IPv6 over Low power WPAN WG (6lowpan)

Chairs:
- Geoff Mulligan <geoff@mulligan.com>
- Carsten Bormann <cabo@tzi.org>

Mailing List:
- 6lowpan@ietf.org

Jabber:
- 6lowpan@jabber.ietch.org
• We assume people have read the drafts

• Meetings serve to advance difficult issues by making good use of face-to-face communications

• Be aware of the IPR principles, according to RFC 3979 and its updates

✓ Blue sheets
✓ Scribe(s)
Milestones (from WG charter page)

Document submissions to IESG:

- Aug 2008 x 2 Improved Header Compression (PS)
- Aug 2008 // 6 Security Analysis (Info)
- Sep 2008 // 3 Architecture (Info)
- Sep 2008 x 4 Routing Requirements (Info)
- Nov 2008 x 1 Bootstrapping and ND Optimizns (PS)
- Dec 2008 x 5 Use Cases (Info)

Also: running documents for implementers, interop
79th IETF: 6lowpan WG Agenda

15:20  Introduction, Agenda  Chairs (10)
15:30  1 – finishing ND
      15:30  ND-14  ZS  (15)
      15:45  NCE/next-hop  SS  (15)
      16:00  multihop DAD, context life  EN  (30)
      16:30  Discussion
17:10  3 – status security work
17:20  0 – new work on HC
      17:25  TCP HC  DR  (15)
      17:40  Generic HC  CB  (10)
17:50  0 – miscellaneous  Chairs (5)
17:55  Next steps/Rechartering...18:10  Chairs (15)
# 79th IETF: 6lowpan WG Agenda

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Chair(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>15:20</td>
<td>Introduction, Agenda</td>
<td>Chairs (10)</td>
</tr>
<tr>
<td>15:30</td>
<td>1 – finishing ND</td>
<td></td>
</tr>
<tr>
<td>15:30</td>
<td>ND-14</td>
<td>ZS (15)</td>
</tr>
<tr>
<td>15:45</td>
<td>NCE/next-hop</td>
<td>SS (15)</td>
</tr>
<tr>
<td>16:00</td>
<td>multihop DAD, context life</td>
<td>EN (30)</td>
</tr>
<tr>
<td>16:30</td>
<td>Discussion</td>
<td></td>
</tr>
<tr>
<td>17:10</td>
<td>3 – status security work</td>
<td></td>
</tr>
<tr>
<td>17:20</td>
<td>0 – new work on HC</td>
<td></td>
</tr>
<tr>
<td>17:25</td>
<td>TCP HC</td>
<td>DR (15)</td>
</tr>
<tr>
<td>17:40</td>
<td>Generic HC</td>
<td>CB (10)</td>
</tr>
<tr>
<td>17:50</td>
<td>0 – miscellaneous</td>
<td>Chairs (5)</td>
</tr>
<tr>
<td>17:55</td>
<td>Next steps/Rechartering...</td>
<td></td>
</tr>
<tr>
<td>18:10</td>
<td></td>
<td>Chairs (15)</td>
</tr>
</tbody>
</table>
“Neighbor Discovery Optimization for Low-power and Lossy Networks”

draft-ietf-6lowpan-nd-14

Zach Shelby, Samita Chakrabarti, Erik Nordmark
Progress since Maastricht

• nd-12
  – Aligned ABRO fields for 32-bit reserved (#90)
  – Clarifications and example of router interaction (#91)
  – Temporary NCE added (#87)
• nd-13
  – Error-to solution added for duplicate MACs (#126)
• nd-14 (to resolve WGLC comments)
  – New DAR and DAC multihop DAD messages
  – MULTIHOP_HOPLIMIT = 64
  – Clarified host de-registration
  – Router next-hop determination section added
  – Removed 6CO infinite lifetime
Current status

- WGLC issues have been resolved
- TODOs found by the authors:
  - Clarification on context distribution lifecycle (#129)
    - Define MIN_CONTEXT_CHANGE_DELAY as greater than the default router lifetime
  - Editorial text trimming (less repetition)
  - General editing round needed
- Next step
  - Release nd-15 within 2 weeks
Host-Router interface
Duplicate address detection
Multihop prefix distribution
Put it all together...

