draft-ietf-lpwan-ipv6-static-context-hc-16

Authors:
Laurent Toutain <Laurent.Toutain@imt-atlantique.fr>
Carles Gomez <carlesgo@entel.upc.edu>
Ana Minaburo <ana@ackl.io>
Dominique Barthel <dominique.barthel@orange.com>
Presentation agenda

- What has happened since IETF101? [3 mn]
- What is coming up next? [1 mn]
- Ticket status [1 mn]
- Single padding [10 mn]
- Appendix D, Ticket #15 [5 mn]
- Comments received since WGLC2 [25 mn]
What has happened since IETF101?
What has happened since IETF101?

- Formally closed tickets solved in -10
- Published -11 on Apr 13th
  - Improved Fig 3, Appendix D, when no Dtag, no R
- Published -12 on May 15th
  - SCHC F/R, LSB(y) -> LSB
- Published -13 on May 22nd
  - variable length field text (Ticket #18)
What has happened since IETF101?

• -14, -15 and -16 published on June 29th
  – L2 Word, single padding, RuleID identical in frag and ACK, UDP checksum elision text, fixed Ack-Always sender FSM, C-bit bump
• Second WGLC initiated on June 29th, closing now
• Pascal’s shepherd review comments July 3rd
  – Presented at interim July 7th
• More comments received recently
  – Lars, Edgar, Soichi (hackathon), Charlie, Juan-Carlos
What is coming up next?
What is coming up next?

• WGLC2 closure today
• Process comments received
  – Pascal, Lars, Edgar, Soichi, Charlie, Juan-Carlos
  – See dedicated section in this presentation
• Publish -17 soon
• Sepherd to request publication to IESG
Ticket status
Tickets

• All Tickets by the LPWAN WG

• Selective link to Tickets pertaining to this draft
  – [ipv6-schc-all-tickets](https://trac.ietf.org/trac/lpwan/report/6)

• As of today, 29 tickets pertain to this draft
  – that is, #2-#26 and #28-#31
  – all CLOSED, ticket #6 might be re-opened (see last comments received)

• Resolution for each Ticket
  – tracked in Appendix to this presentation, see at bottom
  – recap mail to be sent out soon

• New tickets opened as a response to recent comments?
Single padding
Single padding, timeline

- Idea floated at interim May 16th
- Virtual corridor meeting May 22nd
- Full-fledged proposal presented at interim May 30th
- Mail sent out to WG ML on May 30th, again June 5th
- Received 6 positive response, 0 objection
- Decision to integrate proposal at Jun 13th interim
- First appearance in -14, June 29th
Padding, until -13

- If padding enabled, two paddings in series
Padding, until -13

- If padding enabled, two paddings in series

Integer number of bytes

SCHC Packet

Compressed Header Payload Pad1

SCHC Fragments

Frag Header Frag Payload

Frag Header (MIC) Frag Payld Pad2

Integer number of bytes

Weird size

Complementarily-weird size
Padding, until - I 3

- If padding enabled, two paddings in series
Padding, from -14 onward

- Padding done at most once
- L2 Word can be 1 byte, 1 bit, ...

A packet (e.g. an IPv6 packet)

---

<table>
<thead>
<tr>
<th>SCHC Compression</th>
</tr>
</thead>
</table>

If no fragmentation

| SCHC Packet + padding as needed |

---

<table>
<thead>
<tr>
<th>SCHC Fragmentation</th>
</tr>
</thead>
</table>

| SCHC ACK |

| SCHC Fragments + padding as needed |

---

+---- last SCHC Frag with MIC + padding as needed +----

( padding bits dropped)

(MIC checked and removed)
Padding, from -14 onward

- Padding done at most once
- L2 Word can be 1 byte, 1 bit, ...

Integer number of L2 Words

SCHC Packet

Compressed Header Payload Pad1

SCHC Fragments

Frag Header Frag Payload

Frag Header (MIC) Frag Payld Pad2

Weird size

Complementarily-weird size

Integer number of L2 Words
Padding, from -14 onward

- Padding done at most once
- L2 Word can be 1 byte, 1 bit, ...

A packet (e.g. an IPv6 packet)

Padding done at most once

L2 Word can be 1 byte, 1 bit, ...

