RFC 6775 Extension

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

IETF 101

London

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

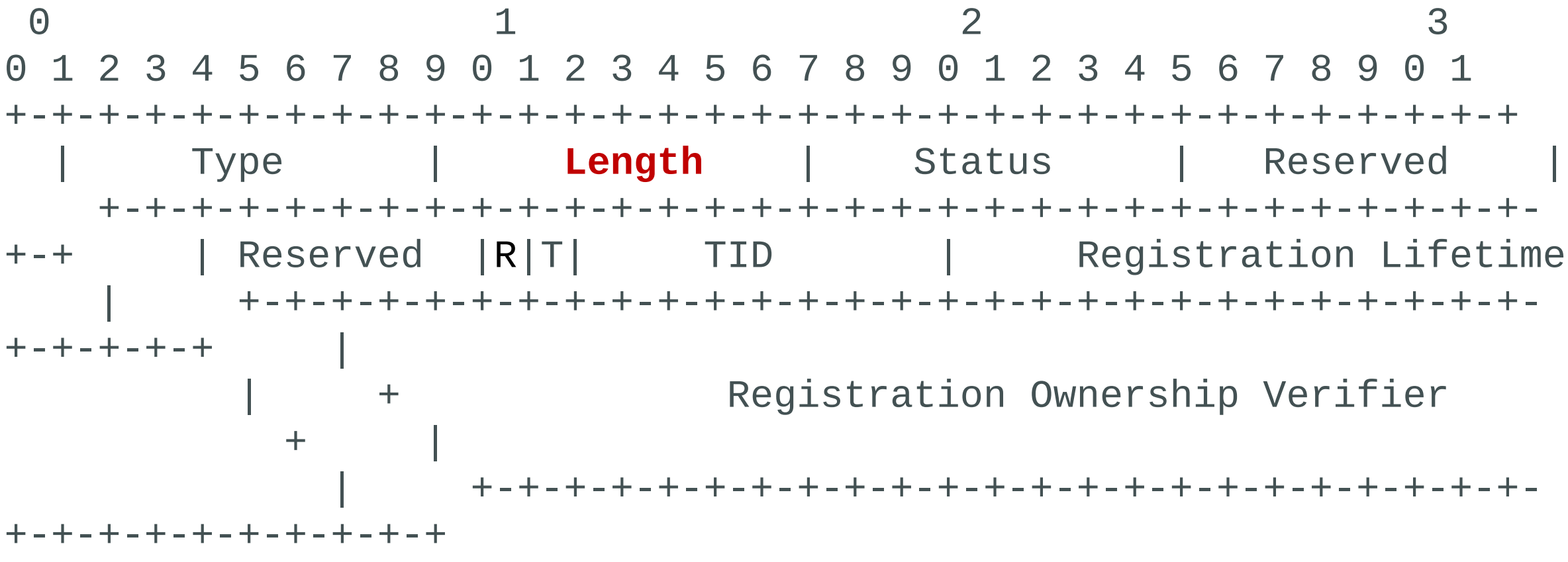
RFC 6775 Update

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

What are the 6LoWPAN ND extensions?

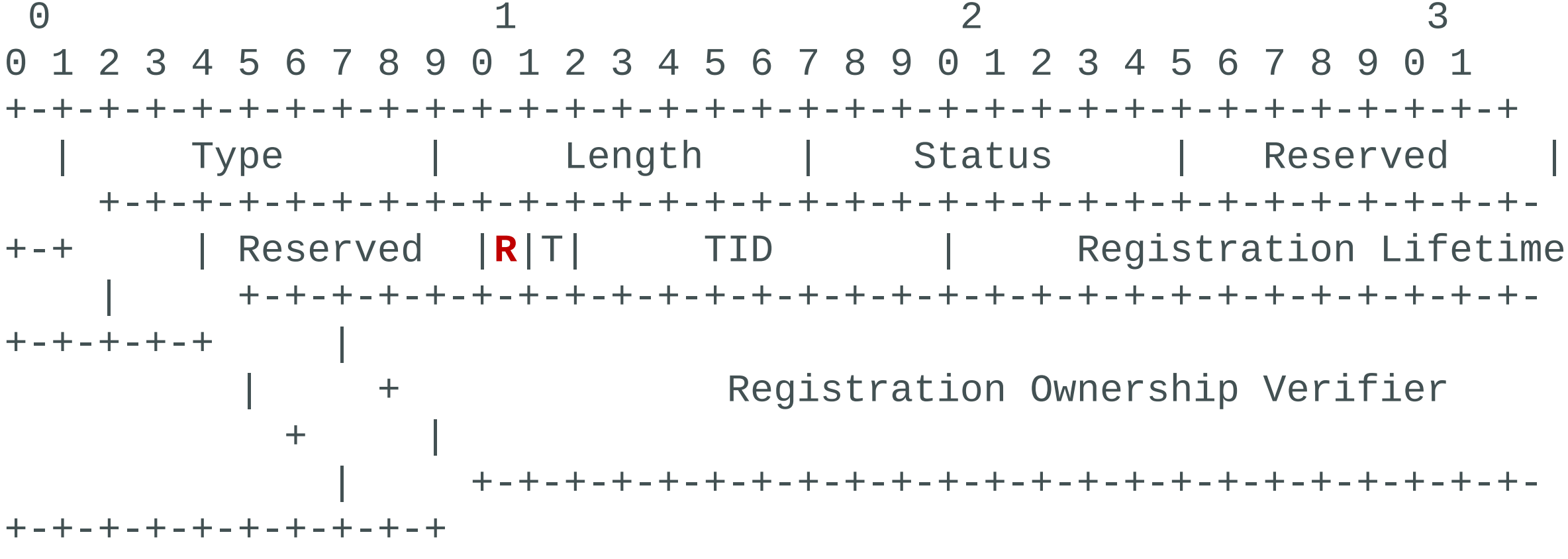
- draft-ietf-6lo-rfc6775-update
  - Simplifies the protocol (no DAR/DAC for LL, no secondary NC)
  - Enables proxy registration
- draft-ietf-6lo-ap-nd
  - Protects addresses against theft (Crypto ID in registration)
- draft-ietf-6lo-backbone-router
  - Federates 6lo meshes over a high speed backbone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

RFC 6775 update new features: the Length



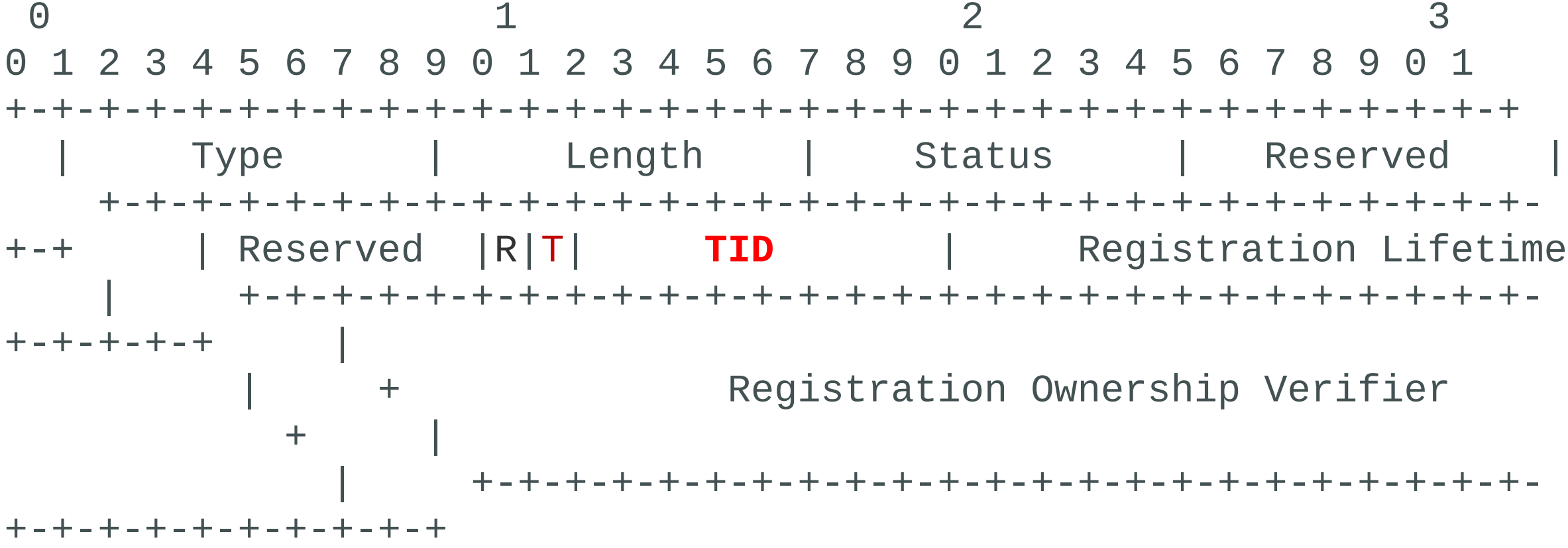
Length: 8-bit unsigned integer. The length of the option in units of 8 bytes. **It MUST be 2 when operating in backward-compatible mode**. It MAY be 3, 4 or 5, denoting a **ROVR size of 128, 192 and 256 bits respectively**.

RFC 6775 update new features: the ‘R’ flag



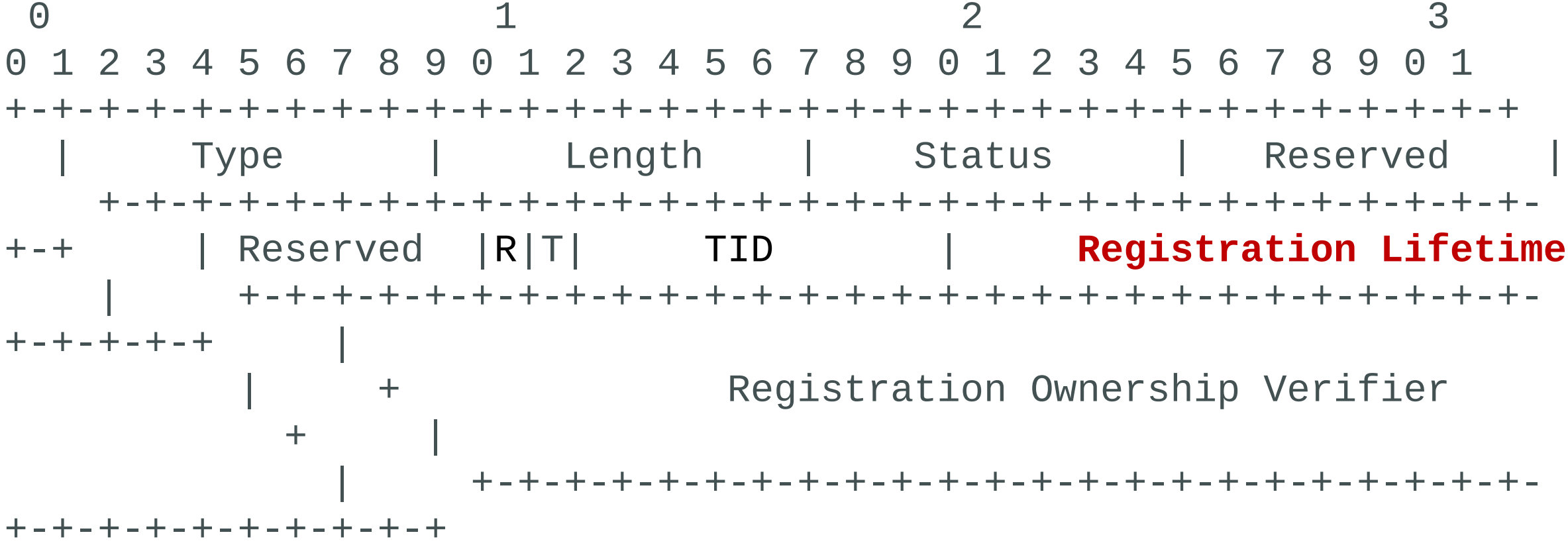
R: One-bit flag. If the 'R' flag is **set**, the registering node expects that **the 6LR ensures reachability for the registered address**, e.g., by injecting the address in a Route-Over routing protocol or proxying ND over a Backbone Link.

RFC 6775 update new features: the Transaction ID



4.2.1. Comparing TID values: **The TID is a sequence counter and its operation is the exact match of the path sequence specified in RPL**, the IPv6 Routing Protocol for Low-Power and Lossy Networks [RFC6550] specification.