Legend:
(mc) = Multicast
(uc) = Unicast
79th IETF: 6lowpan WG Agenda

15:20   Introduction, Agenda                Chairs (10)
15:30   1 – finishing ND
        15:30   ND-14                        ZS   (15)
        15:45   NCE/next-hop               SS   (15)
16:00   multihop DAD, context life        EN   (30)
16:30   Discussion
17:10   3 – status security work
17:20   0 – new work on HC
        17:25   TCP HC                     DR   (15)
        17:40   Generic HC                CB   (10)
17:50   0 – miscellaneous                Chairs (5)
17:55   Next steps/Rechartering...18:10  Chairs (15)

http://6lowpan.tzi.org
“Neighbor Discovery Optimization for Low-power and Lossy Networks”

draft-ietf-6lowpan-nd-14

Zach Shelby, Samita Chakrabarti, Erik Nordmark

zach@sensinode.com
samitac@ipinfusion.com
nordmark@orcale.com
Clarification on NCE and NextHop Determination

WG Comments [Colin and Others]

- Concern on possible neighbor table collision

Example Scenario

Conclusion: Clarification is required for proper understanding of NCE management
Clarification on NCE and NextHop Determination

WG Comments [Colin and Others]

- Concerns on left-behind NCE when node moves away before the registration expiry

Example Scenario

Conclusion: Clarification is required for proper understanding of NCE management
Action Taken in ND-14

• Clarification(1)
  – Tentative NCEs are created when Multihop DAD is performed by the 6LR [already described in section 8.2]
    • We added some text in section 3.5 regarding that as well. However, in nd-15 we will do some more checks/cleanup to remove inconsistency and redundancy

  – Sec 6.5.4: Next Hop Determination at 6LR
    • Tentative or garbage-collectable NCEs are not used for on-link status determination
      – As per RFC 4861 and general IP networking principle, Routers should check the routing table for sending the MDAD packets to 6LBR
Action Taken in ND-14

• Clarification(2) for concern on left-behind NCE on 6LRs
  – Sec 1.3: If possible a moving node should de-register itself from the current default router and then register itself with a new default-router
  – If it is a run-away node, NCE entry expires after registration-lifetime. 6LR will transmit data for that NCE until it expires
    • Use low registration lifetime for nodes where the network is unstable or nodes are mobile
ND-14 : Clarification(2)…

- Mobility optimization is out of scope of the 6LoWPAN ND document.

- More optimization may be possible with movement detection and signaling the previous default-router to delete the NCE before registration expiry, but more thoughts and investigation are needed. Such solution may be formed as an additional extension on local mobility optimization.

- Section 6.5.3 mentions that Routing protocol be notified with addition or removal of NCEs; Thus a Routing protocol may also be used to notify the previous 6LR that the particular node has moved away.
Clarification/Guideline for Implementation

- Problem # 127 Clarification on optional/Mandatory languages
  - Optional behaviors are regarded as SHOULD for implementation and MAY for deployment
  - Changes were made in section 1.3 and section 1.4 is added to reflect the above assertion
  - Section 13 (Guidelines for New Features) was added to clarify implementation and deployment recommendations for 6LN, 6LBR and 6LR nodes.
79th IETF: 6lowpan WG Agenda

15:20 Introduction, Agenda Chairs (10)
15:30 1 – finishing ND
   15:30 ND-14 ZS (15)
   15:45 NCE/next-hop SS (15)
16:00 multihop DAD, context life EN (30)
16:30 Discussion
17:10 3 – status security work
17:20 0 – new work on HC
   17:25 TCP HC DR (15)
   17:40 Generic HC CB (10)
17:50 0 – miscellaneous Chairs (5)
17:55 Next steps/Rechartering...18:10 Chairs (15)
Neighbor Discovery
Duplicate Address Request and Confirmation

