

BESS  
Internet-Draft  
Intended status: Standards Track  
Expires: 4 August 2022

P. Thubert, Ed.  
Cisco Systems  
A. Przygienda  
Juniper Networks, Inc  
J. Tantsura  
Microsoft  
31 January 2022

Secure EVPN MAC Signaling  
draft-thubert-bess-secure-evpn-mac-signaling-03

## Abstract

This specification adds attributes to EVPN to carry IPv6 address metadata learned from [RFC 8505](#) and [RFC 8928](#) so as to maintain a synchronized copy of the 6LoWPAN ND registrar at each EVPN router and perform locally a unicast IPv6 ND service for address lookup and duplicate address detection.

## Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 4 August 2022.

## Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the document authors. All rights reserved.

Internet-Draft

EVPN Secure MAC

January 2022

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the [Trust Legal Provisions](#) and are provided without warranty as described in the Revised BSD License.

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Terminology . . . . .	<a href="#">4</a>
<a href="#">2.1.</a>	Requirements Language . . . . .	<a href="#">4</a>
<a href="#">2.2.</a>	Glossary . . . . .	<a href="#">4</a>
<a href="#">2.3.</a>	References . . . . .	<a href="#">5</a>
<a href="#">3.</a>	6LoWPAN Neighbor Discovery . . . . .	<a href="#">6</a>
<a href="#">3.1.</a>	IPv6 Interface, Link, and Subnet . . . . .	<a href="#">6</a>
<a href="#">3.2.</a>	<a href="#">RFC 6775</a> Address Registration . . . . .	<a href="#">10</a>
<a href="#">3.3.</a>	<a href="#">RFC 8505</a> Extended Address Registration . . . . .	<a href="#">10</a>
<a href="#">3.3.1.</a>	R Flag . . . . .	<a href="#">11</a>
<a href="#">3.3.2.</a>	TID, "I" Field and Opaque Fields . . . . .	<a href="#">11</a>
<a href="#">3.3.3.</a>	Status . . . . .	<a href="#">12</a>
<a href="#">3.3.4.</a>	Route Ownership Verifier . . . . .	<a href="#">12</a>
<a href="#">3.3.5.</a>	Anycast and Multicast Addresses . . . . .	<a href="#">13</a>
<a href="#">3.4.</a>	<a href="#">RFC 8505</a> Extended DAR/DAC . . . . .	<a href="#">13</a>
<a href="#">3.5.</a>	<a href="#">RFC 7400</a> Capability Indication Option . . . . .	<a href="#">14</a>
<a href="#">4.</a>	Extending 6LoWPAN ND . . . . .	<a href="#">15</a>
<a href="#">4.1.</a>	Use of the R flag in NA . . . . .	<a href="#">15</a>
<a href="#">4.2.</a>	Distributing the 6LBR . . . . .	<a href="#">15</a>
<a href="#">4.3.</a>	Unicast Address Lookup with the 6LBR . . . . .	<a href="#">19</a>
<a href="#">5.</a>	Requirements on the EVPN-Unaware Host . . . . .	<a href="#">25</a>
<a href="#">5.1.</a>	Support of 6LoWPAN ND . . . . .	<a href="#">25</a>
<a href="#">6.</a>	Enhancements to EVPN . . . . .	<a href="#">26</a>
<a href="#">6.1.</a>	Updated ARP/ND Extended Community . . . . .	<a href="#">28</a>
<a href="#">6.2.</a>	Updated Mobility Extended Community . . . . .	<a href="#">30</a>
<a href="#">6.3.</a>	Extended ROVR MAC Procedures . . . . .	<a href="#">31</a>
<a href="#">7.</a>	Protocol Operations . . . . .	<a href="#">32</a>
<a href="#">8.</a>	Security Considerations . . . . .	<a href="#">42</a>
<a href="#">9.</a>	IANA Considerations . . . . .	<a href="#">42</a>
<a href="#">9.1.</a>	MAC Mobility Extended Community Flags . . . . .	<a href="#">42</a>
<a href="#">9.2.</a>	ARP/ND Extended Community Flags . . . . .	<a href="#">43</a>
<a href="#">10.</a>	Acknowledgments . . . . .	<a href="#">43</a>

<a href="#">11. Normative References</a>	<a href="#">43</a>
<a href="#">12. Informative References</a>	<a href="#">45</a>
Authors' Addresses	<a href="#">46</a>

## [1. Introduction](#)

"Registration Extensions for IPv6 over 6LoWPAN Neighbor Discovery" [[RFC8505](#)] (ND) provides a zeroconf routing-agnostic Host-to-Router Link-Local interface for Stateful Address Autoconfiguration. "Address-Protected Neighbor Discovery for Low-Power and Lossy Networks" [[RFC8928](#)] (AP-ND) adds a zeroconf anti-theft protection that protects the ownership of the autoconfigured address with autoconfigured proof of ownership called a Registration Ownership Verifier (ROVR).

[[RFC8505](#)] enables the host to claim an IPv6 address and obtain reachability services for that address. It is already used to inject host routes in RPL [[RFC9010](#)] and RIFT "Routing in Fat Trees" [[RIFT](#)], and to maintain a proxy-ND state in a backbone router [[RFC8929](#)]; this specification extends its applicability to the case of Ethernet Virtual Private Network (EVPN).

[[RFC8505](#)] specifies a unicast address registration mechanism that enables the host called a 6LowPAN Node (6LN) to install a ND binding state in the 6LowPAN Router (6LR) that can serve as Neighbor Cache Entry (NCE), though it is not operated as a cache. The protocol provides the means to reject the registration in case of address duplication. It also enables to discriminate mobility from multihoming. [[RFC8928](#)] adds the capability to verify the ownership of the address and prevent an attacker from stealing and/or impersonating an address.

[[RFC8505](#)] defines the 6LoWPAN Border Router (6LBR) as an abstract address registrar that provides authoritative service for Address Registration and duplicate detection. The 6LBR stores address metadata that is obtained during the Address Registration, including an owner ID and a sequence counter. As part of the process of a new Address Registration, the 6LR queries the 6LBR for existing metadata related to the address being registered. This enables in particular to detect a duplication and reject the registration. This

specification extends the 6LBR abstract data model to store the Link Layer Address (LLA) of the Registering Node. This enables the 6LBR to perform locally, and using unicast communication, the IPv6 ND services of address lookup and duplicate address detection.

The [[RFC8505](#)] address registrar can be centralized, but it can also be distributed and maintained synchronized using a routing protocol. This specification adds attributes to EVPN to carry the IPv6 address metadata learned from [[RFC8505](#)] so as to maintain a synchronized copy of the 6LBR abstract data at each EVPN router.

## [2.](#) Terminology

### [2.1.](#) Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [BCP 14](#) [[RFC2119](#)] [[RFC8174](#)] when, and only when, they appear in all capitals, as shown here.

### [2.2.](#) Glossary

This document uses the following acronyms:

6CIO Capability Indication Option [[RFC7400](#)]  
6LN: 6LoWPAN Node (the Host) [[RFC6775](#)]  
6LR: 6LoWPAN router (the router) [[RFC6775](#)]  
6LBR: 6LoWPAN Border router [[RFC6775](#)]  
AMC: Address Mapping Confirmation [[UNICAST-LOOKUP](#)]  
AMR: Address Mapping Request [[UNICAST-LOOKUP](#)]  
ARO Address Registration Option [[RFC6775](#)]  
CIP0: Crypto-ID Parameters Option  
DAD: Duplicate Address Detection [[RFC4862](#)]  
ICMPv6: Internet Control Message Protocol for IPv6  
DAC Duplicate Address Confirmation [[RFC6775](#)]  
DAR Duplicate Address Request [[RFC6775](#)]  
EDAC Extended Duplicate Address Confirmation [[RFC8505](#)]  
EDAR Extended Duplicate Address Request [[RFC8505](#)]  
EARO: Extended Address Registration Option [[RFC8505](#)]

EVPN: Ethernet VPN [[RFC7432](#)]  
LLA: Link-Layer Address (the MAC address on Ethernet)  
LLN Low-Power and Lossy Network [[RFC6550](#)]  
NA: Neighbor Advertisement [[RFC4861](#)]  
NCE: Neighbor Cache Entry [[RFC4861](#)]  
ND: Neighbor Discovery [[RFC4861](#)]  
NDPSO: Neighbor Discovery Protocol Signature Option  
NS: Neighbor Solicitation [[RFC4861](#)]  
RA: Router Advertisement [[RFC4861](#)]  
ROVR: Registration Ownership Verifier [[RFC8505](#)]  
TID: Transaction ID (a sequence counter in the EARO) [[RFC8505](#)]  
SLAAC: Stateless Address Autoconfiguration [[RFC4862](#)]  
SLLAO: Source Link-Layer Address Option [[RFC4861](#)]  
TLLAO: Target Link-Layer Address Option [[RFC4861](#)]  
ROVR MAC: MAC obtained from a host meeting requirements in [Section 5](#)  
Validated ROVR MAC: ROVR MAC validated by procedures specified in [[RFC8928](#)]  
ROVR Node: EVPN node capable of advertising ROVR MACs  
non-ROVR Node: EVPN node not supporting extensions defined in this

document.

VPN: Virtual Private Network

### [2.3](#). References

This document uses the terms Clos fabric and Fat Tree interchangeably, to refer to a folded spine-and-leaf topology as defined in the terminology section of "RIFT: Routing in Fat Trees" [[RIFT](#)].

The term "leaf" represents the access switch that connects the servers to the Fat Tree. The leaf is typically a Top-of-Rack (ToR) switch.

This specification uses the terms 6LN, 6LR and 6LBR to refer specifically to nodes that implement the said roles in [[RFC8505](#)] and does not expect other functionality such as 6LoWPAN Header Compression:

- \* In the context of this document, the 6LN is a server that advertises an address mapping using [[RFC8505](#)], and optionally protects its ownership with [[RFC8928](#)].

- \* The 6LR and 6LBR function are collapsed at the leaf and its state is synchronized with that of the EVPN functional support using an internal interface that is out of scope. That interface could be "pull" meaning that the 6LBR fetches the EVPN information when it needs it, or "push", meaning that any information that EVPN distributes is immediately fed in all the 6LBRs in all the leaves. Note that this is pure control plane and is not subject to abbreviating optimization as the FIB may be.

In this document, readers will encounter terms and concepts that are discussed in the following documents:

EVPN: "BGP MPLS-Based Ethernet VPN" [[RFC7432](#)] and "Network Virtualization Overlay Solution" [[RFC8365](#)],

Classical IPv6 ND: "Neighbor Discovery for IP version 6" [[RFC4861](#)] and "IPv6 Stateless Address Autoconfiguration" [[RFC4862](#)],

6LoWPAN ND: Neighbor Discovery Optimization for Low-Power and Lossy Networks [[RFC6775](#)], "Registration Extensions for 6LoWPAN Neighbor Discovery" [[RFC8505](#)], "Address Protected Neighbor Discovery for Low-power and Lossy Networks" [[RFC8928](#)], and "IPv6 Backbone Router" [[RFC8929](#)].

### [3.](#) 6LoWPAN Neighbor Discovery

6LoWPAN Neighbor Discovery defines a stateful address autoconfiguration mechanism for IPv6. 6LoWPAN ND enables to divorce the L3 abstractions for link and subnet from the characteristics of the L2 link and broadcast domain. It is applicable beyond its original field of IoT to any environment where the broadcast nature of the underlaying network should not be exploited, e.g., in the case of a wireless link where broadcast uses an excessive amount of spectrum, and a distributed cloud, where it may span too widely.

In contrast to Stateless Address Autoconfiguration (SLAAC) [[RFC4862](#)] which relies on broadcast for duplicate address detection (DAD) and address lookup, 6LoWPAN ND installs and maintains a state in the neighbors for the duration of their interaction. Though it is also

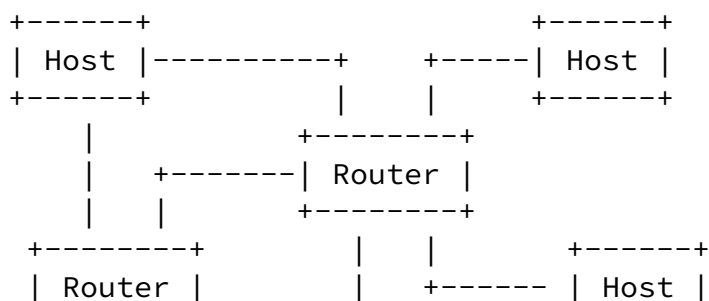
called a Neighbor Cache Entry (BCE) in [RFC6775], and in contrast with the the BCE in SLAAC, that state is not a cache that can be casually flushed and rebuilt. It must be installed proactively and refreshed periodically to maintain the connectivity and enable unicast-only operations.

This section goes through the 6LoWPAN ND network abstractions and mechanisms that this specification leverages, as a non-normative reference to the reader. The relevant normative text is to be found in [RFC6775], [RFC8505], and [RFC8928].

### 3.1. IPv6 Interface, Link, and Subnet

The typical abstraction for an IP Link with 6LoWPAN ND is a logical point-to-point (P2P) link between a node (a host or a router) and a router, regardless of the physical medium between the node and the router, which may or may not be shared with other nodes.

A Subnet is deployed over a mesh of nodes connected with those logical P2P Links, where routers form a connected dominating set as represented in Figure 1; the resulting aggregate is called a multilink subnet (MLSN). An MLSN may be only partially meshed, and the underlaying network is not expected to provide a multicast or a broadcast service across the subnet.



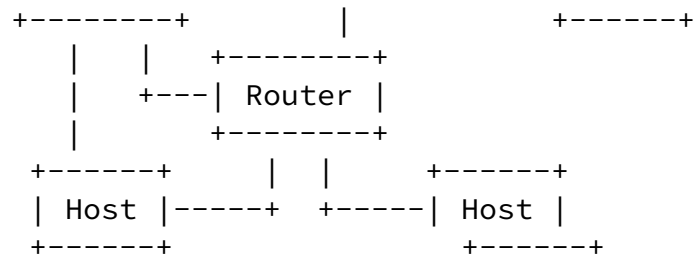


Figure 1: P2P Links in a Multilink Subnet

Consequently, the subnet model is not-on-link, meaning that the any-to-any connectivity across the subnet is ensured through L3 operations (routing or proxy) as opposed to transitive (any-to-any) reachability from L2. It also means that hosts do not lookup other nodes using IPv6 Neighbor Discovery but forward all their traffic via their connected routers. Which in turn means that only routers need to be discovered, which is done by sending Router Advertisement (RA) messages to all directly reachable nodes in the subnet, e.g., using a radio broadcast.

As illustrated in Figure 2, an IP interface bundles multiple sub-interfaces to connect the IP links between this node and peers in the same subnet, which is known as a point-to-multipoint (P2MP) interface.



