IPv6 Specifications to Internet Standard *Open Issues*

Ole Trøan, otroan@employees.org

Plan (from IETF 93)

- Re-classify to Internet Standard draft standard documents that require no changes. (IESG action)
- Start work on those that require updates. Restricted to errata and updates that meet the criteria for Internet standard.
- Phase 2 (Proposed standards documents)
  - Work started on RFC6434 IPv6 Node Requirements

Documents being updated

- RFC2460 – Internet Protocol, Version 6 (IPv6) Specification
<draft-ietf-6man-rfc2460bis-05>

- RFC4291 – IP Version 6 Addressing Architecture
<draft-ietf-6man-rfc4291bis-03>

- RFC1981 - Path MTU Discovery for IP version 6
<draft-ietf-6man-rfc1981bis-02>

Documents ready to advance

- RFC3596 – DNS Extensions to Support IP Version 6
- ~~RFC4941 – Privacy Extensions for Stateless Address Autoconfiguration in IPv6~~
- RFC4443 – Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification

Updates since IETF 95

- Updated 2460bis, 4291bis and 1981bis
- Removed RFC4941 from the core set of specifications to advance
- Initiated WGLC: May 30th -> June 13th
  - Issues tracked at: https://trac.tools.ietf.org/wg/6man/trac/report/1

RFC4291bis

- Updated revision 03:
  - Replaced reference to default-iid with RFC7217 and RFC7721
- 1 can be closed ticket: Reference to default-iid

RFC4291bis IID text

2.4.1. Interface Identifiers

The details of forming interface identifiers are defined in other specifications, such as "Privacy Extensions for Stateless Address Autoconfiguration in IPv6" [RFC4941] **or "A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)"[RFC7217]**. Specific cases are described in appropriate "IPv6 over <link>" specifications, such as "IPv6 over Ethernet" [RFC2464] and "Transmission of IPv6 Packets over ITU-T G.9959 Networks" [RFC7428]. **The security and privacy considerations for IPv6 address generation is described in [RFC7721].**

RFC1981bis

- Updated revision 02:
  - Added regardless of whether it decrements the hop limit
- 1 can be closed issue: Regardless of whether it decrements the Hop Limit

RFC1981bis
Regardless of decrementing HL

3. Protocol Overview

This memo describes a technique to dynamically discover the PMTU of a path. The basic idea is that a source node initially assumes that the PMTU of a path is the (known) MTU of the first hop in the path. If any of the packets sent on that path are too large to be forwarded by some node **(regardless of whether it decrements the Hop Limit)** along the path, that node will discard them and return ICMPv6 Packet Too Big messages [ICMPv6]. Upon receipt of such a message, the source node reduces its assumed PMTU for the path based on the MTU of the constricting hop as reported in the Packet Too Big message.

RFC2460bis

- Updated revision 05:
    - Updated reference: [I-D.ietf-6man-rfc4291bis]
    - Text on header injection
    - s/should/may for HBH processing
- May be closed tickets: HBH header handling, Header injection
- Tim's review: https://mailarchive.ietf.org/arch/msg/ipv6/bqX1kbizkqHM3HMkr4IT662iS40

RFC2460bis
Header injection issue

- Ambiguity in 2460. Can an intermediate node insert (or delete) IPv6 extension headers or options into a packet?
  - RFC4782 (experimental): Has text on deletion options in HBH extension header.
- Not here to design how header injection can work or not work
- >50 messages to the list sine mid June
- Make sure we have future proof and testable text

RFC2460bis Header injection Revision 05

The insertion of Extension Headers by any node other than the source of the packet breaks PMTU-discovery and can result in ICMP error messages being sent to the source of the packet that did not insert the header.

The current approach to allowing a header to be inserted is to encapsulate the packet using another IPv6 header and including the additional extension header after the first IPv6 header, for example, as defined in [RFC2473].

RFC2460bis HBH

4. IPv6 Extension Headers

The exception referred to in the preceding paragraph is the Hop-by-Hop Options header, which carries information that **may** be examined and processed by every node along a packet's delivery path, including the source and destination nodes. The Hop-by-Hop Options header, when present, must immediately follow the IPv6 header. Its presence is indicated by the value zero in the Next Header field of the IPv6 header.

NOTE: While [RFC2460] required that all nodes must examine and process the Hop-by-Hop Options header, it is now expected that nodes along a packet's delivery path only examine and process the Hop-by-Hop Options header if explicitly configured to do so.

4.3. Hop-by-Hop Options Header

The Hop-by-Hop Options header is used to carry optional information that **may** be examined and processed by every node along a packet's delivery path. The Hop-by-Hop Options header is identified by a Next Header value of 0 in the IPv6 header, and has the following format:

Next steps:

- Reach consensus on open issues!
- Request IESG to advance to Internet Standard
    - RFC3596, RFC4941, RFC4443
    - Draft letter to IESG in email link