Federates 6lo meshes over a high speed backbone
  - ND proxy that mimics 802.11 association but at Layer 3

RFC 6775 Update

P.Thubert, E. Nordmark, S. Chakrabarti, C. Perkins


LP Node
6LR
6LBR
6BBR
Router/Serv
Router/Serv
Router/Server
Radio 1 Hop
Radio Mesh
Ethernet
Ethernet
RFC 6775 update
RFC 6775 update
RFC 6775 update
Classical ND
RA (u|mcast)
PIO
MTU
RA (u|mcast)
PIO
MTU
SLLA
RA (u|mcast)
PIO
MTU
SLLA
CONTEXT
ABRO
6CIO
RS (mcast)
SLLA
6CIO
RA (unicast)
PIO
MTU
SLLA
CONTEXT
6CIO



LP Node

6LR

6LBR

6BBR

Router/Serv
er

Radio 1 Hop

RFC 6775 update

NS (EARO)

SRC = LPN_LL *
DST = 6LR_LL *
TGT = LPN **
SLLA = LPN
UID = LPN
TID included

opt: AP-ND

* link local unique
EUI-64
** ULA or GUA

Radio
Mesh

RFC 6775 update

EDAR

SRC = 6LR *
DST = 6LBR
REG = LPN
UID = LPN
TID included

* Global / ULA

Ethernet

RFC 6775 update

Create binding
state

NS (ARO)

