RFC 6775 Extension

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

IETF 102

Montreal
Unmet expectations

• Solicited node multicast requires highly scalable L2 multicast
  IEEE does not provide it => turns everything into broadcast
  IPv6 ND appears to work with broadcast on 802.1 fabrics up to some scale ~10K nodes

• IPv6 ND requires reliable and cheap broadcast
  Radios do not provide that => conserving 802.1 properties over wireless is illusory
  RFC 4862 cannot operate as designed on wireless
  Address uniqueness is an unguaranteed side effect of entropy

• 802.11 expects proxy operation and broadcast domain separation
  802.11 provides a registration and proxy bridging at L2
  Requires the same at L3, which does not exist
  Implementations provide proprietary techniques based on snooping => widely imperfect

⇒ RFC 6775 solves the problem for DAD in one LL
⇒ This update enable establishing proxy services directly (ND for now), over a LLN, across multiple LLNs
What are the 6LoWPAN ND extensions?

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

• draft-ietf-6lo-rfc6775-update
  • Simplifies the protocol (no DAR/DAC for LL, no secondary NC)
  • Enables proxy registration
• draft-ietf-6lo-ap-nd
  • Protects addresses against theft (Crypto ID in registration)
• draft-ietf-6lo-backbone-router
  • Federates 6lo meshes over a high speed backbone
  • ND proxy that mimics 802.11 association but at Layer 3
RFC 6775 Update

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

Radio 1 Hop
RFC 6775 update

6LR

Radio Mesh
RFC 6775 update

6LBR

Ethernet
RFC 6775 update

6BBR

Ethernet
Classical ND

DAD time out

NA (O) *

SRC = 6BBR_II **
DST = NS SRC
TLLA = L6BR
TGT = LPN
UID = LPN
TID included

* Omitted in general
** link local
IESG Review (cont.)

RFC 6775 Update

Draft-…-17 to - 18
Need to vs. MUST on operator behaviour

• From Dave Thaler (added in 17)
  “In order to deploy this, network administrators MUST ensure that 6LR/6LBRs in their network support the number and type of devices that can register to them, based on the number of IPv6 addresses that those devices require and their address renewal rate and behavior. “

• Final text (since 18, with help from Warren Kumari and Ben Campbell)
  “Network administrators need to ensure that 6LR/6LBRs in their network support the number and type of devices that can register to them, based on the number of IPv6 addresses that those devices require and their address renewal rate and behavior.
  “
Mirja Kühlwind (in -18)

- TID Should be zero if the T flag is not set => text added
- Draft reads better if section 6 moves up

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.</td>
<td>Extended Address Registration Option (EARO)</td>
</tr>
<tr>
<td>4.2.</td>
<td>Extended Duplicate Address Message Formats</td>
</tr>
<tr>
<td>4.3.</td>
<td>Extensions to the Capability Indication Option</td>
</tr>
<tr>
<td>5.1.</td>
<td>Extending the Address Registration Option</td>
</tr>
<tr>
<td>5.2.</td>
<td>Transaction ID</td>
</tr>
<tr>
<td>5.2.1.</td>
<td>Comparing TID values</td>
</tr>
<tr>
<td>5.3.</td>
<td>Registration Ownership Verifier (ROVR)</td>
</tr>
<tr>
<td>5.4.</td>
<td>Extended Duplicate Address Messages</td>
</tr>
<tr>
<td>5.5.</td>
<td>Registering the Target Address</td>
</tr>
<tr>
<td>5.6.</td>
<td>Link-Local Addresses and Registration</td>
</tr>
<tr>
<td>5.7.</td>
<td>Maintaining the Registration States</td>
</tr>
<tr>
<td>6.1.</td>
<td>Backward Compatibility</td>
</tr>
<tr>
<td>6.2.</td>
<td>Signaling EARO Support</td>
</tr>
<tr>
<td>6.3.</td>
<td>RFC8775-only 6LN</td>
</tr>
<tr>
<td>6.4.</td>
<td>RFC8775-only 6LBR</td>
</tr>
<tr>
<td>7.1.</td>
<td>Security Considerations</td>
</tr>
<tr>
<td>8.1.</td>
<td>Privacy Considerations</td>
</tr>
<tr>
<td>8.2.</td>
<td>IANA Considerations</td>
</tr>
<tr>
<td>8.3.</td>
<td>New ARO Status values</td>
</tr>
<tr>
<td>9.1.</td>
<td>ARO Flags</td>
</tr>
<tr>
<td>9.2.</td>
<td>EARO T-Field</td>
</tr>
<tr>
<td>9.3.</td>
<td>ICMP Codes</td>
</tr>
<tr>
<td>10.1.</td>
<td>ARO Flags</td>
</tr>
<tr>
<td>10.2.</td>
<td>ICMP Codes</td>
</tr>
</tbody>
</table>
Benjamin Kaduk (in -18)

- "In general the Security and Privacy Considerations seem well thought-out"

- Non Zero status: an error?
  RFC 6775 section 8.2.5 has "In the case where the DAC indicates an error (the Status is non-zero)

- ROVER definition (ended up with text below, later split in the document)

