IPv4 Residual Deployments
Unified Packet Format for Stateless solutions
(4rd-U)

draft-despres-softwire-4rd-u-01
**4rd-U vs. Translation and Encapsulation vs.**

<table>
<thead>
<tr>
<th>TRANSLATION</th>
<th>ENCAPSULATION</th>
<th>4rd-U</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>IPv6</code> <code>Header</code></td>
<td><code>IPv6</code> <code>Header</code></td>
<td>• Fragment header always present</td>
</tr>
<tr>
<td><code>Fragment</code> <code>Header</code></td>
<td><code>Fragment</code> <code>Header</code></td>
<td>• No Transport-layer modification</td>
</tr>
<tr>
<td><code>IPv6</code> <code>Header</code></td>
<td><code>IPv4</code> <code>Header</code></td>
<td>• Shorter header than encapsulation</td>
</tr>
<tr>
<td><code>Transport-Layer</code> <code>Header</code></td>
<td><code>IP-layer</code> <code>Data</code></td>
<td></td>
</tr>
<tr>
<td><code>IP-layer</code> <code>Data</code></td>
<td><code>IP-layer</code> <code>Data</code></td>
<td></td>
</tr>
<tr>
<td><code>Data</code></td>
<td><code>Data</code></td>
<td></td>
</tr>
</tbody>
</table>

(RFC 6145)
Why it is useful?

2. Current O&M tools of IPv6-only domains use port fields of IPv6 packets to do access control (ACLs). Having them ready for encapsulated IPv4 packets MAY take a long time
   ➔ advantage to Double-translation

3. Web redirection in IPv6-only domains MAY require valid TCP checksums in IPv6 payloads
   ➔ advantage to Double-translation

1. IPv4 and IPv6 treat fragmentation differently so that the IPv4 DF bit MAY be lost in Translation
   ➔ advantage to Encapsulation

4. If IPv6-domain traversal by IPv4 packets is subject to its own IPv6 traffic class, the IPv4 TOS MAY be lost
   ➔ advantage to Encapsulation
Why it is possible?

1. IPv6 packets have an optional Fragment header.
2. In this header, the packet ID field has 32 bits more than that of IPv4 headers
3. Only 9 bits of IPv4 headers are missing for end-to-end transparency in case of translation (DF bit and TOS octet)
4. Checksum validity of UDP/TCP can be ensured in 4rd-U packets without any change in IP payload (using for this the 16 last bits of IPv6 addresses)
How it works – (1) From IPv4 to IPv6

HEADER-FIELDS

- 7 are constant
- 7 are COPIED (DF and TOS in packet ID)
- 1 is /MODIFIED/ by adding a constant
- 2 *ADDRESS MAPPINGS*
How it works – (2) From IPv6 to IPv4

**HEADER-FIELDS**

- **3** are constant
- **7** are **COPIED**
  - **1** is /MODIFIED/ by adding a constant
  - **2** are *ADDRESS MAPPING* derived
- **1** is "COMPUTED" *(header checksum)*
A checksum-neutral Address-Mapping (CE address)

CE IPv4 address (32)
CE Max PSID (12)

Rule IPv4 prefix

Rule IPv6 prefix
Max IPv4 suffix
Max PSID
Padding (≥ 0)

Unformatted IPv6 address

IPv6 address

V: 4rd mark
(permits to use the CE IPv6 prefix for 4rd without possible conflict with any valid IPv6 address)

CNP: Checksum Neutrality Preserver
(computed from IPv4 address + A.V.B)
A checksum-neutral Address-Mapping (BR address)

Prefix of the BR that has the Rule whose IPv4 prefix applies to the CE prefix

Checksum Neutrality Preserver (similar computation)
4rd-U in the global picture

<table>
<thead>
<tr>
<th></th>
<th>Possibility of:</th>
<th>MAP Trans</th>
<th>MAP Encap</th>
<th>Stateless DS-lite</th>
<th>4rd-U</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Direct CE-CE routes</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>2</td>
<td>Full IPv4 Transparency</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>3</td>
<td>Use of IPv6 O&amp;M tools and Web redirect</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>4</td>
<td>Changing IPv4 pool and/or sharing ratio without IPv6 renumbering</td>
<td>Y (TBD)</td>
<td>Y (TBD)</td>
<td>Y (TBD)</td>
<td>Y (TBD)</td>
</tr>
<tr>
<td>5</td>
<td>Operation on IPv4-only networks of the NAT444 model</td>
<td>Y (4rd-T/6rd)</td>
<td>Y (4rd-E/6rd)</td>
<td>Y (*) (SDNAT/RFC1918)</td>
<td>Y (4rd-U/6rd)</td>
</tr>
</tbody>
</table>

(*) No IPv6 service
Additional feature (not in draft)
Avoid fragment processing in BR from non-shared-address CE

• In BRs, fragmented packets from shared-address CE need some reassembly processing to check ports of all fragments
• If BRs don't know whether source CE have a shared address or not, they do this processing even if not needed
• CE sources can indicate whether they have shared or non-shared addresses in one of the 7 remaining free bits in IPv6 fragment headers.
Conclusion

The 4rd-U design is a proposed for stateless IPv4 residual deployments across IPv6-capable domains as basis of a unique standard