SRC = 6LBR
DST = 6BBR *
TGT = LPN
SLLA = 6LBR
UID = LPN
TID included

* Can be
Anycast

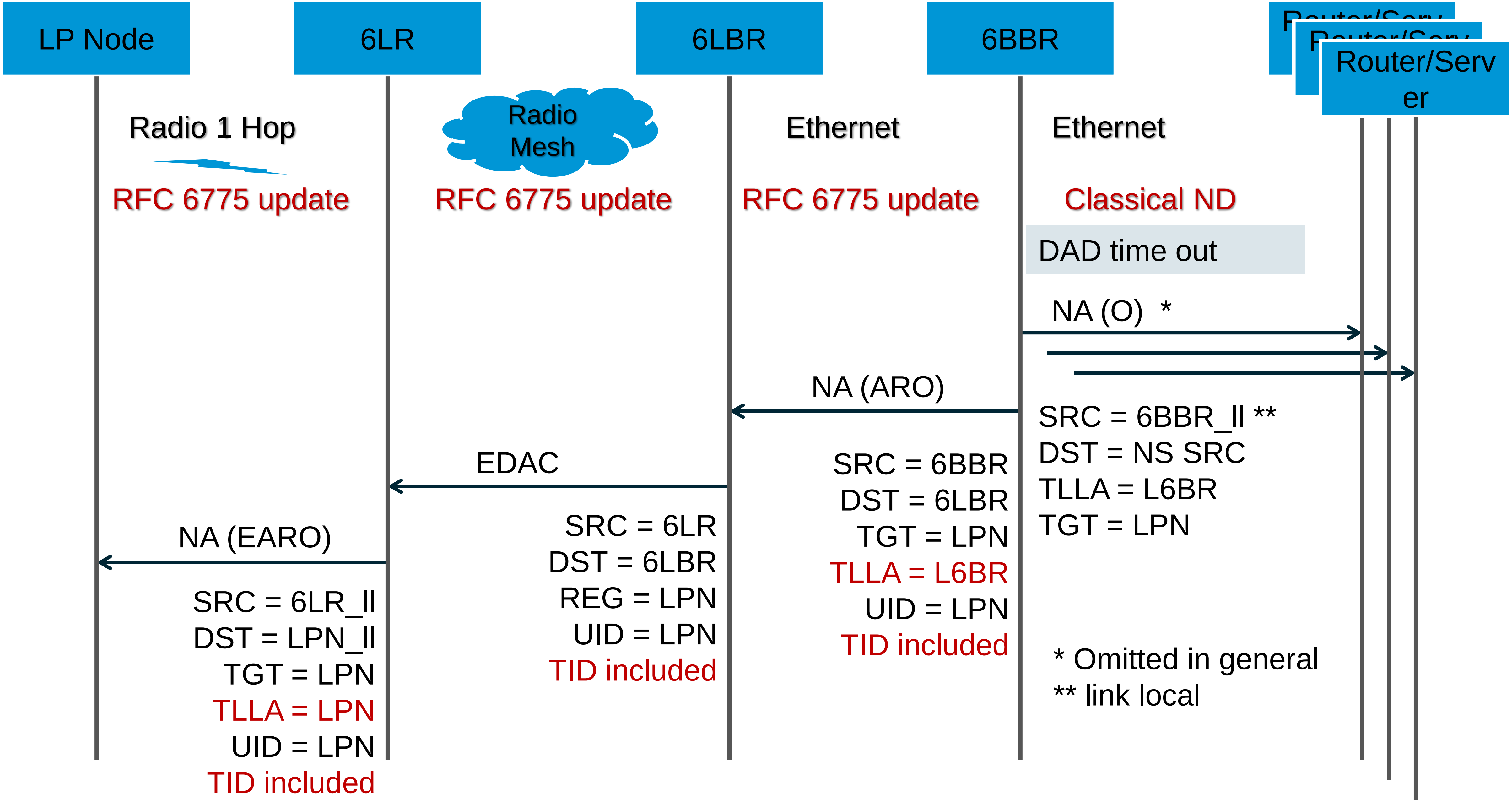
Ethernet

Classical ND

Create proxy state

NS DAD (ARO)

SRC = UNSPEC
DST = SNMA
TGT = LPN
UID = LPN
TID included



LP Node

6LR

6LBR

6BBR

Router/Serv
Router/Serv
Router/Serv
er

Radio 1 Hop

Radio
Mesh

Ethernet

Ethernet

RFC 6775 update

RFC 6775 update

RFC 6775 update

Classical ND

DAD time out

NA (O) *

NA (ARO)

SRC = 6BBR_ll **
DST = NS SRC
TLLA = L6BR
TGT = LPN

EDAC

SRC = 6BBR
DST = 6LBR
TGT = LPN
TLLA = L6BR
UID = LPN
TID included

NA (EARO)

SRC = 6LR
DST = 6LBR
REG = LPN
UID = LPN
TID included

SRC = 6LR_ll
DST = LPN_ll
TGT = LPN
TLLA = LPN
UID = LPN
TID included

* Omitted in general
** link local

Current status

RFC 6775 Update

Draft-….-21

Past IESG review (based on -21)

- IANA steps

  https://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xhtml#icmpv6-parameters-codes-type-157-code-suffix

- Done RFC Editor disambiguations

- RFC Editor state : RFC-EDITOR *

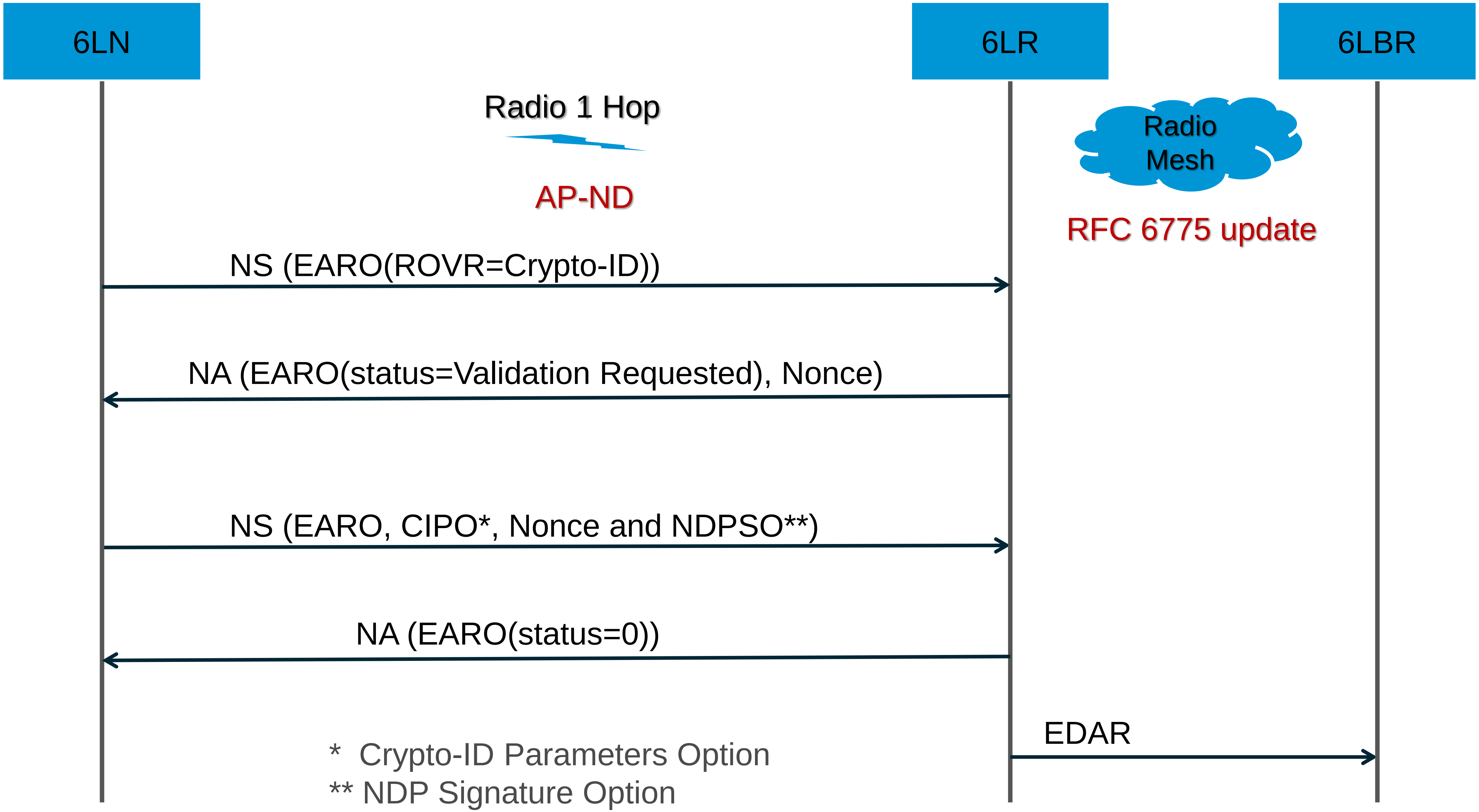
  * Awaiting final RFC Editor review before AUTH48