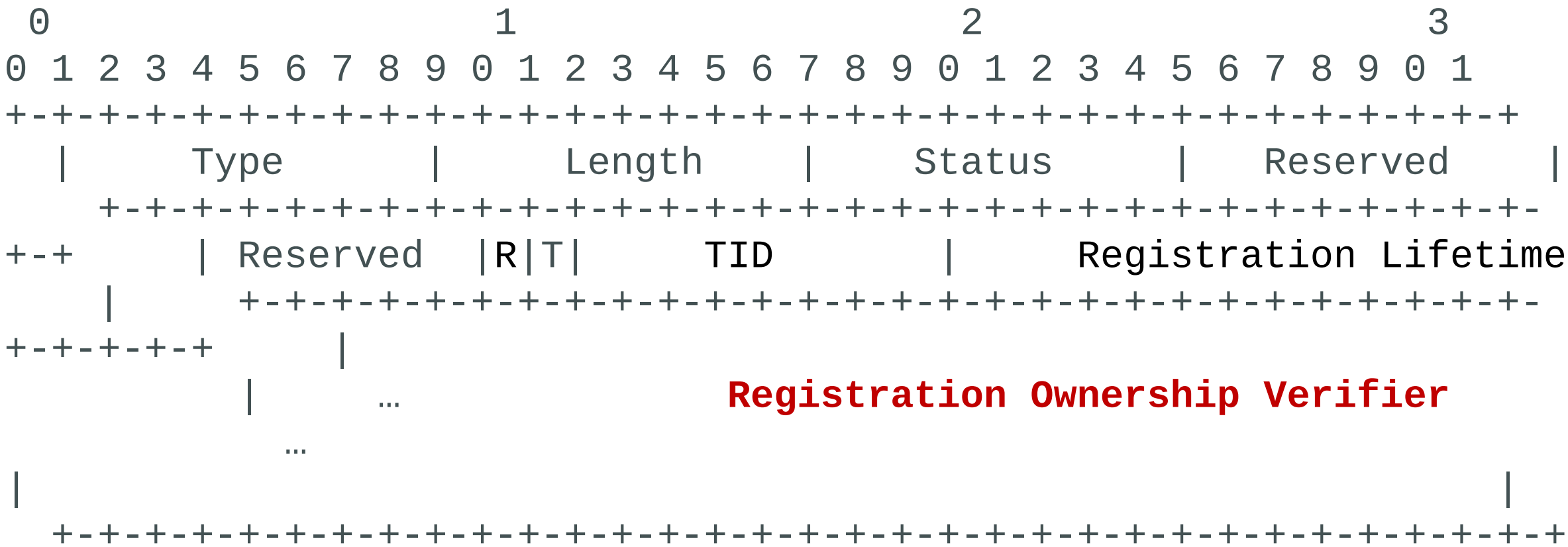
RFC 6775 update new features: Registration Lifetime



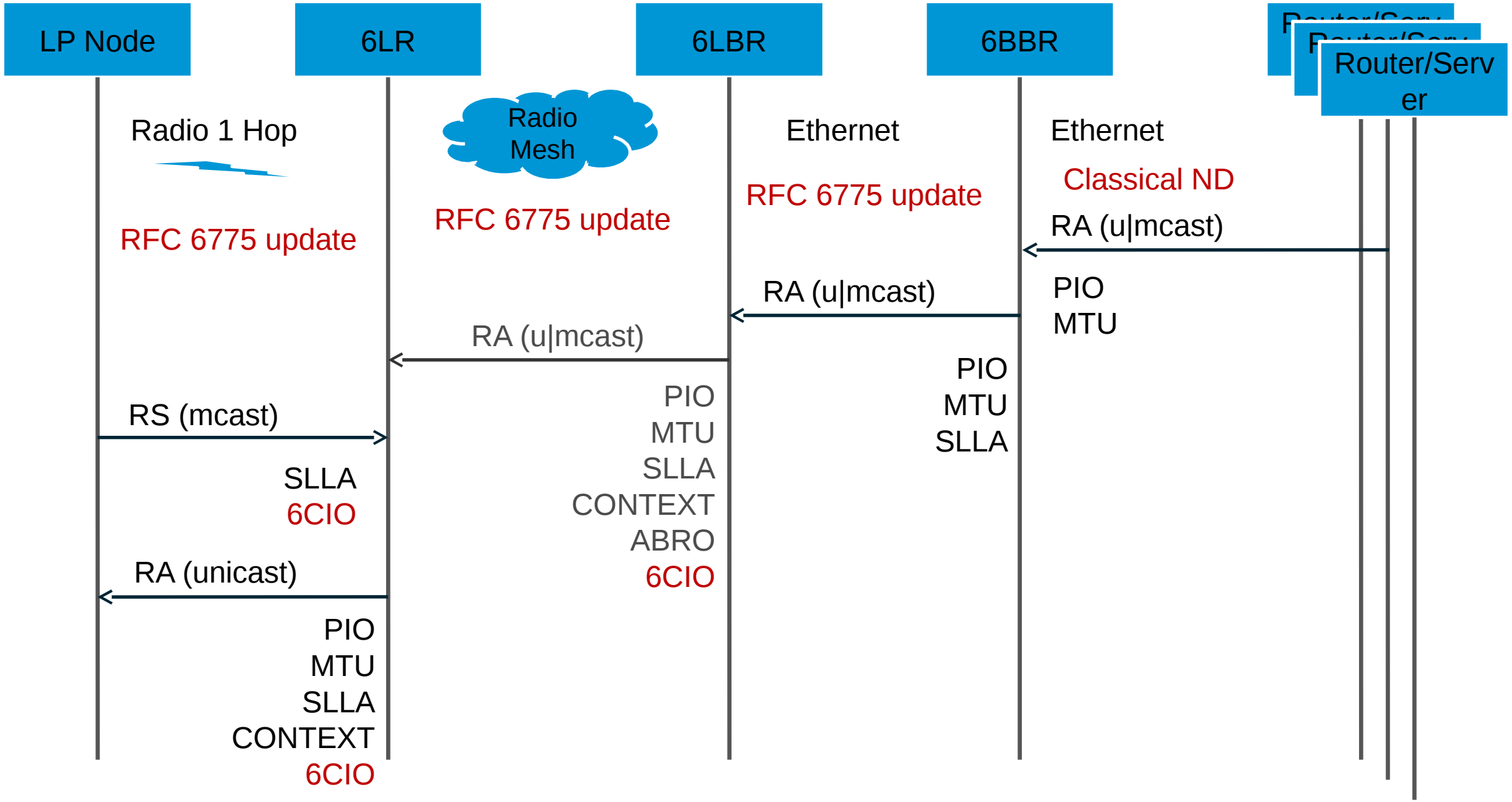
Registration Lifetime: 16-bit integer; expressed in minutes.

