

NETCONF Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: 16 November 2026

Q. Wu  
Q. Ma  
Huawei  
A. Huang-Feng  
INSA-Lyon  
T. Graf  
Swisscom  
15 May 2026

YANG Notification Transport Capabilities  
draft-ietf-netconf-yp-transport-capabilities-06

Abstract

This document specifies a YANG module for YANG notifications transport capabilities which augments the notification capabilities model. The module provides YANG notifications transport protocol, transport encoding, and transport encryption system capabilities for 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.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 16 November 2026.

Copyright Notice

Copyright (c) 2026 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights 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 . . . . .	2
1.1. Terminology . . . . .	3
2. Capabilities for Systems and Datastore Update Notifications . . . . .	3
2.1. Tree Diagram . . . . .	4
3. YANG Module . . . . .	4
4. IANA Considerations . . . . .	7
4.1. Updates to the IETF XML Registry . . . . .	7
4.2. Updates to the YANG Module Names Registry . . . . .	7
5. Implementation Status . . . . .	8
5.1. Huawei VRP . . . . .	8
5.2. Cisco IOS XR . . . . .	8
6. Security Considerations . . . . .	8
7. Contributors . . . . .	8
8. Acknowledgements . . . . .	9
9. References . . . . .	9
9.1. Normative References . . . . .	9
9.2. Informative References . . . . .	11
Appendix A. Usage Example of interaction with UDP-Notif and HTTPS-Notif for Configured Subscription . . . . .	12
Authors' Addresses . . . . .	15

## 1. Introduction

The "ietf-system-capabilities" YANG module defined in [RFC9196] allows a client to discover a set of capabilities supported by a server (including, basic system capabilities and YANG-Push related capabilities) both at implementation time and at runtime. These capabilities allow a client to adjust its behavior to take advantage of the features exposed by the server.

However, clients and servers may support various different YANG notifications transport specific parameters (e.g., transport protocol, encoding format or encryption). As described in Section 3.2 of [RFC8641], a simple negotiation (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. While these error responses help in establishing the subscription, they are not widely supported, which may cause unexpected failures or additional message exchange between client and server.

This document defines a more deterministic solution that relies upon a YANG module for YANG notifications transport capabilities that is built on top of [RFC9196]. The module can be used by a client to discover capability information from 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 terms "client", and "server" are used as defined in [RFC8342].

## 2. Capabilities for Systems and Datastore Update Notifications

Section 3.1 of [RFC8641] lists the server capabilities related to YANG-Push that are supported in the YANG module "ietf-notification-capabilities".

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

This document provides additional transport related attributes associated with system capabilities:

- \* Specification of transport protocols for YANG notifications that a client can request to establish, including HTTPS-based [I-D.ietf-netconf-https-notif] or UDP-based [I-D.ietf-netconf-udp-notif] configured transport connection.
- \* Specification of YANG notifications transport encodings, including XML [RFC7950], JSON [RFC7951] or CBOR [RFC9254] supported by the server;

- \* Specification of secure YANG notifications transport encryption mechanisms that are supported by the server, including DTLS 1.2 [RFC6347], DTLS 1.3 [RFC9147], TLS 1.2 [RFC5246], and TLS 1.3 [RFC8446].
- \* To that end, 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-yp-transport-capabilities