draft-ietf-6lo-ap-nd

P.Thubert, B. Sarikaya, M Sethi, R. Struik

Unmet expectations

- First come first Serve address registration
  - First registration for an address owns that address till it releases it
  - The network prevents hijacking
- Source address validation
  - Address must be topologically correct
  - Source of the packet owns the source address
- First Hop Security only?
  - Proxy ownership and routing advertisements not protected yet



6LN

6LR

6LBR

Radio 1 Hop

AP-ND

Radio Mesh

RFC 6775 update

NS (EARO(ROVR=Crypto-ID))

NA (EARO(status=Validation Requested), Nonce)

NS (EARO, CIPO*, Nonce and NDPSO**)

NA (EARO(status=0))

EDAR

* Crypto-ID Parameters Option
** NDP Signature Option

Recent changes

- Published -08
- René Struik joined as contributing author
- Updated the computation of the Crypto-ID
  - Crypto-Id in EARO is a truncated hash of the node's public-key
  - Digital signature (SHA-256/NIST P-256 or SHA-512/EdDSA) in NDPSO is executed on additional material (nonces, etc…, see updated section 6.2) for proof of ownership of the private key
  - Uses both nonces from the 6LN and 6LR
- Removed SHA-256 for EdCSA to comply with RFC 8032.

Security properties

- We made the size of the ROVR tunable so we can get high security. 64 bits seems inappropriate.
- At the moment a joining 6LN is challenged from the 6LR

  The 6LBR MUST trust the 6LR

  A rogue 6LR may pretend that it represents a 6LN that passed the challenge

  Should we challenge all the way from the 6LBR?

  Can the Crypto-ID be used in routing protocols, how?

Questions to the group

- Should we RECOMMEND larger than 64 bits ROVR?
- Should we allow RFC 8032 divergence for SHA 256?

  This allows smaller foot print in an implementation that does both

  Shall we face resistance?
- What’s missing before WGLC?

