NETCONF Working Group
Internet-Draft
Intended status: Standards Track
Expires: 20 April 2025

Q. Wu
Q. Ma
Huawei
A. Huang Feng
INSA-Lyon
T. Graf
Swisscom
17 October 2024

YANG Notification Transport Capabilities
draft-netana-netconf-yp-transport-capabilities-00

Abstract

This document ~~proposes~~ specifies a YANG module for YANG notifications transport capabilities which augments "ietf-system-capabilities" YANG module defined in ~~[~~ RFC 9196~~]~~. The module ~~and~~ provides transport, encoding, and encryption system capabilities for ~~transport~~ transport-specific notification. This YANG module can be used by the client to learn capability information from the server at runtime or at implementation time, by making use of the YANG instance data file format.

and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction

The ~~Notification~~ notification capabilities model ~~defined in [RFC9196]~~ allows a client to discover a set of capabilities supported by ~~the~~ a server (e.g., basic system capabilities and YANG-Push related capabilities) both at implementation time and at runtime (Section 2 of [RFC9196]). These capabilities allow ~~the~~a client to adjust its behavior to take advantage of the features exposed by the server.

Commenté [MB1]: As where this sentence was mirrored from :-)

However, ~~the~~ clients and ~~the~~ servers may still support various different transport specific parameters (e.g., transport protocol, encoding format, or encryption). As described in Section 3.1 of [RFC8641], a simple negotiation (~~i.e.~~e.g., inserting hints into error responses to a failed RPC request) between subscribers and publishers for subscription parameters increases the likelihood of success for subsequent RPC requests, but not guaranteed, which may cause unexpected failure or additional message exchange between client and server.

This document defines a ~~corresponding~~ more deterministic solution ~~by proposing a~~that relies upon a YANG module for YANG notifications transport capabilities that is built on top of [RFC9196]. The module can be used by ~~the~~ a client to discover capability information from ~~the~~ a server at runtime or at implementation time, by making use of the YANG instance data file format.

1.1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

The terms "subscriber", "publisher", and "receiver" are used as defined in [RFC8639].

The term "server" is used as defined in [RFC8342].

2. Capabilities for Systems and Datastore Update Notifications

Section 3 of [RFC9196] lists the server capabilities related to YANG Push that are supported ~~The~~ in the YANG module "ietf-notification-capabilities" ~~defined in [RFC9196] specifies the following server capabilities related to YANG Push:~~

~~* Supported (reporting) periods for "periodic" subscriptions~~

~~* Maximum number of objects that can be sent in an update~~

~~* The set of datastores or data nodes for which "periodic" or "on-change" notification is supported~~

~~* Supported dampening periods for "on-change" subscriptions~~

Commenté [MB2]: No need to copy/paste those

These server capabilities are transport independent, session level capabilities. They can be provided either at the implementation time or reported at runtime.

This document ~~augments System Capabilities model and~~ provides additional transport related attributes associated with system capabilities:

* Specification of transport protocols that a~~the~~ client can request to establish an HTTPS-based [I-D.ietf-netconf-https-notif] or UDP-based [I-D.ietf-netconf-udp-notif] configured transport connection.~~,~~

* Specification of transport encoding, such as JSON or XML as defined in [RFC8040] or CBOR as defined in [RFC9254] that ~~the~~ a client can request to encode YANG notifications~~,~~.

* Specification of secure transport mechanisms that are needed by ~~the~~ a client to communicate with ~~the~~ a server such as DTLS ~~as defined in~~ [RFC9147], ~~TLS as defined in~~ [RFC8446], or SSH ~~as defined in~~ [RFC4254]~~,~~].

To that aim, the model defined in this document augments the System Capabilities model [RFC9196].

2.1. Tree Diagram

The following tree diagram [RFC8340] provides an overview of the data model.

```
module: ietf-notification-transport-capabilities

  augment /sysc:system-capabilities/notc:subscription-capabilities:
    +-ro transport-capabilities
       +-ro transport-capability* [transport-protocol]
          +-ro transport-protocol    identityref
          +-ro security-protocol?    identityref
          +-ro encoding-format*      identityref
```

