YANG data model -13

Reviews

- Two very constructive and helpful reviews
  - Tom Petch
  - Eric Vyncke

- Thank you very much

Minor revisions:

- # Sect # no need for capitalized “Destination address”
- # Sect 2 *blocking* please use the right template from BCP14
- #Sect 3 no need to repeat the introduction text from sect 1
- # Section 3.2
  - no need to capitalize “Data Model”
  - please expand “RCS” at first use
- # Sect 3.3 use either “YANG data model” or “YANG module” but not “YANG model”
  - s/always derives/is always derived/ ? (Passive voice)
  - s/MUST derive/MUST be derived/ ?

Minor revisions:

- # Sect 3.4 Please do not capitalize “byte” (and you may want to use the plural form)
- # Sect 3.7 Please expand “CDA”
- # Sec 3.9

  s/ shows some CDA definition/ shows some CDA definitions/
- # Sec 3.10.2 It should be clear for the reader that this text is coming out of RFC 8724 and not specified by this I-D.

Minor revisions:

- # Sec 3.10.4

  It should be clear for the reader that this text is coming out of RFC 8724 and not specified by this I-D.

  Why "All1" (capitalized) while previously "all1" (lowercase) was used ?

  # Sec 3.10.5

  "rexpresses" ?

  # Sec 3.10.6

  Should the text be clear that l2-word-size is expressed in bits ?

  # Sec 4.2

  s/milli-seconds for real time/milliseconds for real-time/

  s/micro-second/microsecond/

  s/ computed through/ computed by/ ?

  An RFC must be accurate, so text like "of about 1.05 second" is not suitable. If it is about 2**20 microseconds, then be explicit.

Minor revisions:

- # Section 5

  Thanks for including this section. But, per RFC 7942 section 2.1, a note to the RFC editor must be included to remove this section before publication.

- # Section 9

  The location of the YANG module is unusual, it should come before the "implementation status".

  s/code begins/CODE BEGINS/ same for ends of course __

  Please put "" around the filename.

Done: removed data model in text

- I have never seen a I-D which replicates the YANG in all its detail in the body of the I-D (as opposed to using snippets of tree diagams). A recent IESG Review said 'Reference, do not replicate' and I think is fundamental to avoiding future problems. Having the YANG in all its detail in more than one place can only lead to inconsistencies and contradictions as and when it is updated e.g. as a result of Art and IESG reviews. Also, it makes the I-D harder to read with all the unnecessary YANG syntax and semantics therein.

To be discussed

- Suggest renaming the section into “Conventions for Field Identifiers”
  - Done for all compression rule elements

3. SCHC rules 3
3.1. Compression Rules 3
3.2. Identifier generation 4
3.3. Convention for Field Identifier 5
3.4. Convention for Field length 6
3.5. Convention for Field position 6
3.6. Convention for Direction Indicator 6
3.7. Convention for Target Value 6
3.8. Convention for Matching Operator 7
3.8.1. Matching Operator arguments 7
3.9. Convention for Compression Decompression Actions 7
3.9.1. Compression Decompression Action arguments 7
3.10. Fragmentation rule 7
3.10.1. Fragmentation mode 7
3.10.2. Fragmentation Header 8
3.10.3. Last fragment format 8
3.10.4. Acknowledgment behavior 9
3.10.5. Timer values 10
3.10.6. Fragmentation Parameters 10
3.10.7. Layer 2 parameters 10
4. Rule definition 11

To be discussed: text encoding

- Unsure whether “strings must be converted to binary” is non-ambiguous. How can it be done ? Should there be a reference ?

The first one is about the conversion between string and binary. That's a very good point. Currently it happens only for string fields such ad Uri-path and Uri-query in CoAP, RFC 7252 gives this definition of strings:

`string: A Unicode string that is encoded using UTF-8 [RFC3629] in Net-Unicode form [RFC5198].`

we can keep the same definition and say that the Target Value is the binary representation of this. But we may image other protocols that uses another coding, is it out of the scope of the YANG data model or we try to have a phrasing to include them ?

To be discussed : all1

Eric : # Sec 3.10.3 Suggest to add somewhere that "all1" is lower case "ALL" followed by figure "1".

Tom : I believe that 'All1' will lead to mistakes; mixing alpha and digit in an identifier is often a source of error with O, 0, I, l, 1 being particularly prone to that.