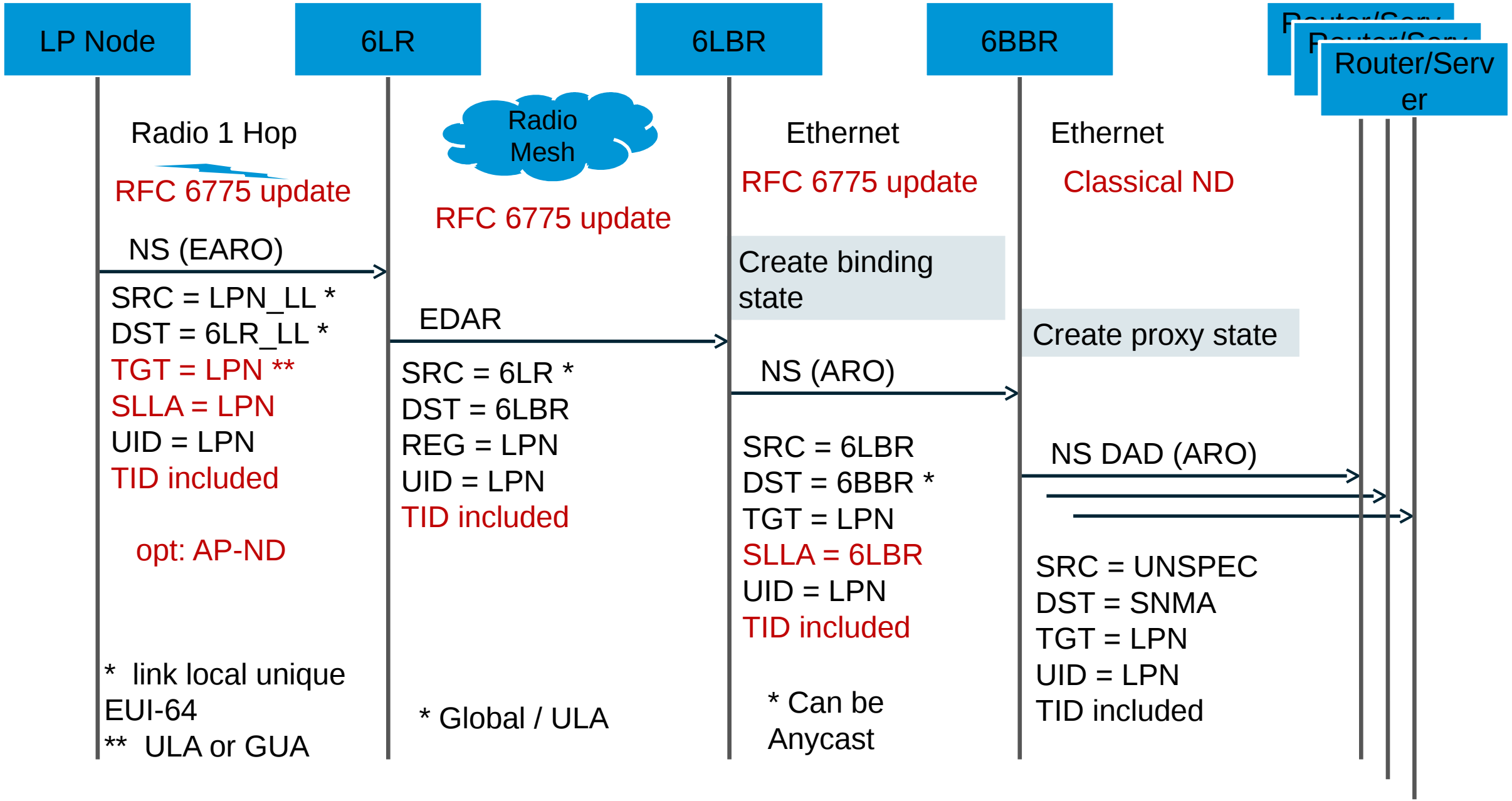
0 Registration Lifetime: 16-bit integer; expressed in minutes. 0 means that the registration has ended and the

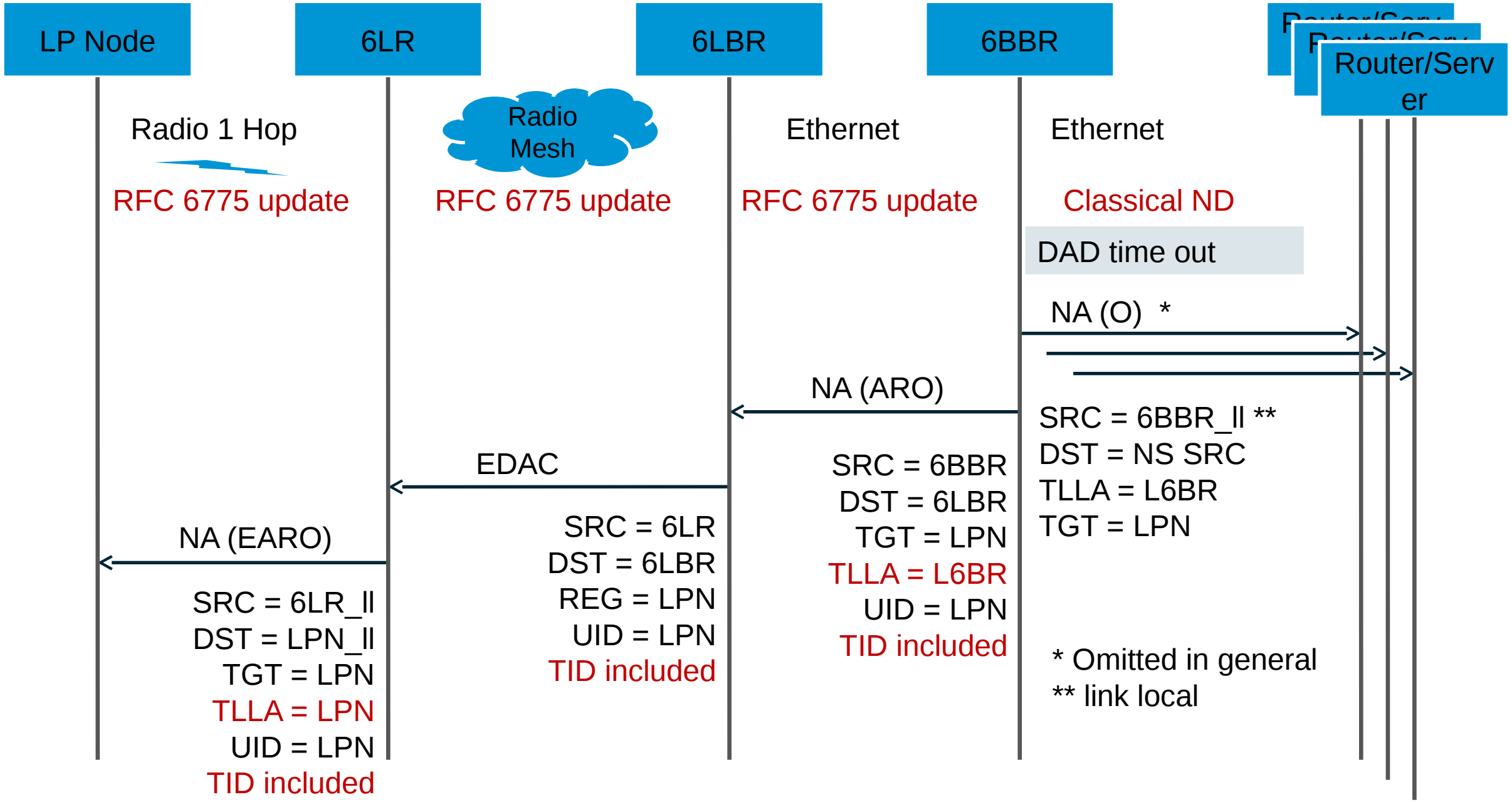
RFC 6775 update new features: ROVR



Registration Ownership Verifier (ROVR): Enables the correlation between multiple attempts to register a same IPv6 Address. This can be a unique ID of the Registering Node, such as