draft-ietf-6lo-backbone-router

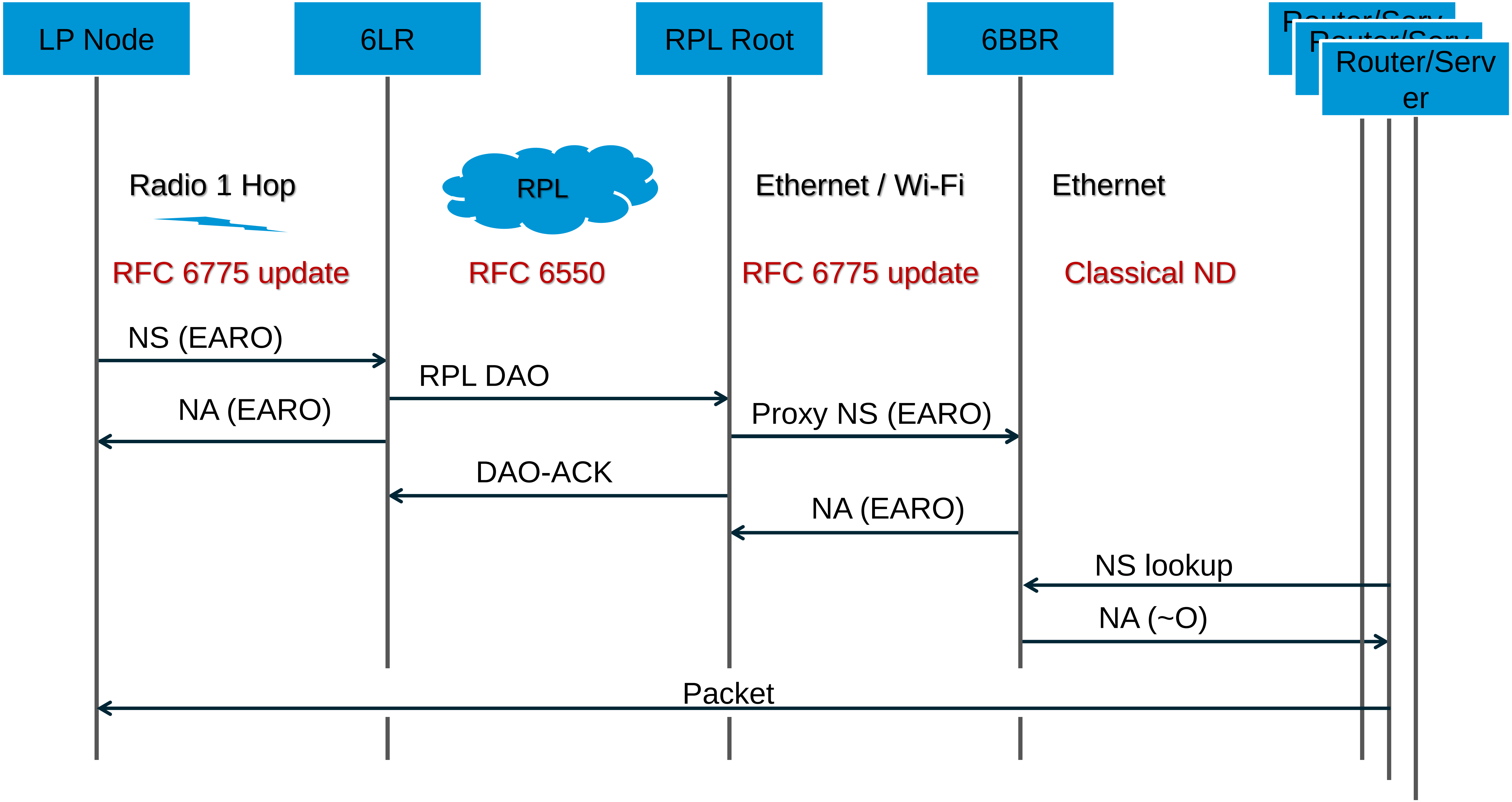
P.Thubert

Unmet expectations

- Scale an IOT subnet to the tens of thousands
  - With device mobility (no renumbering)
  - Controlled Latency and higher Reliability using a backbone
- Deterministic Address presence
  - Route towards the latest location of an address
  - Remove stale addresses

Recent changes

- Published -08
- Charlie Perkins joined as contributing author
- Clean up and reorg by Charlie
- Readable, ready for WGLC



LP Node

6LR

RPL Root

6BBR

Router/Server

Radio 1 Hop

RPL

Ethernet / Wi-Fi

Ethernet

RFC 6775 update

RFC 6550

RFC 6775 update

Classical ND

NS (EARO)

RPL DAO

NA (EARO)

Proxy NS (EARO)

