IPv6 to Internet Standard

Bob Hinden

IETF97 Seoul

Background

- Goal is to move the core IPv6 RFCs to Internet Standard

- Internet Standard is defined in RFC 2026 as
  - An Internet Standard is characterized by a high degree of technical maturity and by a generally held belief that the specified protocol or service provides significant benefit to the Internet community.

RFC6410 Defines Advancement Process

- There are at least two independent interoperating implementations with widespread deployment and successful operational experience.
  (1) There are no errata against the specification that would cause a new implementation to fail to interoperate with deployed ones.
  (2) There are no unused features in the specification that greatly increase implementation complexity.
  (3) If the technology required to implement the specification requires patented or otherwise controlled technology, then the set of implementations must demonstrate at least two independent, separate and successful uses of the licensing process
  (4) If the technology required to implement the specification requires patented or otherwise controlled technology, then the set of implementations must demonstrate at least two independent, separate and successful uses of the licensing process.

Advancing Draft Standards

- Any protocol or service that is currently at the abandoned Draft Standard maturity level will retain that classification, absent explicit actions. Two possible actions are available:

  (1) A Draft Standard may be reclassified as an Internet Standard as soon as the criteria in Section 2.2 are satisfied.

  (2) At any time after two years from the approval of this document as a BCP, the IESG may choose to reclassify any Draft Standard document as Proposed Standard.

Updating RFCs

- RFC6410 doesn’t mention Updating RFCs
- Current advice from the ADs is that updating RFCs need to be incorporated
- Will have to show that updates have been implemented and meet RFC6410 criteria
- If no implementation experience, we can not include in bis version

Plan Presented at IETF93

- 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)

Documents being Updated

- RFC2460 – Internet Protocol, Version 6 (IPv6) Specification
  - <draft-ietf-6man-rfc2460bis-07>
- RFC4291 – IP Version 6 Addressing Architecture
  - <draft-ietf-6man-rfc4291bis-05>
- RFC1981 - Path MTU Discovery for IP version 6
  - <draft-ietf-6man-rfc1981bis-03>

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

Changes to rfc1981bis since IETF96

- 03) Remove text in Section 5.3 regarding RH0 since it was deprecated by RFC5095.

> For source routed packets (i.e. packets containing an IPv6 Routing header [I-D.ietf-6man-rfc2460bis]), the source route may further qualify the local representation of a path. ~~In particular, a packet containing a type 0 Routing header in which all bits in the Strict/ Loose Bit Map are equal to 1 contains a complete path specification. An implementation could use source route information in the local representation of a path.~~

Changes to rfc4291bis since IETF96

- 04) Removed old IANA Considerations text, this was left from the baseline text from RFC4291 and should have been removed earlier.

- 05) Added instructions in IANA Considerations to update references in the IANA registries that currently point to RFC4291 to point to this document.

IANA Considerations

RFC4291 is referenced in a number of IANA registries. These include:

- o Internet Protocol Version 6 Address Space [IANA-AD]
- o IPv6 Global Unicast Address Assignments [IANA-GU]
- o IPv6 Multicast Address Space Registry [IANA-MC]
- o Application for an IPv6 Multicast Address [IANA-MA]
- o Internet Protocol Version 6 (IPv6) Anycast Addresses [IANA-AC]
- o IANA IPv6 Special-Purpose Address Registry [IANA-SP]
- o Reserved IPv6 Interface Identifiers [IANA-ID]
- o Number Resources [IANA-NR]
- o Protocol Registries [IANA-PR]
- o Technical requirements for authoritative name servers [IANA-NS]
- o IP Flow Information Export (IPFIX) Entities [IANA-FE]

The IANA should update these references to point to this document.

There is a reference to RFC4291 (and RFC3307) that appears to be incorrect and should be removed in:

- o Modify a Port Number assignment [IANA-PN]

There are also other references in IANA procedures documents that the IANA should investigate to see if they should be updated.

Changes to rfc4291bis since IETF96

- 04) Added text and a pointer to the ULA specification in Section 2.4.7.

- 05) Rename Section 2.4.7 to "Other Local Unicast Addresses" and rewrote the text to point to ULAs and say that Site-Local addresses were deprecated by RFC3879. The format of Site-Local was removed.

2.4.7. Other Local Unicast IPv6 Addresses

Unique Local Addresses (ULA) [RFC4193], the current form of Local IPv6 Addresses, are intended to be used for local communications, have global unicast scope, and are not expected to be routable on the global Internet.

Site-Local addresses, deprecated by [RFC3879], the previous form of Local IPv6 Addresses, were originally designed to be used for addressing inside of a site without the need for a global prefix.

The special behavior of Site-Local defined in [RFC3513] must no longer be supported in new implementations (i.e., new implementations must treat this prefix as Global Unicast). Existing implementations and deployments may continue to use this prefix.

Changes to rfc4291bis since IETF96

- 05) Added to Section 2.4.1 a reference to RFC7421 regarding the background on the 64 bit boundary in Interface Identifiers.

> For all unicast addresses, except those that start with the binary value 000, Interface IDs are required to be 64 bits long. **Background on the 64 bit boundary can be found in [RFC7421].**

Changes to rfc4291bis since IETF96

- 05) Expanded Security Considerations Section to discuss privacy issues related to using stable interface identifiers to create IPv6 addresses, and reference solutions that mitigate these issues such as RFC7721, RFC4941, RFC7271.

  One area relevant to IPv6 addressing is privacy. IPv6 addresses can be created using interface identifiers constructed with unique stable tokens. The addresses created in this manner can be used to track the movement of devices across the Internet. Since earlier versions of this document were published, several approaches have been developed that mitigate these problems. These are described in "Security and Privacy Considerations for IPv6 Address Generation Mechanisms" [RFC7721], "Privacy Extensions for Stateless Address Autoconfiguration in IPv6" [RFC4941], and "A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)"[RFC7217].

Changes to rfc2460bis since IETF96

- 6) & 7) Revised the text in Section 4.8

New extension headers that require hop-by-hop behavior must not be defined because as specified in Section 4 of this document, the only Extension Header that has hop-by-hop behavior is the Hop-by-Hop Options header.

New hop-by-hop options are not recommended because nodes may be configured to ignore the Hop-by-Hop Option header, drop packets containing a hop-by-hop header, or assign packets containing a hop-by-hop header to a slow processing path. Designers considering defining new hop-by-hop options need to be aware of this likely behavior. There has to a very clear justification why any new hop-by-hop option is needed before it is standardized.

Defining new IPv6 extension headers is not recommended. There has to a very clear justification why any new extension header is needed before it is standardized. Instead of defining new Extension Headers, it is recommended that the Destination Options header is used to carry optional information that need be examined only by a packet's destination node(s), because they provide better handling and backward compatibility.

Changes to rfc2460bis since IETF96

- 06) Moved the text in Section 4.5 regarding the handling of received overlapping fragments to the list of error conditions

If any of the fragments being reassembled overlaps with any other fragments being reassembled for the same packet, reassembly of that packet must be abandoned and all the fragments that have been received for that packet must be discarded and no ICMP error messages should be sent.

Changes to rfc2460bis since IETF96

- 06) Added the Routing Header to the list required extension headers that a full implementation includes.

Hop-by-Hop Options
Fragment
Destination Options
Routing
Authentication
Encapsulating Security Payload

Changes to rfc2460bis since IETF96

- 07) Added additional registries to the IANA Considerations section that IANA needs to update

Internet Protocol Version 6 (IPv6) Parameters [IANA-6P]

Assigned Internet Protocol Numbers [IANA-PN]

ONC RPC Network Identifiers (netids) [IANA-NI]

Technical requirements for authoritative name servers [IANA-NS]

Network Layer Protocol Identifiers (NLPIDs) of Interest [IANA-NL]

Protocol Registries [IANA-PR]

Structure of Management Information (SMI) Numbers (MIB Module Registrations) [IANA-MI]

Changes to rfc2460bis since IETF96

- 07) Added clarification that no ICMP error message should be sent if overlapping fragments are received.