<draft-ietf-6lowpan-nd-14.txt>

Erik Nordmark
erik.nordmark@oracle.com
Multihop DAD Issue in -13

- Two different forms of ARO
  - Length=2 for host to router communication
  - Length=4 for multihop DAD
- The NS/NA with ARO Length=4 was quite different than anything else
  - Hoplimit=255 check does not apply
  - MUST NOT modify the NCEs
- Made it difficult to implement hoplimit check
- Hard for firewall to filter out multihop DAD messages
Make it more clear; separate ICMP types for multihop DAD

- ARO now only has Length=2
- Duplicate Address Request (DAR) replaces multihop NS with ARO Length=4
- Duplicate Address Confirmation (DAC) replaces multihop NA with ARO Length=4
- DAR and DAC are not subject to hoplimit=255
- NS and NA are always subject to hoplimit=255
- The logic of multihop DAD is unchanged
DAR/DAC message format

λ 24 bytes shorter than NS with ARO
Section 7.2 says

Only when it is reasonable to assume that this information was successfully disseminated SHOULD an option with C=1 be sent, enabling the actual use of the context information for compression.

That is, in preparation for a change of context information, its dissemination SHOULD continue for at least MIN_CONTEXT_CHANGE_DELAY with C=0. Only when it is reasonable to assume that the fact that the context is now invalid was successfully disseminated ...
Context distribution; What is “reasonable”?

- Maximum default router lifetime 18 hours
  - Implies host will RS after at most 18 hours
  - RS triggers an RA with the newest 6CO

- Administrator can configure 6LRs to use shorter default router lifetime

- Suggestion: Replace MINCONTEXTCHANGE_DELAY with “at least the configured default router lifetime”, and clarify that this is what “reasonable” means
# 79th IETF: 6lowpan WG Agenda

<table>
<thead>
<tr>
<th>Time</th>
<th>Item</th>
<th>Speaker(s)</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>15:20</td>
<td>Introduction, Agenda</td>
<td>Chairs</td>
<td>(10)</td>
</tr>
<tr>
<td>15:30</td>
<td>1 – finishing ND</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:30</td>
<td>ND-14</td>
<td>ZS</td>
<td>(15)</td>
</tr>
<tr>
<td>15:45</td>
<td>NCE/next-hop</td>
<td>SS</td>
<td>(15)</td>
</tr>
<tr>
<td>16:00</td>
<td>multihop DAD, context life</td>
<td>EN</td>
<td>(30)</td>
</tr>
<tr>
<td></td>
<td><strong>Discussion</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:30</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17:10</td>
<td>3 – status security work</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17:20</td>
<td>0 – new work on HC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17:25</td>
<td>TCP HC</td>
<td>DR</td>
<td>(15)</td>
</tr>
<tr>
<td>17:40</td>
<td>Generic HC</td>
<td>CB</td>
<td>(10)</td>
</tr>
<tr>
<td>17:50</td>
<td>0 – miscellaneous</td>
<td>Chairs</td>
<td>(5)</td>
</tr>
<tr>
<td>17:55</td>
<td>Next steps/Rechartering...</td>
<td>Chairs</td>
<td>(15)</td>
</tr>
</tbody>
</table>

http://6lowpan.tzi.org
6CO Option

Figure 1: 6LoWPAN Context Option format
(valid lifetime up to 655350 s ≈ 7.6 days)
6CO state machine

- **Sane:**
  - C=0
  - C=1

  - active distribution of updates goes right and left slowly
  - timeouts go left, through a deprecated state for a while