SMR Context

SCHC Compression

If no fragmentation

SCHC Packet + padding as needed

SCHC Fragmentation

SCHC Packet + padding as needed

SCHC Reassembly

SCHC ACK

SCHC Fragments

last SCHC Frag with MIC + padding as needed

SENDER

RECEIVER

(padding bits dropped)

(MIC checked and removed)
Appendix D:
parameter/choices left to each
technology-specific document
Appendix D

• Text is still rough
• Is an Appendix the right place for this info?
  – Is this normative content?
Appendix D, current listing

• Use-case, deployment
• Mapping of architectural elements
• L2 integrity checking
• RuleID numbering, format
• L2 Word
• Fragmentation by SCHC?
  – Reliability modes, concurrent transmission, parameters, timers
Comments received since WGLC2
Lars

- traffic class field contains ECN bits. The “ignore” MO will bleach them out
  - Good point, will be taken into account
  - Is a device sensitive to ECN? So far, no Layer 4 in LPWAN space uses ECN, so can safely ignore it.
  - In the future, could transmit it in full or could use send-LSB CDA
• Write “L2 MTU” instead of “L2 data unit”
  – We will update text
Soichi

- Hackathon: working on implementation, with standard CRC library. They are byte-oriented.
  - In theory, CRC can be computed on any bit array
  - Specify byte fill-up for MIC computation?
  - Leave to technology-specific draft to specify MIC computation?
Pascal

- partially filled all-0 windows is complex, creates unnecessary complication and confusion in description
What if windows can be partially filled?

![Diagram showing protocol interaction](image)

Receiver

Ack-Always

Sender

- FCN = 4
- FCN = 3
- FCN = 2
- FCN = all-0

ACK bitmap

Retransmission timer expiration

empty all-0

ACK bitmap

w = 0

w = 1

FCN = 4

Time
Partially filled windows?

• 3 options
  – Leave situation unchanged, retransmission timer will trigger sending the « empty All-0 » frag
  – Mandate that windows MUST be full (but the last)
  – Mandate that (empty) All-0 frag be sent at the end of each retransmission burst
Partially filled windows?

- Proposing to adopt option 2
  - mandate all-0 windows are full, all FCN values used.
If windows must be partially full

Receiver

Sender

Ack-Always

time

w = 0

FCN = 4

FCN = 3

FCN = 2

FCN = 1

FCN = all-0

ACK bitmap

ACK bitmap

w = 1

FCN = 4

draft-ietf-lwan-ipv6-static-context-hc-16
Partially filled windows?

• Proposing to adopt option 2
  – mandate all-0 windows are full, all FCN values used.

• Opinions?
  – Got 5 supports on ML, no objection
Pascal

• #2: “expected window” is both $w=0$ and $w=1$ after receiver sends SCHC ACK
  – Issue disappears if we mandate that windows be full
Pascal

- #3: text on fragmentation still hard to parse. Many "if", "otherwise", "on the other hand"
Figure 41: Sender State Machine for the ACK-Always Mode
Pascal

• #3: text on fragmentation still hard to parse. Many “if”, “otherwise”, “on the other hand”
  – Make the FSM drawing normative, text an help to decipher the drawing?
Charlie

• #1: Since the Sender-Abort doesn't have a MIC, does this mean that the Abort could be spoofed and all fragmented transmissions disabled?
  – L2 has its own anti-spoofing mechanism. The All-1 frag MIC is not meant to protect the message, but to verify the whole reassembly process.
Charlie

• #2: If L2 Word can be one bit, what about this sentence “The size of the All-0 fragment header is generally not a multiple of the L2 Word size.”
  – If L2 Word is one bit, the All-0 fragment header is indeed a multiple of the L2 Word. “generally” catches that exception as well. Better wording?
#3: MIC is only used with fragmentation, yet required for UDP elision at compression. What if UDP datagram is compressed but not fragmented?

- If not fragmented, could send UDP checksum in full. Or rely on L2 CRC if strong enough. Or send one fragment in order to have MIC.
Charlie

• #4: fragmentation/reassembly mechanism in the specification is to be treated as optional.
  – We’ll look at it and try to restructure text. Will rewrite Appendix D in a hierarchical manner, esp. wrt. Fragmentation
Charlie

• #5: Target Value type to be stored in context to check for run-time discrepancies?
Charlie

• #6: implication of allowing out-or-order application of CDAs, such as compute-*?
#1: Make MIC optional? If L2 integrity is good enough, why waste bytes for a MIC? Especially for non-UDP traffic?

- MIC is still needed to make sure that all the fragments of last window have been received. MIC can be made as short as an L2 Word.