  - o If any of the fragments being reassembled overlaps with any other fragments being reassembled for the same packet, reassembly of that packet must be abandoned and all the fragments that have been received for that packet must be discarded **and no ICMP error messages should be sent**.

Changes to rfc2460bis since IETF96

- 07) Moved the text regarding network duplicated fragments to the received fragment error section.

> It should be noted that fragments may be duplicated in the network. Instead of treating these exact duplicate fragments as an overlapping fragments, an implementation may choose to detect this case and drop exact duplicate fragments while keeping the other fragments belonging to the same packet.

Changes to rfc2460bis since IETF96

- 07) Added paragraph to Section 4 to clarify how Extension Headers are numbered and which are upper-layer headers.

> Extension Headers are numbered from IANA IP Protocol Numbers [IANA-PN], the same values used for IPv4 and IPv6. When processing a sequence of Next Header values in a packet, the first one that is not an Extension Header [IANA-EH] indicates that the next item in the packet is the corresponding upper-layer header. A special "No Next Header" value is used if there is no upper-layer header.

Changes to rfc2460bis since IETF96

- 07) Expanded Security Considerations section to include both IPSEC and encryption at higher levels in the protocol stack.

IPv6, from the viewpoint of the basic format and transmission of packets, has security properties similar to IPv4. Risks of corruption, forgery, and interception of packets, resulting in the exposure of private information, may be mitigated by use of the Security Architecture for the Internet Protocol [RFC4301] or encryption at higher layers of the protocol stack.

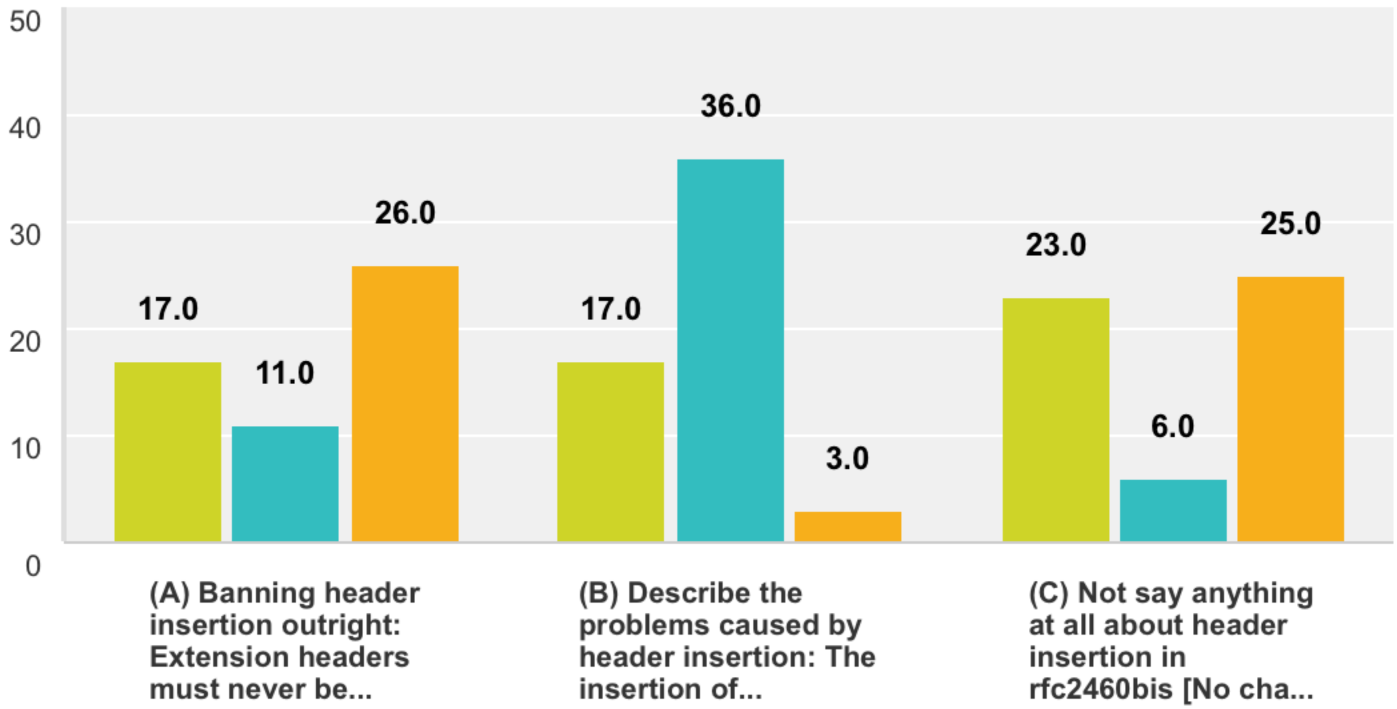
Last Issue: Text on Extension Header Insertion