- **Actual:**
  - (no state)
  - deprecated
  - active

http://6lowpan.tzi.org
### 79th IETF: 6lowpan WG Agenda

<table>
<thead>
<tr>
<th>Time</th>
<th>Topic</th>
<th>Presenter(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>15:20</td>
<td>Introduction, Agenda</td>
<td>Chairs (10)</td>
</tr>
<tr>
<td>15:30</td>
<td>1 – finishing ND</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ND-14</td>
<td>ZS (15)</td>
</tr>
<tr>
<td>15:45</td>
<td>NCE/next-hop</td>
<td>SS (15)</td>
</tr>
<tr>
<td>16:00</td>
<td>multihop DAD, context life</td>
<td>EN (30)</td>
</tr>
<tr>
<td>16:30</td>
<td>Discussion</td>
<td></td>
</tr>
<tr>
<td>17:10</td>
<td>3 – status security work</td>
<td></td>
</tr>
<tr>
<td>17:20</td>
<td>0 – new work on HC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TCP HC</td>
<td>DR (15)</td>
</tr>
<tr>
<td>17:40</td>
<td>Generic HC</td>
<td>CB (10)</td>
</tr>
<tr>
<td>17:50</td>
<td>0 – miscellaneous</td>
<td>Chairs (5)</td>
</tr>
<tr>
<td>17:55</td>
<td>Next steps/Rechartering...</td>
<td>Chairs (15)</td>
</tr>
</tbody>
</table>

http://6lowpan.tzi.org
79th IETF: 6lowpan WG Agenda

15:20  Introduction, Agenda  Chairs (10)
15:30  1 – finishing ND
   15:30  ND-14  ZS  (15)
   15:45  NCE/next-hop  SS  (15)
   16:00  multihop DAD, context life  EN  (30)
   16:30  Discussion
17:10  3 – status security work
17:20  0 – new work on HC
   17:25  TCP HC  DR  (15)
   17:40  Generic HC  CB  (10)
17:50  0 – miscellaneous  Chairs (5)
17:55  Next steps/Rechartering... 18:10  Chairs (15)
79th IETF: 6lowpan WG Agenda

15:20   Introduction, Agenda            Chairs (10)
15:30   1 – finishing ND
   15:30     ND-14                    ZS   (15)
   15:45     NCE/next-hop             SS   (15)
   16:00    multihop DAD, context life EN   (30)
   16:30    Discussion
17:10   3 – status security work
17:20   0 – new work on HC
   17:25     TCP HC                   DR   (15)
   17:40     Generic HC               CB   (10)
   17:50    0 – miscellaneous          Chairs (5)
17:55   Next steps/Rechartering...18:10 Chairs (15)
TCP Header Compression for 6LoWPAN
(draft-aayadi-6lowpan-tcphc-01)

Ahmed Ayadi, David Ros and Laurent Toutain
IETF-79 Beijing
November 9, 2010
Motivation

• TCP allows running useful services like remote login and HTTP in Low-power and Lossy Networks

• But: TCP header overhead is between 20 and 60 bytes

• Currently, LOWPAN_IPHC defines only a compression scheme for UDP (LOWPAN_NHC)

• Goal: define a TCP compression scheme compatible with 6LoWPAN, using LOWPAN_NHC

• Outside to LoWPAN, LoWPAN to outside, LoWPAN to LoWPAN
LOWPAN_TCPHC: overview

- TCPHC is implemented both on the Edge Router and on the (TCP end-point) LoWPAN node which save the context of the TCP connections.
LOWPAN_TCPHC: overview

- TCPHC:
  - does not compress TCP segments in the connection establishment phase (SYN)
  - replaces the source port and destination port by a Context IDentifier (CID)
  - sends only the bytes of dynamic fields (Sequence number, ACK number, Window) that have changed
  - removes unused bits (Reserved)
  - elides the TCP header-length field (value inferred at decompression)
  - compresses SACK and Timestamp TCP options
LOWPAN_TCPHC header types

- Regular header (used outside the LLN)
  
<table>
<thead>
<tr>
<th>TCP header</th>
<th>payload</th>
</tr>
</thead>
</table>

- Full header (sent at the connection establishment phase)
  