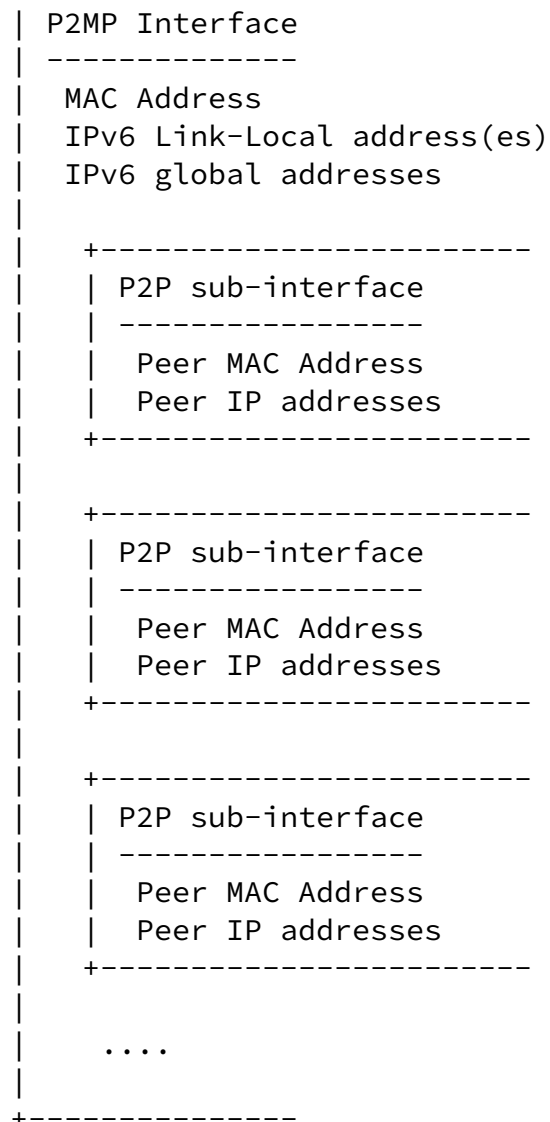


Figure 2: P2MP Interface

In the case of a 6LoWPAN radio, the IP Interface may be physical, and the P2P IP links are virtual based on discovered neighbor routers; the same model can apply when the node is connected via a switch to one or more routers.

In the case of a multihomed NIC card in a datacenter, the NIC is connected to several Top-of-Rack (ToR) switches acting as leaves in the fabric, over as many Ethernet physical interfaces. If the NIC provides a L2 virtual switch, then the stack can apply the same model as above, modeling the virtual port to the virtual switch as a P2MP interface.

On the other hand, if the NIC provides a virtual router, then Ethernet ports are L3 ports and the physical link to the leaf is modeled as P2P. To form the P2MP interface, the router bundles (aggregates) the physical interfaces as the sub-interfaces of a single logical P2MP Link, as shown in Figure 3.

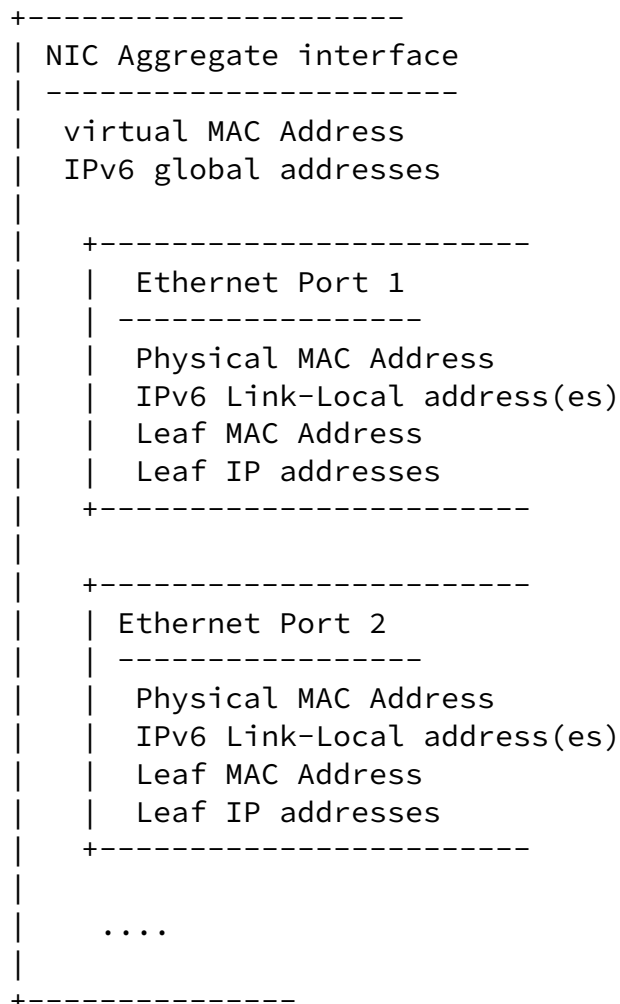


Figure 3: Logical P2MP Interface

To conserve the same model, it makes sense to configure the same (virtual) MAC address on all the physical interfaces, and use it for the purpose of IPv6 ND. In that case, the same MAC address is exposed as Link-layer Address (LLA) to both leaves for the NIC IP addresses, and the IPv6 address still appears as unicast. Note that the Link-Local addresses used to register the global IPv6 addresses to the leaf may be different but that does not affect the exposed

mapping.

When that is not possible, then the same IP address is advertised with the physical MAC address of each port as the LLA over that port. In that case, the global IPv6 address appears as anycast, and SHOULD be advertised as such, more in [Section 3.3.5](#).

### [3.2. RFC 6775](#) Address Registration

The classical "IPv6 Neighbor Discovery (IPv6 ND) Protocol" [[RFC4861](#)] [[RFC4862](#)] was defined for serial links and transit media such as Ethernet. It is a reactive protocol that relies heavily on multicast operations for Address Discovery (aka Lookup) and Duplicate Address Detection (DAD).

"Neighbor Discovery Optimizations for 6LoWPAN networks" [[RFC6775](#)] adapts IPv6 ND for operations over energy-constrained LLNs. The main functions of [[RFC6775](#)] are to proactively establish the Neighbor Cache Entry (NCE) in the 6LR and to prevent address duplication. To that effect, [[RFC6775](#)] introduces a new unicast Address Registration mechanism that contributes to reducing the use of multicast messages compared to the classical IPv6 ND protocol.

[[RFC6775](#)] defines a new Address Registration Option (ARO) that is carried in the unicast Neighbor Solicitation (NS) and Neighbor Advertisement (NA) messages between the 6LoWPAN Node (6LN) and the 6LoWPAN router (6LR). It also defines the Duplicate Address Request (DAR) and Duplicate Address Confirmation (DAC) messages between the 6LR and the 6LBR. In a Low-Power and Lossy Network (LLN), the 6LBR is the central repository of all the Registered Addresses in its domain and the authoritative source of truth for uniqueness and ownership.

### [3.3. RFC 8505](#) Extended Address Registration

"Registration Extensions for 6LoWPAN Neighbor Discovery" [[RFC8505](#)] updates [RFC 6775](#) into a generic Address Registration mechanism that can be used to access services such as routing and ND proxy. To that effect, [[RFC8505](#)] defines the Extended Address Registration Option (EARO), shown in Figure 4:

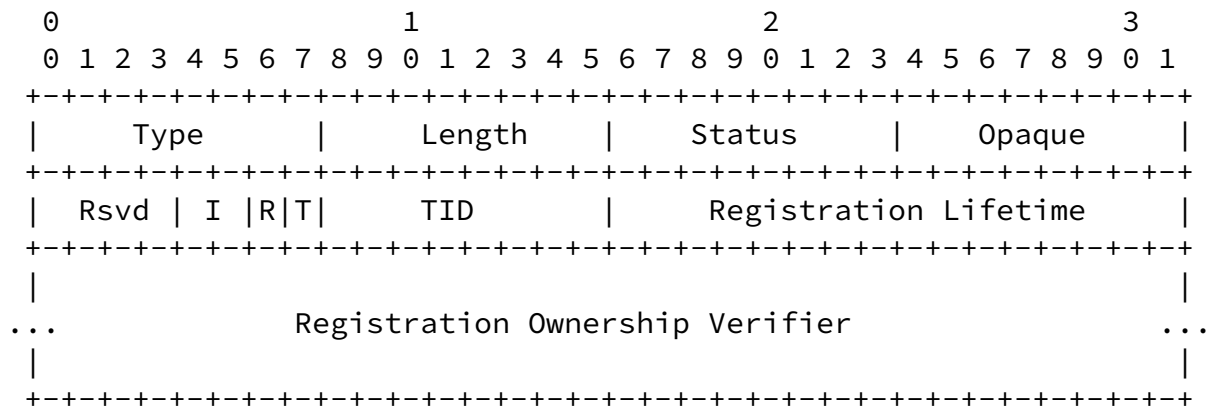


Figure 4: EARO Option Format

### 3.3.1. R Flag

[RFC8505] introduces the R Flag in the EARO. The Registering Node sets the R Flag to indicate whether the 6LR should ensure reachability for the Registered Address. If the R Flag is set to 0, then the Registering Node handles the reachability of the Registered Address by other means. In an EVPN network, this means that either it is a RAN that injects the route by itself or that it uses another EVPN router for reachability services.

This document specifies how the R Flag is used in the context of EVPN. An EVPN Host that implements the 6LN functionality from [RFC8505] requires reachability services for an IPv6 address if and only if it sets the R Flag in the NS(EARO) used to register the address to a 6LR acting as an EVPN border router. Upon receiving the NS(EARO), the EVPN router generates a BGP advertisement for the Registered Address if and only if the R flag is set to 1.

[RFC9010] specifies that the 'R' flag is set in the responded NA messages if and only if the route was installed. This specification echoes that behavior.

### [3.3.2.](#) TID, "I" Field and Opaque Fields

When the T Flag is set to 1, the EARO includes a sequence counter called Transaction ID (TID), that is needed to format the MAC Mobility Extended Community. This is the reason why the support of [\[RFC8505\]](#) by the Host, as opposed to only [\[RFC6775\]](#), is a prerequisite for this specification; this requirement is fully explained in [Section 5.1](#). The EARO also transports an Opaque field and an associated "I" field that describes what the Opaque field transports and how to use it.

This document specifies the use of the "I" field and the Opaque field by a Host.

### [3.3.3.](#) Status

The values of the EARO status are maintained by IANA in the Address Registration Option Status Values subregistry [\[IANA-EARO-STATUS\]](#) of the Internet Control Message Protocol version 6 (ICMPv6) Parameters registry.

[\[RFC6775\]](#) and [\[RFC8505\]](#) defined the original values whereas [\[RFC9010\]](#) reduced range to 64 values and reformatted the octet field to enable to transport an external error, e.g., coming from a routing protocol.

This specification uses the format expressed in [\[RFC9010\]](#). The value of 0 denotes an unqualified success, 1 indicates an address duplication, 3 a TID value that is outdated, and 4 is used in an asynchronous NA to indicate that 6LN should remove that address and possibly form new ones.

### [3.3.4.](#) Route Ownership Verifier

[Section 5.3 of \[RFC8505\]](#) introduces the Registration Ownership Verifier (ROVR) field of variable length from 64 to 256 bits. The ROVR is a replacement of the EUI-64 in the ARO [\[RFC6775\]](#) that was

used to identify uniquely an Address Registration with the Link-Layer address of the owner but provided no protection against spoofing.

"Address Protected Neighbor Discovery for Low-power and Lossy Networks" [[RFC8928](#)] leverages the ROVR field as a cryptographic proof of ownership to prevent a rogue third party from registering an address that is already owned. The use of ROVR field enables the 6LR to block traffic that is not sourced at an owned address.

This specification does not address how the protection by [[RFC8928](#)] could be extended for use in EVPN. On the other hand, it adds the ROVR to the BGP advertisement to share the state with the other routers via the Reflector (see [Section 6.1](#)), which means that the routers that are aware of the Host route are also aware of the ROVR associated to the Target Address, whether it is cryptographic and should be verified.

### [3.3.5.](#) Anycast and Multicast Addresses

"IPv6 Neighbor Discovery Multicast Address Registration" [[I-D.thubert-6lo-multicast-registration](#)] updates [[RFC8505](#)] to enable the address registration of IPv6 anycast and multicast addresses. From the host perspective, the registration is very similar to that of unicast addresses, but for a flag in the EARO that signals that the address is multicast or anycast.

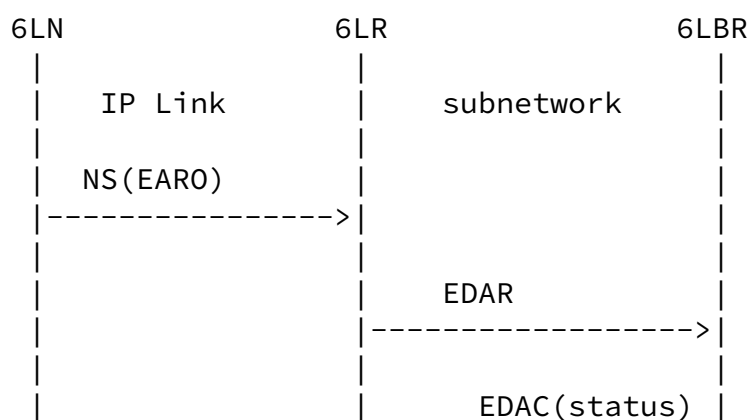
This procedure can be used as a replacement to "Multicast Listener Discovery Version 2 (MLDv2) for IPv6" [[RFC3810](#)] for source-independent multicast operation. As for unicast, the method saves the need for the host to listen to pollings from the router, and allows the host to sleep for periods of time.

### [3.4.](#) [RFC 8505](#) Extended DAR/DAC

[RFC8505] updates the DAR/DAC messages to EDAR/EDAC messages to carry

the ROVR field. The EDAR/EDAC exchange takes place between the 6LR to which the node registers an address, and the abstract 6LBR that stores the reference value for the ROVR and the TID associated to that address. It is triggered by an NS(EARO) message from a 6LN to the 6LR, to create, refresh, compare and delete the corresponding state in the 6LBR.

In the status returned with the EDAC message, the 6LBR indicates if the registration is accepted, should be challenged, or is duplicate. The status of 0 (success) indicates that the address is either new or that the current registration matches, and in particular that the ROVR at the 6LBR and the one in the EDAR message are identical.



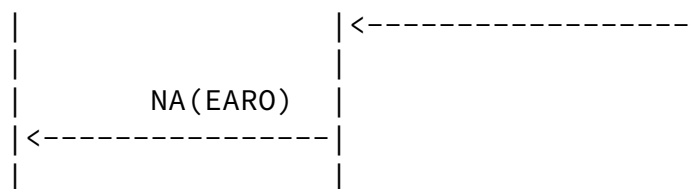


Figure 5: EDAR/EDAC flow

The EDAR/EDAC exchange is protected by the retry mechanism specified in [Section 8.2.6 of \[RFC6775\]](#), though in a data center, a duration significantly shorter than the default value of the Retransmission Timer [\[RFC4861\]](#) of 1 second may be sufficient to cover the round-trip delay between the 6R and the 6LBR.

With this specification, the 6LBR is distributed across the leaves, and all the leaves where an address is currently registered maintain a full 6LBR state for the address, aka local state in the following text. The specification leverages the EDAR/EDAC exchange to ensure that a leaf (acting as a 6LR) that needs to create a 6LBR state for a new registration has the same value for the ROVR as any 6LBR already serving that address on another leaf. At the same time, the specification avoids placing full ROVR information in BGP so 1) it is not observable by a potential attacker and 2) the new attributes remain reasonably small.

### [3.5. RFC 7400](#) Capability Indication Option

"6LoWPAN-GHC: Generic Header Compression for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)" [\[RFC7400\]](#) defines the 6LoWPAN Capability Indication Option (6CIO) that enables a node to expose its capabilities in router Advertisement (RA) messages.

[\[RFC8505\]](#) defines a number of bits in the 6CIO, in particular:

- L: Node is a 6LR.
- E: Node is an IPv6 ND Registrar -- i.e., it supports registrations

based on EARO.

- P: Node is a Routing Registrar, -- i.e., an IPv6 ND Registrar that also provides reachability services for the Registered Address.



