Wireless ND

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

IETF 104

Prague

Wireless IPv6 ND: providing for 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 (well… did) not exist
  - Implementations provide proprietary techniques based on snooping => widely imperfect

⇒ RFC 6775 solves the problem for DAD in one LL

⇒ RFC 8505 enables establishing proxy services directly (ND for now), over a LLN, across multiple LLNs

6lo standard work

A proactive setting of proxy/routing state to avoid multicast due to reactive Duplicate address detection and lookup in IPv6 ND

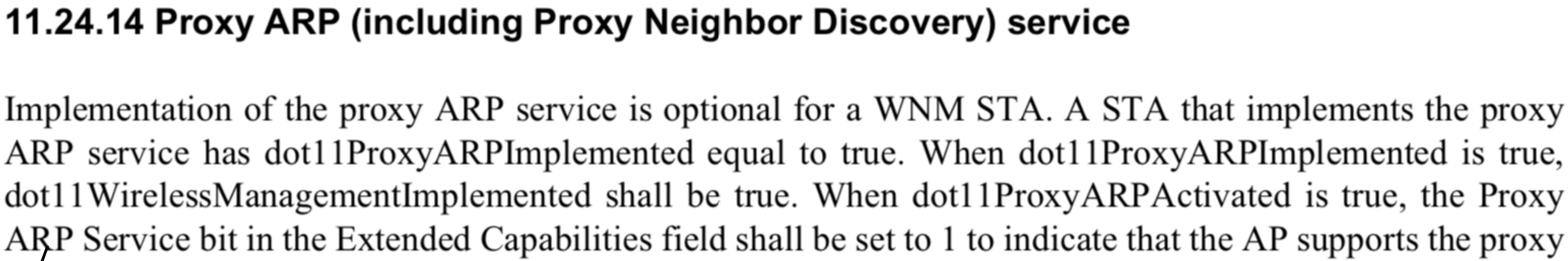
- RFC 8505 (Issued 11/2018)
  - The registration mechanism for proxy and routing services
  - Analogous to a Wi-Fi association but at Layer 3

NEW RFC

- draft-ietf-6lo-backbone-router (WGLC complete 1/25)
  - Federates 6lo meshes over a high speed backbone
  - ND proxy analogous to Wi-Fi bridging but at Layer 3
- draft-ietf-6lo-ap-nd (WGLC complete 3/26)
  - Protects addresses against theft (Crypto ID in registration)
- draft-thubert-6lo-unicast-lookup (new draft)
  - Provides a 6LBR on the backbone to speed up DAD and lookup

NEW DRAFT

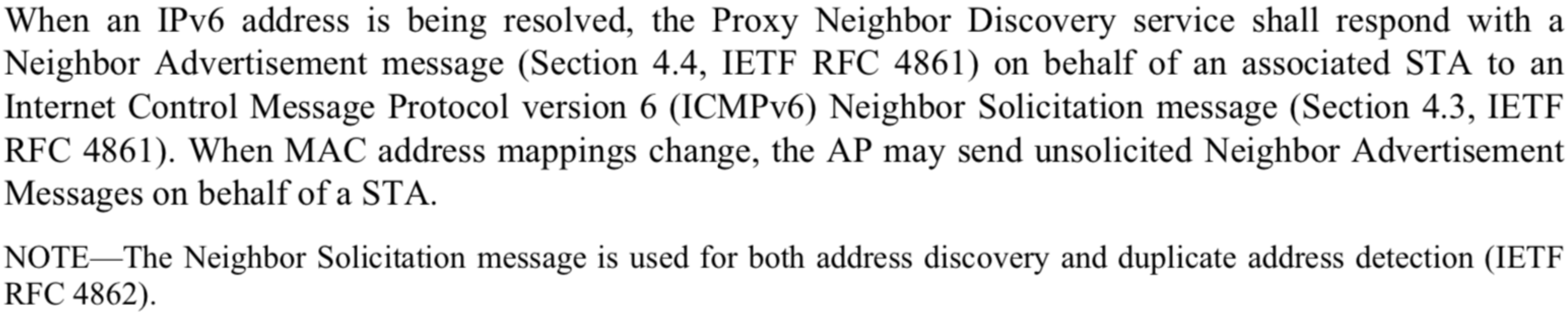
IPv6 and 802.11



11.24.14 Proxy ARP (including Proxy Neighbor Discovery) service

Implementation of the proxy ARP service is optional for a WNM STA. A STA that implements the proxy ARP service has dot11ProxyARPImplemented equal to true. When dot11ProxyARPImplemented is true, dot11WirelessManagementImplemented shall be true. When dot11ProxyARPActivated is true, the Proxy ARP Service bit in the Extended Capabilities field shall be set to 1 to indicate that the AP supports the proxy

…/…

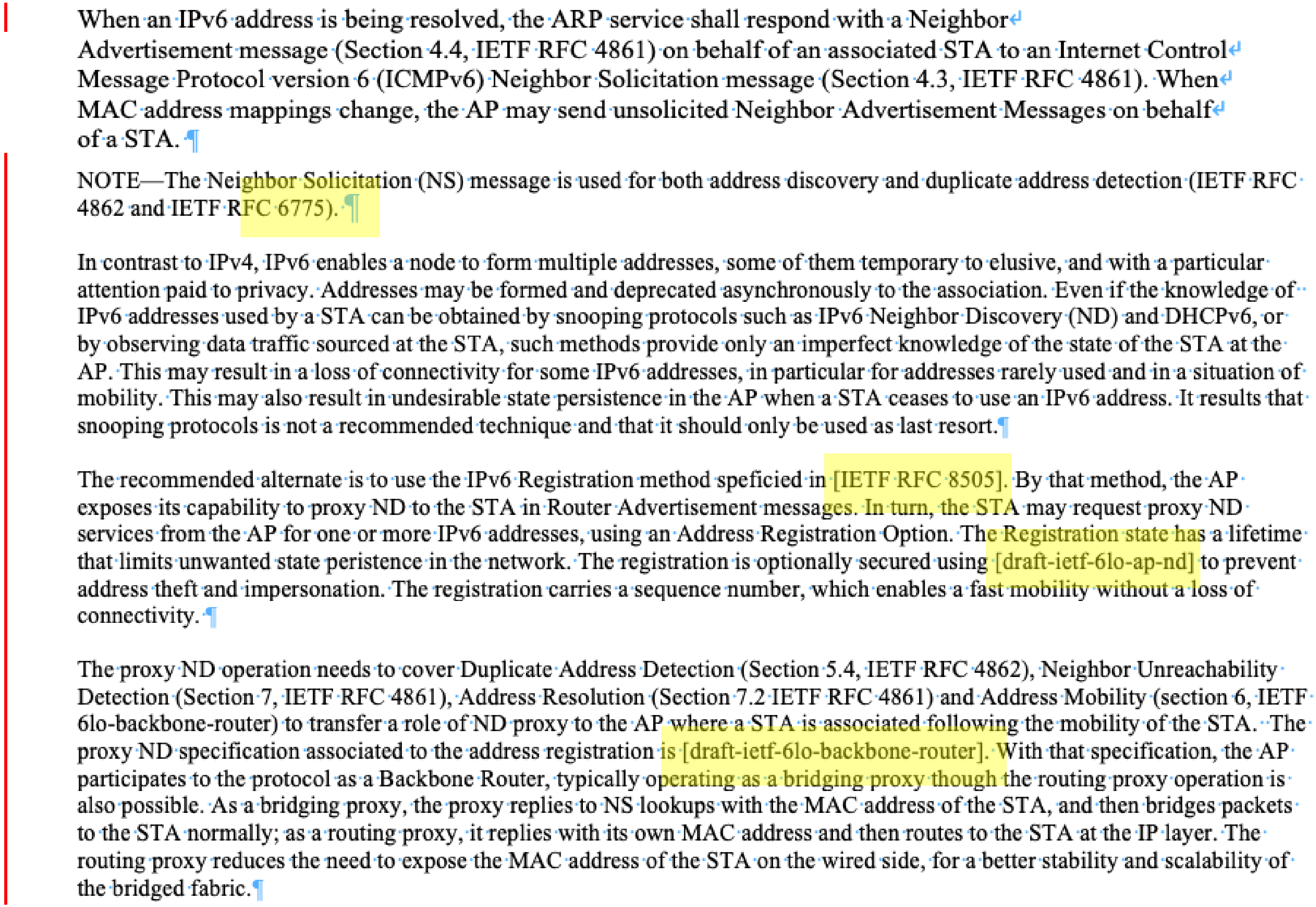


When an IPv6 address is being resolved, the Proxy Neighbor Discovery service shall respond with a Neighbor Advertisement message (Section 4.4, IETF RFC 4861) on behalf of an associated STA to an Internet Control Message Protocol version 6 (ICMPv6) Neighbor Solicitation message (Section 4.3, IETF RFC 4861). When MAC address mappings change, the AP may send unsolicited Neighbor Advertisement Messages on behalf of a STA.

NOTE—The Neighbor Solicitation message is used for both address discovery and duplicate address detection (IETF RFC 4862).

There is no such thing as ARP in IPv6. The equivalent function to IPv4 ARP Proxy is IPv6 ND Service.
This function operates differently from what 11.22.14 describes, as assuming equivalence with IPv4 ARP Proxy is an oversimplification.

Proposed changes to IEEE Std. 802.11



When an IPv6 address is being resolved, the ARP service shall respond with a Neighbor
Advertisement message (Section 4.4, IETF RFC 4861) on behalf of an associated STA to an Internet Control
Message Protocol version 6 (ICMPv6) Neighbor Solicitation message (Section 4.3, IETF RFC 4861). When
MAC address mappings change, the AP may send unsolicited Neighbor Advertisement Messages on behalf
of a STA.

NOTE—The Neighbor Solicitation (NS) message is used for both address discovery and duplicate address detection (IETF RFC 4862 and IETF RFC 6775).

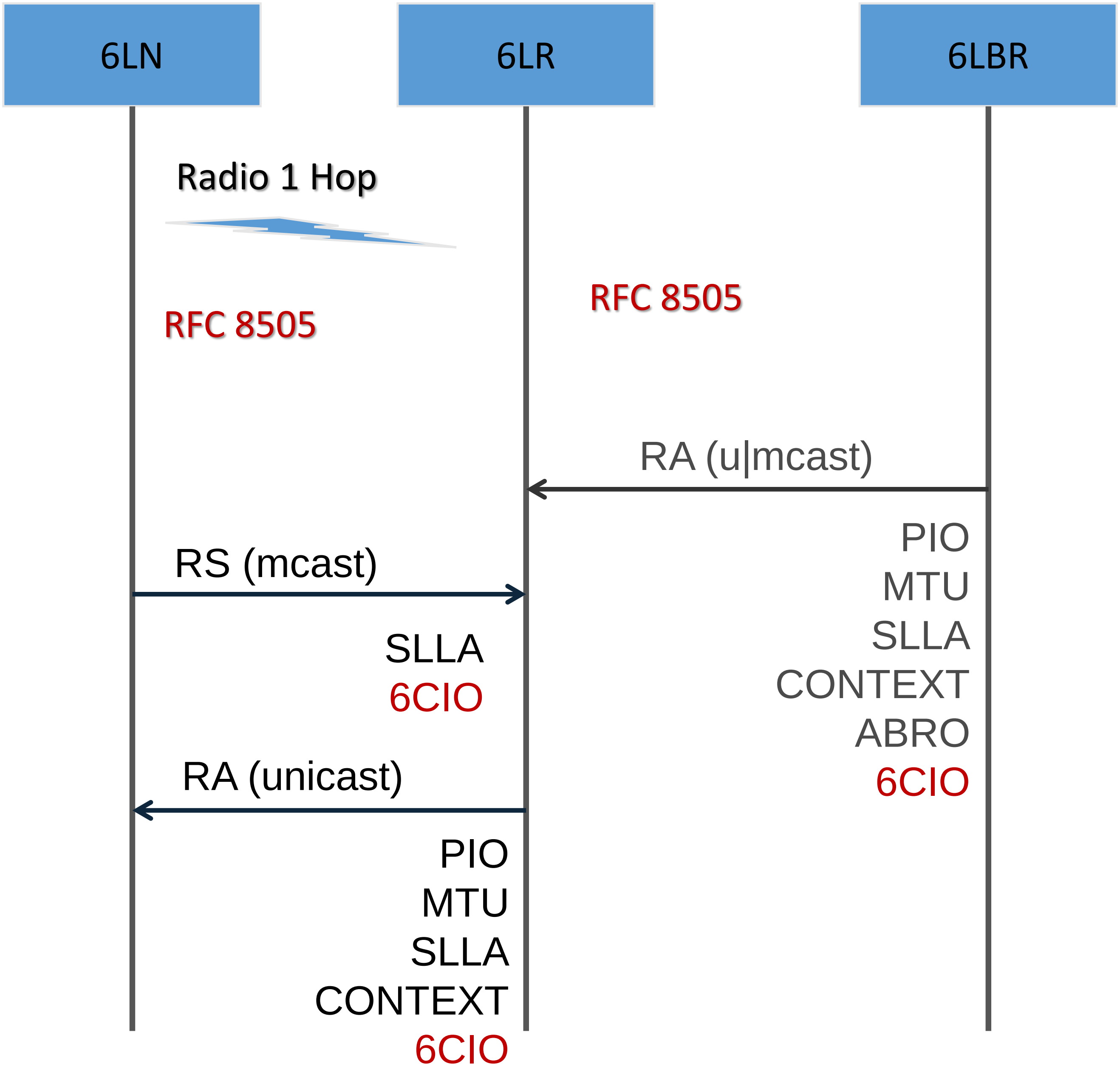
In contrast to IPv4, IPv6 enables a node to form multiple addresses, some of them temporary to elusive, and with a particular attention paid to privacy. Addresses may be formed and deprecated asynchronously to the association. Even if the knowledge of IPv6 addresses used by a STA can be obtained by snooping protocols such as IPv6 Neighbor Discovery (ND) and DHCPv6, or by observing data traffic sourced at the STA, such methods provide only an imperfect knowledge of the state of the STA at the AP. This may result in a loss of connectivity for some IPv6 addresses, in particular for addresses rarely used and in a situation of mobility. This may also result in undesirable state persistence in the AP when a STA ceases to use an IPv6 address. It results that snooping protocols is not a recommended technique and that it should only be used as last resort.

The recommended alternate is to use the IPv6 Registration method speficied in [IETF RFC 8505]. By that method, the AP exposes its capability to proxy ND to the STA in Router Advertisement messages. In turn, the STA may request proxy ND services from the AP for one or more IPv6 addresses, using an Address Registration Option. The Registration state has a lifetime that limits unwanted state peristence in the network. The registration is optionally secured using [draft-ietf-6lo-ap-nd] to prevent address theft and impersonation. The registration carries a sequence number, which enables a fast mobility without a loss of connectivity.

The proxy ND operation needs to cover Duplicate Address Detection (Section 5.4, IETF RFC 4862), Neighbor Unreachability Detection (Section 7, IETF RFC 4861), Address Resolution (Section 7.2 IETF RFC 4861) and Address Mobility (section 6, IETF 6lo-backbone-router) to transfer a role of ND proxy to the AP where a STA is associated following the mobility of the STA. The proxy ND specification associated to the address registration is [draft-ietf-6lo-backbone-router]. With that specification, the AP participates to the protocol as a Backbone Router, typically operating as a bridging proxy though the routing proxy operation is also possible. As a bridging proxy, the proxy replies to NS lookups with the MAC address of the STA, and then bridges packets to the STA normally; as a routing proxy, it replies with its own MAC address and then routes to the STA at the IP layer. The routing proxy reduces the need to expose the MAC address of the STA on the wired side, for a better stability and scalability of the bridged fabric.

RFC 8505

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



6LN

6LR

6LBR

Radio 1 Hop

RFC 8505

RFC 8505

RA (u|mcast)

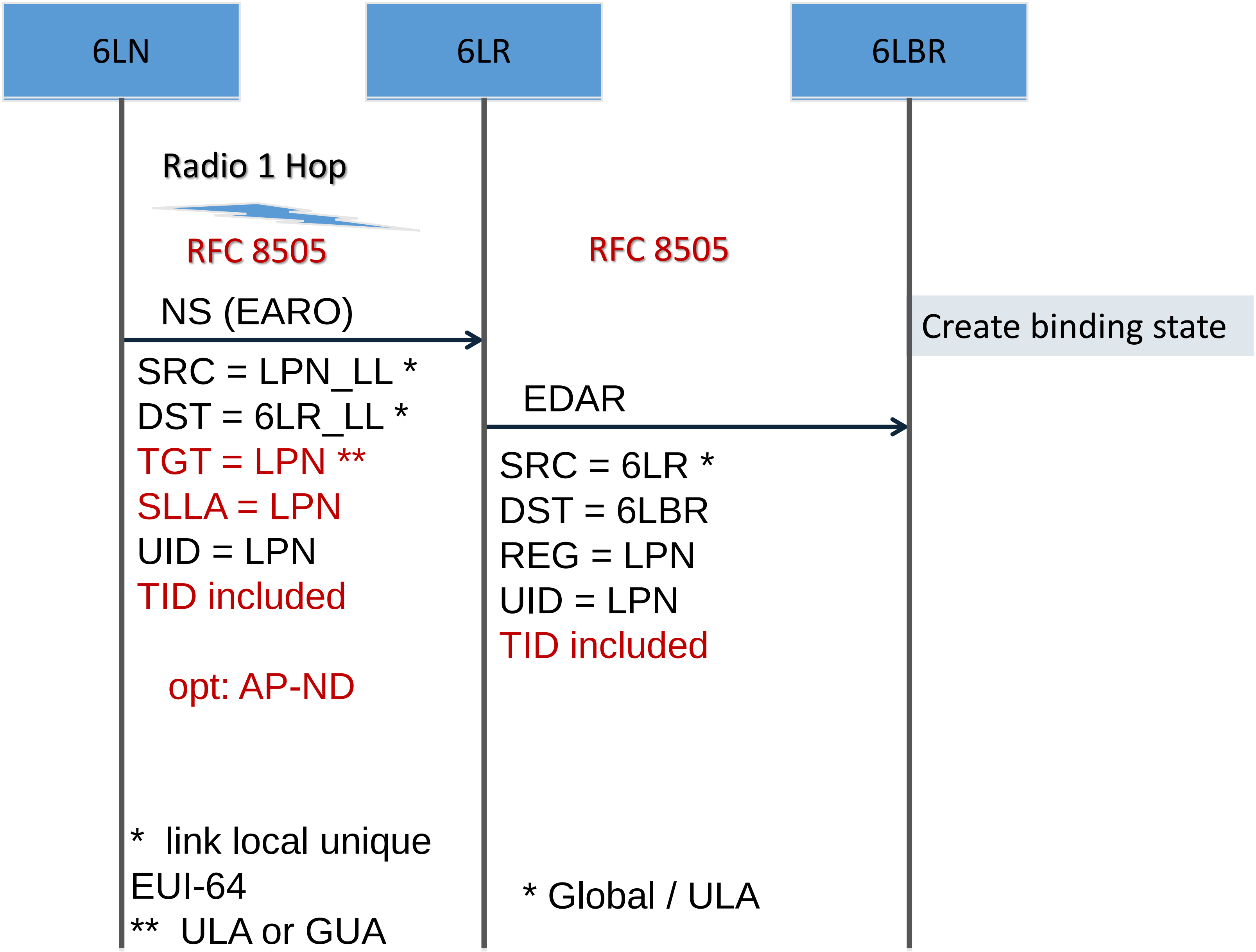
PIO
MTU
SLLA
CONTEXT
ABRO
6CIO

RS (mcast)

SLLA
6CIO

RA (unicast)

PIO
MTU
SLLA
CONTEXT
6CIO



6LN

6LR

6LBR

Radio 1 Hop

RFC 8505

RFC 8505

NS (EARO)

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

opt: AP-ND

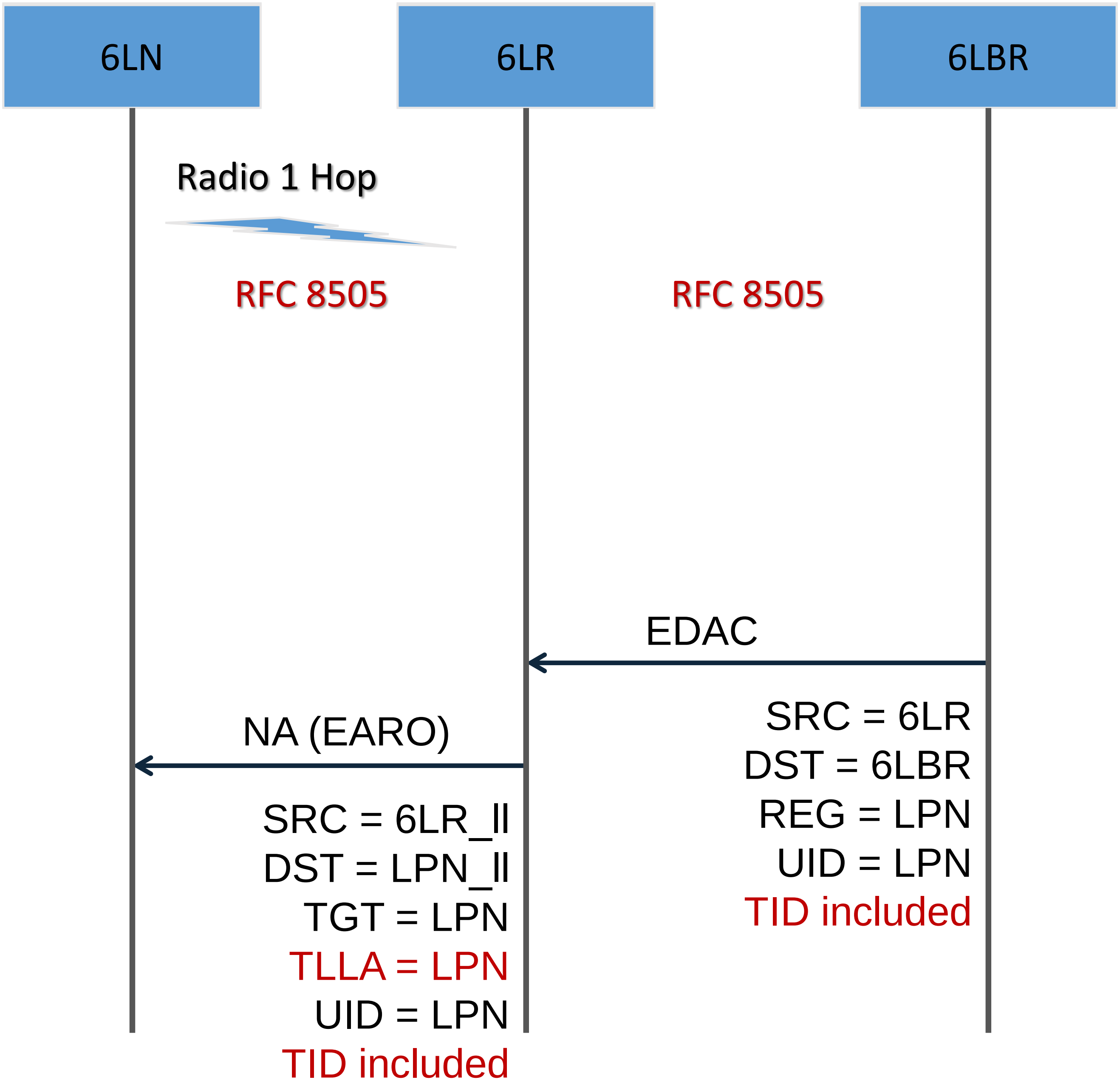
Create binding state

EDAR

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

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

* Global / ULA



6LN

6LR

6LBR

Radio 1 Hop

RFC 8505

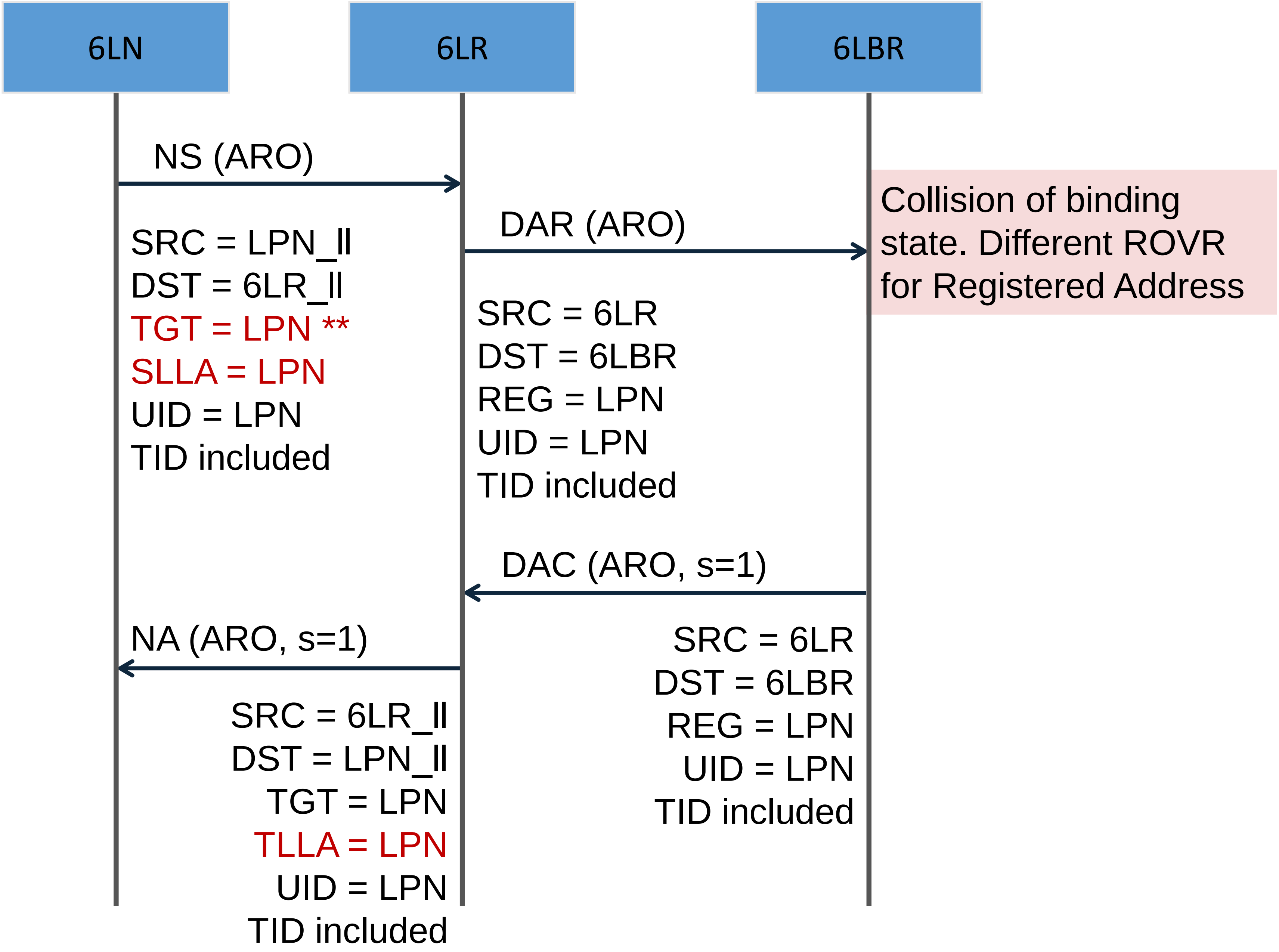
RFC 8505

EDAC

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

NA (EARO)

