Network Configuration   B. M. Chittapragada
Internet-Draft   S. Bhat
Intended status: Standards Track   V. T. Rao
Expires: 9 August 2026   H. Arshad
                                                          M. P. Tahiliani
                    National Institute of Technology Karnataka, Surathkal
                                                          5 February 2026

CBOR Encoding for HTTPS-based YANG Notifications Transport
draft-ietf-netconf-https-notif-cbor-00

Abstract

This document extends [I-D.draft-ietf-netconf-https-notif] by introducing CBOR encoding for YANG notifications over HTTPS Transport in addition to the existing JSON and XML encoding schemes.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://MeherRushi.github.io/draft-ietf-netconf-https-notif-cbor/draft-ietf-netconf-https-notif-cbor.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-ietf-netconf-https-notif-cbor/.

Discussion of this document takes place on the Network Configuration mailing list (mailto:netconf@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/netconf/. Subscribe at https://www.ietf.org/mailman/listinfo/netconf/.

Source for this draft and an issue tracker can be found at https://github.com/MeherRushi/draft-ietf-netconf-https-notif-cbor.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

CBOR offers an efficient and compact representation of YANG.

This document introduces a CBOR encoding scheme for event notifications over HTTPS by using the framework proposed in [I-D.draft-ietf-netconf-https-notif] which supports transfer of YANG notifications over HTTPS using JSON and XML encoding schemes.

In [I-D.draft-ietf-netconf-https-notif], the capabilities HTTP-target resource allows a publisher to retrieve supported encoding formats via GET requests, while the relay-notification resource enables the publisher to send YANG notifications via POST requests. These requests and responses use different content types based on the selected encoding scheme. This document defines support for using CBOR encoding defined in section 1 of [I-D.draft-ietf-netconf-https-notif]

Examples of the GET and POST request and reply encoded in CBOR are also provided.

2. Terminology

This document uses the following terms defined in Section 2,3 and 4 of [I-D.draft-ietf-netconf-https-notif]:

* Capabilities Resource

* Relay-Notification

* Event Notification

The following term(s) are defined in Subscription to YANG Notifications [RFC8639]:

* Publisher

* Receiver

* Subscribed Notifications

The following term(s) are defined in Encoding of Data Modeled with YANG in the Concise Binary Object Representation (CBOR) [RFC9254]:

* Diagnostic Notifications

* YANG Schema Item iDentifier (or "YANG SID" or simply "SID"): 63-bit unsigned integer used to identify different YANG items.

3. CBOR Encoding of the notification(s)

YANG notifications can be encoded in CBOR using Names or SIDs in keys. Notifications encoded using names is similar to JSON encoding as defined in Section 3.4 and 4.3 of [I-D.draft-ietf-netconf-https-notif]. Notification encoded using YANG-SIDs replaces the names of the keys of the CBOR encoded message with a 63 bit unsigned integer. In this case, the term 'SID' is defined in Section 3.2 of [RFC9254], and the keys of the encoded data use SID value as mentioned in 4.3.2 of this document.

3.1. Capabilities Request

The publisher sends a request to the receiver to learn its capabilities. In the below example, the "Accept" states that the publisher wants to receive the capabilities response in CBOR but if not supported then in XML or JSON in that order.

```
GET /some/path/capabilities HTTP/1.1
   Host: example.com
   Accept: application/cbor, application/xml;0.5, application/json;q=0.9
```

3.2. Capabilities Response

If the receiver is able to reply using "application/cbor" and assuming it is only capable of receiving CBOR encoded messages the response would look like this

3.2.1. CBOR using names as keys

```
   HTTP/1.1 200 OK
   Date: Tue, 4 March 2025 20:33:30 GMT
   Server: example-server
   Cache-Control: no-cache
   Content-Type: application/cbor
```

Diagnostic Notation:

```
   {
   "receiver-capabilities": {
     "receiver-capability": [
       "urn:ietf:capability:https-notif-receiver:encoding:cbor"
        ]
     }
   }
```

CBOR Encoding:

```
A1                                      # map(1)
   75                                   # text(21)
      72656365697665722D6361706162696C6974696573 # "receiver-capabilities"
   A1                                   # map(1)
      73                                # text(19)
         72656365697665722D6361706162696C697479 # "receiver-capability"
      81                                # array(1)
         78 36                          # text(54)
            75726E3A696574663A6361706162696C6974793A68747470732D6E6F7469662D7265636569766
5723A656E636F64696E673A63626F72 # "urn:ietf:capability:https-notif-receiver:encoding:cbor
"
```

If the receiver is able to reply using “application/cbor” and assuming it is not capable of receiving cbor, but can receive both json and xml notifications:

3.2.2. CBOR using names as keys

```
   HTTP/1.1 200 OK
   Date: Tue, 4 March 2025 20:33:30 GMT
   Server: example-server
   Cache-Control: no-cache
   Content-Type: application/cbor
```

Diagnostic Notation:

```
   {
   "receiver-capabilities": {
     "receiver-capability": [
       "urn:ietf:capability:https-notif-receiver:encoding:json",
       "urn:ietf:capability:https-notif-receiver:encoding:xml"
        ]
     }
   }
```