-> LT : write ALL1 in the data model

To be done: IANA consideration

- Eric : # Section 6 I am afraid that there must be some IANA considerations for each and every YANG module, e.g., see https://datatracker.ietf.org/doc/html/draft-ietf-dhc-dhcpv6-yang-25#section-6

- Tom: IANA Considerations are what makes a YANG module a YANG module. No IANA Considerations, no YANG module. See RFC8407, YANG Guidelines.

IANA consideration

X. IANA Considerations

This document registers four URIs and four YANG modules.

X.1. URI Registration

This document requests IANA to register the following four URIs in the "IETF XML Registry" [RFC3688]:

URI: **urn:ietf:params:xml:ns:yang:ietf-schc**
Registrant Contact: The IESG.
XML: N/A; the requested URI is an XML namespace.

X.2. YANG Module Name Registration

This document registers the following four YANG modules in the "YANG Module Names" registry [RFC6020].

name:	**ietf-schc**
namespace:	**urn:ietf:params:xml:ns:yang:ietf-schc**
prefix:	**schc**
reference:	**RFC XXXX Data Model for Static Context Header Compression (SCHC)**

To be done: Add “reference”

- More subjectively, I have never seen a YANG module with no YANG Reference clauses. Yes, there are references in the descriptive text but, for me, this is inadequate. YANG Reference clauses faclitate automated processing, slipping them into the text does not. I think that every Reference should have a YANG Reference clause to at least the RFC level.

- References in the YANG module must appear in I-D References.

```
identity fid-base-type {
  description
    "Field ID base type for all fields";
}

identity fid-ipv6-base-type {
  base fid-base-type;
  description
    "Field ID base type for IPv6 headers described in RFC 8200";
  reference
    "RFC 8200 Internet Protocol, Version 6 (IPv6) Specification";
}

identity fid-ipv6-version {
  base fid-ipv6-base-type;
  description
    "IPv6 version field from RFC8200";
}
```

To be done:

- I would like more in the Abstract; the Introduction reveals that this is more than a YANG module for the operation of some protocol and the Abstract should say that IMHO.

To be done: Security

- Tom: Security Considerations must follow the guidelines in RFC8407 YANG
  Guidelines; this will add a number of references.

- Eric # Section 7

  Please use the YANG security template:
  https://trac.ietf.org/trac/ops/wiki/yang-security-guidelines

Security template

Security Considerations

The YANG module specified in this document defines a schema for data that is designed to be accessed via network management protocols such as NETCONF [RFC6241] or RESTCONF [RFC8040]. The lowest NETCONF layer is the secure transport layer, and the mandatory-to-implement secure transport is Secure Shell (SSH) [RFC6242]. The lowest RESTCONF layer is HTTPS, and the mandatory-to-implement secure transport is TLS [RFC 8446].

The Network Configuration Access Control Model (NACM) [RFC8341] provides the means to restrict access for particular NETCONF or RESTCONF users to a preconfigured subset of all available NETCONF or RESTCONF protocol operations and content.

-- if you have any writable data nodes (those are all the -- "config true" nodes, and remember, that is the default) -- describe their specific sensitivity or vulnerability.

There are a number of data nodes defined in this YANG module that are writable/creatable/deletable (i.e., config true, which is the default). These data nodes may be considered sensitive or vulnerable in some network environments. Write operations (e.g., edit-config) to these data nodes without proper protection can have a negative effect on network operations. These are the subtrees and data nodes and their sensitivity/vulnerability:

<list subtrees and data nodes and state why they are sensitive>

-- for all YANG modules you must evaluate whether any readable data -- nodes (those are all the "config false" nodes, but also all other -- nodes, because they can also be read via operations like get or -- get-config) are sensitive or vulnerable (for instance, if they -- might reveal customer information or violate personal privacy -- laws such as those of the European Union if exposed to -- unauthorized parties)

Some of the readable data nodes in this YANG module may be considered sensitive or vulnerable in some network environments. It is thus important to control read access (e.g., via get, get-config, or notification) to these data nodes. These are the subtrees and data nodes and their sensitivity/vulnerability:

<list subtrees and data nodes and state why they are sensitive>

~~-- if your YANG module has defined any rpc operations -- describe their specific sensitivity or vulnerability.~~

~~Some of the RPC operations in this YANG module may be considered sensitive or vulnerable in some network environments. It is thus important to control access to these operations. These are the operations and their sensitivity/vulnerability:~~

~~<list RPC operations and state why they are sensitive>~~