IESG comments for SCHC YANG DM

Laurent Toutain
Ana Minaburo
Full comments and answers

• In github repository
  • https://github.com/lp-wan/datamodel/blob/master/IESG_review.txt

• Not sent to IESG members:
  • Wait for WG comments
  • Most of the comments are minor
  • Few of them require actions

• Current versions:
  • Draft: -17
  • YANG DM: 2022-08-25
Hi,

Thanks for this document. I would like to discuss whether it is possible/appropriate to add an instance data example (as per my comment 1 below) to this document, or if that is inappropriate or unhelpful for some reason.

Moderate level comments:

(1) p 8, sec

Data Model for Static Context Header Compression (SCHC)

draft-ietf-lpwan-schc-yang-data-model-16

This document is missing an instance data example of the YANG data. Generally, examples (e.g., see the appendixes in RFC 8343), is very helpful both for the authors of the YANG module, to see/know that the structure is right, and also to give helpful context to readers/users of the YANG module). I would strongly encourage you to add such an example (which should be validated to be correct) to this document.

(2) p 41, sec 6. YANG Module
Hi,

Thanks for this document. I would like to discuss whether it is possible/appropriate to add an instance data example (as per my comment 1 below) to this document, or if that is inappropriate or unhelpful for some reason.
AM+LT ==> We can add something in JSON, Do you think it is what is expected ?