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


LP Node
6LR
6LBR
6BBR
Router/Server
Radio 1 Hop
RFC 6775 update
Radio Mesh
RFC 6775 update
Ethernet
RFC 6775 update
Ethernet
Classical ND
NS (EARO)
SRC = LPN_LL *
DST = 6LR_LL *
TGT = LPN **
SLLA = LPN
UID = LPN
TID included
opt: AP-ND
EDAR
SRC = 6LR *
DST = 6LBR
REG = LPN
UID = LPN
TID included
Create binding state
NS (ARO)
SRC = 6LBR
DST = 6BBR *
TGT = LPN
SLLA = 6LBR
UID = LPN
TID included
Create proxy state
NS DAD (ARO)
SRC = UNSPEC
DST = SNMA
TGT = LPN
UID = LPN
TID included
* link local unique EUI-64
** ULA or GUA
* Global / ULA
* Can be Anycast


LP Node
6LR
6LBR
6BBR
Router/Server
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

IESG Review

RFC 6775 Update

Draft-…-12 to -16

INT-DIR (Tim Chown) => v-12

- Use of EUI-64, should it be deprecated (for privacy reasons) ?
- Clarifications on privacy addresses
- Added a matrix matching specs and requirements in appendix
- Added a glossary
- Suggestion to ask 6MAN about the need for a LRU algorithm

OPS-DIR (Jürgen Schönwälder) + SEC-DIR (Chris Lonvick) => v-13

- Moved terminology up for readability
- Changed “legacy” to “RFC6775-only” refering to RFC 6775
- Changed OUI field to RUID
- Added Appendix B.7.

  “Requirements Related to Operations and Management”

IOT-DIR (Dave Thaler) => v-14

- Reworded Intro (and many other things)
- Introduced the ‘R’ flag based on parallel discussion with ROLL
- Reworded RUID description
- Limiting the number of addresses => What is the minimum?
- Clarification on address duplication over backbone

RTG-DIR (Adrian Farrel) => v-15

- RUID => ROVR Registration Ownership Verifier ; new text on ROVR functionality and collision scope and consequences
- 6CIO now the only way to discover 6LR capabilities. New flag for 6LBR capability to support extended DA messages
- Use of ICMP code: non-NULL code => Extended DA message
- EARO Length extended due to side discussion on AP-ND

GEN-ART (Peter Yee) => v-16

- Clarifications, e.g., RECOMMENDED for implementations
- How properties are discovered (completing Adrian’s review)
- Review of the requirements and security section
- Clarified / fixed IEEE references
- A lot of editorials, syntax corrections

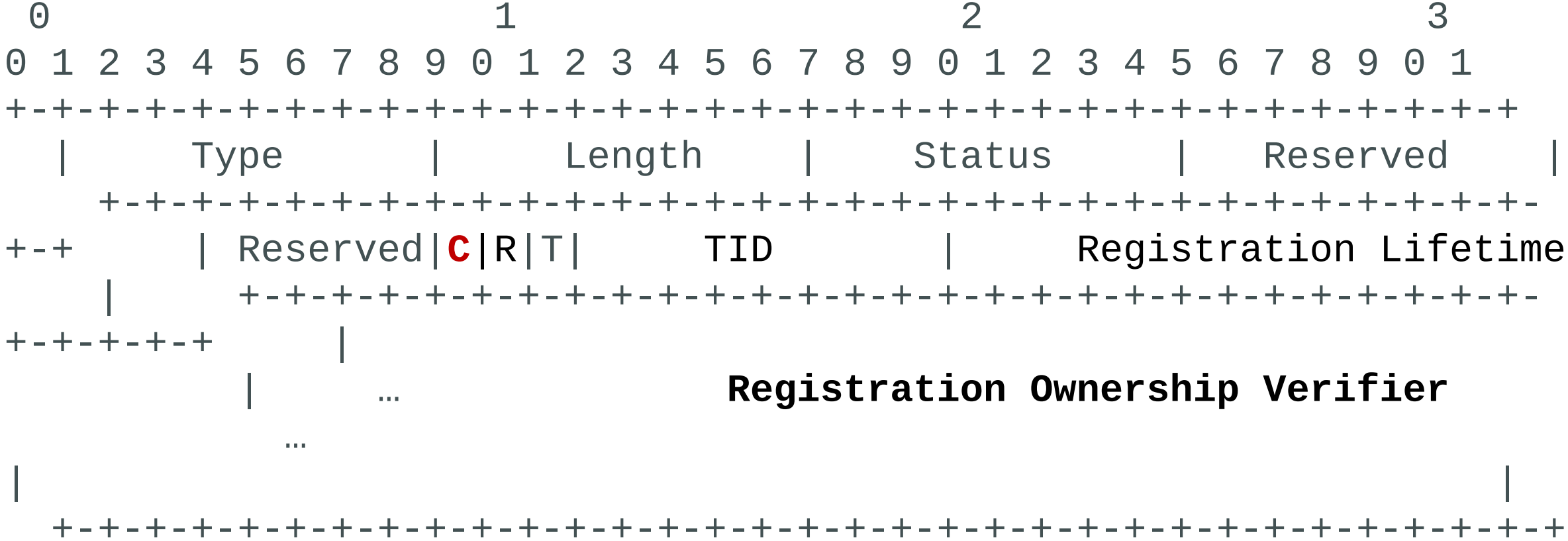
draft-ietf-6lo-ap-nd

P.Thubert, B. Sarikaya, M Sethi, (and expecting R. Struik but not there yet)