3. YANG Module

```
<CODE BEGINS>
  file "ietf-notification-transport-capabilities@2024-10-14.yang"
module ietf-notification-transport-capabilities {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-notification-transport-
capabilities";
  prefix ntc;

  import ietf-subscribed-notifications {
    prefix sn;
    reference
      "RFC 8639: Subscription to YANG Notifications";
  }
  import ietf-system-capabilities {
    prefix sysc;
    reference
      "RFC 9196: YANG Modules Describing Capabilities for
          Systems and Datastore Update Notifications, Section
4";
  }
  import ietf-notification-capabilities {
    prefix notc;
    reference
      "RFC 9196: YANG Modules Describing Capabilities for
          Systems and Datastore Update Notifications, Section
5";
  }

  organization "IETF NETCONF (Network Configuration) Working Group";
  contact
    "WG Web:   <https://datatracker.ietf.org/group/netconf/>
     WG List:  <mailto:netconf@ietf.org>

     Authors:  Qin Wu
               <mailto:bill.wu@huawei.com>
               Qiufang Ma
               <mailto:maqiufang1@huawei.com>
               Alex Huang Feng
               <mailto:alex.huang-feng@insa-lyon.fr>
               Thomas Graf
               <mailto:thomas.graf@swisscom.com>";

  description
```

```
        "This module defines an extension to System Capability and YANG
Push
         Notification Capabilities model and that provides additional
         transport specific capabilities for YANG notifications.

         Copyright (c) 2024 IETF Trust and the persons identified as
         authors of the code.  All rights reserved.

         Redistribution and use in source and binary forms, with or
         without modification, is permitted pursuant to, and subject
         to the license terms contained in, the Simplified Revised BSD
License
         set forth in Section 4.c of the IETF Trust's Legal Provisions
         Relating to IETF Documents
         (http://trustee.ietf.org/license-info).

         This version of this YANG module is part of RFC XXXX;
         see the RFC itself for full legal notices.";

      revision 2024-10-14 {
        description
          "Initial revision.";
        reference
          "RFC XXXX: YANG Notifications Transport Capabilities";
      }

      identity security-protocol {
        description
          "Identity for security protocols.";
      }

      identity tls {
        base security-protocol;
        description
          "Identity forIndicates TLS security protocol.";
      }

      identity dtls12 {
        base security-protocol;
        description
          "Identity for Indicates DTLS 1.2 security protocol.";
      }

      identity dtls13 {
        base security-protocol;
        description
          "Identity forIndicates DTLS 1.3 security protocol.";
      }

      identity ssh {
        base security-protocol;
        description
          "Identity forIndicates ssh transport protocolSSH.";
      }

      augment "/sysc:system-capabilities/notc:subscription-capabilities" {
        description
          "Adds system level capabilitycapabilities.";
```

Commenté [MB3]: You may clarify why versioning matters here, while this is not done for TLS?

```
       container transport-capabilities {
         description
           "Specifies Capabilities capabilities related to YANG-Push
transports.";
         list transport-capability {
           key "transport-protocol";
           description
             "Indicates a Capability list of capabilities related to
notification transport capabilities.";
           leaf transport-protocol {
             type identityref {
               base sn:transport;
             }
             description
               "Indicates Supported supported transport protocol for
YANG-Push.";
           }
           leaf security-protocol {
             type identityref {
               base security-protocol;
             }
             description
               "Type Indicate of securea transport security protocol.";
           }
           leaf-list encoding-format {
             type identityref {
               base sn:encoding;
             }
             description
               "Indicates Supported supported encoding formats.";
           }
         }
       }
     }
   }
   <CODE ENDS>
```

Commenté [MB4]: You may clarify why a container with leaf-lists wouldn't be sufficient to reflect the capabilities vs using a list.

Are there case where the encoding format will be specific to a given transport/sec Protocol?

4. IANA Considerations

4.1. Updates to the IETF XML Registry

This document registers a URI in the "IETF XML Registry" [RFC3688]. Following the format in [RFC3688], the following registration has been made:

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

4.2. Updates to the YANG Module Names Registry

This document registers one YANG module in the "YANG Module Names" registry [RFC6020]. Following the format in [RFC6020], the following

registration has been made:

name:
ietf-notification-transport-capabilities
namespace:
urn:ietf:params:xml:ns:yang:ietf-notification-transport-capabilities
prefix:
ntc
reference:
RFC XXXX (RFC Ed.: replace XXX with actual RFC number and remove this note.)

5. Security Considerations

This section is modeled after the template described in Section 3.7 of [I-D.ietf-netmod-rfc8407bis]

The "ietf-notification-transport-capabilities" YANG module defines a data model that is designed to be accessed via YANG-based management protocols, such as NETCONF [RFC6241] and RESTCONF [RFC8040]. These protocols have to use a secure transport layer (e.g., SSH [RFC4252], TLS [RFC8446], and QUIC [RFC9000]) and have to use mutual authentication.