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



6LN

6LR

6LBR

NS (ARO)

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

DAR (ARO)

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

Collision of binding state. Different ROVR for Registered Address

DAC (ARO, s=1)

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

NA (ARO, s=1)

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

draft-ietf-6lo-ap-nd

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

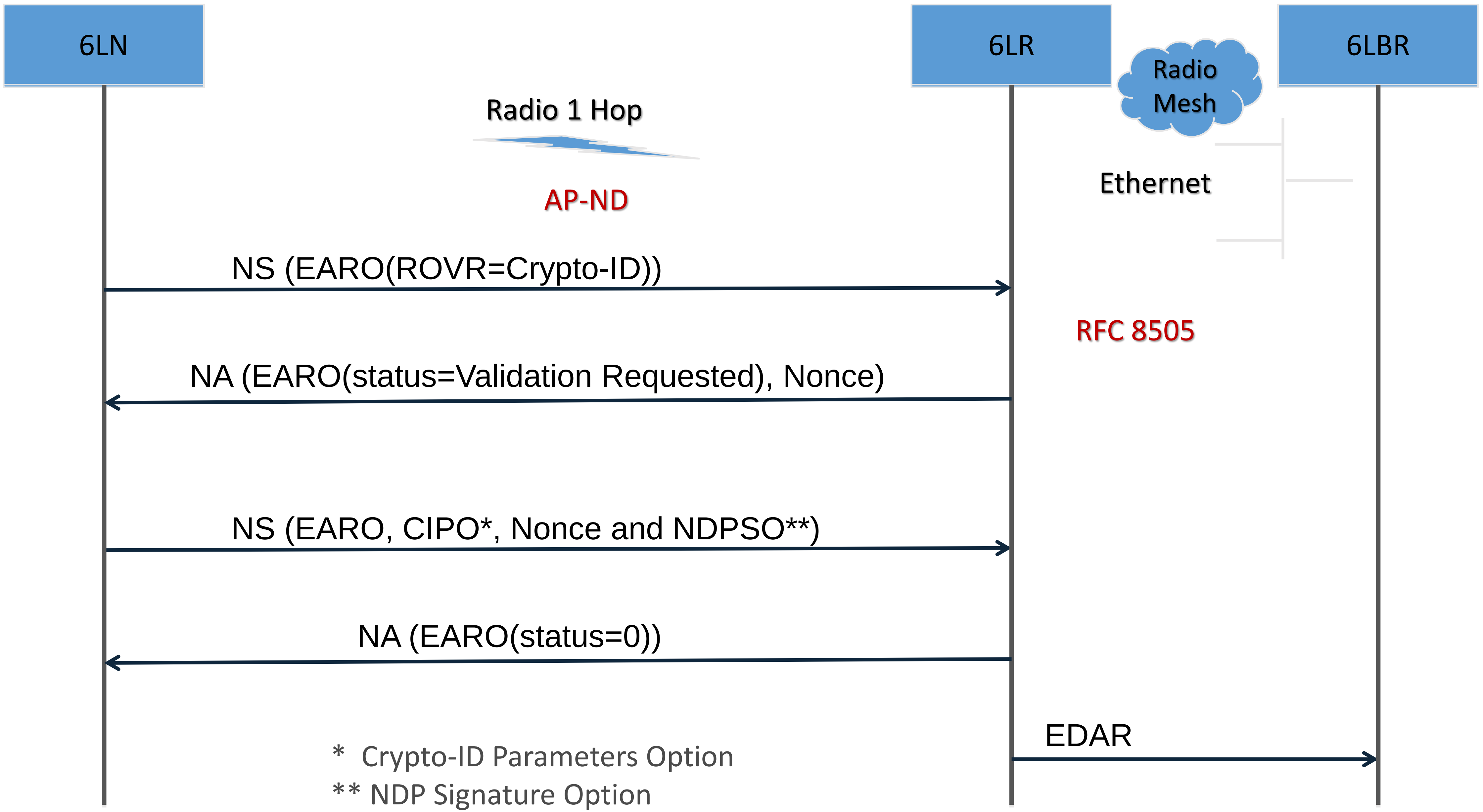
Unmet expectations

- 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

Status

- Draft-11 published with René’s latest updates
- WGLC completed March 26th
- 3 crypto types =>

Crypto-Type value	0 (ECDSA256)	1 (Ed25519)	2 (ECDSA25519)
Elliptic curve	NIST P-256 [FIPS186-4]	Curve25519 [RFC7748]	Curve25519 [RFC7748]
Hash function	SHA-256 [RFC6234]	SHA-512 [RFC6234]	SHA-256 [RFC6234]
Signature algorithm	ECDSA [FIPS186-4]	Ed25519 [RFC8032]	ECDSA [FIPS186-4]
Representation conventions	Weierstrass, (un)compressed, MSB/msb first	Edwards, compressed, LSB/lsb first	Weierstrass, (un)compressed, MSB/msb first
Defining specification	RFC THIS	RFC THIS	RFC THIS



6LN

6LR

6LBR

Radio 1 Hop

Radio Mesh

Ethernet

AP-ND

NS (EARO(ROVR=Crypto-ID))

RFC 8505

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

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

NA (EARO(status=0))

EDAR

* Crypto-ID Parameters Option

** NDP Signature Option

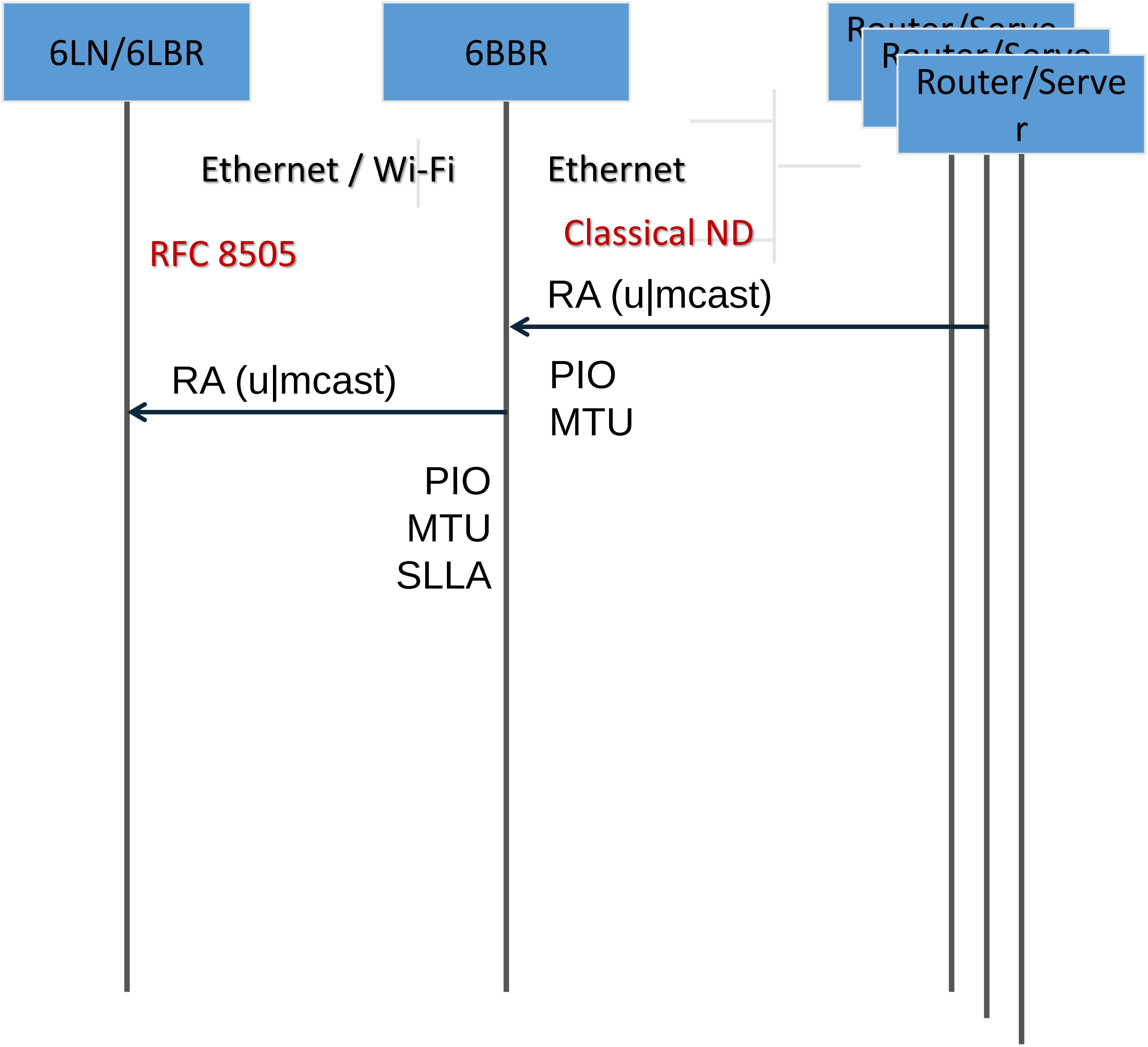
Security properties

- We made the size of the ROVR tunable in RFC 8505 so we can get high security when using it for Crypto-ID.
- New appendix B on Signature Schemes and representations
- Discussion on implementation attacks:

… **implementors should be aware of [breaking-ed25519]. Implementors should be particularly aware that a secure implementation of Ed25519 requires a protected implementation of the hash function SHA-512, whereas this is not required with implementations of SHA-256 used with ECDSA.**

draft-ietf-6lo-backbone-router

P.Thubert



6LN/6LBR

6BBR

Router/Serve
r

Ethernet / Wi-Fi

Ethernet

Classical ND

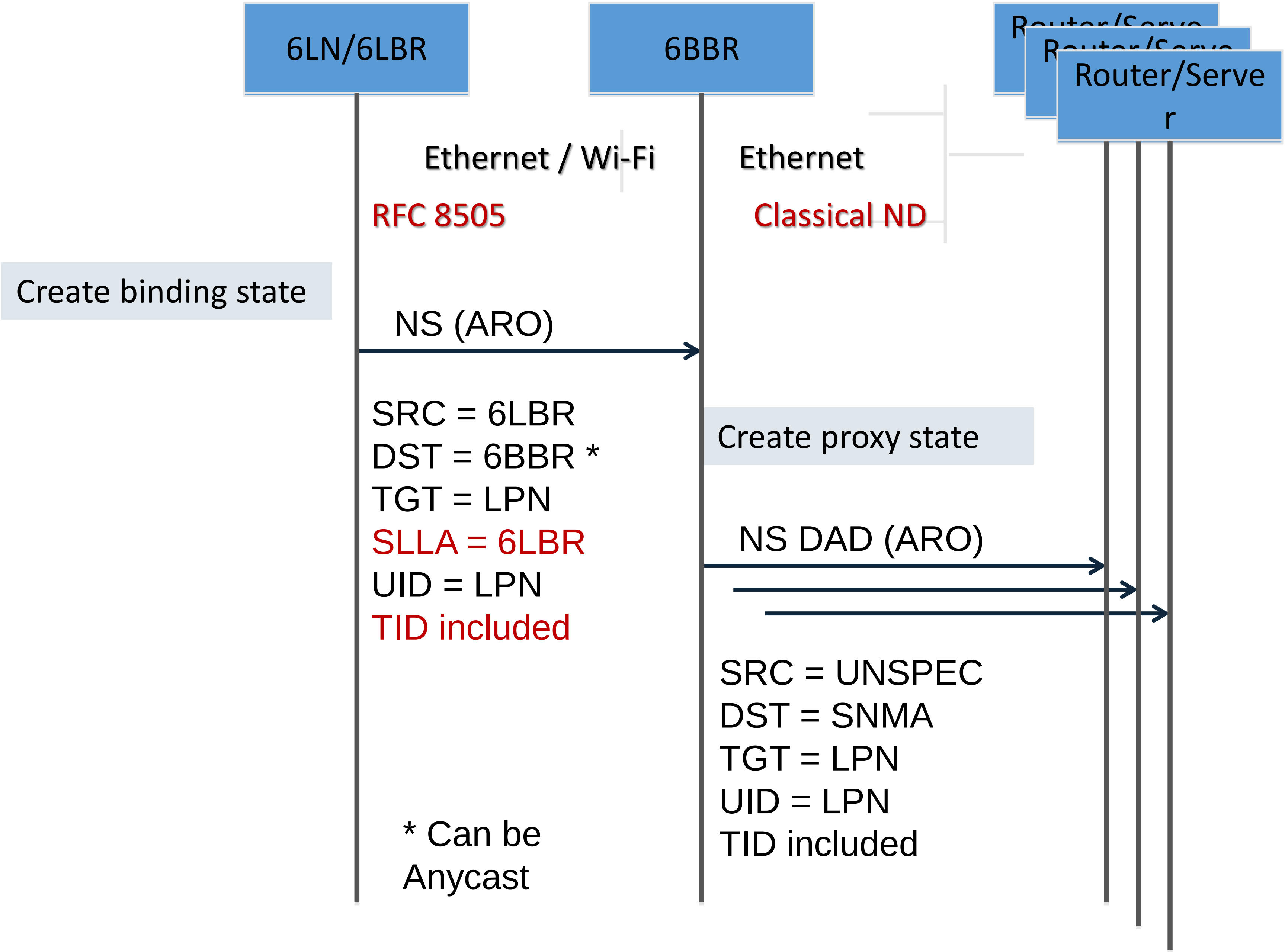
RFC 8505

RA (u|mcast)