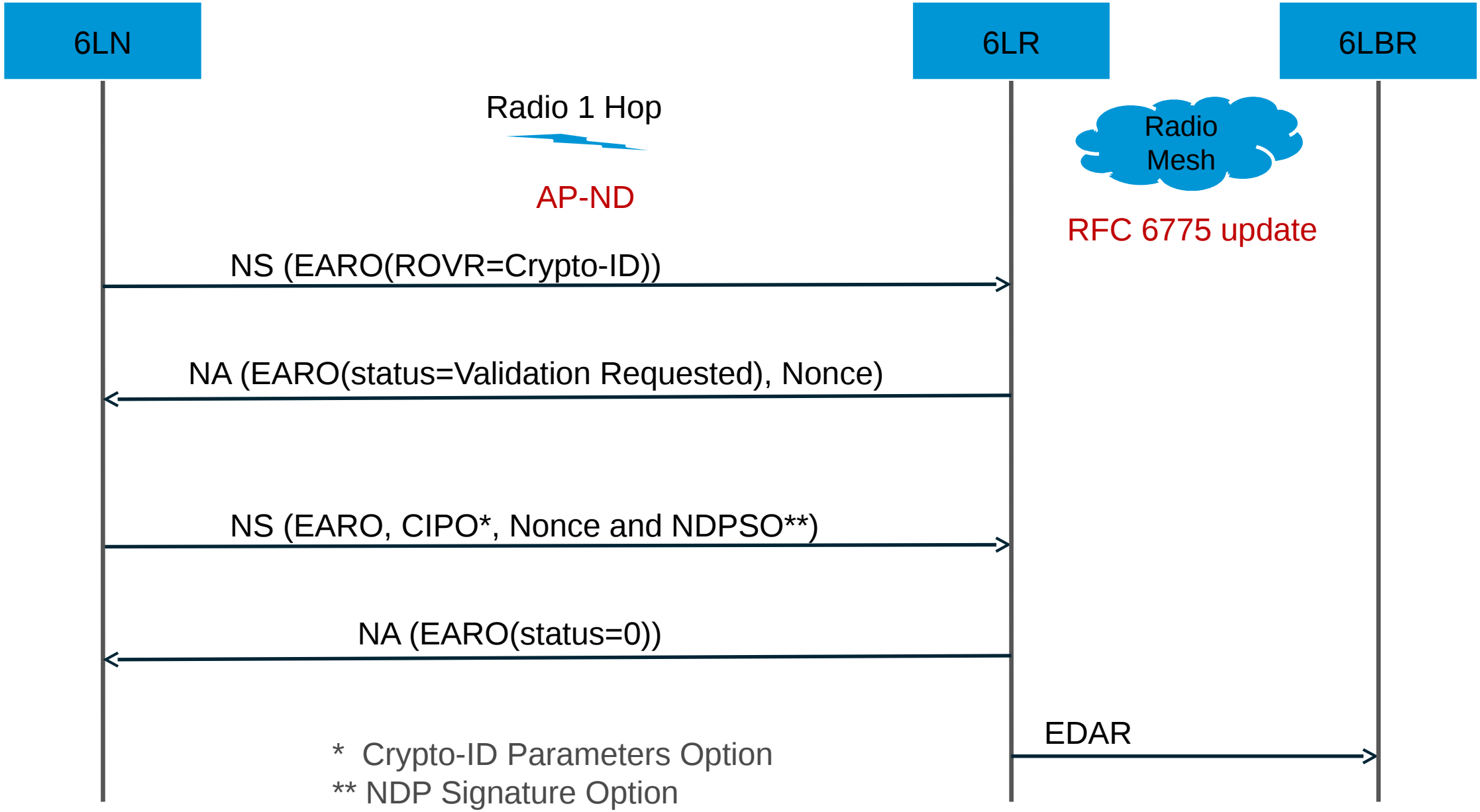
Unmet expectations

- 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

AP-ND new features: ‘C’ flag



C: The "C" flag is set to indicate that the Registration Ownership Verifier field contains a Crypto-ID and that the 6LN MAY be


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

- Simplified the computation of the Crypto-ID
  - Digital signature (SHA-256 then either NIST P-256 or EdDSA) is executed on the concatenation of short modifier and public key
  - Modifier not used to make computation complex as opposed to CGA. This simplifies the operation of a constrained node
  - But 64 bits ROVR might not suffice for adequate protection => Longer ROVR
- Reuse options defined in RFC 3971 for SEND
  - Crypto-ID Parameters Option, a variation of the CGA Option
  - Nonce Option
  - NDP Signature Option, a variation of the RSA Signature Option
    - the option is extended for non-RSA Signatures
    - this specification defines an alias to avoid the confusion.

Security properties

- We made the size of the ROVR tunable so we can get high security
- At the moment a joining 6LN is challenge 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?