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

### 3. YANG Module

```
<CODE BEGINS> file "ietf-yp-transport-capabilities@2026-05-15.yang"
module ietf-yp-transport-capabilities {
  yang-version 1.1;
  namespace
    "urn:ietf:params:xml:ns:yang:ietf-yp-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";
  }
  import ietf-notification-capabilities {
    prefix notc;
    reference
      "RFC 9196: YANG Modules Describing Capabilities for
      Systems and Datastore Update Notifications";
  }
}
```

```
import ietf-tls-common {
  prefix tlscmn;
  reference
    "RFC 9645: YANG Groupings for TLS Clients and TLS Servers";
}

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 YANG-Push
  Notification Capabilities model that provides additional
  transport specific capabilities for YANG notifications.

  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 (RFC 2119) (RFC 8174) when, and only when,
  they appear in all capitals, as shown here.

  Copyright (c) 2026 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 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
  (https://www.rfc-editor.org/info/rfcXXXX); see the RFC itself
  for full legal notices.";

revision 2026-05-15 {
  description
    "Initial revision.";
```

```
    reference
      "RFC XXXX: YANG Notifications Transport Capabilities";
  }

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

  identity dtls12 {
    base security-protocol;
    description
      "Indicates DTLS Protocol Version 1.2. DTLS 1.2 is obsolete,
       and thus it is NOT RECOMMENDED to enable this feature.";
    reference
      "RFC 6347: The Datagram Transport Layer Security (DTLS)
       Protocol Version 1.2.";
  }

  identity dtls13 {
    base security-protocol;
    description
      "Indicates DTLS Protocol Version 1.3.";
    reference
      "RFC 9147: The Datagram Transport Layer Security (DTLS)
       Protocol Version 1.3.";
  }

  augment "/sysc:system-capabilities"
    + "/notc:subscription-capabilities" {
    description
      "Adds subscription-related system level capabilities.";
    container transport-capabilities {
      description
        "Specifies capabilities related to YANG-Push transports.";
      list transport-capability {
        key "transport-protocol";
        description
          "Indicates supported YANG notifications transport protocol
           for Subscribed Notifications [RFC8639] and YANG-Push
           [RFC8641]. Defines the supported transports, security
           protocols and supported notification encodings.";
        leaf transport-protocol {
          type identityref {
            base sn:transport;
          }
          description
            "Indicates the supported YANG notifications transport
```

```

    protocol for Subscribed Notifications [RFC8639] and
    YANG-Push [RFC8641].";
}
leaf-list security-protocol {
    type union {
        type identityref {
            base security-protocol;
        }
        type identityref {
            base tlscmn:tls-version-base;
        }
    }
    description
        "Indicates the supported YANG notifications transport
        encryption protocols.";
}
leaf-list encoding-format {
    type identityref {
        base sn:encoding;
    }
    description
        "Indicates supported encoding formats for YANG notifications.";
}
}
}
}
<CODE ENDS>
```

## 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-yp-transport-capabilities
Registrant Contact: The IESG.
XML: N/A; the requested URI is an XML namespace.
Reference: RFC XXXX (RFC Ed.: replace XXX with actual RFC number
and remove this note.)
```

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

## 5. Implementation Status

Note to the RFC-Editor: Please remove this section before publishing.

### 5.1. Huawei VRP

Huawei implemented this document for a YANG Push publisher in their VRP platform.

### 5.2. Cisco IOS XR

Cisco implemented this document for a YANG Push publisher in their IOS XR platform.

## 6. Security Considerations

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

The "ietf-yp-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].

## 7. 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

## 8. Acknowledgements

The authors would like to thank Mohamed Boucadair, Kent Watson, Jan Lindblad, Reshad Rahman, Xiao Min, Per Andersson and Rob Wilton for their review and valuable comments.

## 9. References

### 9.1. 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>>.
- [RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <<https://www.rfc-editor.org/info/rfc5246>>.

- [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>>.
- [RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, DOI 10.17487/RFC6347, January 2012, <<https://www.rfc-editor.org/info/rfc6347>>.
- [RFC7950] Bjorklund, M., Ed., "The YANG 1.1 Data Modeling Language", RFC 7950, DOI 10.17487/RFC7950, August 2016, <<https://www.rfc-editor.org/info/rfc7950>>.
- [RFC7951] Lhotka, L., "JSON Encoding of Data Modeled with YANG", RFC 7951, DOI 10.17487/RFC7951, August 2016, <<https://www.rfc-editor.org/info/rfc7951>>.
- [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>>.
- [RFC8342] Bjorklund, M., Schoenwaelder, J., Shafer, P., Watsen, K., and R. Wilton, "Network Management Datastore Architecture (NMDA)", RFC 8342, DOI 10.17487/RFC8342, March 2018, <<https://www.rfc-editor.org/info/rfc8342>>.
- [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>>.
- [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/info/rfc8639>>.
- [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>>.

## 9.2. 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]  
Feng, A. H., Francois, P., Zhou, T., Graf, T., and P. Lucente, "UDP-based Transport for Configured Subscriptions", Work in Progress, Internet-Draft, draft-ietf-netconf-udp-notif-25, 28 January 2026, <<https://datatracker.ietf.org/doc/html/draft-ietf-netconf-udp-notif-25>>.
- [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-28, 5 June 2025, <<https://datatracker.ietf.org/doc/html/draft-ietf-netmod-rfc8407bis-28>>.
- [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".

===== NOTE: '\ ' line wrapping per RFC 8792 =====