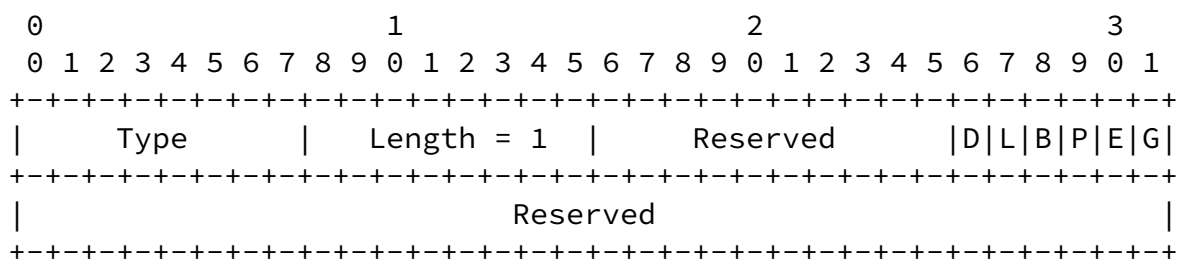


Figure 6: 6CIO flags

A 6LR that provides reachability services for a Host in an EVPN network as specified in this document includes a 6CIO in its RA messages and set the L, P and E flags to 1 as prescribed by [\[RFC8505\]](#).

#### 4. Extending 6LoWPAN ND

#### 4.1. Use of the R flag in NA

This document extends [RFC8928] and [RFC8505] as follows

This document also updates the behavior of a 6LR acting as EVPN router and of a 6LN acting as Host in the 6LoWPAN ND Address Registration as follows:

- \* The use of the R Flag is extended to the NA(EAR0) to confirm whether the route was installed.

## 4.2. Distributing the 6LBR

This specification enables to distribute the 6LBR at the edge of the EVPN network and collapse the 6LBR function with that of the EVPN support. In that model, the EVPN to 6LBR interaction becomes an internal interface, where each side informs the other in case of new information concerning an IP to Link-Layer Address (LLA) mapping. Since this is an internal interface, this specification makes no assumption on whether the 6LBR stores its own representation of the full EVPN state, which means that the EVPN support informs the 6LBR in case of any change on the EVPN side (this is called the push model, see Figure 13), or if the 6LBR queries the EVPN support when it does not have a mapping to satisfy a request (pull model, see Figure 12).

This specification leverages [[RFC8929](#)] that augments the abstract data model of the 6LBR to store the LLA associated with the registered address. Based on that additional state, the 6LBR in a leaf can communicate the mapping to the collocated EVPN function and respond to unicast address mapping lookups from the server side.

In an environment where the server ranges from a classical host to a more complex platform that runs a collection of virtual hosts interconnected by a virtual switch, but where the host-to-leaf interface remains at layer 2, the 6LR and the 6LBR functions can be collapsed in the leaf. The 6LR to 6LBR interaction also becomes an internal interface, and there is no need for EDAR/EDAC messages.

In that case, the MAC address associated to the Registered Address is indicated in the Target Link-Layer Address Option (TLLAO) in the NS message used for the registration, as shown in Figure 7. In the case of a pull model, if the 6LBR does not have a local state for the mapping, it queries the EVPN support to obtain the EVPN state if any. If a mapping is known then the 6LR/6LBR evaluates the registration for address duplication and other possible issues per [[RFC8505](#)]. Else (this is for a new mapping), if the registration is accepted, then the 6LBR notifies the EVPN support to inject a route type 2 in the fabric.

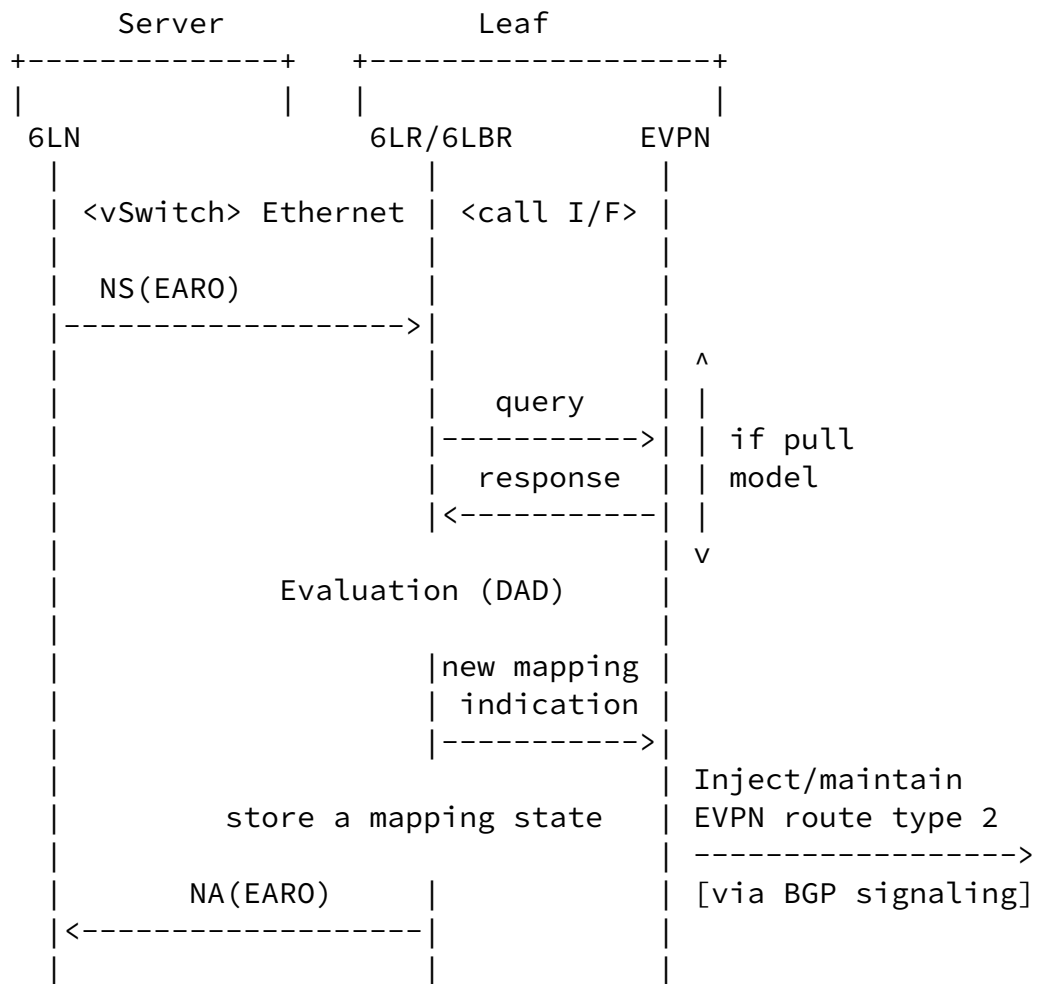


Figure 7: Direct Registration

In another type of deployment, the 6LR may be a virtual router in the server whereas the 6LBR runs in the leaf node. To address that case, the EDAR/EDAC may be used to communicate as shown in figure 5 of [\[RFC8505\]](#). This draft leverages the capability to insert IPv6 ND options in the EDAR and EDAC messages introduced in [\[RFC8929\]](#) to place a TLLAO that carries the MAC address associated to the Registered address in the EDAR and EDAC messages as shown in Figure 8:

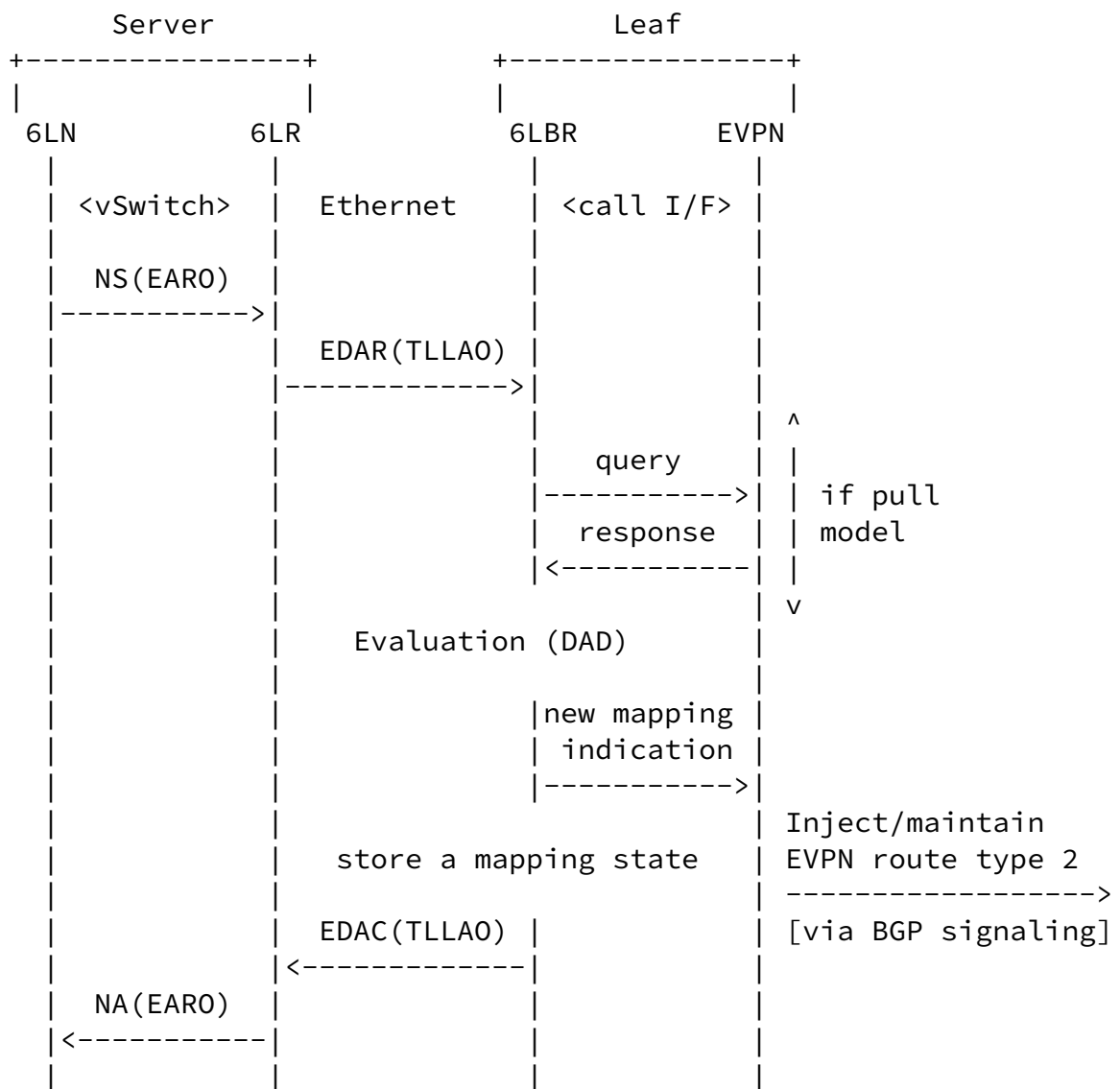


Figure 8: leveraging EDAR

[RFC8505] updates the DAR/DAC messages into the Extended DAR/DAC to carry the ROVR field. With this specification, the abstract 6LBR is distributed in all the Leaf nodes and synchronized with EVPN. When a server successfully registers an address to a leaf, the 6LR on that leaf becomes 6LBR for that address. It stores the full state for that address including the ROVR and the TID. When the address registration moves to another leaf, an EDAR/EDAC flow between the 6LR in the new leaf and the 6LBR in the old leaf confirms that the ROVR in the NS(EARO) received at the new leaf is correct, in which case the 6LR in the new leaf becomes 6LBR.

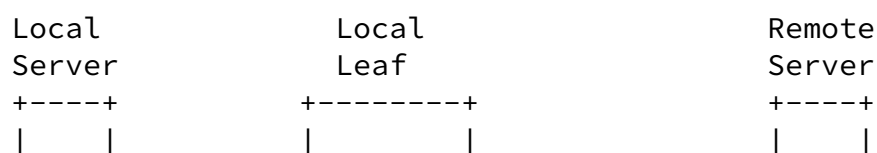
When the address is already registered to the local leaf, the EDAR/EDAC exchange is either local between a virtual router in the server and the leaf, or internal to the leaf between a collapsed 6LR and

6LBR. Based on its local state, the 6LBR in the leaf checks whether the proposed address/route is new and legit, and can reject it otherwise.

It results that duplicate addresses and address impersonation attacks can be filtered at the level of IPv6 ND by the 6LBR before the information reaches EVPN.

#### [4.3.](#) Unicast Address Lookup with the 6LBR

A classical IPv6 ND stack in the server that treats the subnet prefix as on-link (more in [section 4.6.2. of \[RFC4861\]](#)), will resolve an unknown LLA mapping with a multicast NS(lookup) message addressed to the solicited node multicast address (SNMA) associated with the destination address being resolved. The RECOMMENDED operation in that case is for the 6LBR that has a mapping state to forward the packet as a unicast MAC to the LLA that is stored for the IPv6 address as expected by [\[RFC6085\]](#). The actual owner of the address can then answer unicast with a NA message, setting the override (O) bit to 1, as shown in Figure 9.



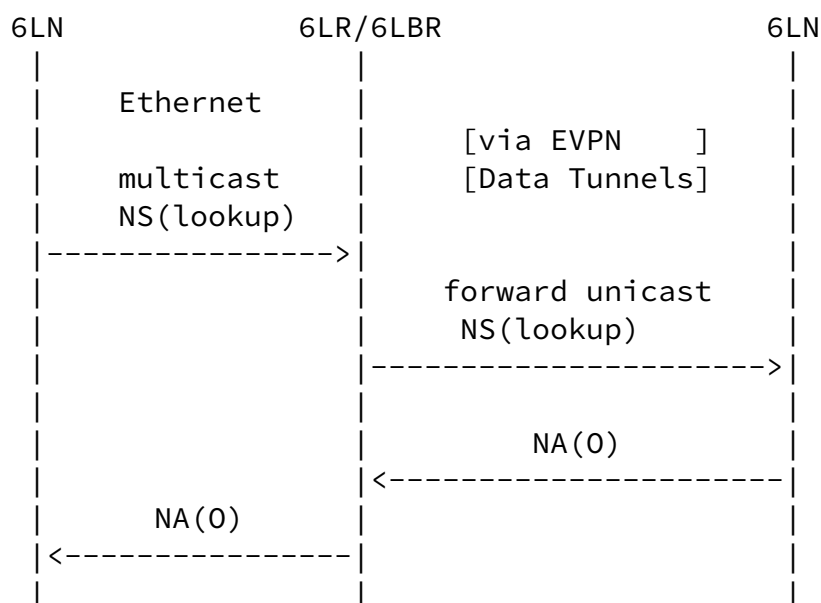


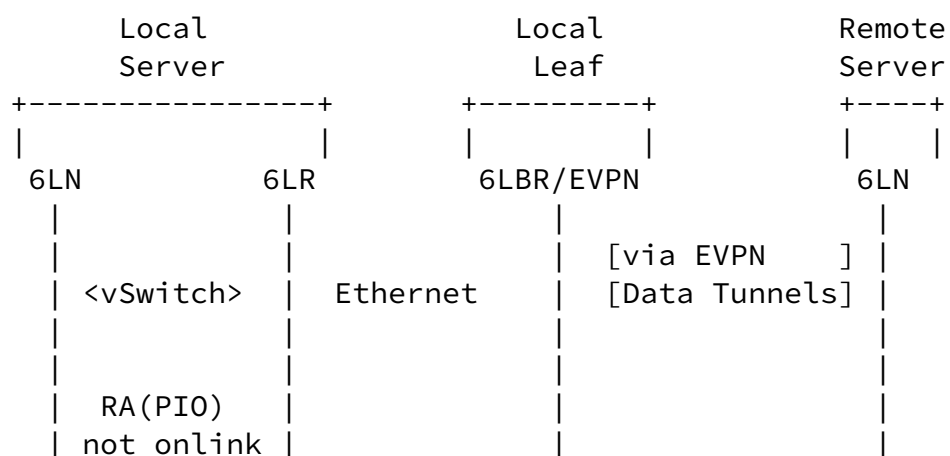
Figure 9: Forwarding legacy NS (Lookup)

[Section 3.1. of \[RFC8929\]](#) adds the capability to insert IPv6 ND options in the EDAR and EDAC messages. This enables the 6LBR to store the link-layer address associated with the Registered Address and to serve as a mapping server. [\[UNICAST-LOOKUP\]](#) leverages that state to define a new unicast address lookup operation, extending the EDAR and EDAC messages as the Address Mapping Request (AMR) and Confirmation (AMC) with a different Code Prefix [\[RFC8505\]](#).