PIO
MTU

RA (u|mcast)

PIO
MTU
SLLA



6LN/6LBR

6BBR

Router/Server

Ethernet / Wi-Fi

Ethernet

RFC 8505

Classical ND

Create binding state

NS (ARO)

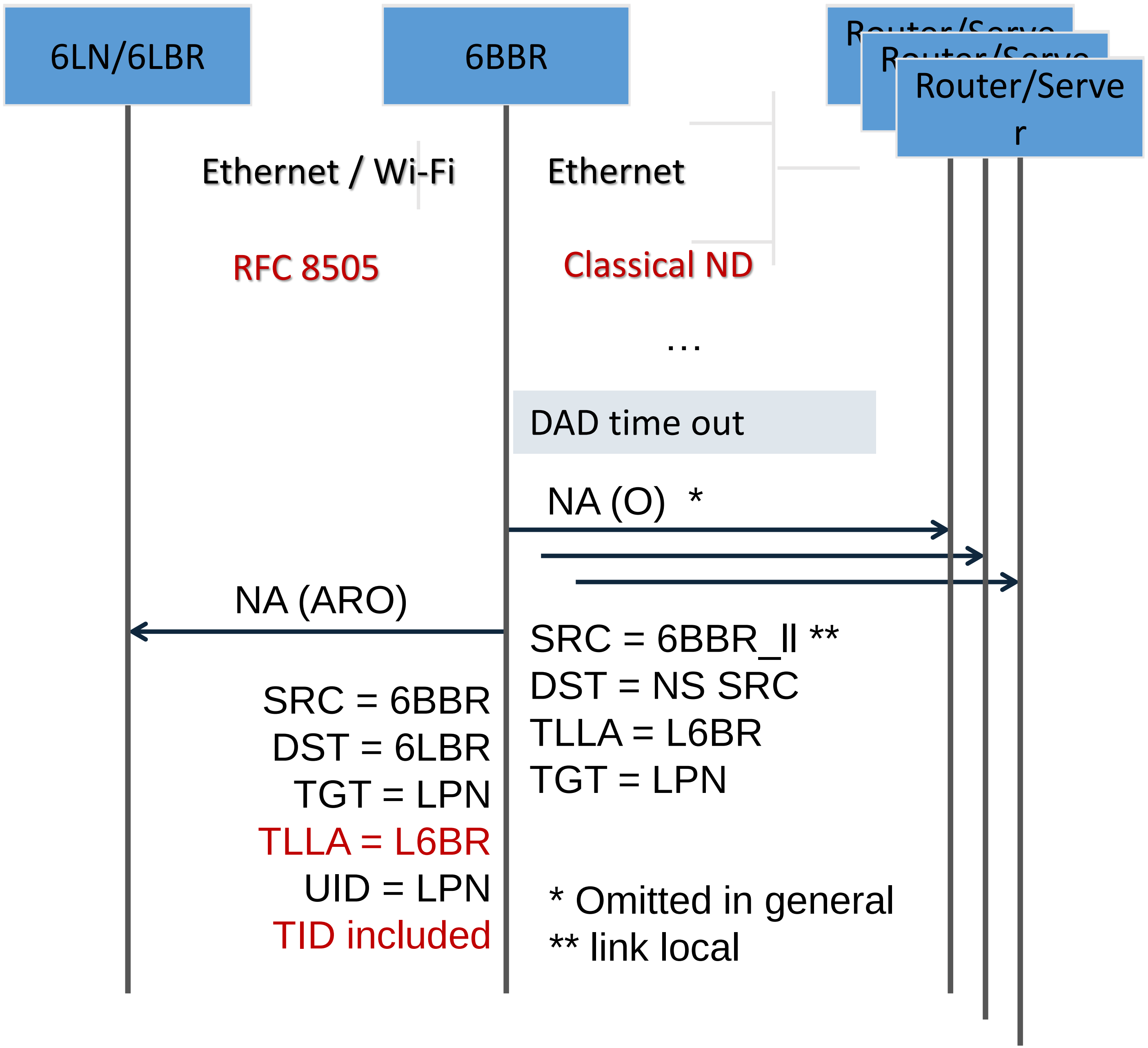
SRC = 6LBR
DST = 6BBR *
TGT = LPN
SLLA = 6LBR
UID = LPN
TID included

Create proxy state

NS DAD (ARO)

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

* Can be Anycast



6LN/6LBR

6BBR

Router/Server

Ethernet / Wi-Fi

Ethernet

RFC 8505

Classical ND

…

DAD time out

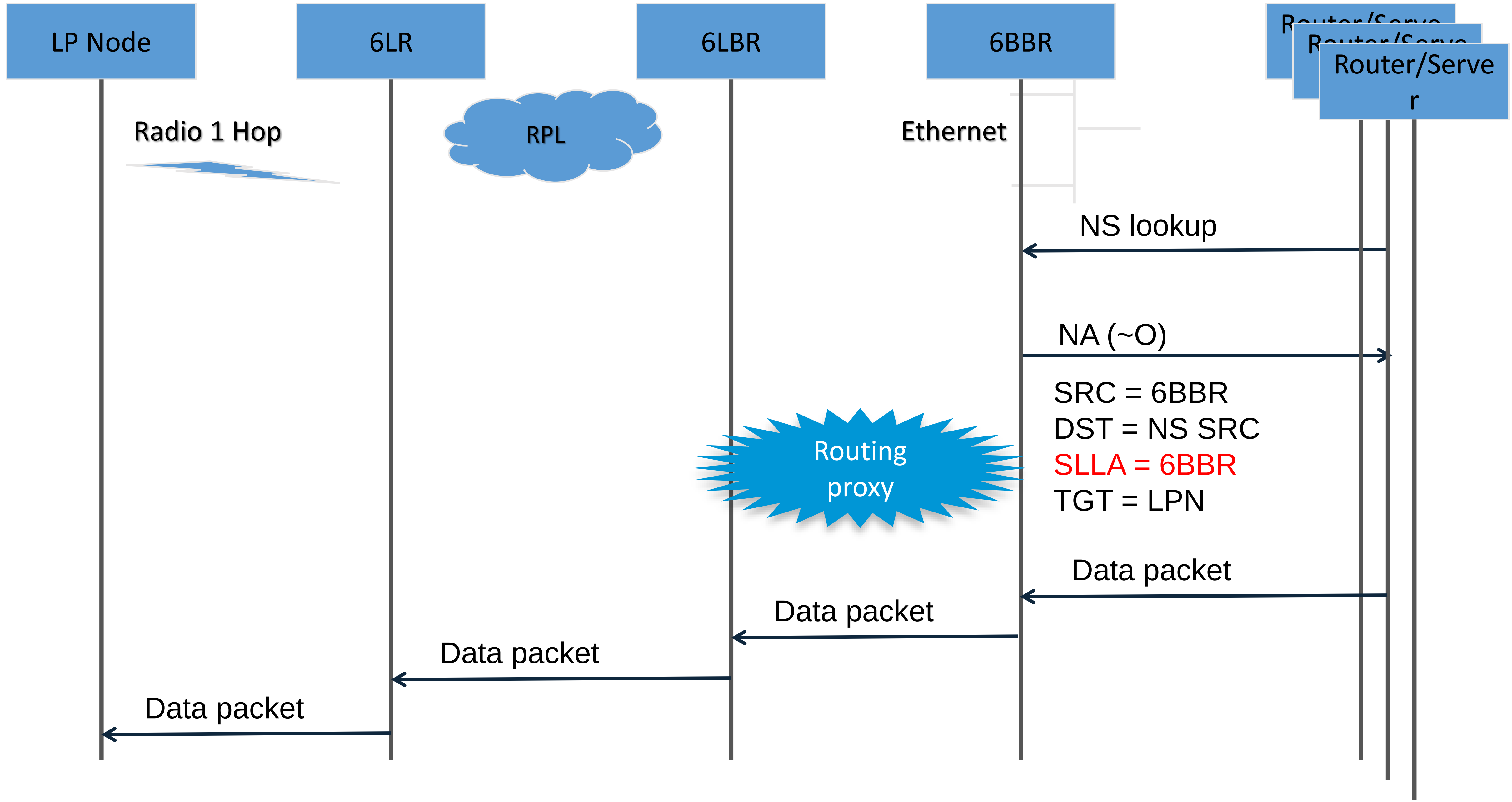
NA (O) *

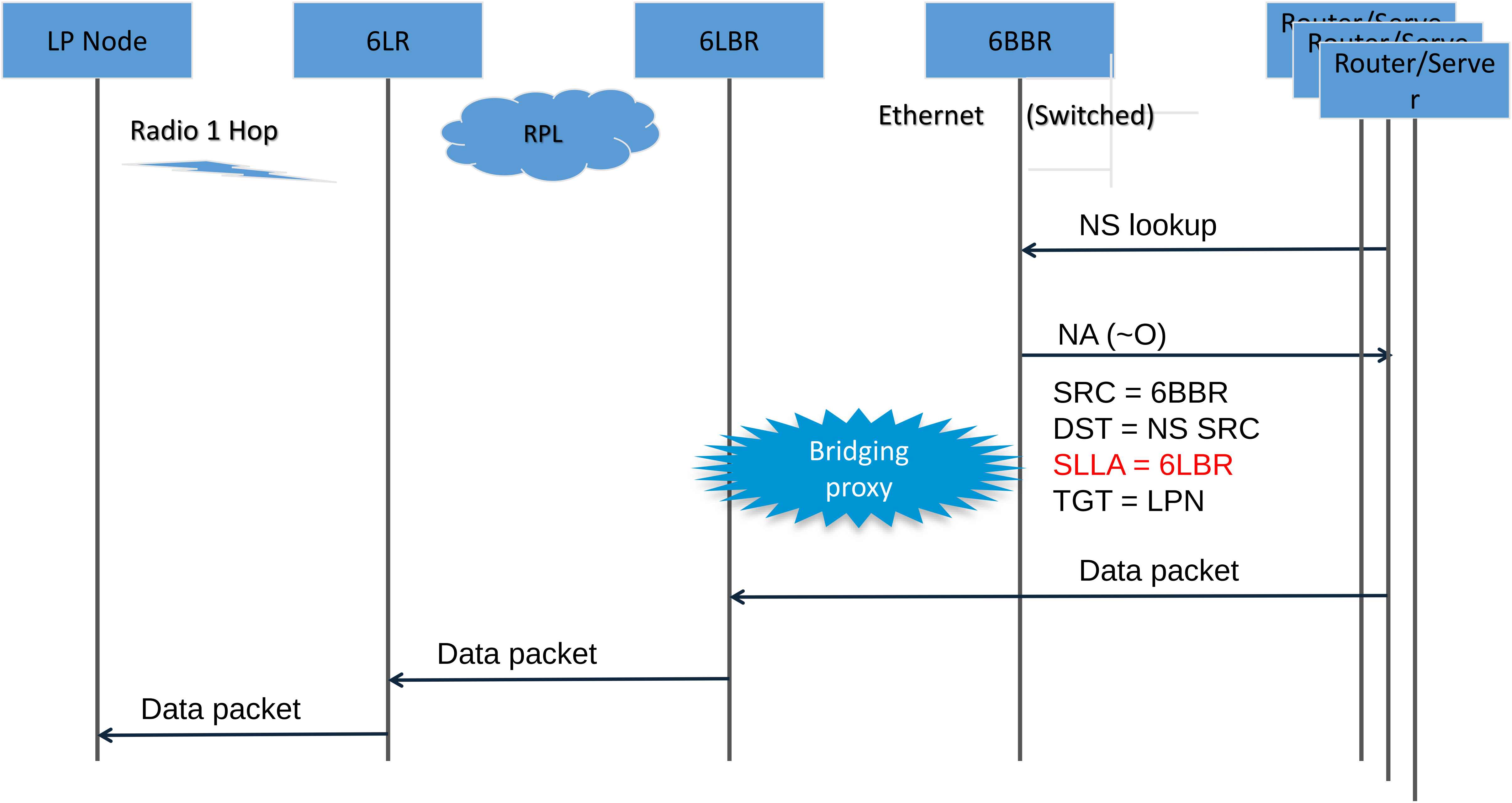
NA (ARO)

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

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

* Omitted in general
** link local


LP Node
6LR
6LBR
6BBR
Router/Serve
Router/Serve
Router/Server
Radio 1 Hop
RPL
Ethernet
NS lookup
NA (~O)
SRC = 6BBR
DST = NS SRC
SLLA = 6BBR
TGT = LPN
Routing proxy
Data packet
Data packet
Data packet
Data packet



LP Node

6LR

6LBR

6BBR

Router/Serve
r

Radio 1 Hop

RPL

Ethernet (Switched)

NS lookup

NA (~O)