  Enables the correlation between multiple attempts to register a same IPv6 Address. The ROVR is stored in the 6LR and the 6LBR in the state associated to the registration.
  This can be a unique ID of the Registering Node, such as the EUI-64 address of an interface. This can also be a token obtained with cryptographic methods which can be used in additional protocol exchanges to associate a cryptographic identity (key) with this registration to ensure that only the owner can modify it later.
  The scope of a ROVR is the registration of a particular IPv6 Address and it cannot be used to correlate registrations of different addresses.
This specification updates 6LoWPAN ND to simplify the registration operation in 6LoWPAN routers and to extend the protocol as a more generic registration technique. The specified updates enable other specifications to define new services such as Source Address Validation (SAVI) with [I-D.ietf-6lo-ap-nd], participation as an unaware leaf to an abstract routing protocol such as the "Routing Protocol for Low Power and Lossy Networks" [RFC6550] (RPL) with [I-D.thubert-roll-unaware-leaves], and registration to a backbone routers performing proxy Neighbor Discovery in a Low-Power and Lossy Network (LLN) with [I-D.ietf-6lo-backbone-router].
The Address Registration Option (ARO) is defined in section 4.1 of [RFC6775]. This specification introduces the Extended Address Registration Option (EARO) based on the ARO for use in NS and NA messages. The EARO conveys additional information such as a sequence counter called Transaction ID (TID) that is used to determine the latest location of a registering mobile device. A 'T' flag is added to indicate that the TID field is populated.

The EARO also signals whether the 6LN expects routing or proxy services from the 6LR using a new 'R' flag.

The EUI-64 field is overloaded and renamed ROVR in order to carry different types of information, e.g., cryptographic information of variable size. A larger ROVR size may be used if and only if backward compatibility is not an issue in the particular deployment.
Eric Rescorla (in -18)

- Cross check with AP ND, fixed mismatch in Leftmost vs. Rightmost bits
- Misc. Clarifications
- More comments / fixes on the ROVR field, e.g., be very specific on the length
Ben Campbell (in -18)

- Down references added during IESG review in terminology section
  - Not really solved to date. Created a separate reference section

11.2. Terminology Related References


Final fixes

RFC 6775 Update

Draft-…-19 to - 21
Charlie Perkins

• As an author and native speaker, Charlie made a final pass on the language and the organization
• Found that text was repeated, other was scattered
• Fixed the language, regrouped items
• E.g., took functional text out of the definition, to appropriate section
• Also removed extraneous references
• Work happened over draft 19-21
Issue 1: EDAR / EDAC extensibility

- The size of the ROVR was inferred from the size of the message
- Did not leave a possibility to insert options
- This might be desirable in the future, e.g., MAC Address option for a MAP server
- Long discussion, tried multiple possibilities
- Ended up with split ICMP Code, similar to what we discussed with Adrian Farrell
- Added in draft -20
RFC 6775 update new features: ICMP code split

Code: The ICMP Code [RFC4443] for Duplicate Address Messages is split in two 4-bit fields, the Code Prefix and the Code Suffix.
Code:

The ICMP Code [RFC4443] for Duplicate Address Messages is split in two 4-bit fields, the Code Prefix and the Code Suffix. The Code Prefix MUST be set to zero by the sender and MUST be ignored by the receiver. A non-null value of the Code Suffix indicates support for this specification. It MUST be set to 1 when operating in a backward-compatible mode, indicating a ROVR size of 64 bits. It MAY be 2, 3 or 4, denoting a ROVR size of 128, 192, and 256 bits, respectively.
Issue 2: Enabling Other Routing Registrars

• 6BBR is only one possible routing registrar. Others include RPL [I-D.thubert-roll-unaware-leaves] and RIFT [I-D.ietf-rift-rift]

• Resolution to use a generic term as opposed to mention 6BBR specifically

• Also allow an opaque field. RPL uses it for instance ID.

• Added in draft -19

• Generalization to the term « routing registrars » in -21
RFC 6775 update new features: the Opaque field

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
<th>Status</th>
<th>Opaque</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Rsvd</th>
<th>I</th>
<th>R</th>
<th>T</th>
<th>TID</th>
<th>Registration Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

... Registration Ownership Verifier (ROVR) ...

Opaque:
An octet opaque to ND; the 6LN MAY pass it transparently to another process. It MUST be set to zero when not used.
### RFC 6775 update new features: the I field

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

| +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ |
| | Type | Length | Status | Opaque | |
| +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ |
| | Rsvd | I | R | T | TID | Registration Lifetime | |
| +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ |
| | ... | Registration Ownership Verifier (ROVR) | ... |
| +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ |

**I:** Two-bit Integer: A value of zero indicates that the Opaque field carries an abstract index that is used to decide in which routing topology the address is expected to be injected.
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
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?
AP-ND Status, talks with Eric Rescorla

• Quite Stable, not republished since IETF 101
• Fixed inconsistency with RFC 6775 update in RFC 6775 update (Eric Rescorla)
• Multiple talks to sync with Eric, but then no change done yet.
• Need to clarify key encoding
  Draft uses DER. Behcet recommended lihter like Jason Web Key.
  Eric: “Aren't you using EC keys? If so, why do you need *either* encoding.” ?
• Remove text on 64-bits identifiers since ROVR is up to 256 bits
• 256 bits solves many concerns about security that Eric had.
Radio 1 Hop

AP-ND

NS (EARO(ROVR=Crypto-ID))

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

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

NA (EARO(status=0))

* Crypto-ID Parameters Option
** NDP Signature Option

RFC 6775 update
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

Radio 1 Hop  RPL  Ethernet / Wi-Fi  Ethernet

RFC 6775 update  RFC 6550  RFC 6775 update  Classical ND

NS (EARO)  RPL DAO  Proxy NS (EARO)

NA (EARO)  DAO-ACK  NA (EARO)

NA (EARO)  NS lookup  NA (~O)

Packet
RPL cannot DAD for lack of ROVR

Radio 1 Hop

NS (ARO)

SRC = LPN
DST = 6LR
TGT = LPN
SLLA = LPN
UID = LPN
TID included

RPL DAO

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

* Parent in storing mode

NS (ARO)

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

* From binding state

NS lookup

NA (~O)

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

- Quite Stable, not republished since IETF 101
- WGLC?