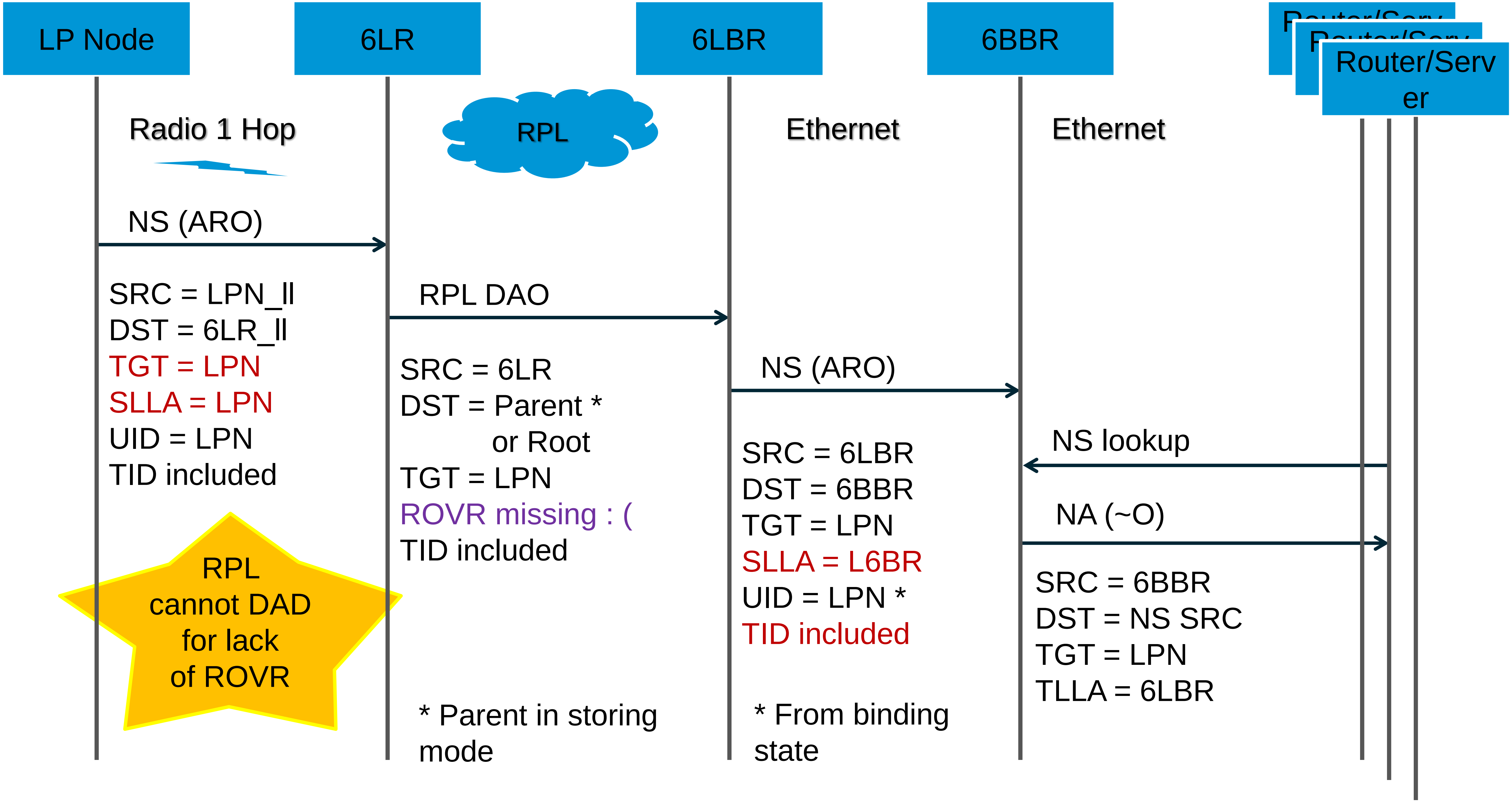
DAO-ACK

NA (EARO)

NS lookup

NA (~O)

Packet



LP Node

6LR

6LBR

6BBR

Router/Server

Radio 1 Hop

RPL

Ethernet

Ethernet

NS (ARO)

SRC = LPN_ll
DST = 6LR_ll
TGT = LPN
SLLA = LPN
UID = LPN
TID included

RPL cannot DAD for lack of ROVR

RPL DAO

SRC = 6LR
DST = Parent *
or Root
TGT = LPN
ROVR missing : (
TID included

* Parent in storing mode

NS (ARO)

SRC = 6LBR
DST = 6BBR
TGT = LPN
SLLA = L6BR
UID = LPN *
TID included

* From binding state

NS lookup

NA (~O)

SRC = 6BBR
DST = NS SRC
TGT = LPN
TLLA = 6LBR

6BBR Status

- Quite Stable, no recent change
- WGLC is needed to make final progress