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

Bridging proxy

Data packet

Data packet

Data packet

draft-thubert-6lo-unicast-lookup

P. Thubert

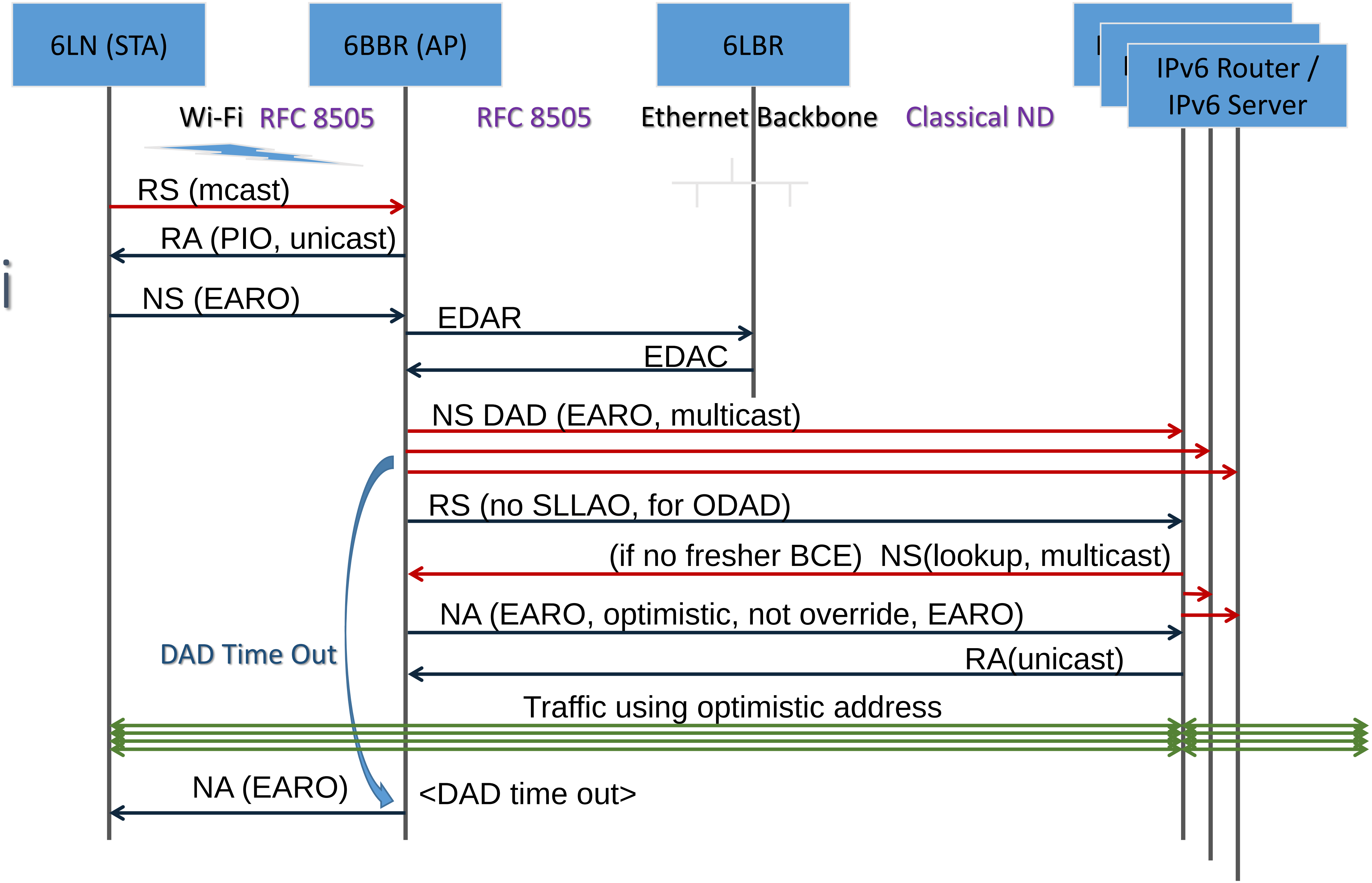
Unicast Lookup

- Backbone Routers operate as a distributed 6LBR
  - Use RFC4861/4862 on the backbone
  - EARO in NS/NA to differentiate mobility from duplication
- The new draft positions a 6LBR on the backbone
  - Can be used by 6LBRs and any node to register addresses
  - Can reply to a DAD or an Address lookup for a registered address
  - Avoids multicast on the backbone for scalability
  - Saves time (e.g., IEEE Std 802.11ai FILS aka Tokyo Station scenario)

New stuff

- New « Address Mapping » message using same ICMP Type as EDAR
- New Code Prefix to differentiate Address Mapping from EDAR
- New EARO Status «Not Found»: *The address is not present in the Address Registrar*
- Added SLLAO/TLLAO to EDAR/EDAC and Address Mapping msg.
- New capability in 6CIO to advertise 6LBR with Address Mapping

e.g., Wi-Fi FILS flow



6LN (STA)

6BBR (AP)

6LBR

IPv6 Router / IPv6 Server

Wi-Fi RFC 8505

RFC 8505

Ethernet Backbone

Classical ND

RS (mcast)

RA (PIO, unicast)

NS (EARO)

EDAR

EDAC

NS DAD (EARO, multicast)

RS (no SLLAO, for ODAD)

(if no fresher BCE) NS(lookup, multicast)

NA (EARO, optimistic, not override, EARO)

RA(unicast)

DAD Time Out

Traffic using optimistic address

NA (EARO)

<DAD time out>

Asks

- Reviews
- Rapid adoption
  - This is a simple draft and a logical complement
  - Need a draft-ietf for a reference in IEEE Std 802.11
  - Saves time (e.g., IEEE Std 802.11ai FILS aka Tokyo Station scenario)

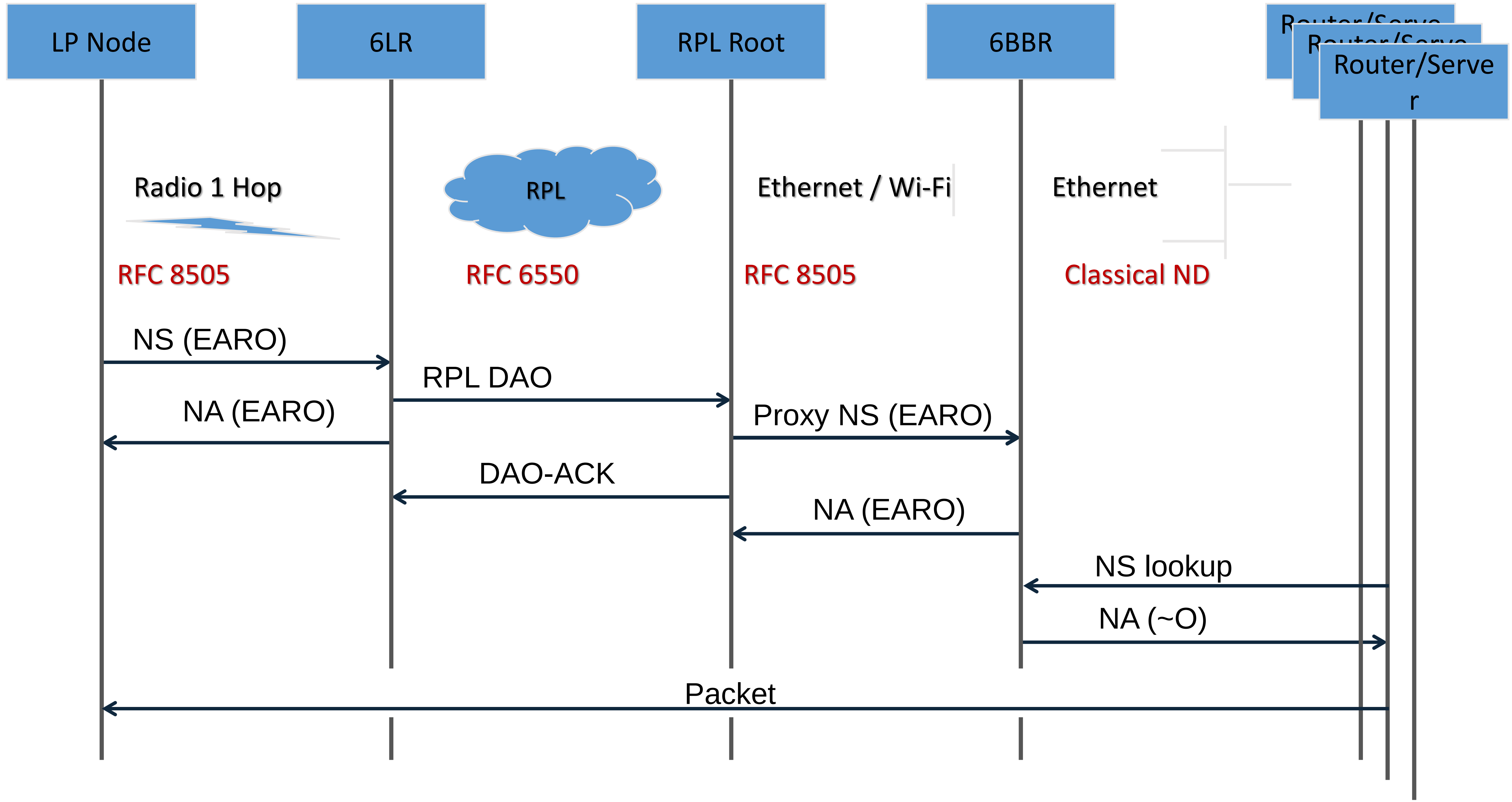
Questions

draft-thubert-roll-unaware-leaves

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



LP Node

6LR

RPL Root

6BBR

Router/Serve
r

Radio 1 Hop

RPL

Ethernet / Wi-Fi

Ethernet

RFC 8505

RFC 6550

RFC 8505

Classical ND

NS (EARO)

RPL DAO

NA (EARO)

Proxy NS (EARO)