```
<?xml version="1.0" encoding="UTF-8"?>
<instance-data-set
  xmlns="urn:ietf:params:xml:ns:yang:ietf-yang-instance-data"
  xmlns:hnt="urn:ietf:params:xml:ns:yang:ietf-https-notif-transport"
  xmlns:sn="urn:ietf:params:xml:ns:yang:ietf-subscribed-notifications"
  xmlns:tlscmn="urn:ietf:params:xml:ns:yang:ietf-tls-common"
  xmlns:tlscmn="urn:ietf:params:xml:ns:yang:ietf-tls-common"
  xmlns:unt="urn:ietf:params:xml:ns:yang:ietf-udp-notif-transport">
  <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-yp-transport-capabilities@2025-06-07</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:ietf\
-notification-capabilities">
        <transport-capabilities xmlns="urn:ietf:params:xml:ns:yang:ietf-\
yp-transport-capabilities">
          <transport-capability>
            <transport-protocol>hnt:https</transport-protocol>
            <encoding-format>sn:encode-xml</encoding-format>
            <encoding-format>sn:encode-json</encoding-format>
            <security-protocol>tlscmn:tls12</security-protocol>
            <security-protocol>tlscmn:tls13</security-protocol>
          </transport-capability>
          <transport-capability>
            <transport-protocol>unt:udp-notif</transport-protocol>
            <encoding-format>sn:encode-json</encoding-format>
            <encoding-format>unt:encode-cbor</encoding-format>
            <security-protocol>dtls12</security-protocol>
            <security-protocol>dtls13</security-protocol>
          </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.

===== NOTE: '\ ' line wrapping per RFC 8792 =====

```
<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-system-capabilities">
        <subscription-capabilities xmlns="urn:ietf:params:xml:ns:yang:ietf-notification-capabilities">
          <transport-capabilities xmlns="urn:ietf:params:xml:ns:yang:ietf-yp-transport-capabilities"/>
        </subscription-capabilities>
      </system-capabilities>
    </filter>
  </get>
</rpc>
```

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

===== NOTE: '\ ' line wrapping per RFC 8792 =====

```
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
  xmlns:sc="urn:ietf:params:xml:ns:yang:ietf-system-capabilities"
  xmlns:nc="urn:ietf:params:xml:ns:yang:ietf-notification-capabilities"
  xmlns:tc="urn:ietf:params:xml:ns:yang:ietf-yp-transport-capabilities"
  xmlns:hnt="urn:ietf:params:xml:ns:yang:ietf-https-notif-transport"
  xmlns:sn="urn:ietf:params:xml:ns:yang:ietf-subscribed-notifications"
  xmlns:unt="urn:ietf:params:xml:ns:yang:ietf-udp-notif-transport"
  xmlns:tlscmn="urn:ietf:params:xml:ns:yang:ietf-tls-common" message-id=\
  "101">
  <data>
    <sc:system-capabilities>
      <nc:subscription-capabilities>
        <transport-capabilities xmlns="urn:ietf:params:xml:ns:yang:ietf-\
          yp-transport-capabilities">
          <transport-capability>
            <transport-protocol>hnt:https</transport-protocol>
            <encoding-format>sn:encode-xml</encoding-format>
            <encoding-format>sn:encode-json</encoding-format>
            <security-protocol>tlscmn:tls12</security-protocol>
            <security-protocol>tlscmn:tls13</security-protocol>
          </transport-capability>
          <transport-capability>
            <transport-protocol>unt:udp-notif</transport-protocol>
            <encoding-format>sn:encode-json</encoding-format>
            <encoding-format>unt:encode-cbor</encoding-format>
            <security-protocol>dtls12</security-protocol>
            <security-protocol>dtls13</security-protocol>
          </transport-capability>
        </transport-capabilities>
      </nc:subscription-capabilities>
    </sc:system-capabilities>
  </data>
</rpc-reply>
```

#### Authors' Addresses

Qin Wu  
Huawei  
101 Software Avenue, Yuhua District  
Nanjing  
Jiangsu, 210012  
China  
Email: bill.wu@huawei.com

Qiufang Ma  
Huawei  
101 Software Avenue, Yuhua District  
Nanjing  
Jiangsu, 210012  
China  
Email: maqiufang1@huawei.com

Alex Huang Feng  
INSA-Lyon  
Lyon  
France  
Email: alex.huang-feng@insa-lyon.fr

Thomas Graf  
Swisscom  
Binzring 17  
CH-8045 Zurich  
Switzerland  
Email: thomas.graf@swisscom.com