CBOR Encoding:

```
A1                                      # map(1)
   75                                   # text(21)
      72656365697665722D6361706162696C6974696573 # "receiver-capabilities"
   A1                                   # map(1)
      73                                # text(19)
         72656365697665722D6361706162696C697479 # "receiver-capability"
      82                                # array(2)
         78 36                          # text(54)
            75726E3A696574663A6361706162696C6974793A68747470732D6E6F7469662D7265636569766
5723A656E636F64696E673A6A736F6E # "urn:ietf:capability:https-notif-receiver:encoding:json
"
         78 35                          # text(53)
            75726E3A696574663A6361706162696C6974793A68747470732D6E6F7469662D7265636569766
5723A656E636F64696E673A786D6C # "urn:ietf:capability:https-notif-receiver:encoding:xml"
```

If the receiver is unable to reply using "application/cbor", but is capable of receiving only cbor then the response might look like this:

```
HTTP/1.1 200 OK
Date: Tue, 4 March 2025 20:33:30 GMT
Server: example-server
Cache-Control: no-cache
Content-Type: application/json
{
"receiver-capabilities": {
  "receiver-capability": [
    "urn:ietf:capability:https-notif-receiver:encoding:cbor"
     ]
   }
}
```

3.3. Relay Notification request

The publisher sends an HTTP POST request to the "relay-notification" resource on the receiver with the "Content-Type" header set to "application/cbor" in case the receiver is CBOR capable and a body containing the notification encoded in CBOR.

3.3.1. CBOR encoding using names as keys

```
POST /some/path/relay-notification HTTP/1.1
   Host: example.com
   Content-Type: application/cbor
```

Diagnostic notation:

```
{
  "ietf-https-notif:notification": {
    "eventTime": "2013-12-21T00:01:00Z",
    "example-mod:event" : {
      "event-class" : "fault",
      "reporting-entity" : { "card" : "Ethernet0" },
      "severity" : "major"
    }
  }
}
```

Cbor Encoding:

```
A1                                      # map(1)
   78 1D                                # text(29)
      696574662D68747470732D6E6F7469663A6E6F7469669636174696F6E # "ietf-https-notif:noti
fication"
   A2                                   # map(2)
      69                                # text(9)
         6576656E7454696D65             # "eventTime"
      74                                # text(20)
         323031332D31322D32315430303A30313A30305A # "2013-12-21T00:01:00Z"
      71                                # text(17)
         6578616D706C652D6D6F643A6576656E74 # "example-mod:event"
      A3                                # map(3)
         68                             # text(8)
            7365766572697479            # "severity"
         65                             # text(5)
            6D616A6F72                  # "major"
         6B                             # text(11)
            6576656E742D636C617373      # "event-class"
         65                             # text(5)
            6661756C74                  # "fault"
         70                             # text(16)
            7265706F7274696E672D656E74697479 # "reporting-entity"
         A1                             # map(1)
            64                          # text(4)
               63617264                 # "card"
            69                          # text(9)
               45746865726E657430       # "Ethernet0"
```

3.3.2. CBOR encoding using SIDs as keys

Diagnostic Notation:

```
{
 2601: {
    1: "2013-12-21T00:01:00Z",
    "example-mod:event" : {
      "event-class" : "fault",
      "reporting-entity" : { "card" : "Ethernet0" },
      "severity" : "major"
    }
  }
}
```

The above is assuming the YANG module for event notifications has a corresponding .sid file with these entries

```
   "item": [
         {
           "namespace": "module",
           "identifier": "ietf-notification",
           "sid": "2600"
         },
         {
           "namespace": "data",
           "identifier": "/ietf-notification:notification",
           "sid": "2601"
         },
         {
           "namespace": "data",
           "identifier": "/ietf-notification:notification/eventTime",
           "sid": "2602"
         }
       ]
```

CBOR Encoding:

```
A1                                  # map(1)
   19 0A28                          # unsigned(2600)
   A2                               # map(2)
      01                            # unsigned(1)
      74                            # text(20)
         323031332D31322D32315430303A30313A30305A # "2013-12-21T00:01:00Z"
      71                            # text(17)
         6578616D706C652D6D6F643A6576656E74 # "example-mod:event"
      A3                            # map(3)
         68                         # text(8)
            7365766572697479        # "severity"
         65                         # text(5)
            6D616A6F72              # "major"
         6B                         # text(11)
            6576656E742D636C617373  # "event-class"
         65                         # text(5)
            6661756C74              # "fault"
         70                         # text(16)
            7265706F7274696E672D656E74697479 # "reporting-entity"
         A1                         # map(1)
            64                      # text(4)
               63617264             # "card"
            69                      # text(9)
               45746865726E657430   # "Ethernet0"
```

3.4. Relay Notification Response

The response on success is "204 (No Content)". In case of corrupted or malformed event, the response is an appropriate HTTP error response.

3.5. Implementation Status

This section records the status of known implementations of the specification defined by this document at the time of posting. The information is provided to assist the IETF in evaluating the maturity and implementability of the specification. This section will be removed prior to publication as an RFC.