In that model, the router advertises the subnet prefix as not on-link by setting the L flag to 0 in the Prefix Information Option (PIO), more in [section 4.6.2. of \[RFC4861\]](#). The expected behavior is that the host that communicates with a peer in the same subnet refrains from resolving the address mapping and passes the packets directly to the router.

In the case where the router is a virtual 6LR running in the server, and the source and destination are in the same subnet served by EVPN, the router then resolves the address mapping on behalf of the host. To that effect, the router sends a unicast AMR message to the 6LBR.

The message contains the SLLAO of the router to which the 6LBR will reply. If the binding is found, the 6LBR replies with an AMC message that contains the TLLOA with the requested MAC address, as shown in Figure 10.



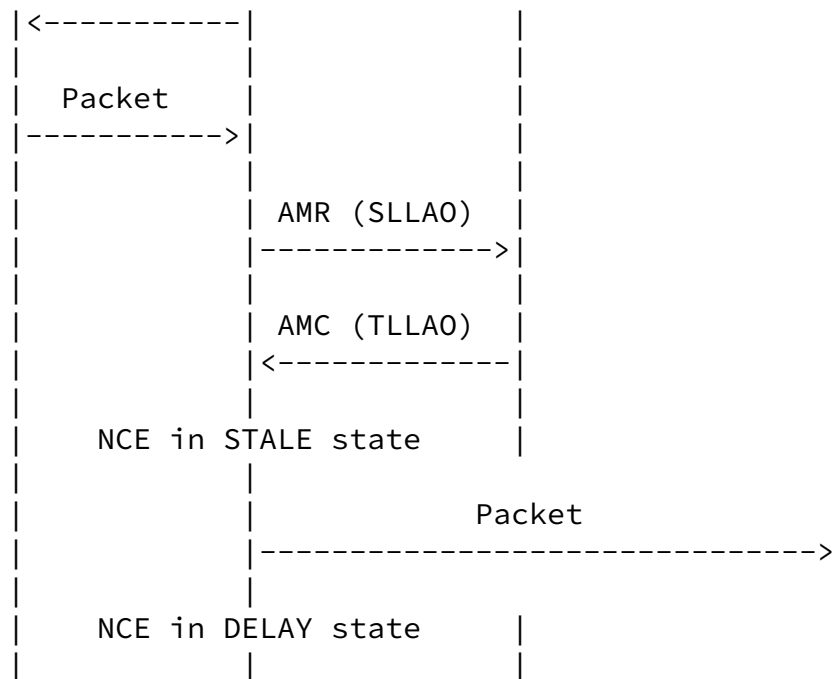


Figure 10: Unicast Lookup from the virtual Host

If it is not found, [[UNICAST-LOOKUP](#)] provides the capability to indicate immediately that the mapping is not known with a "not found" status in the AMC, as opposed to waiting for an NS(lookup) and retries to time out per [[RFC4861](#)].

In a fully stateful subnet where all nodes register all their addresses with [[RFC8505](#)], this means that the looked up address is not present in the network; in that case the packet is dropped and an ICMP error type 1 "Destination Unreachable" code 3 "Address unreachable" [[RFC4443](#)] is returned as shown in Figure 11.





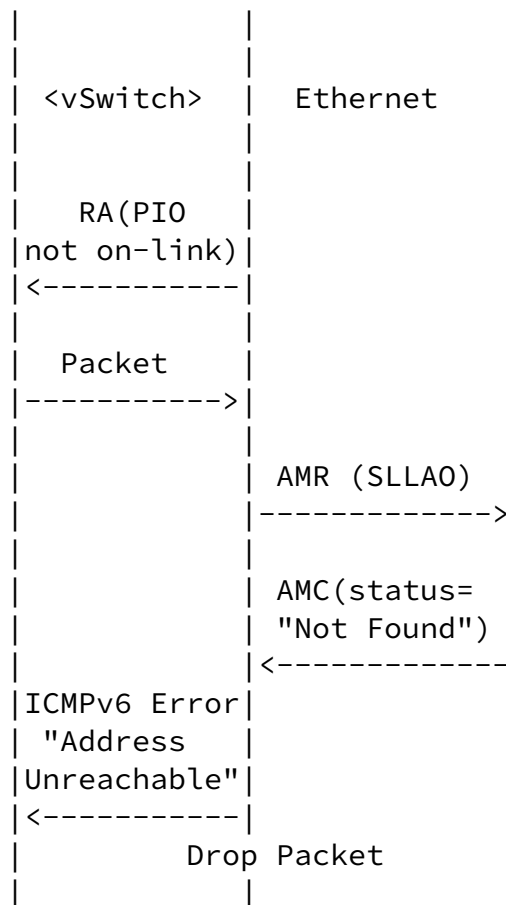


Figure 11: Unicast Lookup failure

Note that the figures above make no assumption on the pull vs. push model. In the case of pull model, the 6LBR queries the EVPN support when it does not have the mapping information to satisfy a request. Figure 12 illustrates a successful pull model lookup flow, when the route type 2 for the mapping is already known on the EVPN side.

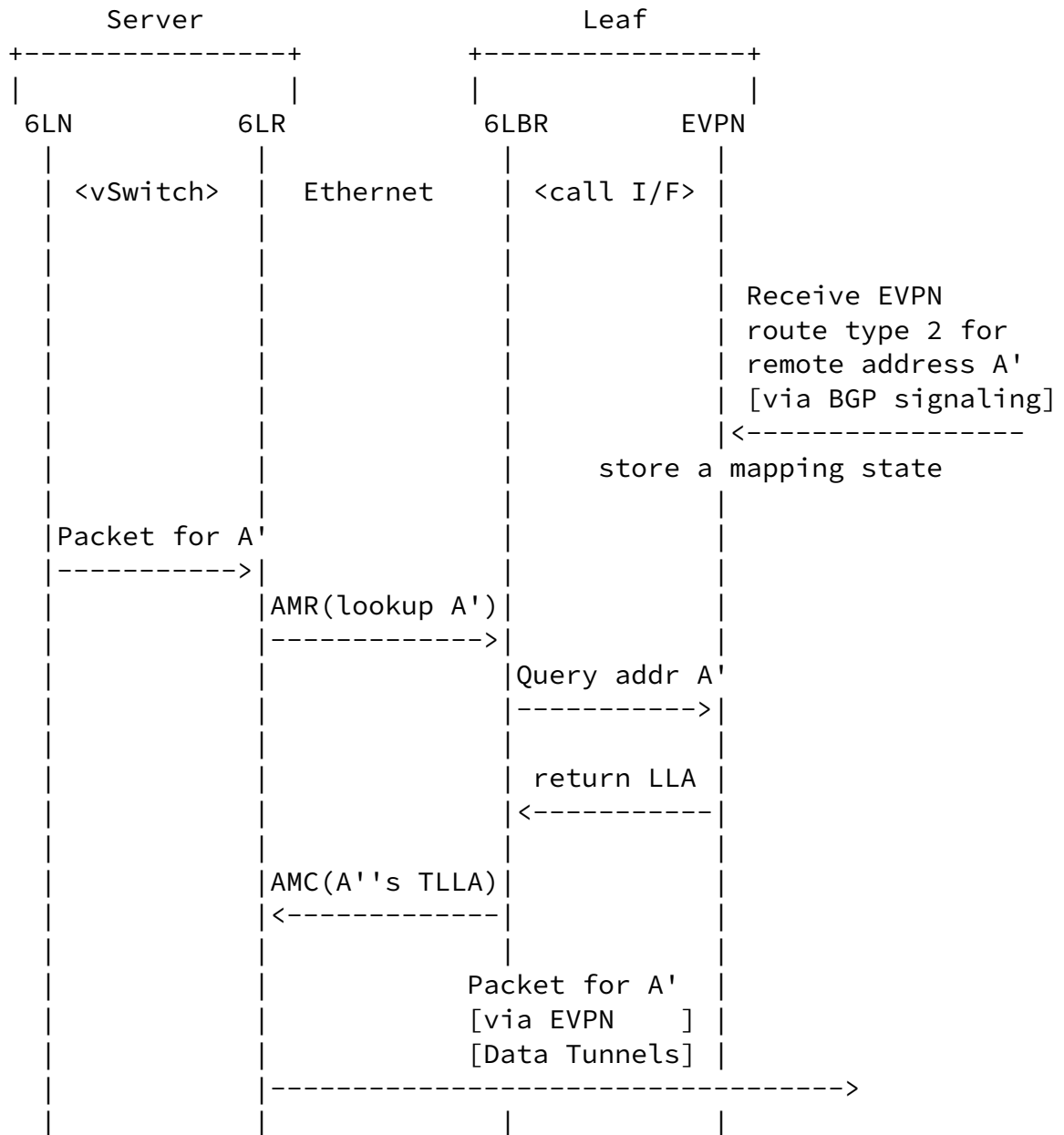


Figure 12: Pull model

In the case of push model, the EVPN support synchronizes its state upon a route type 2 with the 6LBR, and the 6LBR maintains an abstract data structure for all information known to EVPN. This way, the 6LBR already has the mapping information to satisfy any request for an existing mapping and it can answer right away. Figure 13 illustrates a successful push model lookup flow, when the 6LBR is already in possession of the mapping.

Internet-Draft

EVPN Secure MAC

January 2022

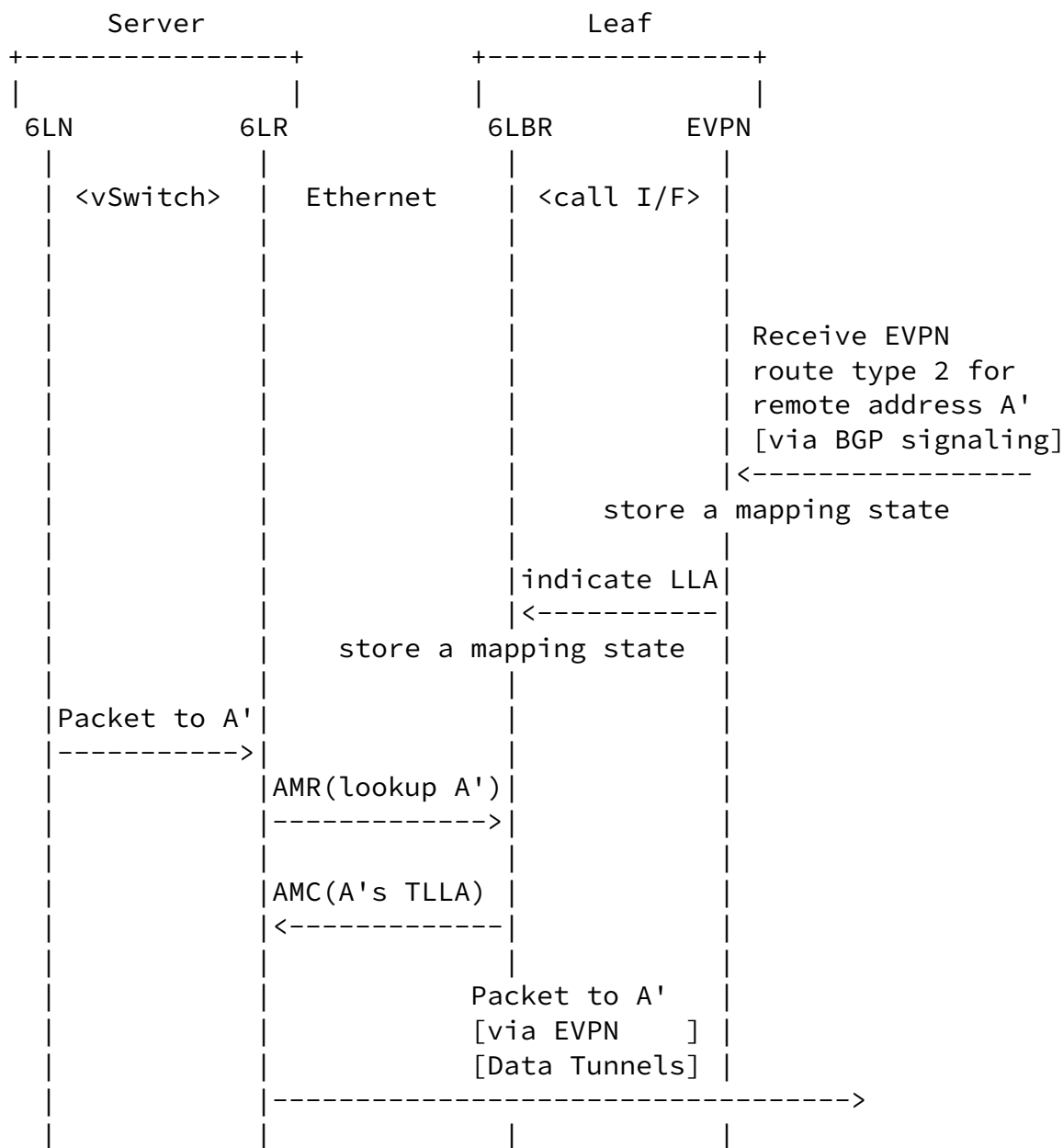


Figure 13: Push model

In a mixed environment, a lookup failure (the mapping is not found though the address is present in the network) may be caused by a legacy node that was node discovered (aka a silent node). In that case, it is an administrative decision for the 6LR to broadcast an NS(lookup) or to return an error as shown in Figure 11.

## [5.](#) Requirements on the EVPN-Unaware Host

This document describes how EVPN routing can be extended to reach a Host. This section specifies the minimal EVPN-independent functionality that the Host needs to implement to obtain routing services for its addresses.

### [5.1.](#) Support of 6LoWPAN ND

A host sees a prefix as not on-link (e.g., it learned that prefix in a PIO in a RA with the L flag not set) should not attempt to resolve an address within that prefix using a multicast NS(lookup). Instead, it must pass its packets to a router, preferably one that advertises that prefix in a PIO; it must register the address that it uses as source to that router to enable source address validation using [\[RFC8505\]](#). It is recommended that the Host also implements [\[RFC8928\]](#) to prove its ownership of its addresses.

The Host is expected to request routing services from a router only if that router originates RA messages with a 6CIO that has the L, P, and E flags all set to 1 as discussed in [Section 3.5](#), unless configured to do so. To obtain routing services for one of its addresses, the host must register the address to a router that advertises the prefix, setting the "R" and "T" flags in the EARO to 1 as discussed in [Section 3.3.1](#) and [Section 3.3.2](#), respectively.

This document echoes the behavior specified in [\[RFC9010\]](#) whereby, when the R Flag set to 1 in a NS(EARO) is not echoed in the NA(EARO), the host must understand that the route injection failed, and if the R flag is reset later in an asynchronous NA(EARO), the host must understand that routing service has failed.

The host may attach to multiple 6LRs and is expected to prefer those that provide routing services. The abstract model for this is a P2MP interface that wraps together as many P2P IP Links the host has

adjacencies to 6LRs over that interface. The IPv6 address and the subnet are associated to that interface. The interface may be virtual and it may bundle multiple physical Ethernet interfaces that connect to the individual 6LRs over point to point wires, possibly via a software switch. It can also be associated to one physical interface to an external switch, either way the PI Links can be associated to sub-interface of the interface.