- Lots of discussion on mailing list and face to face meetings.
- Chairs ran an online Survey to better access w.g. concensus
- Three choices:
  - A) Ban header insertion
  - B) Describe the problems with header insertion
  - C) Say nothing

Results of Survey

Indicate your preference for how to handle Extension Header Insertion in RFC2460bis.
1 is the highest preference, 3 is the lowest.

Answered: 57 Skipped: 0



Chairs Conclusions

- There is much stronger support to describe the problem than the other two choices. Specifically if the we combine the high and medium choices:

A) Ban Header Insertion	28
B) Describe the Problem	53
C) Not say anything	29

- Condorcet calculator confirmed the B) choice as the result of the poll.
- Chairs declare there is a consensus to include the text that describes the problems with Header Insertion in rfc2460bis.

Proposed Text

The insertion of Extension Headers by any node other than the source of the packet causes serious problems. Two examples include breaking the integrity checks provided by the Authentication Header Integrity [RFC4302], and breaking Path MTU Discovery which can result in ICMP error messages being sent to the source of the packet that did not insert the header.

One approach to avoid these problems 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].

神明達哉 Jinmei Proposal

In the original design of IPv6 extension headers at the time [RFC2460], extension headers are not supposed to be inserted (or deleted) by any node other than the source of the packet. In fact, the insertion of Extension Headers by an intermediate node causes serious problems. Two examples include breaking the integrity checks provided by the Authentication Header Integrity [RFC4302], and breaking Path MTU Discovery which can result in ICMP error messages being sent to the source of the packet that did not insert the header.

Some recently developed attempts have sought to loosen the restriction and allow the insertion and removal of extension headers at intermediate nodes under some particular set of conditions. A future update to the protocol may allow such flexible behavior. Until the conditions that can safely allow it are figured out, however, it is prudent for newer protocols to assume the originally intended restrictions.

One **safe** approach to avoid these problems 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].

Closure on Header Insertion

- Chairs would like feedback from working group on Header Insertion text

- Important to close discussion on this topic today and confirm on mailing list

Next Steps

- ✓ Plan sent to IPv6 list 21 March 2016
  - http://mailarchive.ietf.org/arch/msg/ipv6/2OLUuUpuGfv3N6e0oHSuAL-djOU
- ✓ Working group last calls for Internet Standard
  - RFC2460bis, RFC4291bis, RFC1981bis
  - Request reviewers for the set
- Submit RFC2460bis, RFC4291bis, RFC1981bis for Internet Standard
- Request IESG to reclassify as Internet Standard
  - RFC3596 and RFC4443

QUESTIONS / COMMENTS?