3.6. Implementation: HTTPS Notification CBOR Draft Implementation

* _Organization_: National Institute of Technology Karnataka (NITK), Surathkal

* _Implementation Name / Web Page_: HTTPS Notification CBOR Draft Implementation https://github.com/MeherRushi/https-notif-draft-impl (https://github.com/MeherRushi/https-notif-draft-impl)

* _Description_: This implementation provides a Python-based prototype of the mechanism defined in this document for transporting YANG notifications over HTTPS using JSON, XML and CBOR encoding. It supports name-based CBOR encoding and includes basic publisher and receiver roles to demonstrate end-to-end message exchange.

* _Maturity Level_: Prototype

* _Coverage_:

  - Capabilities discovery via HTTP GET to /capabilities

  - Event publication via HTTP POST to /relay-notification

  - Support for name-based CBOR encoding as described in this document

* _Version Compatibility_: The implementation is based on draft-ietf-netconf-https-notif-15 and draft-ietf-netconf-https-notif-cbor-00.

* _Licensing_: Freely distributable under an MIT-style license.

* _Implementation Experience_:

- Developed and demonstrated at IETF 121 and 122 Hackathon.

- Worked toward enabling CBOR encoding in the libyang library as part of the hackathon effort (slides (https://datatracker.ietf.org/meeting/123/materials/slides-123-hackathon-sessd-adding-cbor-support-in-libyang-00)).

- Evaluated CBOR efficiency compared to JSON and XML in constrained environments.

- Built tooling to simulate and measure notification transfer behavior over varying network conditions.

- Diagnostic encoding examples used for validation of CBOR structures.

* _Contact Information_:

  - Bharadwaja Meherrushi Chittapragada (meher.211cs216@nitk.edu.in)

  - Vartika T Rao (vartikatrao.211it077@nitk.edu.in)

  - Siddharth Bhat (sidbhat.211ee151@nitk.edu.in)

  - Hayyan Arshad (hayyanarshad.211cs222@nitk.edu.in)

* _Last Updated_: July 24, 2025

4. Security Considerations

Addition of the CBOR encoding introduces no specific security exposures or risks other that the ones mentioned in [RFC9254] and [I-D.draft-ietf-netconf-https-notif] (An HTTPS-based Transport for YANG Notifications)

5. IANA Considerations

This document requests that IANA include an additional entry in the “Capabilities for HTTPS Notification Receivers” registry, defined in [I-D.draft-ietf-netconf-https-notif]. The following entry is added:

```
Record:
   URN:         urn:ietf:params:yang-notif:https-capability:encoding:cbor
   Reference:   RFC XXXX:An HTTPS-based Transport for YANG Notifications
   Description: Identifies support for CBOR-encoded notifications.
```

6. References

6.1. Normative References

[I-D.draft-ietf-netconf-https-notif]
Jethanandani, M. and K. Watsen, "An HTTPS-based Transport for YANG Notifications", Work in Progress, Internet-Draft, draft-ietf-netconf-https-notif-15, 1 February 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-netconf-https-notif-15>.

[RFC8639] Voit, E., Clemm, A., Gonzalez Prieto, A., Nilsen-Nygaard, E., and A. Tripathy, "Subscription to YANG Notifications", RFC 8639, DOI 10.17487/RFC8639, September 2019, <https://www.rfc-editor.org/rfc/rfc8639>.

[RFC8949] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", STD 94, RFC 8949, DOI 10.17487/RFC8949, December 2020, <https://www.rfc-editor.org/rfc/rfc8949>.

[RFC9254] Veillette, M., Ed., Petrov, I., Ed., Pelov, A., Bormann, C., and M. Richardson, "Encoding of Data Modeled with YANG in the Concise Binary Object Representation (CBOR)", RFC 9254, DOI 10.17487/RFC9254, July 2022, <https://www.rfc-editor.org/rfc/rfc9254>.

6.2. Informative References

[RFC3553] Mealling, M., Masinter, L., Hardie, T., and G. Klyne, "An IETF URN Sub-namespace for Registered Protocol Parameters", BCP 73, RFC 3553, DOI 10.17487/RFC3553, June 2003, <https://www.rfc-editor.org/rfc/rfc3553>.

Acknowledgments

The authors acknowledge the support of Kent Watsen and Mahesh Jethanandani, the authors of [I-D.draft-ietf-netconf-https-notif] for their guidance and support provided to draft this document.

Authors’ Addresses

Bharadwaja Meherrushi Chittapragada
National Institute of Technology Karnataka, Surathkal
Email: meherrushi2@gmail.com

Siddharth Bhat
National Institute of Technology Karnataka, Surathkal
Email: siddharth.bhat10@gmail.com

Vartika T Rao
National Institute of Technology Karnataka, Surathkal
Email: vartikatrao@gmail.com

Hayyan Arshad
National Institute of Technology Karnataka, Surathkal
Email: hayyanhamnah@gmail.com

Mohit P. Tahiliani
National Institute of Technology Karnataka, Surathkal
Email: tahiliani@nitk.edu.in