The Host needs to register to all the 6LRs from which it desires routing services. The multiple Address Registrations to several 6LRs should be performed in a rapid sequence, using the same EAR0 for the same Address. Gaps between the Address Registrations will invalidate some of the routes till the Address Registration finally shows on

those routes. The routers recognize the same (ROVR, TID) as the signal of a multihomed address and maintain all the routes. In the case of EVPN, the Ethernet Segment must also be the same. The flow for a successful multihomed registration is illustrated in Figure 17.

[RFC8505] introduces error Status values in the NA(EAR0) which can be received synchronously upon an NS(EAR0) or asynchronously. The Host needs to support both cases and refrain from using the address when the Status value indicates a rejection.

This specification can be used to register Anycast and Multicast IPv6 addresses as discussed in [Section 3.3.5](#) and replace MLDv2. To benefit from that capability, both the host and the 6LR MUST support the "A" and "M" flags that indicate Anycast and Multicast Addresses respectively. Those flags are defined in [\[I-D.thubert-6lo-multicast-registration\]](#) for use in the EAR0 and in the EDAR and EDAC messages.

## [6.](#) Enhancements to EVPN

This section addresses the necessary changes to EVPN formats and behavior to support address registration security per [\[RFC8928\]](#) and mobility per [\[RFC8505\]](#) while retaining interoperability with traditional nodes. Basically the MAC Mobility Extended Community [\[RFC7432\]](#) and the ARP/ND Extended Community [\[RFC9047\]](#) are extended to advertise the sequencing and ownership validation information received in the EAR0. With 6LRs injecting not only MACs via packet sources and TLLAO options but also ROVR into MAC Mobility and ARP/ND

Extended Community, their semantics must be extended. Specifically following issues have to be addressed:

- \* The ROVR extends the semantics of the type-2 MAC advertisement via changes in ARP/ND and MAC Mobility Extended Community in the sense that the MAC must be aligned with the ROVR and under normal circumstances only the validity of ROVR guarantees that the type-2 MAC can be allocated to the requester. A MAC validated by ROVR should take precedence over MAC addresses allocated without using it given it presents a much more trustworthy topological information (it will be called ROVR MAC in further text). EVPN nodes not supporting extensions introduced by this document will need to be led to believe that a ROVR MAC is to be preferred over any advertisement they see as long a ROVR MAC route is present. The primary key of NRLI is still the (IP, MAC, Ethernet Tag ID) tuple as defined in [\[RFC7432\]](#), [Section 7.2](#) and 7.7. This implies that the same MAC (and consequently ROVR MAC) can be assigned multiple IP addresses with different ROVRs and those represent independent NLRIs.

- \* The TID field in the EARO is smaller than the mobility sequence number in [\[RFC7432\]](#). To allow a ROVR MAC mobility to "win" over legacy MACs in every circumstance, signaling must be introduced that enables to distinguish a TID-generated sequence number from a legacy sequence number.
- \* [\[RFC8505\]](#) supports IP multihoming, but does not differentiate multihoming from anycast or MAC address rotation. If an anycast IP address is registered with a different ROVR it will be rejected as duplicate. If it is registered with a different TID, the older sequence will be withdrawn. So the basic expectation with [\[RFC8505\]](#) is that the advertisement of an anycast address is coordinated, with the same keypair known to all parties, and the same value of the TID used by all nodes (and possibly never increasing), in other words, with no concept of mobility.
- \* [\[I-D.thubert-6lo-multicast-registration\]](#) adds new flags in the EARO to signal that an address is anycast or multicast, respectively. This specification injects that information in the ARP/ND extended community using matching flags as follows:

- This specification uses the "O" flag in the ARP/ND extended community to signal that the IP address is anycast, and requires the local 6LBR to ignore the duplication if the same IP address is registered locally, and then to inject the NLRI with the "O" flag set on the ARP/ND Extended Community as well.
  - This specification adds the new "M" flag in the ARP/ND extended community to signal that the IP address is multicast, and requires the local 6LBR to ignore the duplication if the same IP address is registered locally, and then to inject the NLRI with the "M" flag set on the ARP/ND Extended Community as well.
- \* [\[RFC8928\]](#) needs the full ROVR to validate the address ownership, but the full ROVR can be too large to advertise through BGP. When an IP address is advertised through EVPN, it is REQUIRED that the EVPN Next Hop represents the address of the 6LBR of the leaf where the address was registered as well. This way, if the address is registered later on a second leaf, the 6LR in second leaf can leverage an out-of-band, i.e. via EVPN traffic carrying tunnels, EDAR/EDAC exchange with that 6LBR to validate that the ROVR in the registration is indeed the same. When that is the case, it can continue with the registration procedure and if successful, become a 6LBR for that IP address, either as a mobility event or as a multihomed registration.

- \* [\[RFC8928\]](#) expects nodes to autoconfigure the keypair that is used to form the ROVR, in which case the IPv6 address can be locally autoconfigured with no central coordination; in that case, the ROVR protects the address ownership and allows the fabric to enforce first-come first-serve and source address validation (SAVI). But it is also possible to provision the ROVR in the 6LBR in advance and later configure the keypair in the node, e.g., in the case of a trusted server. To enable that capability in EVPN, this specification adds a flag (U) to signal that the 6LBR that injects the address in EVPN does not provide reachability to the address. When that flag is set, the value of the TID is ignored in the mobility computation, the mapping to the MAC address is ignored, and the route to the IP address is not injected in the RIB on ROVR nodes. Non-ROVR nodes will consider the node a

"honey-pot". Once the address is registered by a 6LN in the network and the according validation with the node advertising the U-bit version of the route is performed, the owner will inject the route without the U-bit. A node advertising the NLRI with U-bit in its ARP/ND Extended Community MUST withdraw the U-bit route once it sees a validated NLRI without the U-bit and it MAY reinject the route with the U-bit once all routes without the U-bit are withdrawn to protect the address again.

#### [6.1.](#) Updated ARP/ND Extended Community

The ARP/ND Extended Community defined in [[RFC9047](#)] is a transitive EVPN Extended Community (Type field value of 0x06) with a Sub-Type of 0x08. It is advertised along with EVPN MAC/IP Advertisement routes that carry an IPv4 or IPv6 address. This the ARP/ND Extended Community to transport fields from the EARO is natural since the EARO is an extension to IPv6 ND.

EVPN signaling is not used to carry the full ROVR since without challenge per [[RFC8928](#)] they do not represent any difference over using the IP/MAC combination. A Hash of the ROVR is still passed in the ARP/ND Extended Community to immediately detect a duplication, with 2 different values of the hash for the same address. The full ROVR is verified upon a movement or a multi-homed advertisement using an EDAR/EDAC exchange with the 6LBR that advertised the address first.

Additionally, backwards compatibility could not be preserved given comparing routes based on ROVR would present a change in primary key of NLRIs which non-ROVR routers do not implement. An indication from a ROVR node that a MAC has been validated by proof of ownership is enough to convey the necessary information.

ROVR nodes MUST set the "H" flag in the ARP/ND Extended Community to indicate that the advertisement carries a TID and a ROVR Hash in case the host followed the according procedures.

ROVR nodes MUST set the "V" flag if the address assignment passed proof of ownership per [[RFC8928](#)]. Such "validated" ROVR MAC addresses will be preferred by ROVR nodes over non-validated ROVR



MACs.

In case a ROVR node configures the address as "sticky" (since the sticky bit semantics have been changed to the point a ROVR cannot tell whether address is really sticky unless advertised as such by non-ROVR node) a new "X" flag called "super sticky" is introduced.

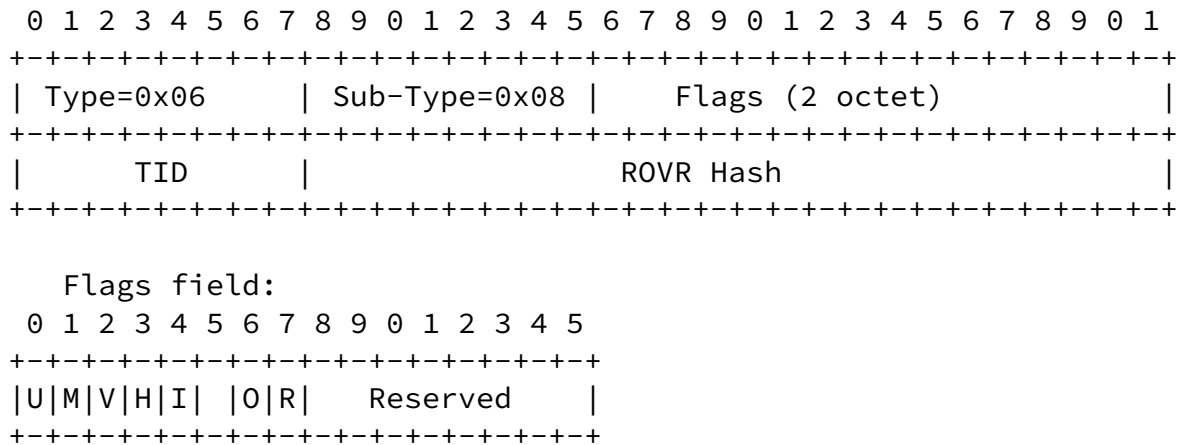


Figure 14: Updated ARP/ND Extended Community

The "I", "O", and "R" flags are defined in [\[RFC9047\]](#). The following new fields are defined:

- U: 1-bit flag. "Unreachable", indicating that the IP address is not reachable via that EVPN next hop, but is advertised for the purpose of protecting the value of the ROVR until a first 6LBR that can reach the address becomes available.
- M: 1-bit flag. "Multicast", indicating that the IP address duplication should be ignored. When this bit is set, TID should be ignored in comparison of EVPN advertisements, i.e. all ROVR MACs at same level of validation MUST be considered having same TID.
- V: 1-bit flag. "ROVR Validated" indicates that the MAC passed proof of ownership per [\[RFC8928\]](#). Presence of this bit implies the "R" bit being set regardless of its value.
- H: 1-bit flag. "ROVR Capable" indicates that the advertisement is

originated after processing signaling from host meeting the requirements in [Section 5](#), and that the advertised MAC address is a ROVR MAC. This also indicates that the TID and ROVR Hash fields are populated based on information from the most recent EARO [[RFC8505](#)] from the host.

TID: 8-bits structure. The TID [[RFC8505](#)] from the Registering Node.

ROVR Hash: 16-bits hash of ROVR [[RFC8505](#)] from the Registering Node. The Hash is built by XOR'ing ROVR bytes in network order into the least significant byte and rotating the two bytes result after every byte by one bit to the left.

## 6.2. Updated Mobility Extended Community

This specification extends the MAC Mobility Extended Community to transport the TID instead of increasing the normal sequence number. The TID is placed in the high bits of the sequence number field to "override" any normal MAC advertisement (further considerations will be provided in [Section 6.3](#)). this allows to design a solution that, while backwards compatible, allows to introduce ROVR MAC as "more trusted" entities. Figure 15 presents the according extensions that will however necessitate some further explanation.