<table>
<thead>
<tr>
<th>LOWPAN_TCPHC</th>
<th>CID</th>
<th>TCP header</th>
<th>payload</th>
</tr>
</thead>
</table>

- Compressed header
  
<table>
<thead>
<tr>
<th>LOWPAN_TCPHC</th>
<th>CID</th>
<th>non-elided TCP header fields</th>
<th>payload</th>
</tr>
</thead>
</table>

  compressed & uncompressed fields, in TCP-header order
LOWPAN_TCPHC
format for compressed headers

bits:  3  1  2  2  2  1  1  1  1  1  1

1 1 0  ID  Seq  Ack  Win  Cwr  Ece  F  P  T  S

CID field size
compressed fields size
Advertised window
Congestion window reduced

SACK option
Timestamp option
PUSH flag
FIN flag
ECN echo
Compression of TCP options

- MSS and SACK-permitted are sent uncompressed in SYN segments
- SACK:
  - Only one SACK block is allowed
  - SACK block values are replaced by their offset w.r.t. the ACK number
- Time Stamp:
  - Only bytes that have changed, compared to last segment, are carried in-line.
  - A bitmap field is added to describe if a byte is omitted or carried in-line.
- Other options are assumed to be unused / not useful in LNNs
  - E.g. Window Scale option (low bit rates, memory constraints)
Current status

• We have an alpha version of TCPHC for Contiki OS already implemented
  • We plan to keep it in sync with the draft, and to release the code «soon»
• Some (very) preliminary results
  • TCPHC reduces the TCP header to 6 bytes in more than 95% of cases
  • TCPHC reduces energy consumption by up to ~15%
• Interest in adopting LOWPAN_TCPHC as a WG item?
79th IETF: 6lowpan WG Agenda

15:20 Introduction, Agenda Chairs (10)
15:30 1 – finishing ND
   15:30 ND-14 ZS (15)
   15:45 NCE/next-hop SS (15)
   16:00 multihop DAD, context life EN (30)
   16:30 Discussion
17:10 3 – status security work
17:20 0 – new work on HC
   17:25 TCP HC DR (15)
   17:40 Generic HC CB (10)
17:50 0 – miscellaneous Chairs (5)
17:55 Next steps/Rechartering...18:10 Chairs (15)
New proposal: 6LoWPAN-GHC

- Generic compression of remaining headers and header-like payloads: ICMPv6, ND, RPL; DHCP; ...

- draft-bormann-6lowpan-ghc: simple LZ77 based on bytecode
  - single-page specification: simple
  - stateless (but can use 6LoWPAN-HC context)

- provides modest compression factors between 1.65 and 1.85 on realistic examples

- fits in 6LoWPAN-HC’s NHC

- is this something we want to pursue?
Example: ND Neighbor Solicitation

- Payload:
  
  87 00 a7 68 00 00 00 00 fe 80 00 00 00 00 00 00 00
  02 1c da ff fe 00 30 23 01 01 3b d3 00 00 00 00
  1f 02 00 00 00 00 00 00 06 00 1c da ff fe 00 20 24

- Pseudoheader:

  20 02 0d b8 00 00 00 00 00 00 00 ff fe 00 3b d3
  fe 80 00 00 00 00 00 00 00 00 02 1c da ff fe 00 30 23
  00 00 00 30 00 00 00 3a

  copy: 04 87 00 a7 68

  4 nulls: 82

  ref(32): fe 80 00 00 00 00 00 00 00 00 02 1c da ff fe 00 30 23
  -> ref 101nssss 1 2/11nnnkkk 0: b2 f0

  copy: 04 01 01 3b d3

  4 nulls: 82

  copy: 02 1f 02

  5 nulls: 83

  copy: 02 06 00

  ref(24): 1c da ff fe 00 -> ref 101nssss 0 2/11nnnkkk 3 3: a2 db

  copy: 02 20 24

- Compressed:

  04 87 00 a7 68 82 b2 f0 04 01 01 3b d3 82 02 1f
  02 83 02 06 00 a2 db 02 20 24

  Was 48 bytes; compressed to 26 bytes, compression factor 1.85
### 79th IETF: 6lowpan WG Agenda