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.

All protocol-accessible data nodes are read-only and cannot be modified. The data in the module is not security sensitive. It inherits all the security considerations of [RFC9196].

6. Contributors

Ran Tao
Huawei
101 Software Avenue, Yuhua District
Nanjing, Jiangsu 210012
China
Email: taoran20@huawei.com

Liang Geng
China Mobile
32 Xuanwumen West St, Xicheng District
Beijing 10053
China
Email: gengliang@chinamobile.com

Peng Liu
China Mobile
Beiqijia Town, Changping District
Beijing 10053
China
Email: liupengyjy@chinamobile.com

Wei Wang

China Telecom
32 Xuanwumen West St, Xicheng District
Beijing 102209
China
Email: wangw36@chinatelecom.cn

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC4254] Ylonen, T. and C. Lonvick, Ed., "The Secure Shell (SSH) Connection Protocol", RFC 4254, DOI 10.17487/RFC4254, January 2006, <https://www.rfc-editor.org/info/rfc4254>.

[RFC6241] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J., Ed., and A. Bierman, Ed., "Network Configuration Protocol (NETCONF)", RFC 6241, DOI 10.17487/RFC6241, June 2011, <https://www.rfc-editor.org/info/rfc6241>.

[RFC6242] Wasserman, M., "Using the NETCONF Protocol over Secure Shell (SSH)", RFC 6242, DOI 10.17487/RFC6242, June 2011, <https://www.rfc-editor.org/info/rfc6242>.

[RFC8040] Bierman, A., Bjorklund, M., and K. Watsen, "RESTCONF Protocol", RFC 8040, DOI 10.17487/RFC8040, January 2017, <https://www.rfc-editor.org/info/rfc8040>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8341] Bierman, A. and M. Bjorklund, "Network Configuration Access Control Model", STD 91, RFC 8341, DOI 10.17487/RFC8341, March 2018, <https://www.rfc-editor.org/info/rfc8341>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

[RFC8641] Clemm, A. and E. Voit, "Subscription to YANG Notifications for Datastore Updates", RFC 8641, DOI 10.17487/RFC8641, September 2019, <https://www.rfc-editor.org/info/rfc8641>.

[RFC9147] Rescorla, E., Tschofenig, H., and N. Modadugu, "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3", RFC 9147, DOI 10.17487/RFC9147, April 2022, <https://www.rfc-editor.org/info/rfc9147>.

[RFC9196] Lengyel, B., Clemm, A., and B. Claise, "YANG Modules Describing Capabilities for Systems and Datastore Update Notifications", RFC 9196, DOI 10.17487/RFC9196, February 2022, <https://www.rfc-editor.org/info/rfc9196>.

[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/info/rfc9254>.

7.2. Informative References

[I-D.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>.

[I-D.ietf-netconf-udp-notif]
Zheng, G., Zhou, T., Graf, T., Francois, P., Feng, A. H., and P. Lucente, "UDP-based Transport for Configured Subscriptions", Work in Progress, Internet-Draft, draft-ietf-netconf-udp-notif-14, 4 July 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-netconf-udp-notif-14>.

[I-D.ietf-netmod-rfc8407bis]
Bierman, A., Boucadair, M., and Q. Wu, "Guidelines for Authors and Reviewers of Documents Containing YANG Data Models", Work in Progress, Internet-Draft, draft-ietf-netmod-rfc8407bis-18, 11 October 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-netmod-rfc8407bis-18>.

[RFC3688] Mealling, M., "The IETF XML Registry", BCP 81, RFC 3688, DOI 10.17487/RFC3688, January 2004, <https://www.rfc-editor.org/info/rfc3688>.

[RFC4252] Ylonen, T. and C. Lonvick, Ed., "The Secure Shell (SSH) Authentication Protocol", RFC 4252, DOI 10.17487/RFC4252, January 2006, <https://www.rfc-editor.org/info/rfc4252>.

[RFC6020] Bjorklund, M., Ed., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", RFC 6020, DOI 10.17487/RFC6020, October 2010, <https://www.rfc-editor.org/info/rfc6020>.

[RFC8340] Bjorklund, M. and L. Berger, Ed., "YANG Tree Diagrams", BCP 215, RFC 8340, DOI 10.17487/RFC8340, March 2018, <https://www.rfc-editor.org/info/rfc8340>.