To introduce a "precedence" of ROVR MACs over normal EVPN MACs ROVR MACs are advertised to look like "sticky" MACs for non-ROVR nodes. As defined in the glossary, for simplicity reasons such nodes will be called non-ROVR nodes vs. ROVR nodes. The "sticky" bit will force non-ROVR nodes to disregard the sequence number and accept any IP/MAC route provided.

```

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Type=0x06      | Sub-Type=0x00 | Flags = 0 |X|S|  Reserved = 0 |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|T| Flags = 0    |      TID      |      Reserved = 0      |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

Figure 15: Updating the MAC Mobility Extended Community for ROVR MACs

This specification updates the Sequence Number field defined in [[RFC7432](#)]. The field is split in 3 parts, one 8-bit flags field, the TID, and a reserver 2-byte field. The unspecified flags and the reserved fields MUST be set to 0 by the sender and ignored by the receiver.

The "S" flag is defined in [[RFC7432](#)]. The following new fields are defined:

Internet-Draft

EVPN Secure MAC

January 2022

X: 1-bit flag. "Super Sticky" indicates that the ROVR MAC is sticky and should follow procedures of sticky per [\[RFC7432\]](#).

T: 1-bit flag. "TID Present", MUST be set to 1 when this specification is used. This ensures that the TID always wins vs. the sequence counter defined in [\[RFC7432\]](#)

TID: The TID copied from the most recent EARO [\[RFC8505\]](#) from the Registering Node.

### [6.3](#). Extended ROVR MAC Procedures

In case a non-ROVR node advertises a sticky MAC by setting the "S" bit and a ROVR node sees an ROVR address registration for the same MAC it MUST follow procedures per [\[RFC7432\]](#).

In case a non-ROVR node advertises a sequence number larger than the one generated by TID on a ROVR node, the ROVR node SHOULD advertise a Sequence Number consisting of all bits being set to force a "roll-over" on all nodes and then fall back to advertising the TID generated sequence number again. In case a non-ROVR node persists in increasing the sequence number after that it is indication of violation of [\[RFC7432\]](#) on its part.

A ROVR node advertising a ROVR MAC that has not been validated and receiving same type-2 route that has been validated MUST immediately withdraw its advertisement.

A ROVR node advertising a ROVR MAC and receiving an equivalent ROVR MAC from other node with a higher TID MUST immediately withdraw its advertisement. This will allow the non-ROVR nodes to correctly interpret the sequence as MAC move despite ignoring the sequence number due to presence of "S" bit.

A ROVR node that receives a ROVR MAC with "super sticky" indication and seeing the MAC locally MUST follow analogous procedures to [\[RFC7432\]](#).

Multi-homing a MAC on mix of ROVR and non-ROVR nodes will lead to operational notifications since per [\[RFC7432\]](#) the non-ROVR node will interpret the situation as a sticky MAC that has shown up on its local interface unless an implementation is somewhat clever and understands that the presence of the same ESI on all the routes

indicates that this situation does not represent a sticky MAC being moved.

## [7.](#) Protocol Operations

Following section illustrates several situations and resulting signaling in EVPN from the point of view of a ROVR node.

Figure 16 illustrates the registration flow of a new address protected by [\[RFC8928\]](#). The ROVR in the EARO is a Crypto-ID that derives from a public address through hashing with some other terms. The router challenges the host with a status of 5 (validation requested).

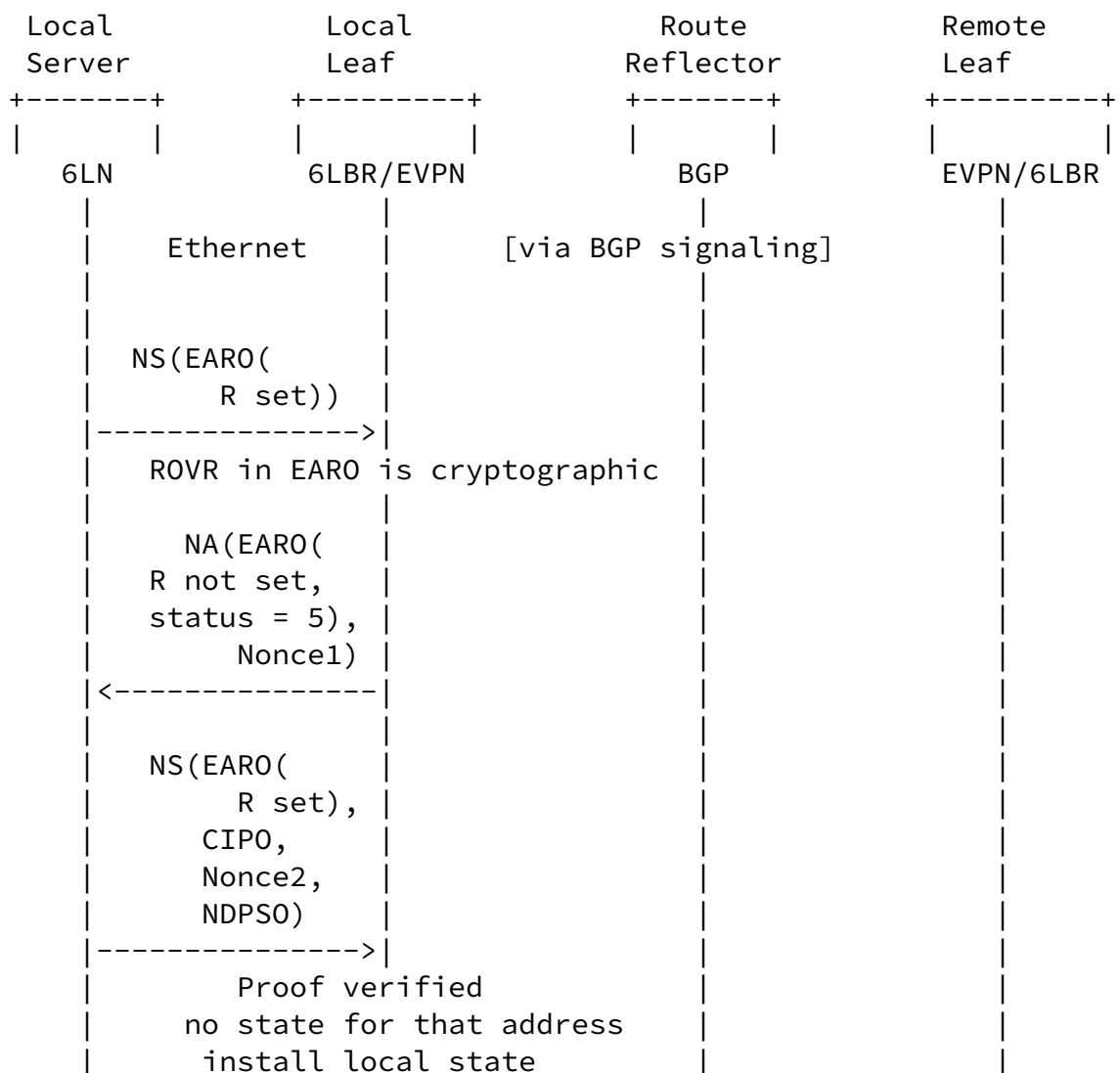
The host performs the NS again, passing the parameters that enable to build the Crypto-ID in a Crypto-ID Parameters Option (CIPO), and signing that set of parameters together with a pair of Nonce values, one from each side, in a resulting Neighbor Discovery Protocol Signature Option (NDPSO). The 6LR first verifies that the Crypto-ID can be rebuilt based on the public key, then verifies that the signature in the NDPSO was effectively performed with the associated public key. When that is the case, the registration flow can continue, else the registration is rejected with a status of 10 (Validation Failed) in the NA(EARO).

With this specification, the 6LBR communicates internally with the collocated EVPN router to inject the route in EVPN. Since the [\[RFC8928\]](#) validation was performed, the V flag is set. Once this is done, the local 6LBR installs a local state associated to the NCE and becomes owner of the registration, whereas the remote leaves optionally install a remote state for the address with the indication of the 6LBR that owns the registration. The local 6LBR MUST be signalled as EVPN Next Hop for the route.

Internet-Draft

EVPN Secure MAC

January 2022



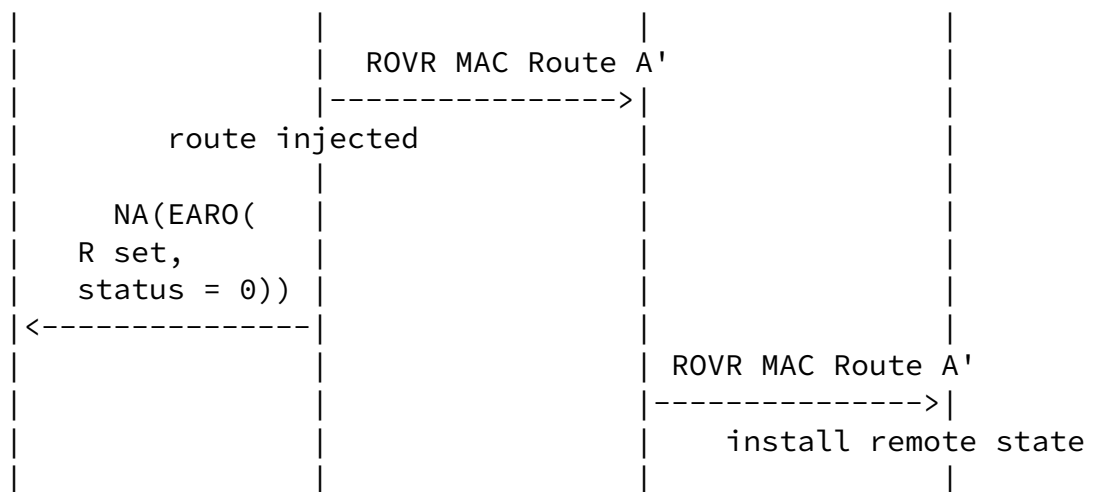
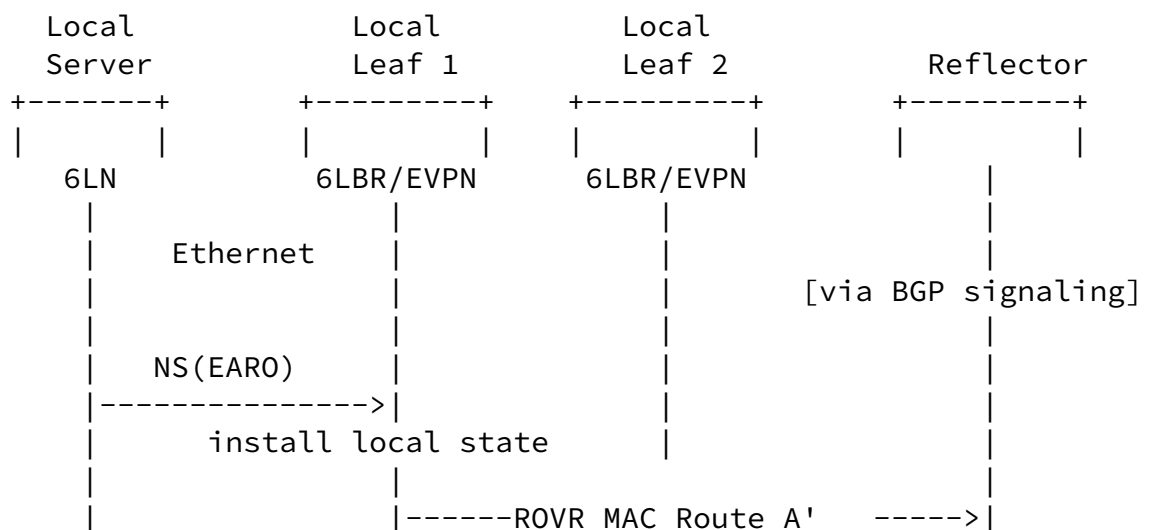


Figure 16: Host Registration