- Could make all ACK retransmission requests be All-0, even in last window: rename it “SCHC ACK Request”
Juan Carlos

- #2: Ack-on-Error. Currently, on loss of All-0 Frag or loss of ACK : unexpected window, therefore Abort. Proposal to treat Frag with unexpected w value as a roll-back signal.
Juan Carlos

• #3: allow N>1 in No-Ack mode
  – For Alignment? Looks like Reserved bits
  – To convey some information to the receiver: however, since FCN starts from MAX_WIND_FCN, no information is conveyed
Thank you for your attention
Details on Ticket resolution
## Ticket resolution (1/5)

<table>
<thead>
<tr>
<th>ticket #</th>
<th>nickname</th>
<th>resolution first appeared in</th>
<th>section(s), in that version</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Rule ID default size</td>
<td>-10</td>
<td>5, 6.2, 7.2</td>
</tr>
<tr>
<td>3</td>
<td>Zip bomb</td>
<td>-10</td>
<td>10.1</td>
</tr>
<tr>
<td>4</td>
<td>DNS lookup</td>
<td>-10</td>
<td>6.1</td>
</tr>
<tr>
<td>5</td>
<td>Decouple Compr. and Fragm.</td>
<td>-10</td>
<td>3, 4, 3, 7.1, 7.2</td>
</tr>
<tr>
<td>6</td>
<td>Fully-used fragmentation windows</td>
<td>-10</td>
<td>7.2, 7.5.2</td>
</tr>
<tr>
<td>7</td>
<td>Hop Limit default values</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>
### Ticket resolution (2/5)

<table>
<thead>
<tr>
<th>ticket #</th>
<th>nickname</th>
<th>resolution first appeared in</th>
<th>section(s), in that version</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Different RuleIDs with same Dtag?</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>9</td>
<td>Reordering between RGW and NGW</td>
<td>-10</td>
<td>Intro, 7.1</td>
</tr>
<tr>
<td>10</td>
<td>Interleaving of packets</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>11</td>
<td>ACK format, padding</td>
<td>-10</td>
<td>7.4.3, 8</td>
</tr>
<tr>
<td>12</td>
<td>Padding place</td>
<td>-10</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-14</td>
<td>3, 8</td>
</tr>
<tr>
<td>13</td>
<td>Terminology, sublayers</td>
<td>-11</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-13</td>
<td>4</td>
</tr>
</tbody>
</table>
## Ticket resolution (3/5)

<table>
<thead>
<tr>
<th>ticket #</th>
<th>nickname</th>
<th>resolution first appeared in</th>
<th>section(s), in that version</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>Beg./ending rule, legacy devices</td>
<td>-10</td>
<td>5</td>
</tr>
<tr>
<td>15</td>
<td>Parameters to be specified in technology-specific documents</td>
<td>-11</td>
<td>Appendix D</td>
</tr>
<tr>
<td>16</td>
<td>Compression terminology</td>
<td>See #13</td>
<td>See #13</td>
</tr>
<tr>
<td>17</td>
<td>New compression terms</td>
<td>-10</td>
<td>3, 5, 6.1</td>
</tr>
<tr>
<td>18</td>
<td>MSB/LSB arguments</td>
<td>-12</td>
<td>6.5</td>
</tr>
<tr>
<td>19</td>
<td>Fragmentation terminology</td>
<td>-14</td>
<td>3, 7.2</td>
</tr>
</tbody>
</table>
## Ticket resolution (4/5)

<table>
<thead>
<tr>
<th>ticket #</th>
<th>nickname</th>
<th>resolution first appeared in</th>
<th>section(s), in that version</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>« byte boundary » term</td>
<td>-14</td>
<td>7.4, 8</td>
</tr>
<tr>
<td>21</td>
<td>C-bit, All-1 SCHC ACK « bump »</td>
<td>-14</td>
<td>7.5, App. D</td>
</tr>
<tr>
<td>22</td>
<td>Make fragmentation optional</td>
<td>-11</td>
<td>Abstract, 1</td>
</tr>
<tr>
<td>23</td>
<td>NB-IoT, multiRAT, fragmentation</td>
<td>-14</td>
<td>7.1</td>
</tr>
<tr>
<td>24</td>
<td>What if Dtag not present?</td>
<td>-13</td>
<td>7.2</td>
</tr>
<tr>
<td>25</td>
<td>Rule synch. between both ends</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>26</td>
<td>Frag and ACK RuleID match?</td>
<td>-14</td>
<td>7.4.3</td>
</tr>
</tbody>
</table>
## Ticket resolution (5/5)

<table>
<thead>
<tr>
<th>ticket #</th>
<th>nickname</th>
<th>resolution first appeared in</th>
<th>section(s), in that version</th>
</tr>
</thead>
<tbody>
<tr>
<td>27</td>
<td>N/A to this draft</td>
<td></td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>Ill-formed sentence in 7.5.2</td>
<td>-14</td>
<td>7.5.2</td>
</tr>
<tr>
<td>29</td>
<td>Rephrase Bitmap encoding section</td>
<td>-14</td>
<td>7.4.3.1</td>
</tr>
<tr>
<td>30</td>
<td>Fix Ack-Always FSM drawing (1)</td>
<td>-14</td>
<td>App. C</td>
</tr>
<tr>
<td>31</td>
<td>Fix Ack-Always FSM drawing (2)</td>
<td>-14</td>
<td>App. C</td>
</tr>
</tbody>
</table>