[RFC9000] Iyengar, J., Ed. and M. Thomson, Ed., "QUIC: A UDP-Based Multiplexed and Secure Transport", RFC 9000, DOI 10.17487/RFC9000, May 2021, <https://www.rfc-editor.org/info/rfc9000>.

Appendix A. Usage Example of interaction with UDP-Notif and HTTPS-Notif for Configured Subscription

The following instance-data example describes the notification transport capabilities of a hypothetical "acme-router".

```
<?xml version="1.0" encoding="UTF-8"?>
<instance-data-set xmlns=
"urn:ietf:params:xml:ns:yang:ietf-yang-instance-data">
  <name>acme-router-notification-capabilities</name>
  <content-schema>
    <module>ietf-system-capabilities@2020-03-23</module>
    <module>ietf-notification-capabilities@2020-03-23</module>
    <module>ietf-notification-transport-capabilities@2024-10-14</module>
  </content-schema>
  <!-- revision date, contact, etc. -->
  <description>Server Capability Discovery</description>
  <content-data>
    <system-capabilities xmlns="urn:ietf:params:xml:ns:yang:ietf-system\
      -capabilities">
      <subscription-capabilities xmlns="urn:ietf:params:xml:ns:yang:iet\
        f-notification-capabilities">
        <transport-capabilities xmlns="urn:ietf:params:xml:ns:yang:ietf\
          -notification-transport-capabilities">
          <transport-capability>
            <transport-protocol xmlns:hnt="urn:ietf:params:xml:ns:yang:\
            ietf-https-notif-transport">hnt:https</transport-protocol>
            <encoding-format xmlns:sn="urn:ietf:params:xml:ns:yang:ietf\
              -subscribed-notifications">sn:encode-xml</encoding-format>
            <encoding-format xmlns:sn="urn:ietf:params:xml:ns:yang:ietf\
             -subscribed-notifications">sn:encode-json</encoding-format>
          </transport-capability>
          <transport-capability>
            <transport-protocol xmlns:unt="urn:ietf:params:xml:ns:yang:\
            ietf-udp-notif-transport">unt:udp-notif</transport-protocol>
            <encoding-format xmlns:unt="urn:ietf:params:xml:ns:yang:iet\
              f-udp-notif-transport">unt:encode-cbor</encoding-format>
          </transport-capability>
        </transport-capabilities>
      </subscription-capabilities>
    </system-capabilities>
  </content-data>
</instance-data-set>
```

In addition, the client could also query notification transport capabilities from the server. For example, the client sends <get> request message to the the server to query from the server.

```
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
   <get>
     <filter type="subtree">
     <system-capabilities xmlns="urn:ietf:params:xml:ns:yang:ietf-syste\
       m-capabilities">
       <subscription-capabilities xmlns="urn:ietf:params:xml:ns:yang:ie\
         tf-notification-capabilities">
       <transport-capabilities/>
       </subscription-capabilities>
     </system-capabilities>
    </filter>
   </get>
```

```
 </rpc>
```

The server returns server data export capability using <rpc-reply> as follows:

```
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
  message-id="101">
  <data>
    <system-capabilities xmlns="urn:ietf:params:xml:ns:yang:ietf-system\
      -capabilities">
      <subscription-capabilities xmlns="urn:ietf:params:xml:ns:yang:iet\
        f-notification-capabilities">
        <transport-capabilities xmlns="urn:ietf:params:xml:ns:yang:ietf\
          -notification-transport-capabilities">
          <transport-capability>
            <transport-protocol xmlns:hnt="urn:ietf:params:xml:ns:yang:\
            ietf-https-notif-transport">hnt:https</transport-protocol>
            <encoding-format xmlns:sn="urn:ietf:params:xml:ns:yang:ietf\
            -subscribed-notifications">sn:encode-xml</encoding-format>
            <encoding-format xmlns:sn="urn:ietf:params:xml:ns:yang:ietf\
             -subscribed-notifications">sn:encode-json</encoding-format>
          </transport-capability>
          <transport-capability>
            <transport-protocol xmlns:unt="urn:ietf:params:xml:ns:yang:\
            ietf-udp-notif-transport">unt:udp-notif</transport-protocol>
            <encoding-format xmlns:unt="urn:ietf:params:xml:ns:yang:iet\
              f-udp-notif-transport">unt:encode-cbor</encoding-format>
          </transport-capability>
        </transport-capabilities>
      </subscription-capabilities>
    </system-capabilities>
  </data>
</rpc-reply>
```