Figure 17 presents the same flow but for a multihomed address; here and in the following flows, the proof of ownership section is not shown, but its use is RECOMMENDED. The interesting piece is that

when the node registers to the second 6LBR, that second 6LBR find that there is a first 6LBR that already own the registration. Using and EDAR / EDAC flow, the second 6LBR validates that the ROVR and TID are identical, in which case it accepts the registration and becomes another 6LBR owner of the registration. The result is that the 2 6LBRs are synchronized and any of the 2 can now be used, e.g., if the address is registered a third time.



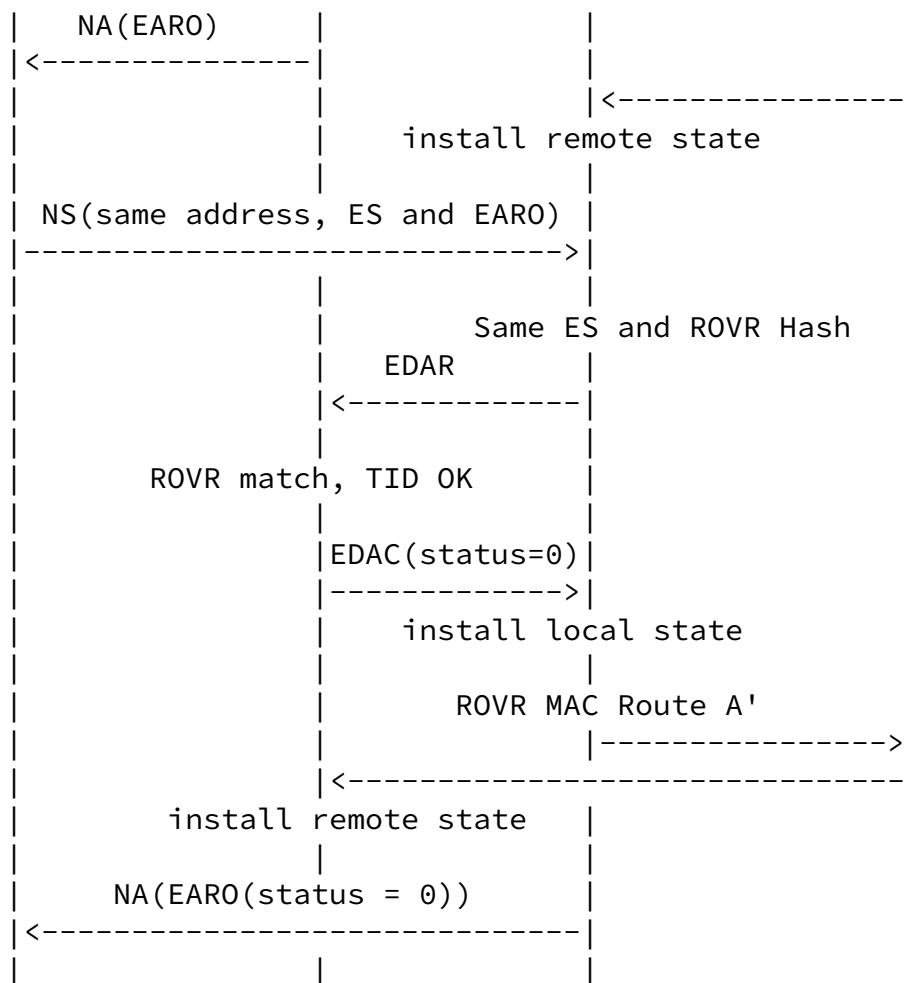
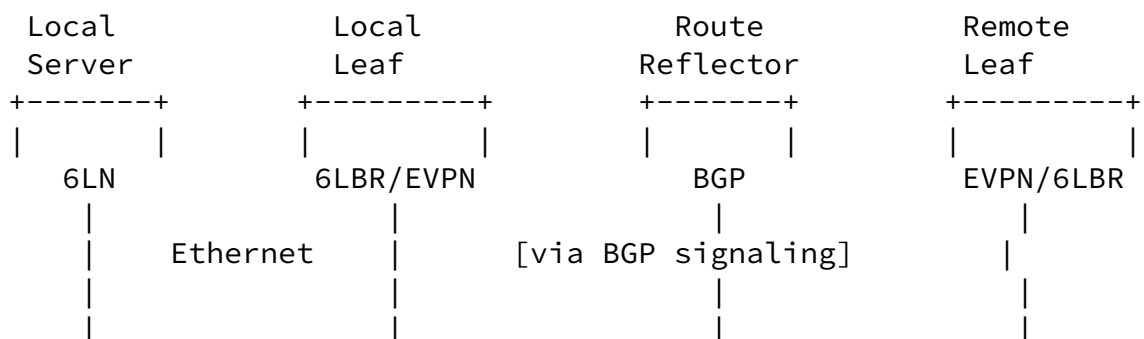


Figure 17: Multihoming

The registration is associated with a lifetime, and it must be renewed with an incremented TID. The new TID is propagated in EVPN as illustrated in Figure 18.



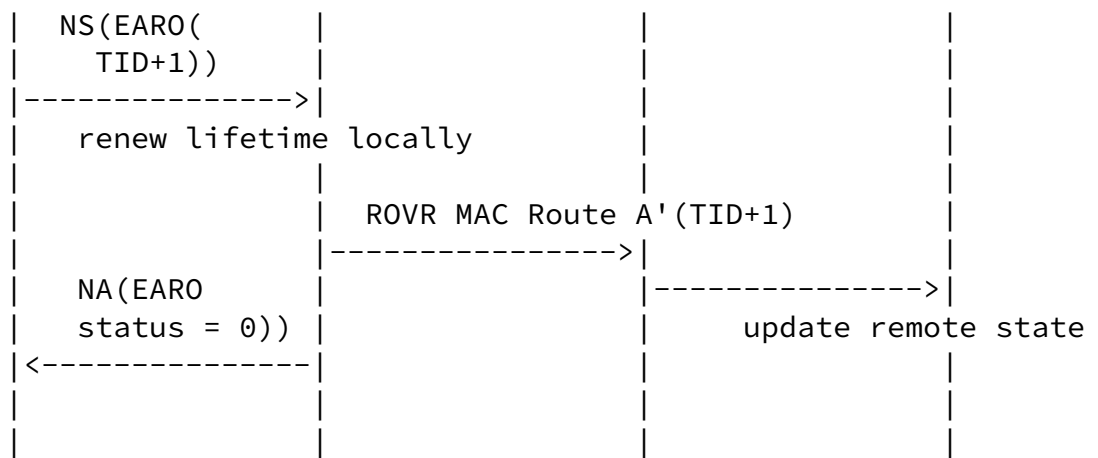
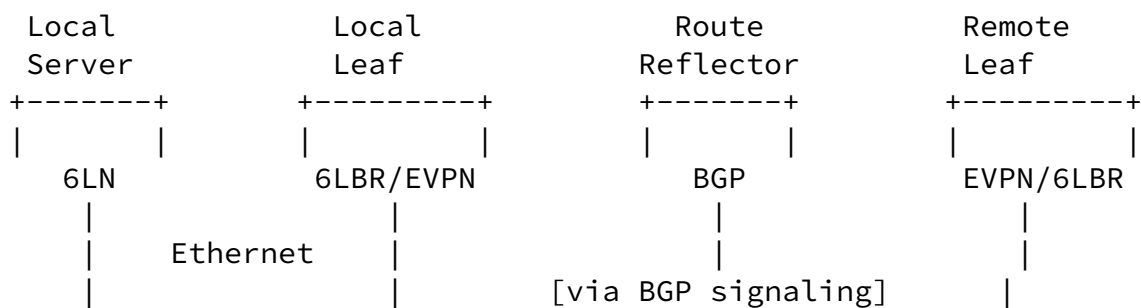


Figure 18: Host Registration Renewal

Figure 19 illustrates the case where a second host registers the same address, creating a potential address duplication situation. In most cases, the ROVR hash will be different, and the local 6LBR can reject the registration with a status of 1 (duplicate) right away.





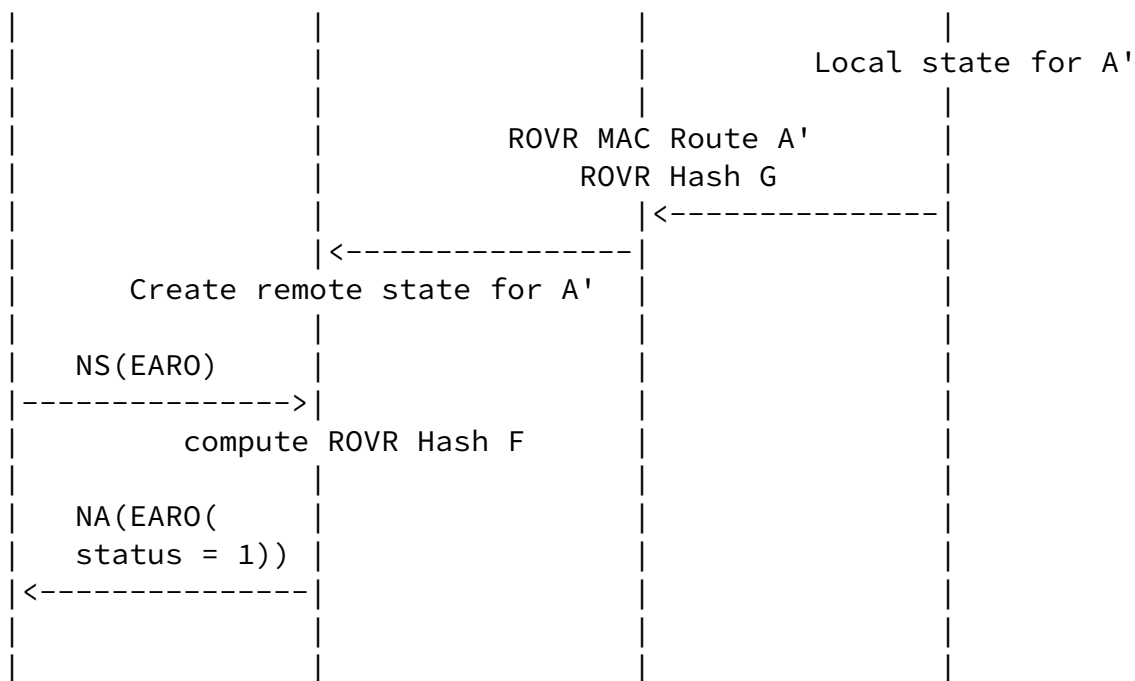


Figure 19: Duplicate Addresses

Figure 20 illustrates the case of an address duplication situation where by chance, the ROVR hashes are the same. In that case, the local 6LR checks with the 6LBR that owns the registration using an EDAR/EDAC message exchange. As opposed to the ROVR hash, the full ROVRs do not collide and the registration is also rejected.

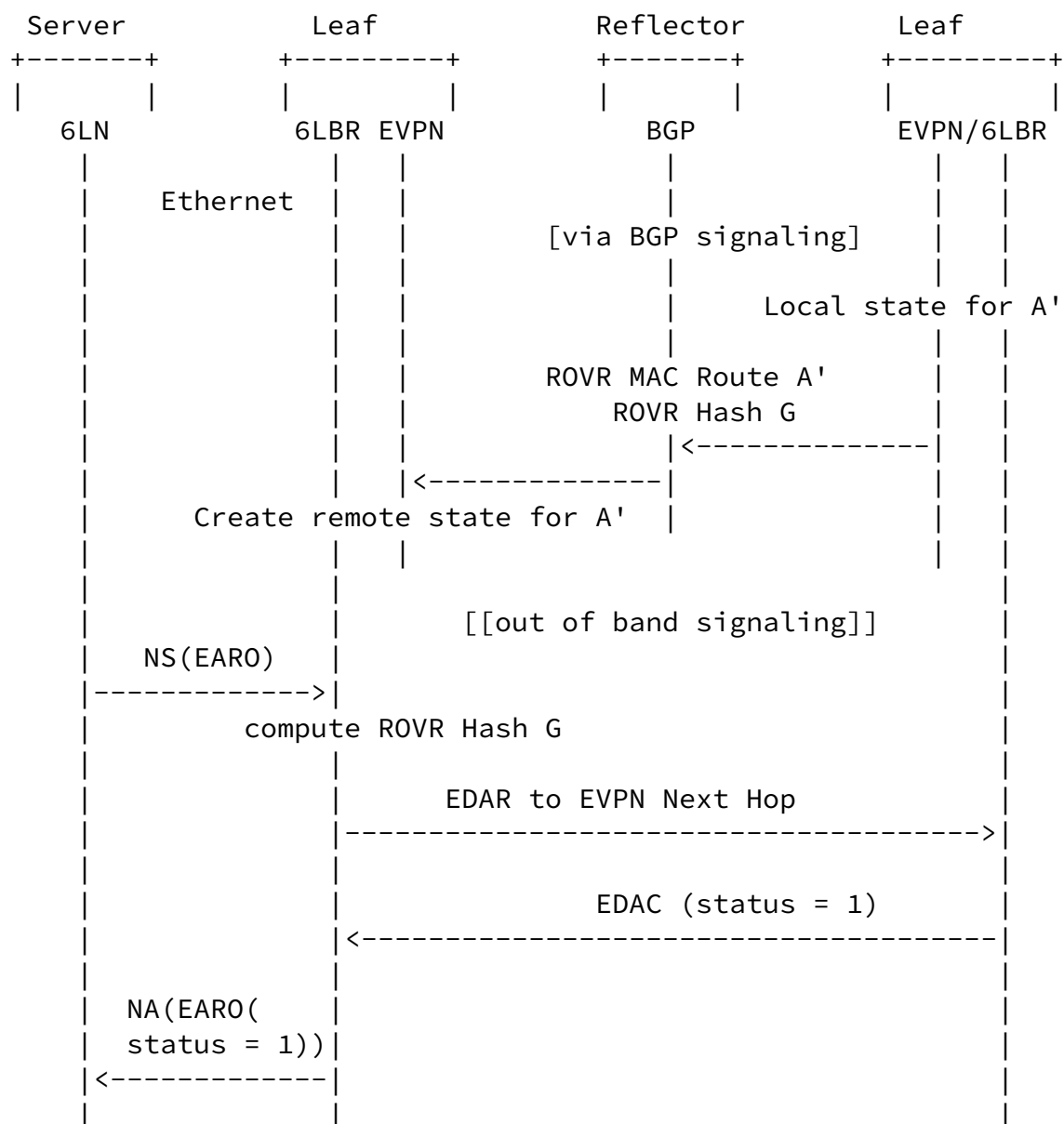


Figure 20: Duplicate Addresses, ROVR Hash Collision

Figure 21 shows a rare case where the registration has already moved elsewhere with an incremented TID when the local registration is received after being delayed in the network. In that case, the registration is rejected with a status of 3 (moved).

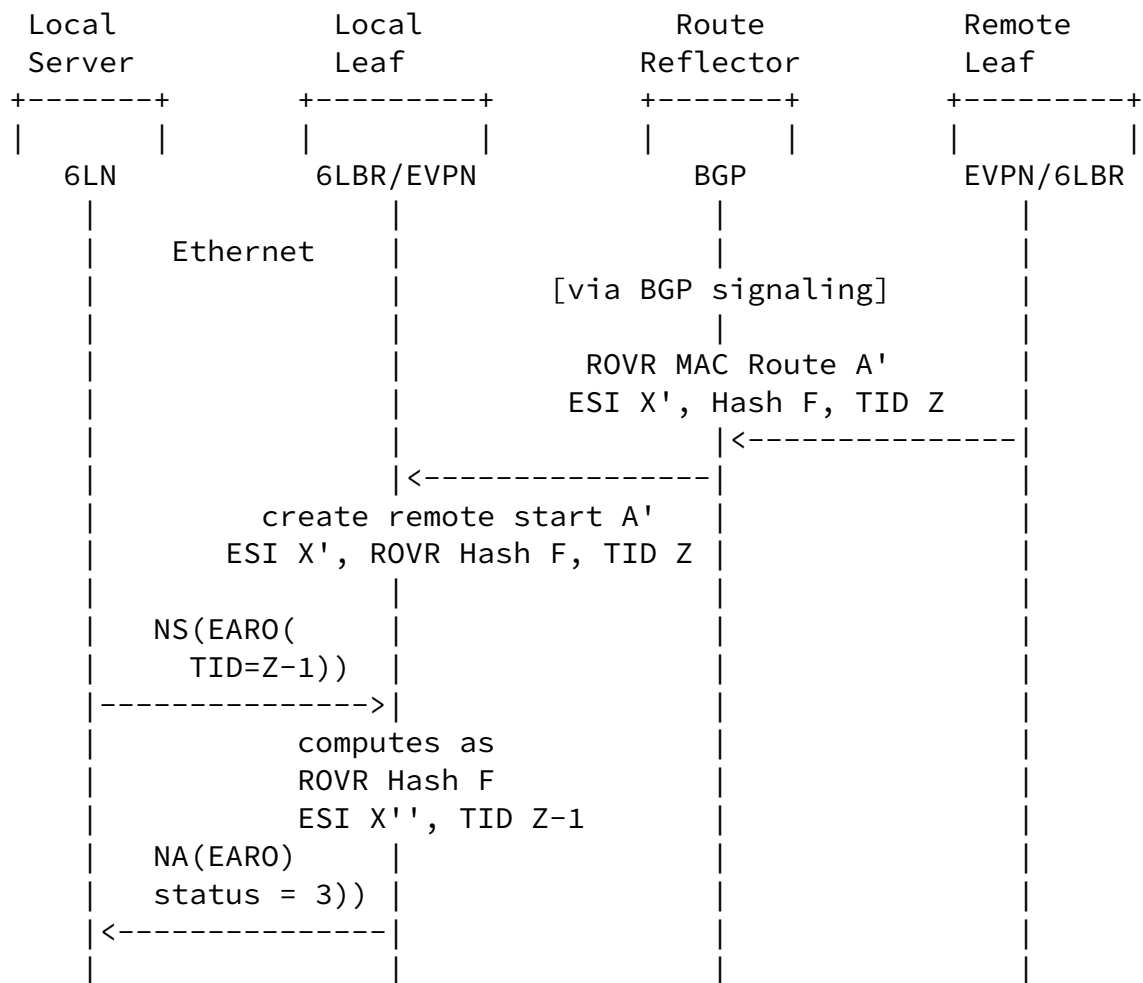


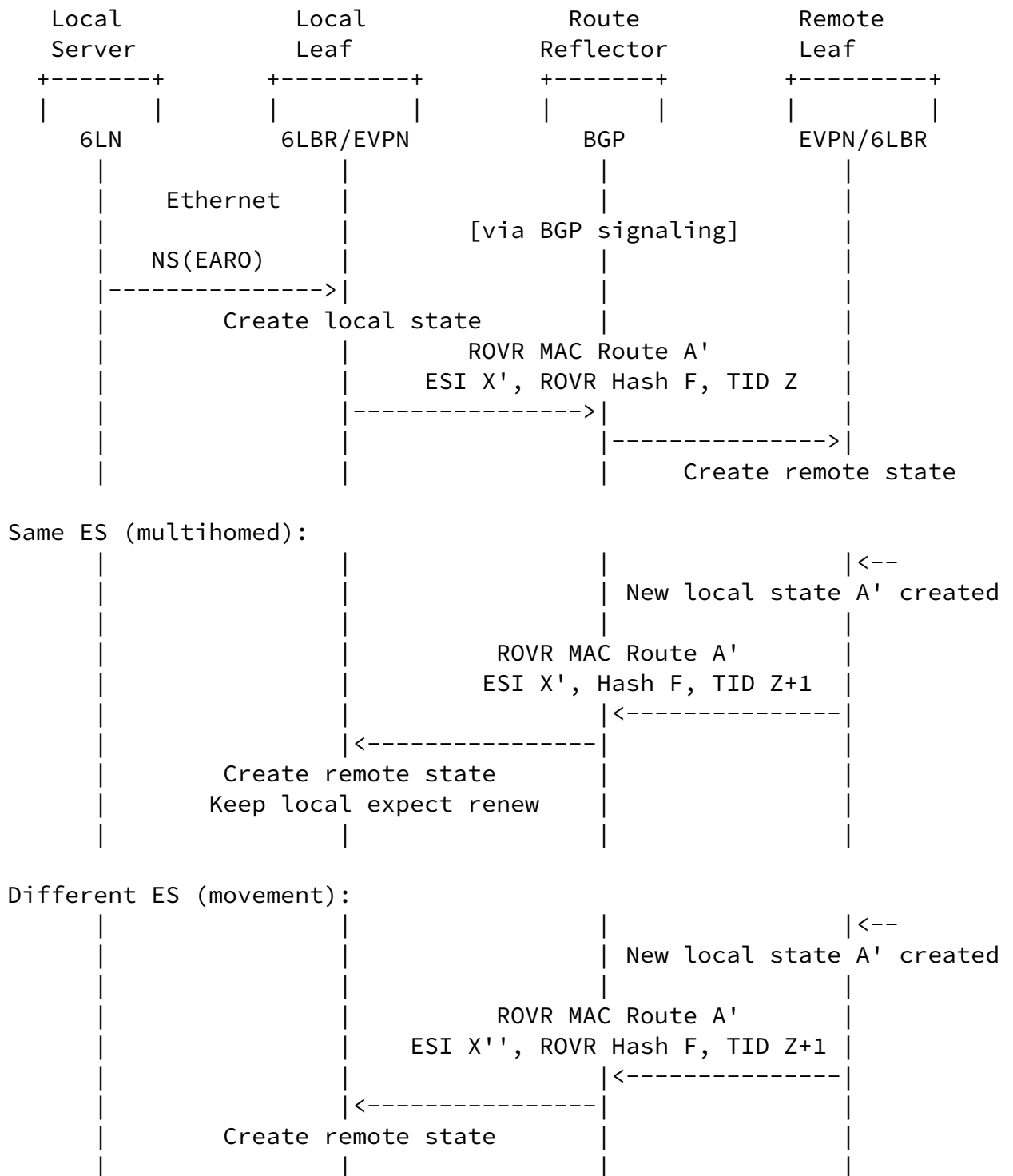
Figure 21: Address Already Moved

Address move differs from multi-homing by the ESI being different as visualized by Figure 22. In case of different ESI BGP signalling happens immediately, in case of multi-homing we can reasonably expect for the signalling to catch up on the other leg with a new, higher TID. However, since ESI matches TID doesn't matter strictly speaking and the new remote state can be installed as is. However, if 6LN is not refreshing its registration we can expect elapsed lifetime to create scenario Figure 25 over time.

Internet-Draft

EVPN Secure MAC

January 2022



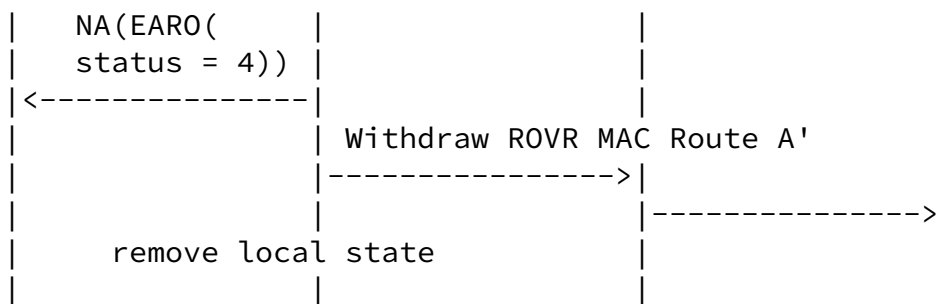


Figure 22: Address Move

The host that registered the address may cancel the registration at any time, e.g., if the address is removed from its own interface. This is done by registering with a lifetime of 0 as shown in Figure 23. The Leaf may respond with a status of 0 to indicate success, but a status of 4 (removed) is preferred for this situation.

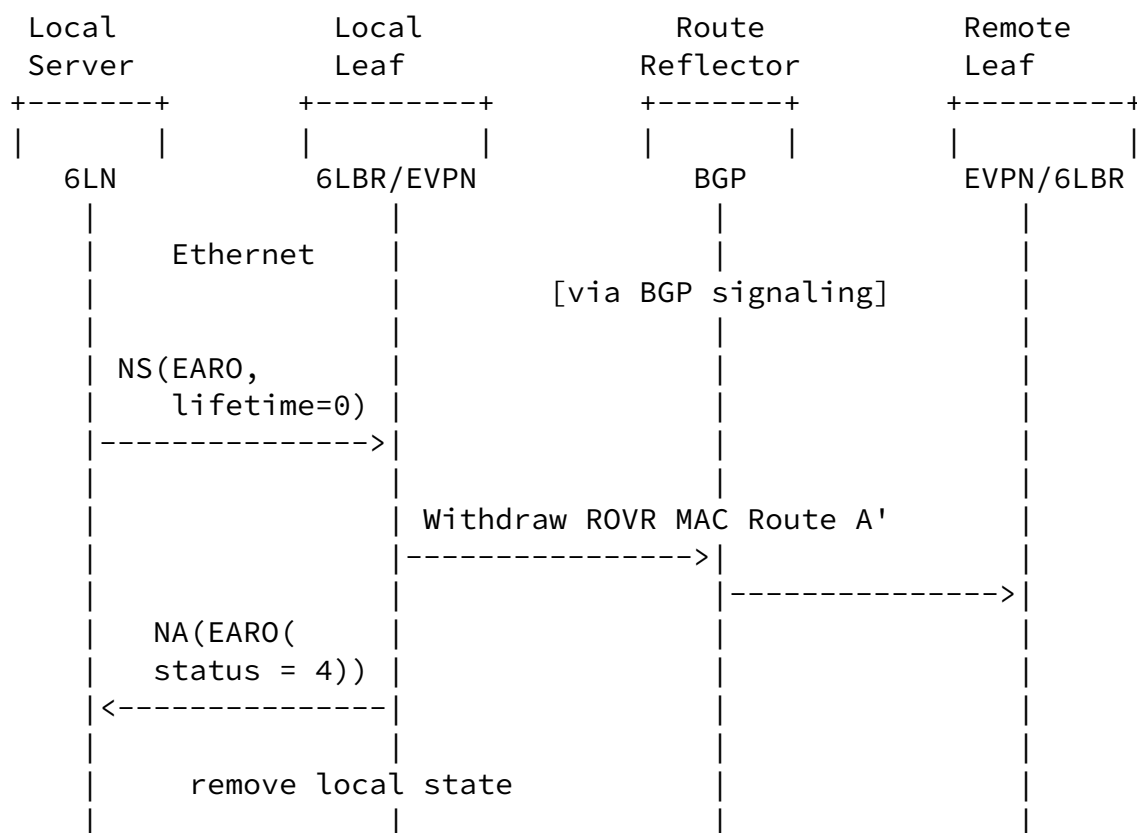


Figure 23: Address Removal

The host that registered the address may withdraw the route but maintain the NCE, e.g., in the case where it is multihomed but does not want to use one interface for the traffic back as this time. This is done by registering with the R flag set to 0 as shown in Figure 24.

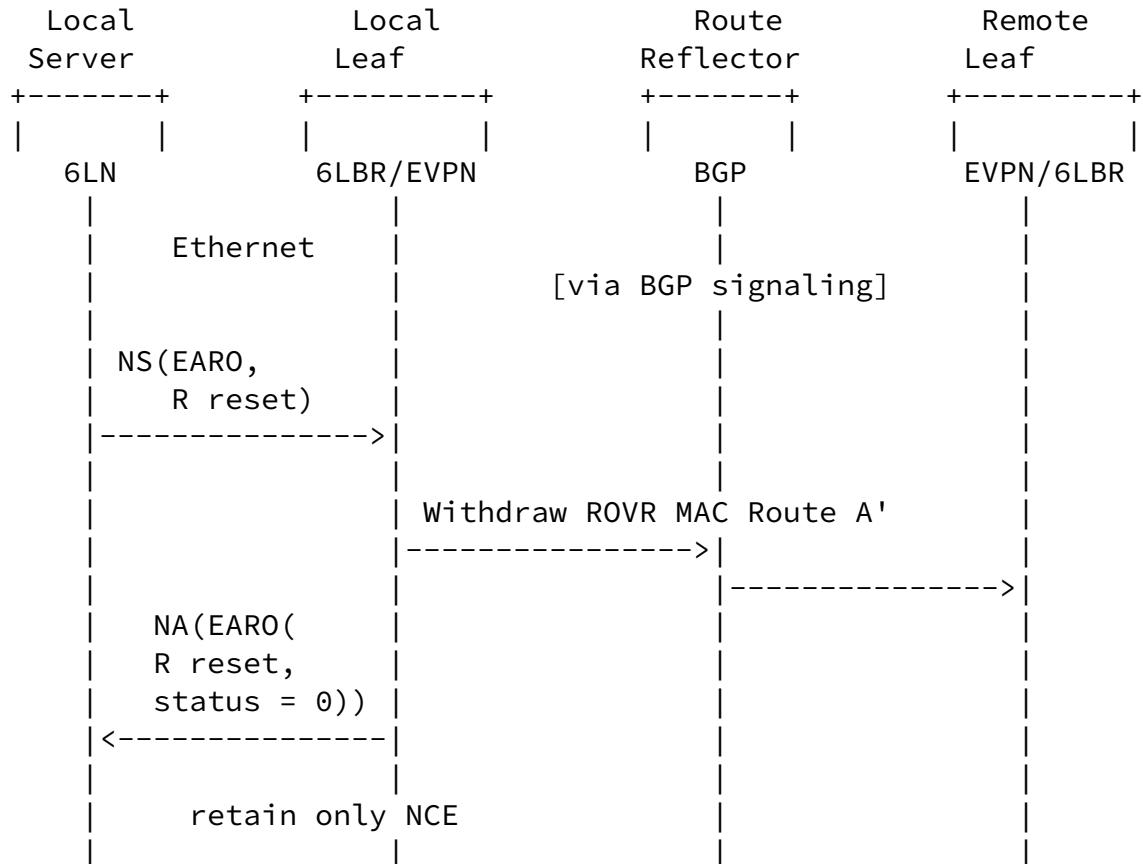
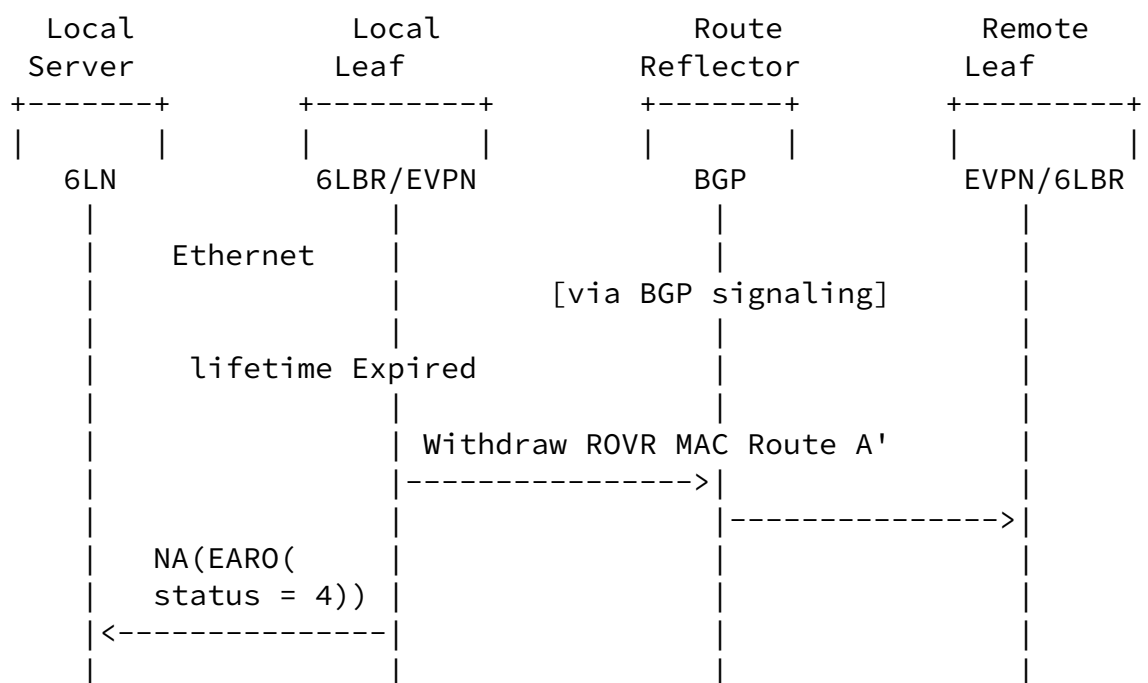


Figure 24: Route Type 2 Removal

When the lifetime elapses, the 6LBR requires the collocated EVPN router to withdraw the route.



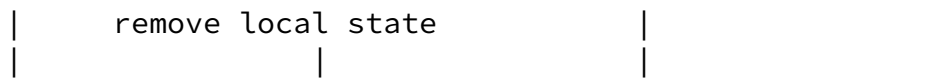


Figure 25: Lifetime Elapse

## 8. Security Considerations

TBD

## 9. IANA Considerations

### 9.1. MAC Mobility Extended Community Flags

This document creates the "MAC Mobility Extended Community Flags" registry based on one flag initially defined in [\[RFC9047\]](#) and more flags defined in [Section 6.2](#) as shown in Table 1:

Flag Position	Name	Reference
0..5	Unassigned	N/A
6	Super-sticky (X)	THIS RFC
7	Sticky (S)	<a href="#">RFC 7432</a>

Table 1: MAC Mobility Extended Community Flags

### 9.2. ARP/ND Extended Community Flags

This document modifies the "ARP/ND Extended Community Flags" registry initially created in [Section 5 of \[RFC9047\]](#). [Section 6.1](#) suggests to assign new entries in the Registry as indicated in Table 2:

Flag Position	Name	Reference
0 (Suggested)	Unreachable(U)	THIS RFC



1 (Suggested)   Multicast (M)   THIS RFC
+-----+-----+-----+
2 (Suggested)   ROVR Validated (V)   THIS RFC
+-----+-----+-----+
3 (Suggested)   ROVR Capable (H)   THIS RFC
+-----+-----+-----+

Table 2: New ARP/ND Extended Community Flags

## 10. Acknowledgments

The authors wish to thank you for reading that far. We acknowledge and express gratitude to Wen Lin, Stephane Litkowski, Eric Levy-Abegnoli, Lukas Krattiger, Jerome Tollet, and Ali Sajassi, for their help and support.