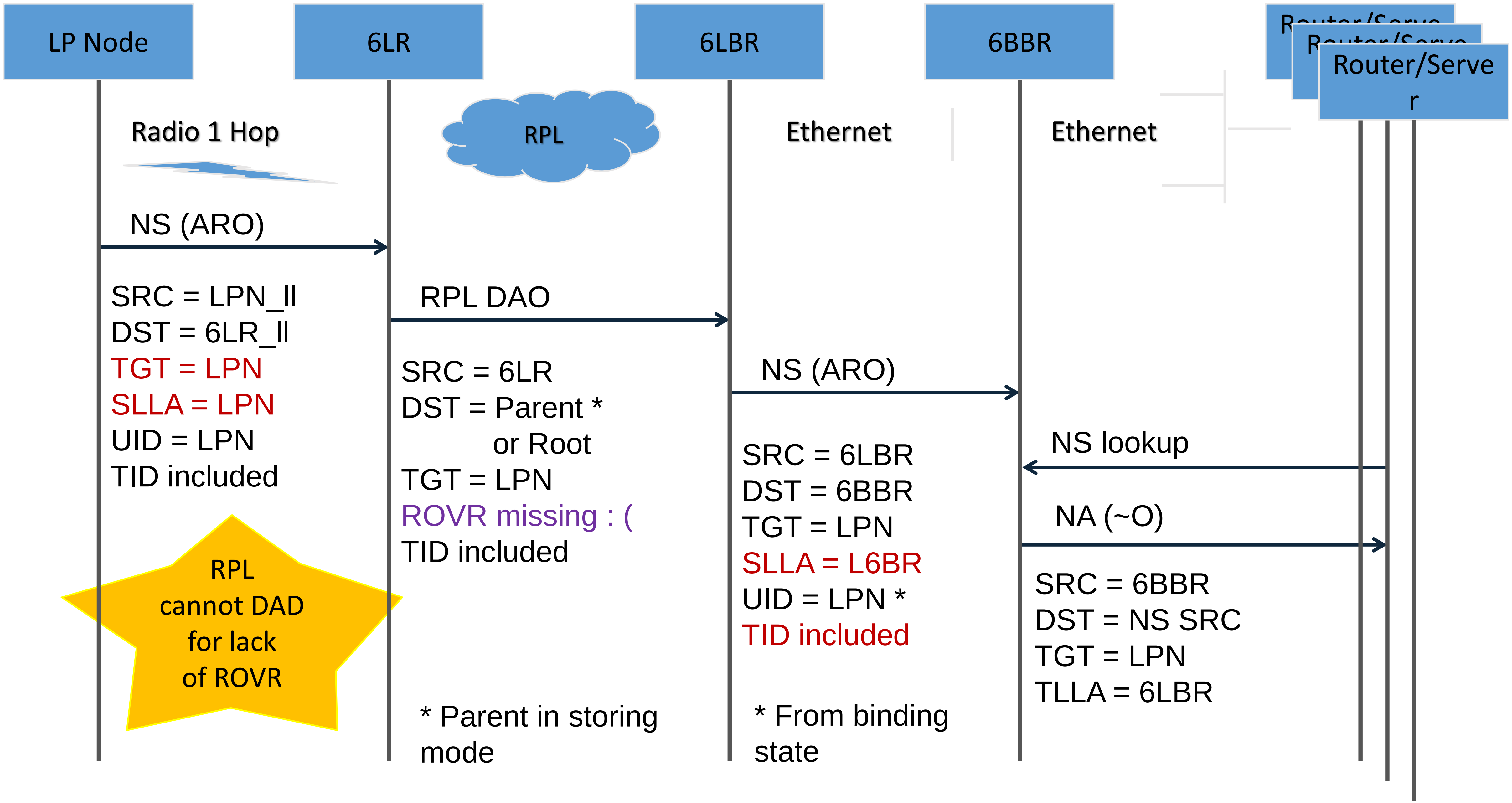
DAO-ACK

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

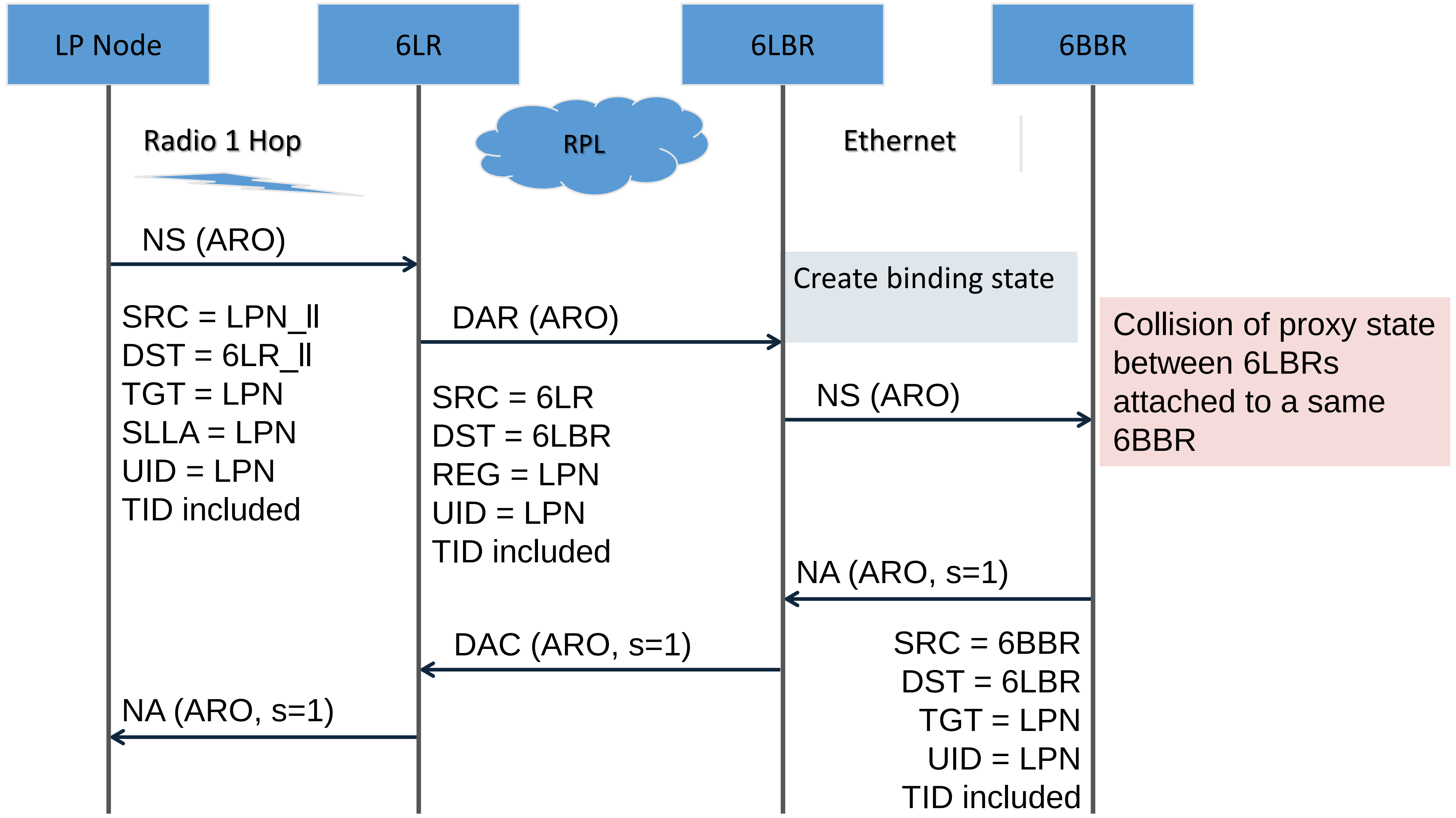
* From binding state

NS lookup

NA (~O)

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

Duplicate registration



LP Node

6LR

6LBR

6BBR

Radio 1 Hop

RPL

Ethernet

NS (ARO)

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

DAR (ARO)

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

Create binding state

NS (ARO)

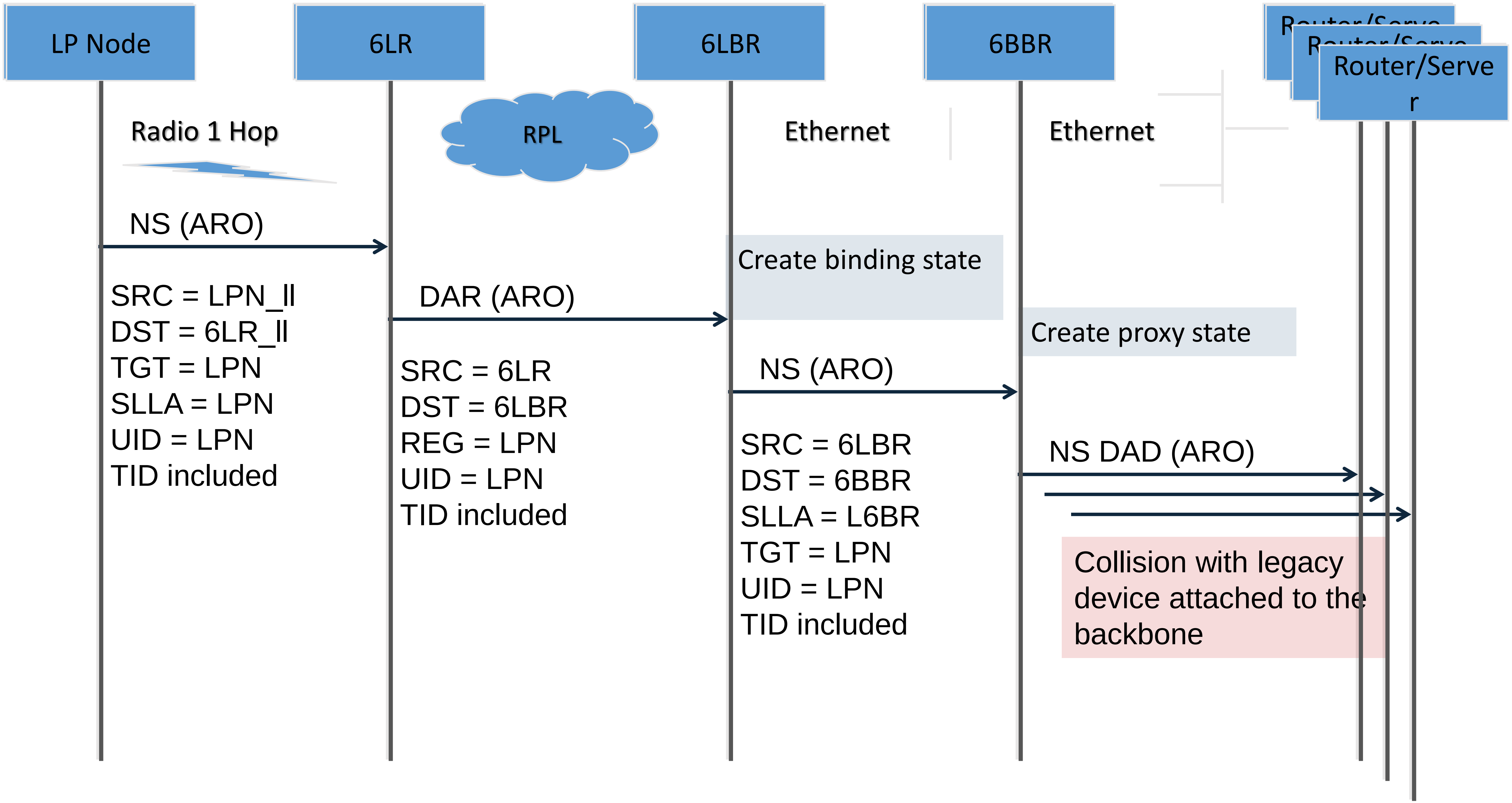
Collision of proxy state between 6LBRs attached to a same 6BBR

NA (ARO, s=1)

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

DAC (ARO, s=1)

NA (ARO, s=1)



LP Node

6LR

6LBR

6BBR

Router/Serve
r

Radio 1 Hop

RPL

Ethernet

Ethernet

NS (ARO)

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

DAR (ARO)

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

Create binding state

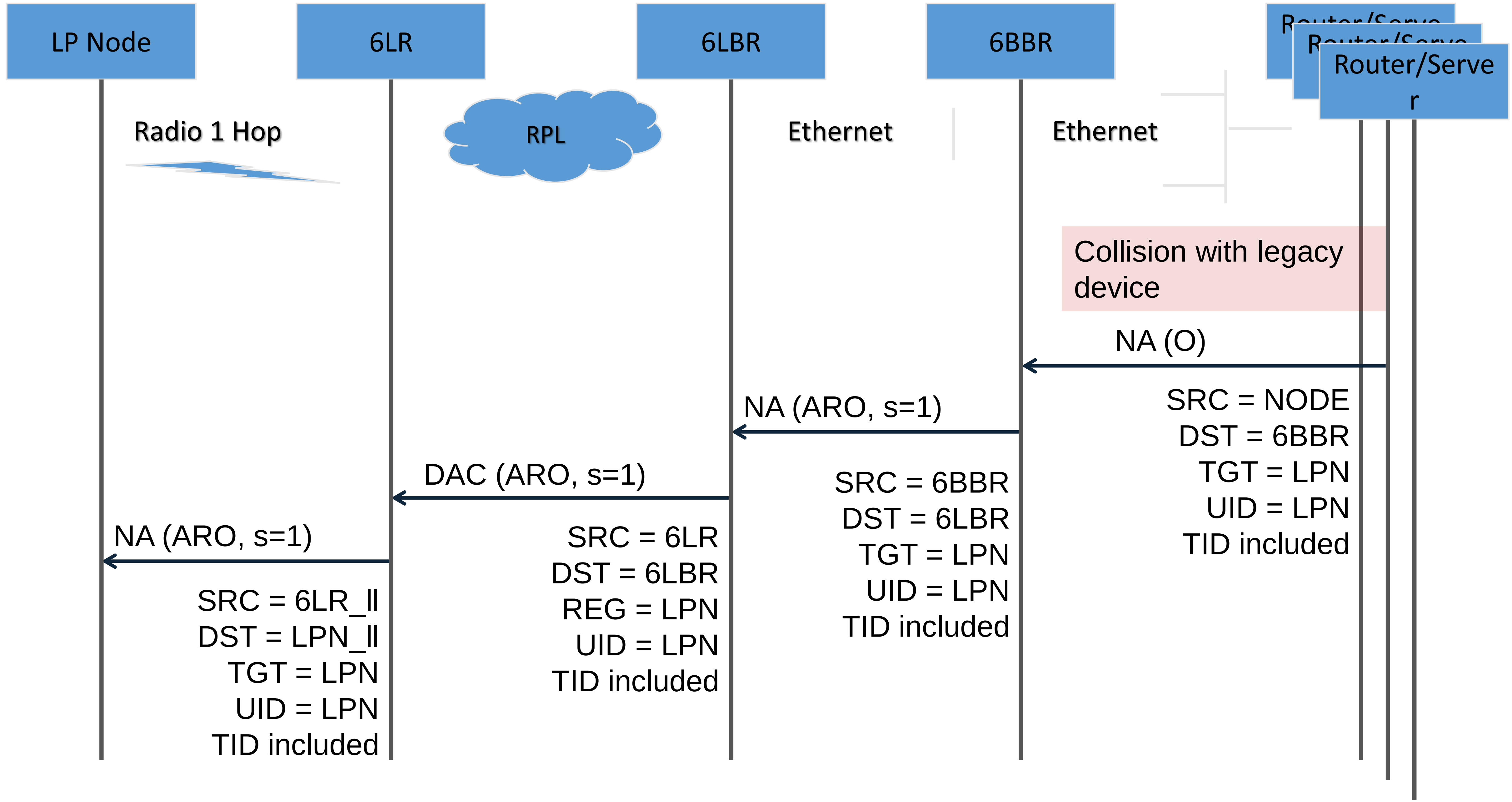
NS (ARO)

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

Create proxy state

NS DAD (ARO)

Collision with legacy device attached to the backbone



LP Node

6LR

6LBR

6BBR

Router/Serve
r

Radio 1 Hop

RPL

Ethernet

Ethernet

Collision with legacy device

NA (O)

SRC = NODE
DST = 6BBR
TGT = LPN
UID = LPN
TID included

NA (ARO, s=1)

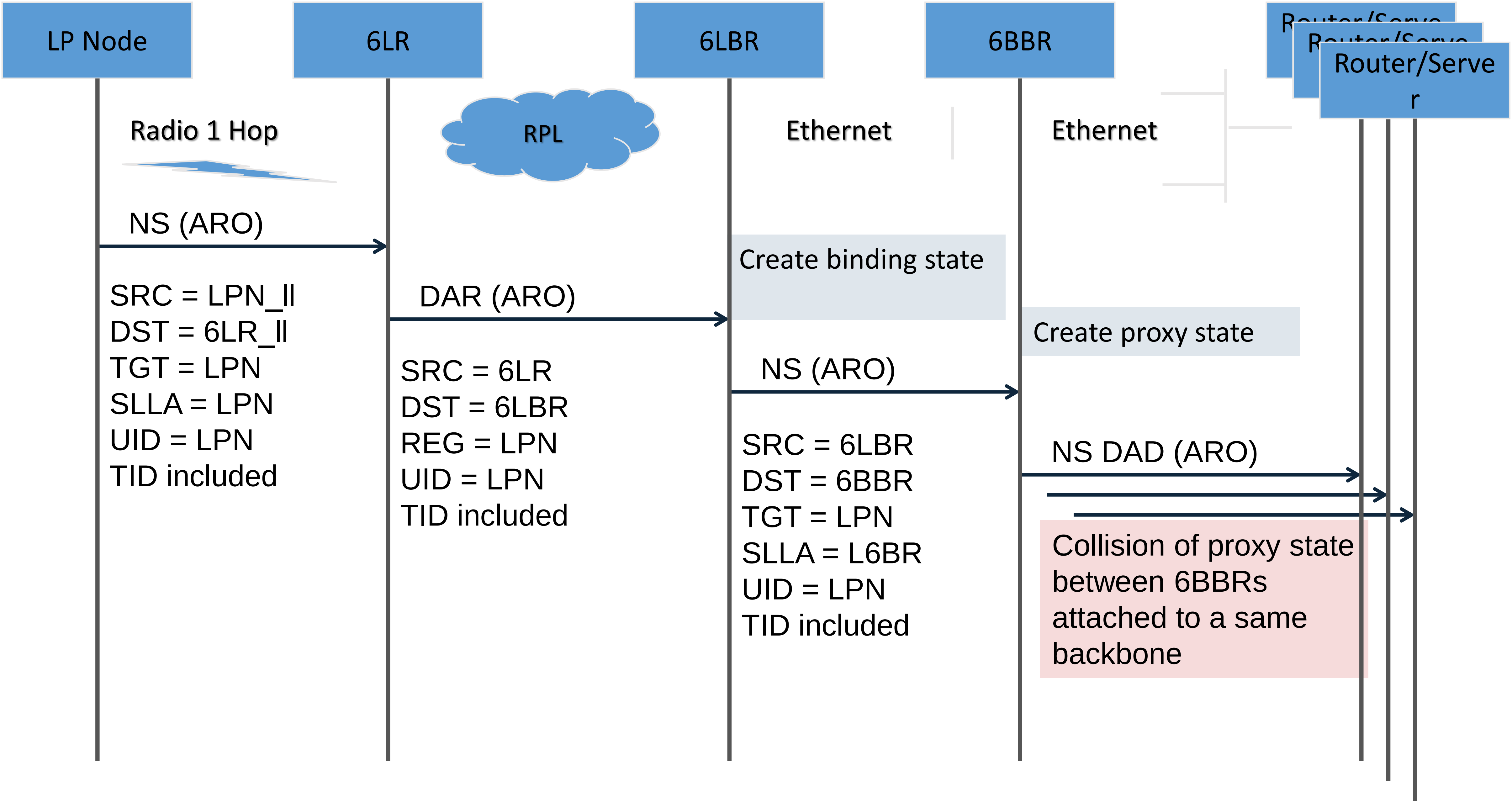
SRC = 6BBR
DST = 6LBR
TGT = LPN
UID = LPN
TID included