draft-ietf-6lo-backbone-router

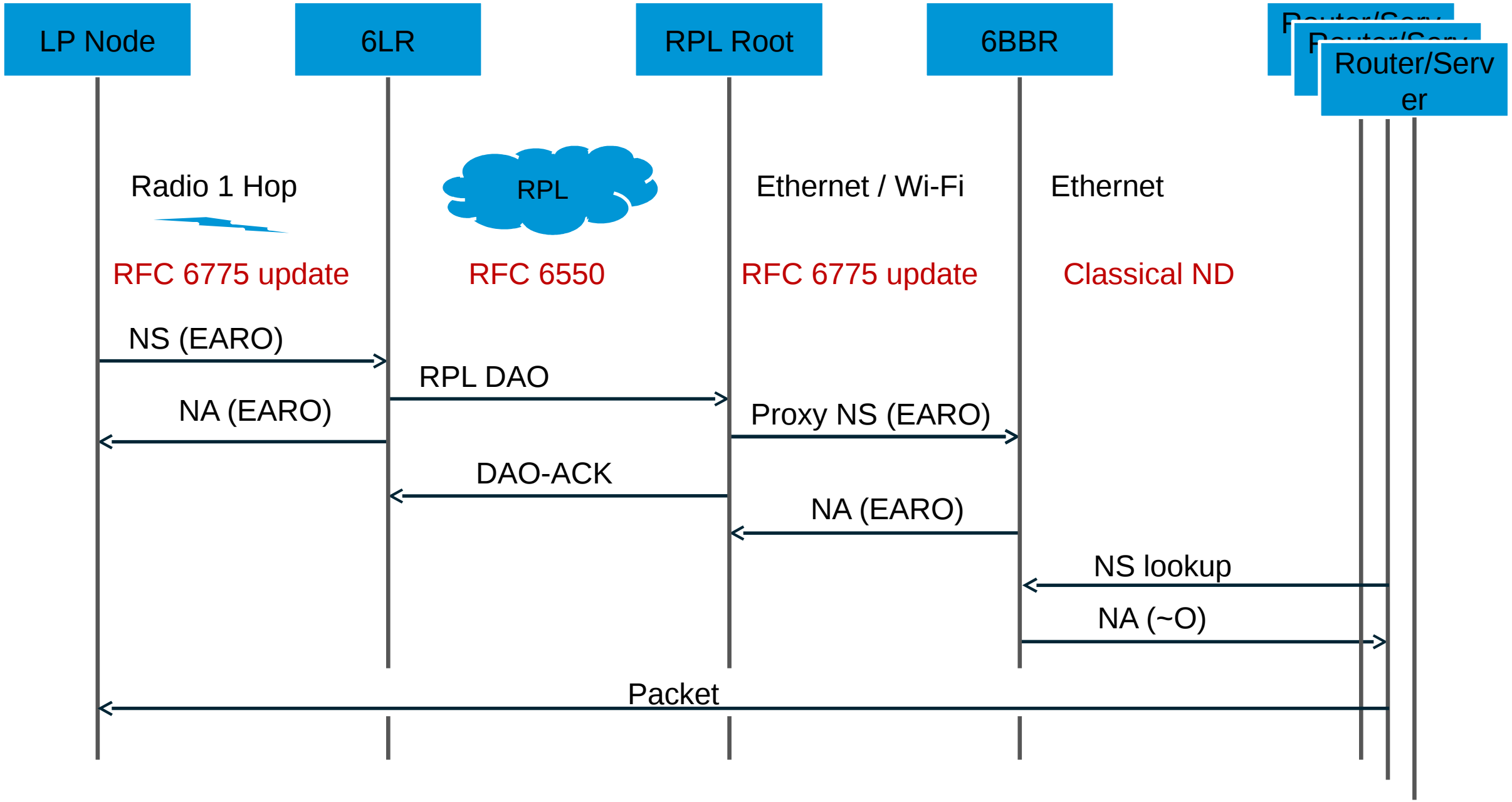
P.Thubert

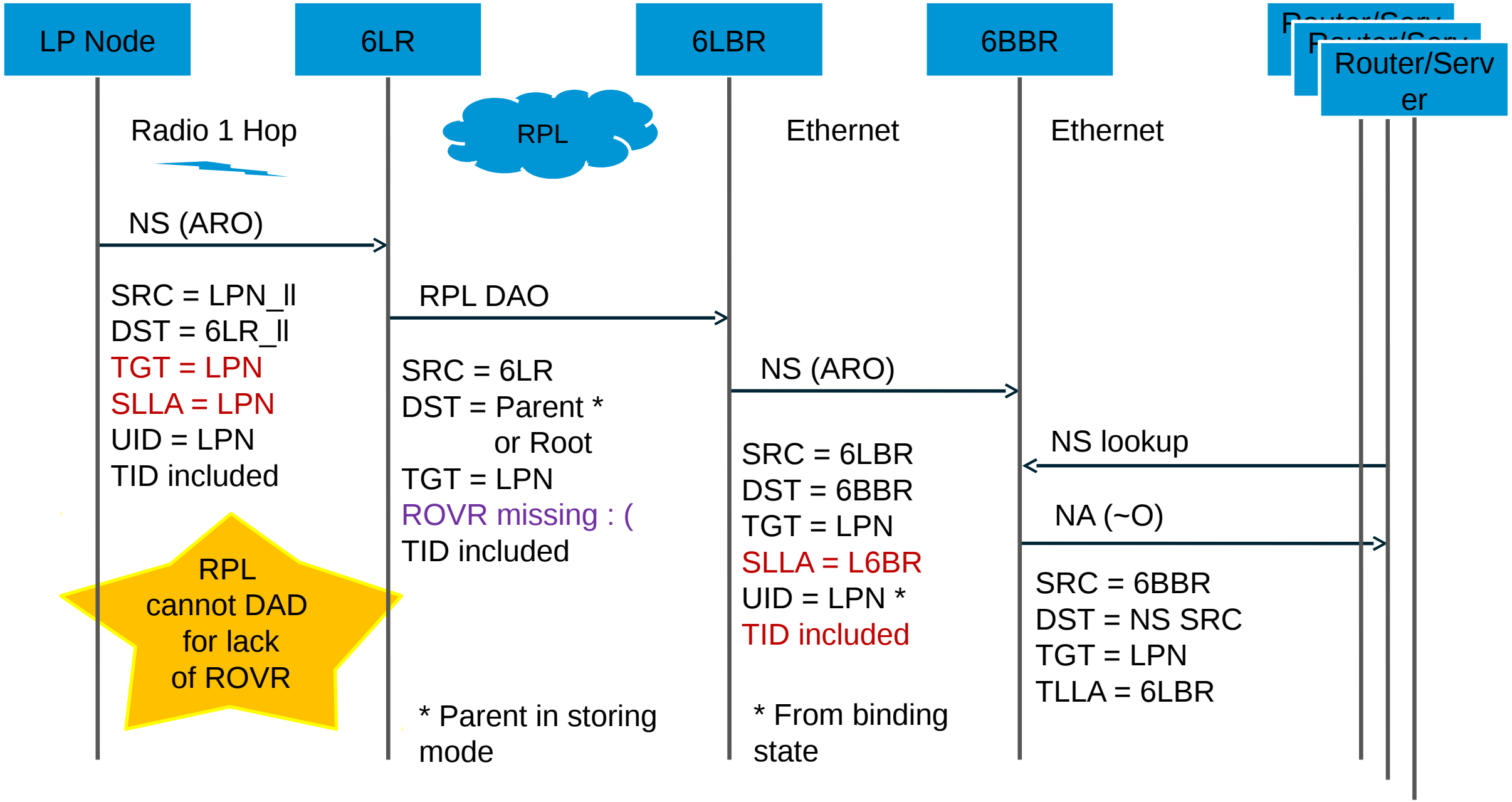
Unmet expectations

- 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

- Uses of the ‘R’ flag
  - Indicates the need for proxy operation
- Clarifications
- TBD : RPL Root / 6LBR separation


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 DAO
SRC = 6LR
DST = Parent *
or Root
TGT = LPN
ROVR missing : (
TID included
NS (ARO)
SRC = 6LBR
DST = 6BBR
TGT = LPN
SLLA = L6BR
UID = LPN *
TID included
NS lookup
NA (~O)
SRC = 6BBR
DST = NS SRC
TGT = LPN
TLLA = 6LBR
RPL
cannot DAD
for lack
of ROVR
* Parent in storing mode
* From binding state

WGLC?

-

draft-thubert-roll-unaware-leaves

P.Thubert

IETF 101

London

Terminology

- RFC 6550:
  - A RPL leaf may understands RPL
  - But does not Act as a router
- This draft: A RPL-unaware leaf does not implement anything specific to RPL, but it MUST support draft-rfc6775-update

Notes on the ‘R’ flag (defined in draft-rfc-6775-update)

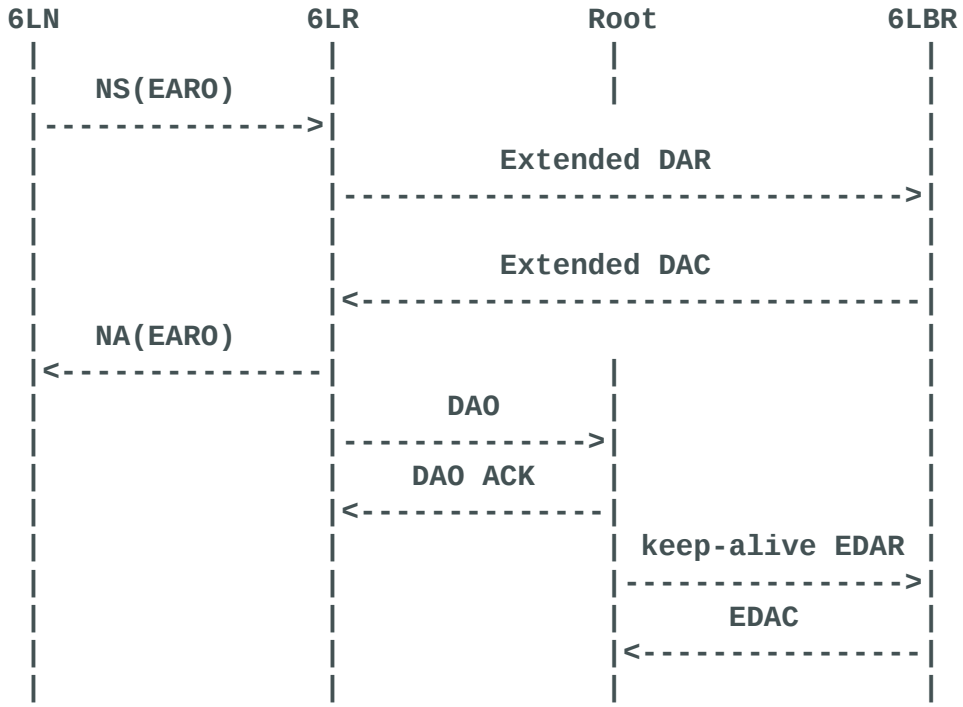
- A RPL Unaware Leaf does not know that there is routing in place and that the routing is RPL; draft-thubert-roll-unaware-leaves does not require anything from the Leaf.
- draft-rfc-6775-update specifies a new flag in the EARO, the 'R' flag.
- If the 'R' flag is set, the Registering Node expects that the 6LR ensures reachability for the Registered Address, e.g., by means of routing or proxying ND.
- Conversely, when it is not set, the 'R' flag indicates that the Registering Node is a router, which for instance participates to RPL and that it will take care of injecting its Address over the routing protocol by itself.
- A 6LN that acts only as a host, when registering, MUST set the 'R' to indicate that it is not a router and that it will not handle its own reachability.
- A 6LR that manages its reachability SHOULD NOT set the 'R' flag; if it does, routes towards this router may be installed on its behalf and may interfere with those it injects.