<table>
<thead>
<tr>
<th>Time</th>
<th>Item</th>
<th>Presenter(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>15:20</td>
<td>Introduction, Agenda</td>
<td>Chairs (10)</td>
</tr>
<tr>
<td>15:30</td>
<td>1 – finishing ND</td>
<td></td>
</tr>
<tr>
<td>15:30</td>
<td>ND-14</td>
<td>ZS (15)</td>
</tr>
<tr>
<td>15:45</td>
<td>NCE/next-hop</td>
<td>SS (15)</td>
</tr>
<tr>
<td>16:00</td>
<td>multihop DAD, context life</td>
<td>EN (30)</td>
</tr>
<tr>
<td>16:30</td>
<td>Discussion</td>
<td></td>
</tr>
<tr>
<td>17:10</td>
<td>3 – status security work</td>
<td></td>
</tr>
<tr>
<td>17:20</td>
<td>0 – new work on HC</td>
<td></td>
</tr>
<tr>
<td>17:25</td>
<td>TCP HC</td>
<td>DR (15)</td>
</tr>
<tr>
<td>17:40</td>
<td>Generic HC</td>
<td>CB (10)</td>
</tr>
<tr>
<td>17:50</td>
<td>0 – miscellaneous</td>
<td>Chairs (5)</td>
</tr>
<tr>
<td>17:55</td>
<td>Next steps/Rechartering...</td>
<td>Chairs (15)</td>
</tr>
</tbody>
</table>

http://6lowpan.tzi.org
Interesting individual submissions

- **Split-off from ND:**
  - draft-thubert-6lowpan-backbone-router-02.txt (to support LoWPANs with multiple border routers)
- **Extensively discussed, limited usecase:**
  - draft-thubert-6lowpan-simple-fragment-recovery-07.txt (special encapsulation with adaptation layer retransmit of individual fragments)
- **For each of these, decide:**
  - (A) We want to continue work as WG
  - (B) We encourage author to continue as individual submission
  - (C) We discourage further work
79th IETF: 6lowpan WG Agenda

<table>
<thead>
<tr>
<th>Time</th>
<th>Item</th>
<th>Speaker</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>15:20</td>
<td>Introduction, Agenda</td>
<td>Chairs</td>
<td>(10)</td>
</tr>
<tr>
<td>15:30</td>
<td>1 – finishing ND</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:30</td>
<td>ND-14</td>
<td>ZS</td>
<td>(15)</td>
</tr>
<tr>
<td>15:45</td>
<td>NCE/next-hop</td>
<td>SS</td>
<td>(15)</td>
</tr>
<tr>
<td>16:00</td>
<td>multihop DAD, context life</td>
<td>EN</td>
<td>(30)</td>
</tr>
<tr>
<td>16:30</td>
<td>Discussion</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17:10</td>
<td>3 – status security work</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17:20</td>
<td>0 – new work on HC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17:25</td>
<td>TCP HC</td>
<td>DR</td>
<td>(15)</td>
</tr>
<tr>
<td>17:40</td>
<td>Generic HC</td>
<td>CB</td>
<td>(10)</td>
</tr>
<tr>
<td>17:50</td>
<td>0 – miscellaneous</td>
<td>Chairs</td>
<td>(5)</td>
</tr>
<tr>
<td>17:55</td>
<td>Next steps/Rechartering...</td>
<td>Chairs</td>
<td>(15)</td>
</tr>
</tbody>
</table>
Securing 6LoWPAN ND

• 6LoWPAN ND is not secure and subject to attacks, it needs to be secured

• Secure 6LoWPAN ND can not use SeND directly because SeND uses computationally heavy cryprographical algorithms, etc.

• Simple extension to SeND (RFC 3971 & 3972) is needed
  – Use Elliptic Curve Cryptography public keys
  – Use SHA-2
  – Use efficient design