For set of rules

```
/------------------------------------------\
|Rule 6/3 | 110 |
|-------------------------------------------|
|IPV6.VER | 4 | 1|BI| 6|EQUAL | NOT-SENT |
|IPV6.TC  | 8 | 1|BI| 8|EQUAL | NOT-SENT |
|IPV6.FL  | 20| 1|BI| 0|IGNORE| NOT-SENT |
|IPV6.LEN | 16| 1|BI| IGNORE|COMPUTE-LENGTH |
|IPV6.NXT | 8 | 1|BI| 0|EQUAL | NOT-SENT |
|IPV6.HOP_LMT| 8| 1|BI| 255|IGNORE |NOT-SENT |
|IPV6.DEV_PREFIX| 64| 1|BI| 200104701f2101d2|EQUAL |NOT-SENT |
|IPV6.DEV_IID | 64| 1|BI| 0000000000000001|EQUAL |NOT-SENT |
|IPV6.APP_PREFIX| 64| 1|BI| 0000000000000000|EQUAL |COMPUTE-LENGTH |
|IPV6.APP_IID | 64| 1|BI| NOT-SENT |
|IPV6.APPL_PREFIX| 64| 1|BI| NOT-SENT |
|IPV6.APPL_IID | 64| 1|BI| NOT-SENT |
|-------------------------------------------|
```

```
/------------------------------------------\
|Rule 12/11 | 00001100 |
|-------------------------------------------|
|IPv6_VER   | 6| 1|BI| 0|EQUAL |NOT-SENT |
|IPv6.TC    | 8 | 1|BI| 0|EQUAL |NOT-SENT |
|IPv6.FL    | 20| 1|BI| 0|IGNORE| NOT-SENT |
|IPv6.LEN   | 16| 1|BI| 0|IGNORE|COMPUTE-LENGTH |
|IPv6.NXT   | 8 | 1|BI| 0|EQUAL | NOT-SENT |
|IPv6.HOP_LMT| 8| 1|BI| 255|IGNORE |NOT-SENT |
|IPv6.DEV_PREFIX| 64| 1|BI| 200104701f2101d2|EQUAL | NOT-SENT |
|IPv6.DEV_IID | 64| 1|BI| 0000000000000001|EQUAL | NOT-SENT |
|IPv6.APP_PREFIX| 64| 1|BI| NOT-SENT |
|IPv6.APP_IID | 64| 1|BI| NOT-SENT |
|-------------------------------------------|
```

```
/------------------------------------------\
|Rule 100/8 | 01100100 |
|NO COMPRESSION RULE |
|------------------------------------------/
** Section 8.

An attacker by changing a rule content may block the communication or intercept the traffic.

...

The full tree is sensitive, since it represents all the elements that can be managed. This module aims to be encapsulated into a YANG module including access control and identities.

[ballet for -15 text]

Thanks for calling out the entire tree as “sensitive.” Please be more specific. There is mention of write sensitivity (i.e., re-writing the rules). Please also discuss any issues with reading the tree.

Consider following the template of https://trac.ietf.org/trac/ops/wiki/yang-security-guidelines to distinguish between write and read access.

[ballet for -17 text]

Thanks for the additional words about write sensitivity. What is the impact of an attacker reading the module?
Roman Danyliw
Discuss (2022-08-24 for -15)

**Section 8.

An attacker by changing a rule content may block the communication or intercept the traffic.

The full tree is sensitive, since it represents all the elements that can be managed. This module aims to be encapsulated into a YANG module including access control and identities.

Thanks for calling out the entire tree as “sensitive.” Please be more specific. There is mention of write sensitivity (i.e., re-writing the rules). Please also discuss any issues with reading the tree.

Consider following the template of https://trac.ietf.org/trac/ops/wiki/yang-security-guidelines to distinguish between write and read access.

AM+LT => if you have any idea what to add here, in fact the main problem, it that this YANG DM is just a description of RFC 8724 and RFC 8824 and in not directly operational, we need more information around, such as a device identifier in the Core SCHC.

The architecture draft has expired, and we think we cannot expect that document before publish the YANG DM. Linked to that we have this comment:
Thank you to Carl Wallace for the SECDIR review.

Thanks for addressing some of the COMMENTS.

===
(updated for -17)

**Section 8.**
The rule contains some sensible informations such as the application
IPv6 address.

Can this be restated? What is “sensible information”? Is this perhaps "sensitive" -->
s/sensible/sensitive/?

**Section 8.**
Therefore, the identity of
the requester must be validated. This can be done through
certificates or access lists.

Is there a particular way which this should be done, or is it expected to follow NACM, and
associated NETCONF and RESTCONF?
Section 8.

Therefore, the identity of

the requester must be validated. This can be done through

certificates or access lists.

Is there a particular way which this should be done, or is it expected to follow NACM, and associated NETCONF and RESTCONF?

This for us should be treated in the architecture document.
As is right now, the YANG module assumes that all implementations support all FID types defined to be derived from field-id-base-type. It includes fields related IPv6, COAP/OSCORE, and ICMPv6 all in the same module. Is there a possibility that some implementations won't implement all three of those protocol groups? If so, it might be worth considering making FID type groups either optional using YANG 'feature' statements or break them out into separate modules to be advertised separately.

**> Not done yet, should be discussed in the WG

For us, it is not necessary, the creation of FID will just generate new identifier. If an implementation is not aware of this identifier an error will be generated
There is currently no correlation between field-id type and field-length types in the same compression rule entry. I.e. the current YANG permits a field-identifier 'fid-ipv6-version' combined with a field-length 'fl-token-length' in a rule entry, which I understand to be nonsensical.

==> not yet done, have to be discussed in the WG, test can be done to ensure that length function are used with the right fid, but how to take into account augmentation if we say for instance that fl-variable must be linked to fid-coap-uri-path and fid-coap-uri-query. If someone defines another compression for let say MQTT how do we accept it?
3. See 3.10.1. Fragmentation mode, three modes are defined in the SCHC protocol, Have we considered model 'ack-on-error', 'ack-always','no-ack' as action statements defined in RFC7950, One typical example of action is "set-operator-state" action defined in RFC8632.

**> Not done, have to understand in detail, but in SCHC we cannot change easily a rule from one behavior to another, only parameters could be adapted to the environment.
5. Please follow guidance in section 4.23.3.1 to define a foo-state module in the appendix.

*** > Don't understand

6. Please provide an example to explain how target-value, matching-operator-value, comp-decomp-action-value are used in the appendix.

*** > TBD
5. Please follow guidance in section 4.23.3.1 to define a foo-state module in the appendix.

**> Don't understand

6. Please provide an example to explain how target-value, matching-operator-value, comp-decomp-action-value are used in the appendix.

**> TBD

In addition, section 3.7 only discuss how to specify value for 'Equal', 'MSB', 'Matching mapping' matching operators cases, what about other cases such as ignore, MSB?

**> TBD; can add a condition, if not-sent or LSB, TV should not be empty. Need to update YANG DM
5. Section 3.7 said: "If the header field contains a text, the binary sequence uses the same encoding.” how this last sentence related to YANG data model defined in this document? If not relevant, please remove this sentence.

**> It was discussed in the WG, may be add the "same encoding as in the original packet ? ” to avoid to take into consideration how the text is encoded.
Paul Wouters
Discuss (2022-08-24 for -15)

- Section 1 [I-D.ietf-lpwan-architecture] is a broken reference

**> Ask the group to issue a new version, may be this reference should be removed, to avoid to wait too much for publication.
choice mode {
  case no-ack;
  case ack-always;
}

The case statement never turn up in the instance data that conforms to the YANG schema, so users of the module would never be able to differentiate between no-ack and ack-always. You might want to put a leaf, of type empty, under each of these two case statements.

**> Agree, these empty cases are just here to allow augmentation if needed for these modes. There is another leaf giving the mode: