464XLAT/NAT64 Deployment Guidelines in Operator and Enterprise Networks

LACNIC 32 / LACNOG 2019
Panamá
September, 2019

@JordiPalet
(jordi.palet@theipv6company.com)
draft-ietf-v6ops-nat64-deployment

- https://datatracker.ietf.org/doc/draft-ietf-v6ops-nat64-deployment
RFCxxx (approved ALREADY by IESG, still no number)

- How an ISP (broadband or cellular) or Enterprise should deploy 464XLAT/NAT64?

- Is NAT64 (with DNS64) a valid approach?

- What are the possible deployment scenarios?

- What are the issues to consider?
Scenarios Considerations

- There are hosts that will be validating DNSSEC?
- Are IPv4 literals or non-IPv6-compliant APIs used?
- There are IPv4-only hosts or apps?

- As a result, two major groups
  - Known to work
  - Known to work under special conditions
    - Not part of this presentation, very special scenarios
    - Example, “close networks” or ”strict control” of all the clients or servers
NAT64 + DNS64

Figure 1: NAT64 with DNS64

Figure 2: NAT64 in external service provider

Figure 3: NAT64 and DNS64 in external provider

Figure 4: NAT64; DNS64 by external provider
464XLAT without DNS64

Figure 8: 464XLAT without DNS64

Figure 9: 464XLAT without DNS64; NAT64 in external provider
Comparing Scenarios (1)

Criteria:

a. DNSSEC: Are there hosts validating DNSSEC?
b. Literal/APIs: Are there applications using IPv4 literals or non-IPv6 compliant APIs?
c. IPv4-only: Are there hosts or applications using IPv4-only?
d. Foreign DNS: Is the scenario surviving if the user, Operating System, applications or devices change the DNS?
e. DNS load opt. (DNS load optimization): Are there extra queries that may impact DNS infrastructure?
f. Connect. opt. (Connection establishment delay optimization): Is the UE/CE issuing only the AAAA query or also an A query and waiting for both responses?
Comparing Scenarios (2)

<table>
<thead>
<tr>
<th>Item / Figure</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNSSEC</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Literal/APIs</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>-</td>
</tr>
<tr>
<td>IPv4-only</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>-</td>
</tr>
<tr>
<td>Foreign DNS</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>-</td>
</tr>
<tr>
<td>DNS load opt.</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Connect. opt.</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
</tbody>
</table>

"-" Scenario "bad" for that criteria.

"+" Scenario "good" for that criteria.

"*" Scenario "bad" for that criteria, however it is typically resolved, with the support of Happy Eyeballs v2 [RFC8305].
Scenarios Summary

As a general conclusion, if the network must support applications using any of the following:
  - IPv4 literals
  - non-IPv6-compliant APIs
  - IPv4-only hosts or applications

Then, only the scenarios with 464XLAT, a CLAT function, or equivalent built-in local address synthesis features, will provide a valid solution.

Further to that, those scenarios will also keep working if the DNS configuration is modified. Clearly also, depending on if DNS64 is used or not, DNSSEC may be broken for those hosts doing DNSSEC validation.

All the scenarios are good in terms of DNS load optimization, and in the case of 464XLAT it may provide an extra degree of optimization.

Finally, all them are also good in terms of connection establishment delay optimization. However, in the case of 464XLAT without DNS64, it requires the usage of Happy Eyeballs v2.
  - This is not an issue, as commonly it is available in actual Operating Systems.
Issues (1)

• What the ISP needs to consider for a deployment?
• All the issues may bring to a specific decision points about how to approach the deployment
Issues (2)

- DNSSEC Considerations and Possible Approaches
  - Not using DNS64
  - DNSSEC validator aware of DNS64
  - Stub validator
  - CLAT with DNS proxy and validator
  - ACL of clients
  - Mapping-out IPv4 addresses
Issues (3)

• DNS64 and Reverse Mapping
  – Just works!

• Using 464XLAT with/without DNS64
  – With DNS64:
    • Double-translation, about 1% CLAT usage (literals & non-compliant APIs) + NAT64
    • NAT64 single translation, about 24%
  – Without DNS64:
    • 25% double-translation
Issues (4)

• Foreign DNS
  – Manual Configuration of DNS
  – DNS Privacy/Encryption Mechanisms
    • Big issue with DNS64
      – Not supported by DNS over TLS/DTLS/HTPS/QUIC
    – Split DNS/VPNs
Issues (5)

- Well-Known Prefix (WKP) vs Network-Specific Prefix (NSP)
- IPv4 literals and non-IPv6 Compliant APIs
- IPv4-only Host or Applications
- CLAT Translation Considerations
- EAM Considerations
- Incoming Connections
  - STUN, TURN, ICE, PCP, EAM
Deployment in Enterprise Networks

Figure 14: IPv6-only enterprise with NAT64 and DNS64

Figure 15: DS enterprise with CLAT, DS Internet, without DNS64

Figure 16: DS enterprise with CLAT, IPv6-only Access, without DNS64
Summary

• NAT64 (with DNS64) is not a solution
• 464XLAT works in all the cases
  – A CLAT solve the issues even if DNS64 is not present or is broken
• Host OSs should consider self-synthesis

• Annex A: Example of Broadband Deployment with 464XLAT
• Annex B: CLAT Implementation
Thanks!

Contact:

@JordiPalet
jordi.palet@theipv6company.com