DAC (ARO, s=1)

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

NA (ARO, s=1)

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



LP Node

6LR

6LBR

6BBR

Router/Serve
r

Radio 1 Hop

RPL

Ethernet

Ethernet

NS (ARO)

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

DAR (ARO)

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

Create binding state

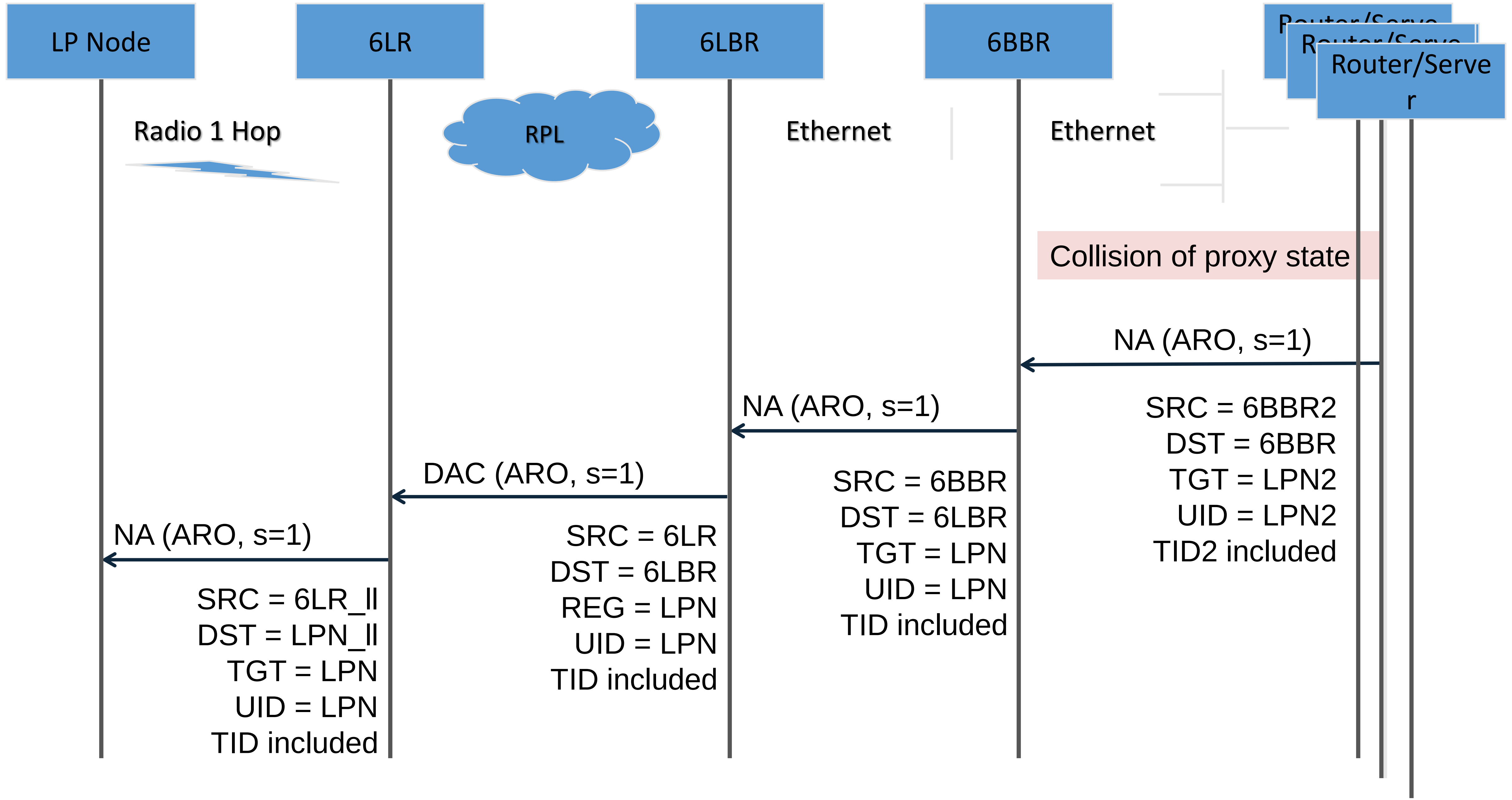
NS (ARO)

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

Create proxy state

NS DAD (ARO)

Collision of proxy state between 6BBRs attached to a same backbone



LP Node

6LR

6LBR

6BBR

Router/Serve
r

Radio 1 Hop

RPL

Ethernet

Ethernet

Collision of proxy state

NA (ARO, s=1)

SRC = 6BBR2
DST = 6BBR
TGT = LPN2
UID = LPN2
TID2 included

NA (ARO, s=1)

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

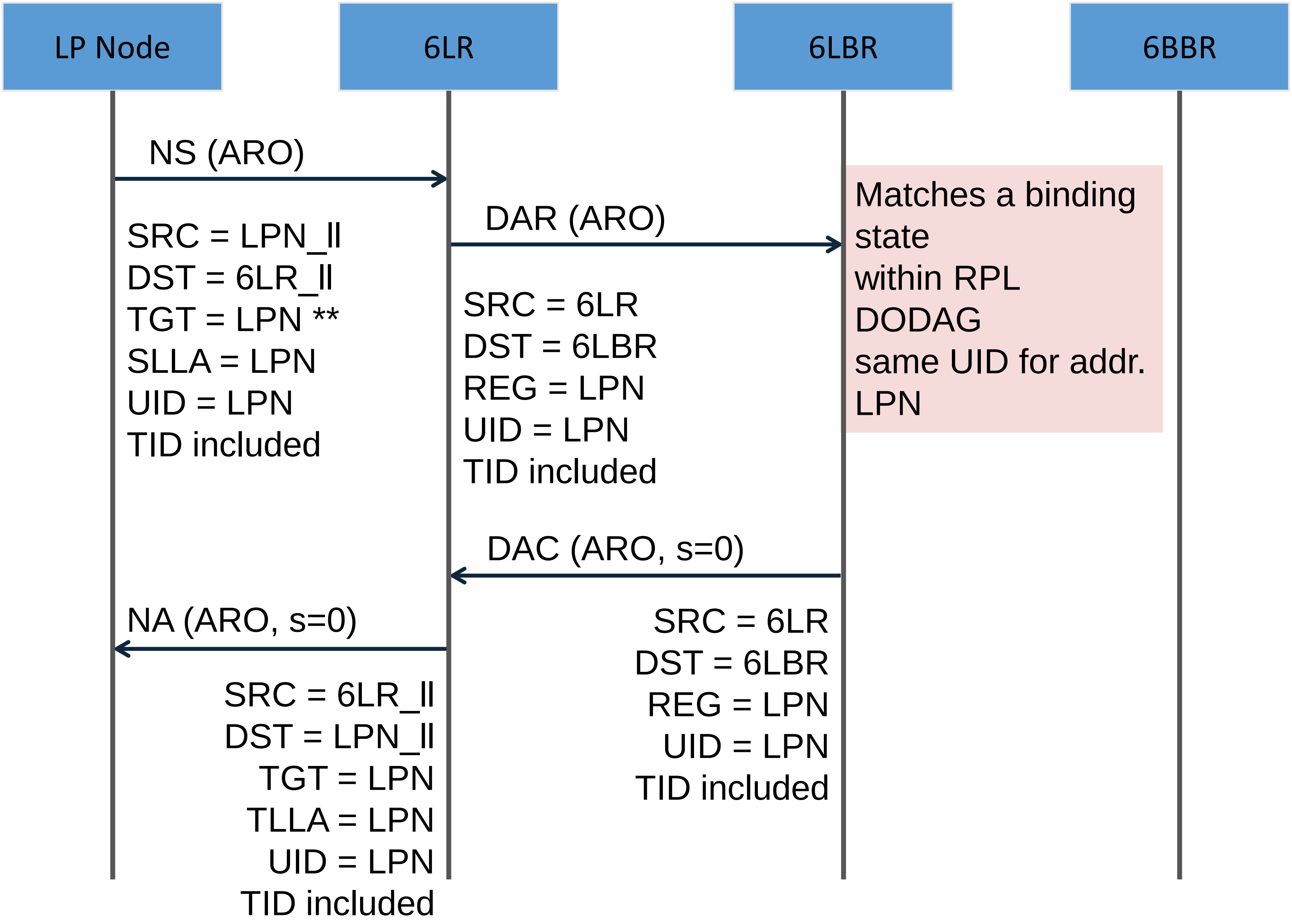
DAC (ARO, s=1)

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

NA (ARO, s=1)

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

Mobility



LP Node

6LR

6LBR

6BBR

NS (ARO)

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

DAR (ARO)

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

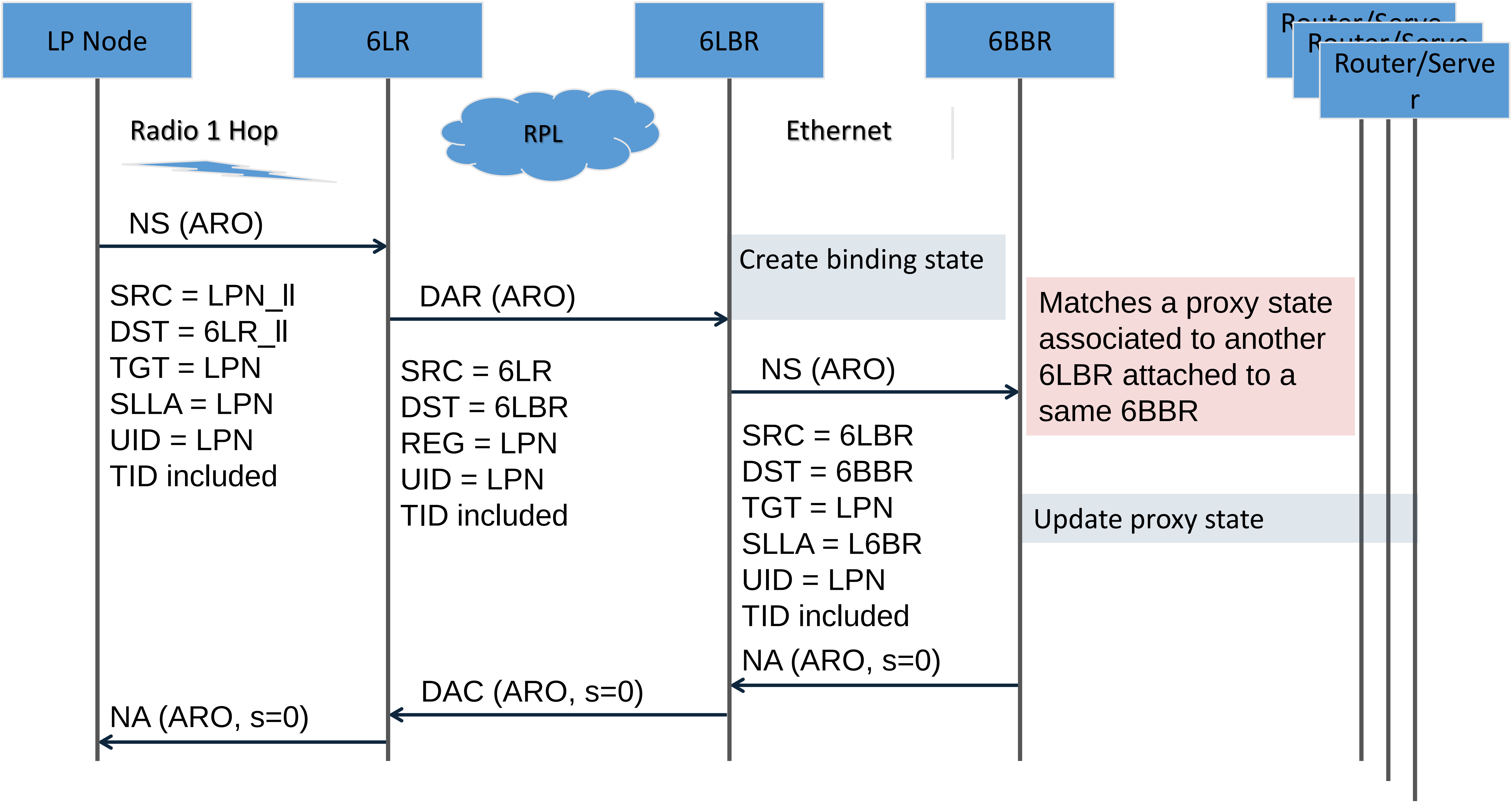
Matches a binding state
within RPL DODAG
same UID for addr. LPN