RPL Unaware Leaf (RUL) operation

- Note: The RUL does not know that there is routing in place and that the routing is RPL; draft-thubert-roll-unaware-leaves does not require anything from the Leaf Node. The ‘R’ flag is defined in draft-rfc-6775-update and plain 6LNs MUST set it.
- A RPL-Unaware Leaf (RUL) sets the 'R' flag in the EARO to declare itself as a host with the expectation that the 6LR that accepts the registration injects routing information for the Registered Address in the RPL domain as described in draft-rfc-6775-update.
- The packet forwarding operation by the 6LR serving a Leaf 6LN is described in draft-ietf-roll-useofrplinfo.
- This doc draft-thubert-roll-unaware-leaves adds the capability by a 6LR to advertise the IPv6 address(es) of the 6LN in the RPL protocol.
- Examples of routing-agnostic 6LN may include lightly-powered sensors such as window smash sensor (alarm system), or the kinetically powered light switch.

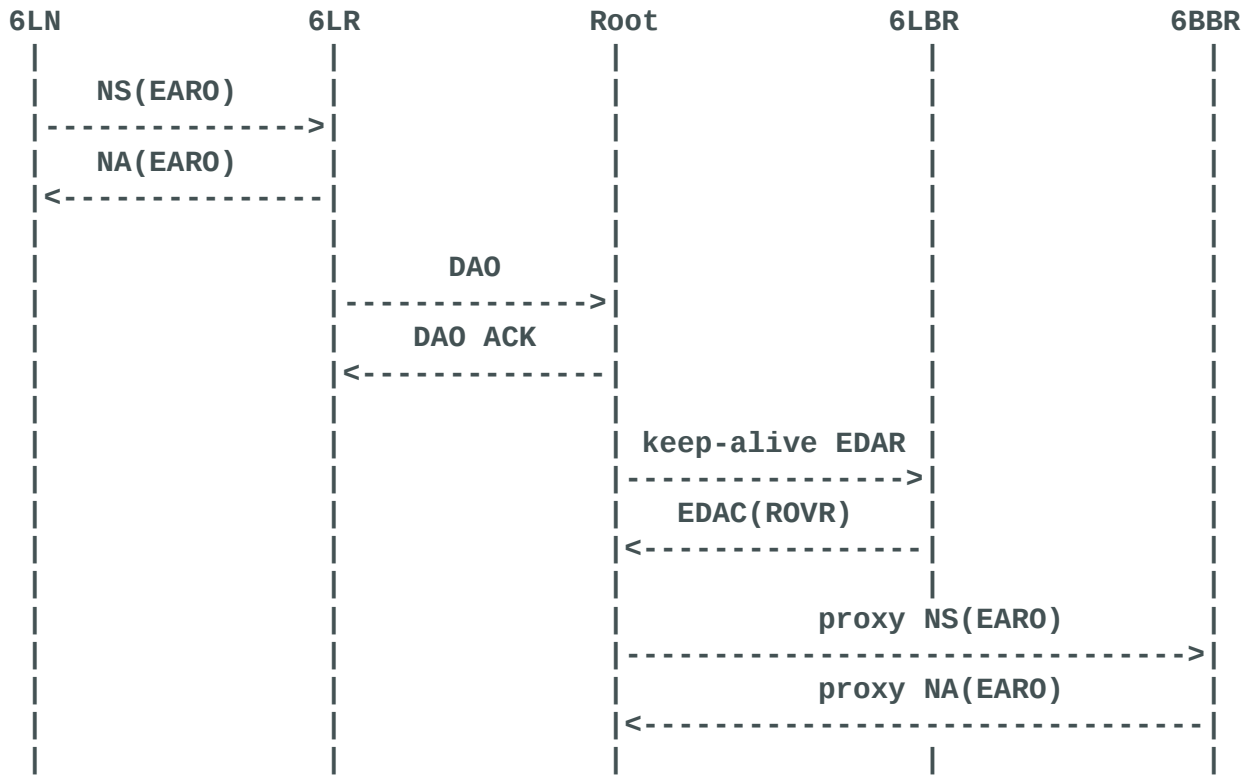
First registration

- Upon the first registration, the EDAR / EDAC populates a state in the 6LBR including the ROVR field and the 6LR sends a first DAO message.
- The RPL Root acts as a proxy on behalf of the 6LR upon the reception of the DAO propagation initiated at the 6LR. Should we allow splitting from the 6LBR, e.g.:



EDA (DAR, DAC) message Proxying

- Upon the renewal of a 6lowPAN ND registration: if the 'R' flag is set, the 6LR injects a DAO targeting the Registered Address, and refrains from sending a DAR message.
- With a Root/6LBR split that could give:



Mapping Fields from RPL DAO to NS(EARO) and EDA

- The Registered Address in a RPL Target Option is a direct match to the Registered Address field of the EDAR message and in the Target field of the NS, respectively
- EARO's TID is a direct match to Path Sequence in Transit Information option (TIO)
- EARO's Lifetime unit is 60s. RPL uses Lifetime Units that is passed in the DODAG Configuration Option. Converting EARO to DAO and back requires mapping of units.
- The Registration Ownership Verifier (ROVR) field in keep-alive EDAR messages by the Root is set to 64-bits of all ones to indicate that it is not provided. It is obtained in the EDAC from the 6LBR and used in proxy registration.

  Q: Should we carry it in a RPL option in DAO messages?