## 11. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.
- [RFC3810] Vida, R., Ed. and L. Costa, Ed., "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", [RFC 3810](#), DOI 10.17487/RFC3810, June 2004, <<https://www.rfc-editor.org/info/rfc3810>>.
- [RFC4443] Conta, A., Deering, S., and M. Gupta, Ed., "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", STD 89, [RFC 4443](#), DOI 10.17487/RFC4443, March 2006, <<https://www.rfc-editor.org/info/rfc4443>>.

- [RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", [RFC 4861](#), DOI 10.17487/RFC4861, September 2007, <<https://www.rfc-editor.org/info/rfc4861>>.

- [RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", [RFC 4862](#), DOI 10.17487/RFC4862, September 2007, <<https://www.rfc-editor.org/info/rfc4862>>.
- [RFC6775] Shelby, Z., Ed., Chakrabarti, S., Nordmark, E., and C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", [RFC 6775](#), DOI 10.17487/RFC6775, November 2012, <<https://www.rfc-editor.org/info/rfc6775>>.
- [RFC6085] Gundavelli, S., Townsley, M., Troan, O., and W. Dec, "Address Mapping of IPv6 Multicast Packets on Ethernet", [RFC 6085](#), DOI 10.17487/RFC6085, January 2011, <<https://www.rfc-editor.org/info/rfc6085>>.
- [RFC7400] Bormann, C., "6LoWPAN-GHC: Generic Header Compression for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", [RFC 7400](#), DOI 10.17487/RFC7400, November 2014, <<https://www.rfc-editor.org/info/rfc7400>>.
- [RFC7432] Sajassi, A., Ed., Aggarwal, R., Bitar, N., Isaac, A., Uttaro, J., Drake, J., and W. Henderickx, "BGP MPLS-Based Ethernet VPN", [RFC 7432](#), DOI 10.17487/RFC7432, February 2015, <<https://www.rfc-editor.org/info/rfc7432>>.
- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in [RFC 2119](#) Key Words", [BCP 14](#), [RFC 8174](#), DOI 10.17487/RFC8174, May 2017, <<https://www.rfc-editor.org/info/rfc8174>>.
- [RFC8505] Thubert, P., Ed., Nordmark, E., Chakrabarti, S., and C. Perkins, "Registration Extensions for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery", [RFC 8505](#), DOI 10.17487/RFC8505, November 2018, <<https://www.rfc-editor.org/info/rfc8505>>.
- [RFC8365] Sajassi, A., Ed., Drake, J., Ed., Bitar, N., Shekhar, R., Uttaro, J., and W. Henderickx, "A Network Virtualization Overlay Solution Using Ethernet VPN (EVPN)", [RFC 8365](#), DOI 10.17487/RFC8365, March 2018, <<https://www.rfc-editor.org/info/rfc8365>>.

- [RFC8928] Thubert, P., Ed., Sarikaya, B., Sethi, M., and R. Struik, "Address-Protected Neighbor Discovery for Low-Power and Lossy Networks", [RFC 8928](#), DOI 10.17487/RFC8928, November 2020, <<https://www.rfc-editor.org/info/rfc8928>>.
- [RFC9047] Rabadan, J., Ed., Sathappan, S., Nagaraj, K., and W. Lin, "Propagation of ARP/ND Flags in an Ethernet Virtual Private Network (EVPN)", [RFC 9047](#), DOI 10.17487/RFC9047, June 2021, <<https://www.rfc-editor.org/info/rfc9047>>.
- [UNICAST-LOOKUP]  
Thubert, P. and E. Levy-Abegnoli, "IPv6 Neighbor Discovery Unicast Lookup", Work in Progress, Internet-Draft, [draft-thubert-6lo-unicast-lookup-02](#), 8 November 2021, <<https://datatracker.ietf.org/doc/html/draft-thubert-6lo-unicast-lookup-02>>.
- [I-D.thubert-6lo-multicast-registration]  
Thubert, P., "IPv6 Neighbor Discovery Multicast Address Registration", Work in Progress, Internet-Draft, [draft-thubert-6lo-multicast-registration-02](#), 8 October 2021, <<https://datatracker.ietf.org/doc/html/draft-thubert-6lo-multicast-registration-02>>.

## 12. Informative References

- [RFC6550] Winter, T., Ed., Thubert, P., Ed., Brandt, A., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, JP., and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", [RFC 6550](#), DOI 10.17487/RFC6550, March 2012, <<https://www.rfc-editor.org/info/rfc6550>>.
- [RFC8929] Thubert, P., Ed., Perkins, C.E., and E. Levy-Abegnoli, "IPv6 Backbone Router", [RFC 8929](#), DOI 10.17487/RFC8929, November 2020, <<https://www.rfc-editor.org/info/rfc8929>>.
- [RFC9010] Thubert, P., Ed. and M. Richardson, "Routing for RPL (Routing Protocol for Low-Power and Lossy Networks) Leaves", [RFC 9010](#), DOI 10.17487/RFC9010, April 2021, <<https://www.rfc-editor.org/info/rfc9010>>.
- [RIFT] Sharma, A., Thubert, P., Rijsman, B., Afanasiev, D., and A. Przygienda, "RIFT: Routing in Fat Trees", Work in Progress, Internet-Draft, [draft-ietf-rift-rift-15](#), 3 January 2022, <<https://datatracker.ietf.org/doc/html/draft-ietf-rift-rift-15>>.

Internet-Draft

EVPN Secure MAC

January 2022

[IANA-EARO-STATUS]

IANA, "Address Registration Option Status Values",  
<[https://www.iana.org/assignments/icmpv6-parameters/  
icmpv6-parameters.xhtml#address-registration](https://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xhtml#address-registration)>.

#### Authors' Addresses

Pascal Thubert (editor)  
Cisco Systems, Inc  
France

Phone: +33 497 23 26 34  
Email: pthubert@cisco.com

Tony Przygienda  
Juniper Networks, Inc  
Switzerland

Email: prz@juniper.net

Jeff Tantsura  
Microsoft

Email: jefftant.ietf@gmail.com