DAC (ARO, s=0)

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

NA (ARO, s=0)

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



LP Node

6LR

6LBR

6BBR

Router/Serve
r

Radio 1 Hop

RPL

Ethernet

NS (ARO)

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

DAR (ARO)

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

Create binding state

NS (ARO)

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

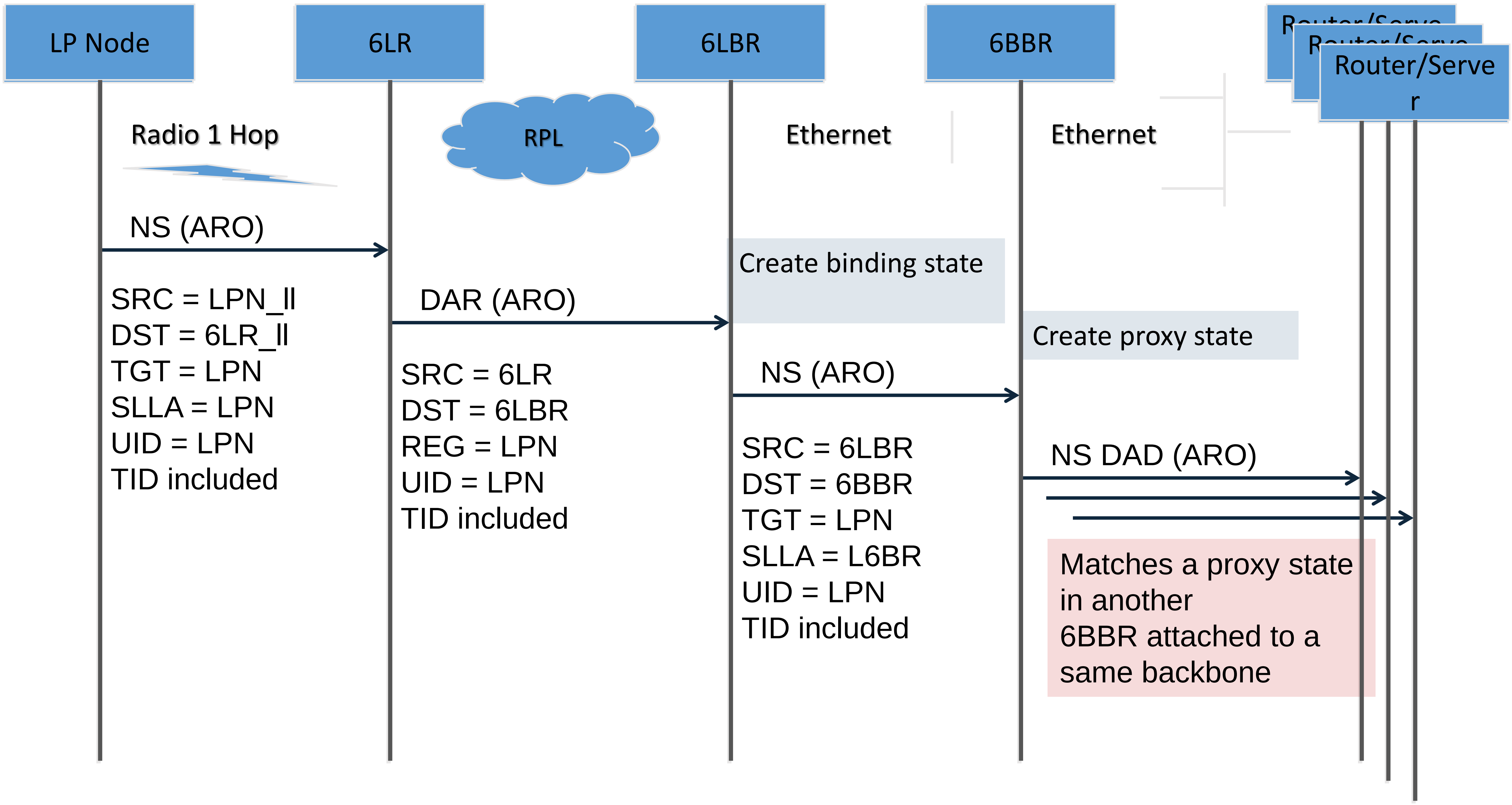
Matches a proxy state associated to another 6LBR attached to a same 6BBR

Update proxy state

NA (ARO, s=0)

DAC (ARO, s=0)

NA (ARO, s=0)



LP Node

6LR

6LBR

6BBR

Router/Serve r

Radio 1 Hop

RPL

Ethernet

Ethernet

NS (ARO)

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

DAR (ARO)

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

Create binding state

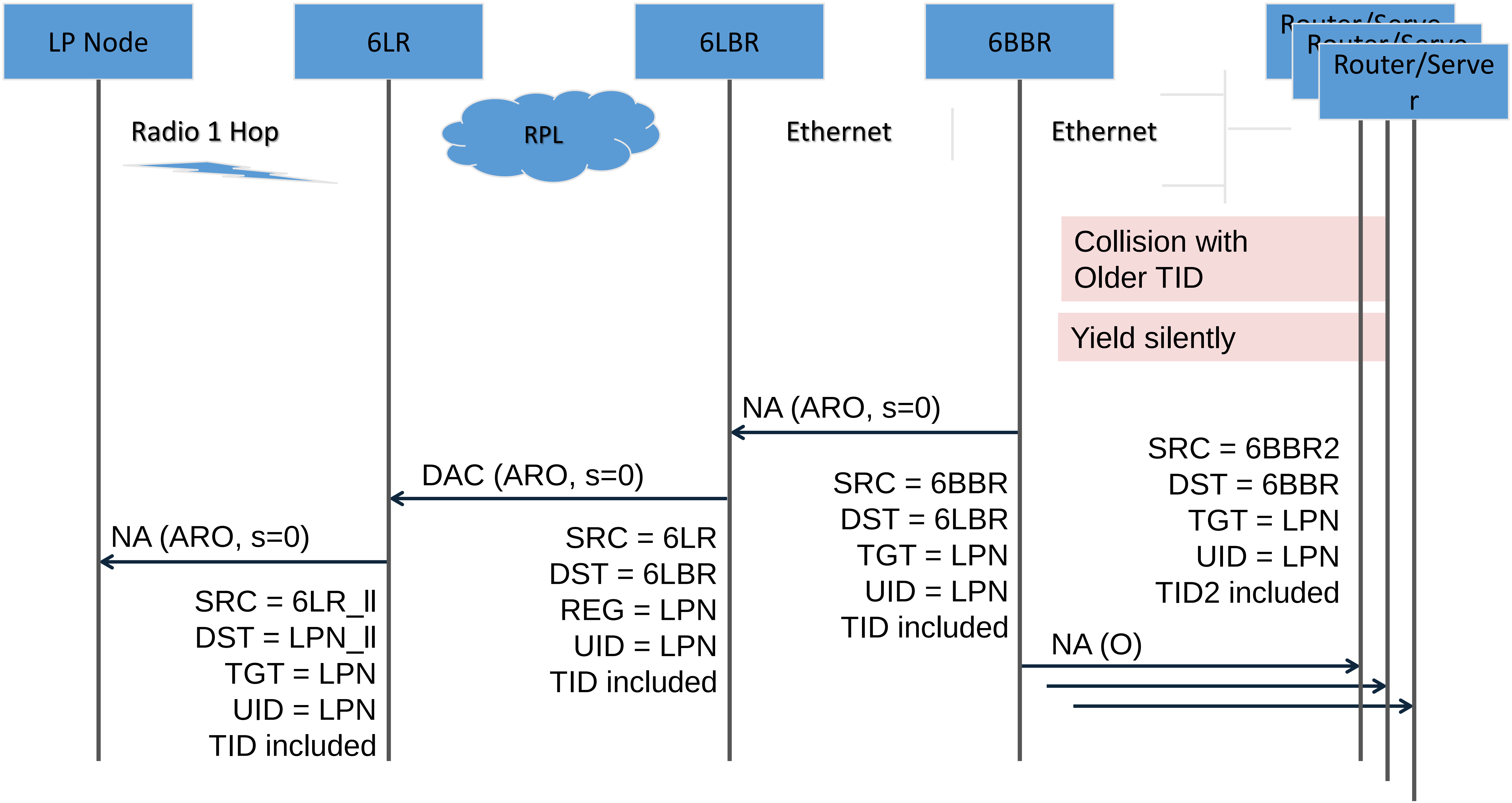
NS (ARO)

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

Create proxy state

NS DAD (ARO)

Matches a proxy state in another 6BBR attached to a same backbone



LP Node

6LR

6LBR

6BBR

Router/Serve

Router/Serve

Router/Serve
r

Radio 1 Hop

RPL

Ethernet

Ethernet

Collision with
Older TID

Yield silently

NA (ARO, s=0)

SRC = 6BBR2
DST = 6BBR
TGT = LPN
UID = LPN
TID2 included

DAC (ARO, s=0)

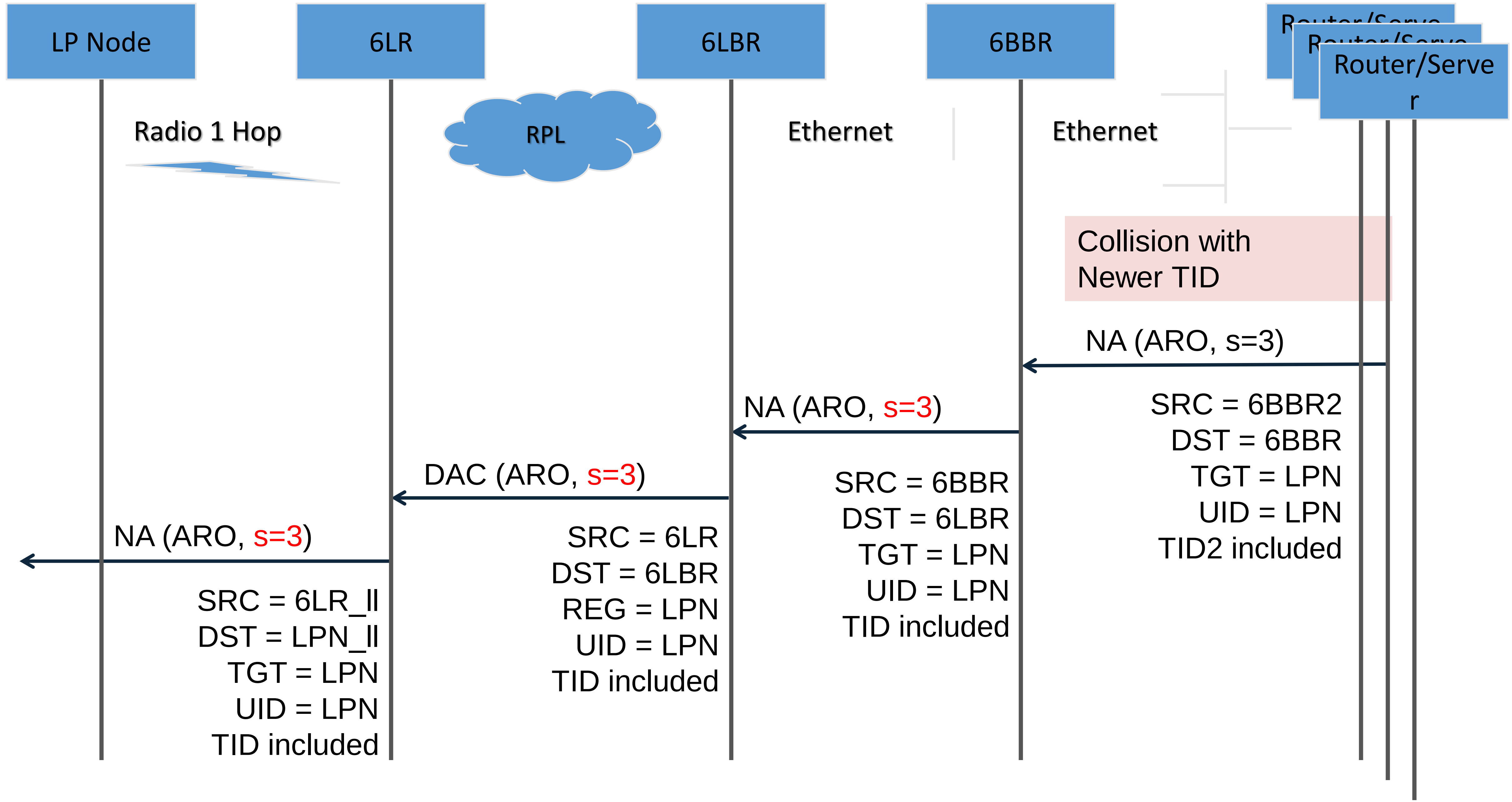
SRC = 6BBR
DST = 6LBR
TGT = LPN
UID = LPN
TID included

NA (ARO, s=0)

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

NA (O)

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



LP Node

6LR

6LBR

6BBR

Router/Serve
r

Radio 1 Hop

RPL

Ethernet

Ethernet

Collision with
Newer TID

NA (ARO, s=3)

SRC = 6BBR2
DST = 6BBR
TGT = LPN
UID = LPN
TID2 included

NA (ARO, s=3)

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

DAC (ARO, s=3)

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

NA (ARO, s=3)

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