Workgroup: Network Working Group
Internet-Draft:
draft-ahuang-netconf-udp-client-server-00
Published: 23 October 2023
Intended Status: Standards Track
Expires: 25 April 2024
Authors: A. Huang Feng P. Francois K. Watsen
INSA-Lyon INSA-Lyon Watsen Networks

YANG Grouping for UDP Clients and UDP Servers

Abstract

This document defines two YANG 1.1 modules to support the configuration of UDP clients and UDP servers. The modules include basic parameters for configuring UDP based clients and servers and a DTLS container when encryption needs to be enabled.

Requirements Language

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.

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 25 April 2024.

Copyright Notice

Table of Contents

1. Introduction

This documents defines two YANG 1.1 [RFC7950] modules to support the configuration of UDP clients and UDP servers, either as standalone or in conjunction with configuration of other protocol layers.

2. The "ietf-udp-client" Module

The "ietf-udp-client" YANG module defines two groupings for configuring UDP clients: the "udp-client-grouping" for UDP clients and the "udp-dtls-client-grouping" for UDP clients with DTLS 1.3 [RFC9147] enryption.

2.1. The "udp-client-grouping" Grouping

The following tree diagram [RFC8340] illustrates the "udp-client-grouping" grouping:

```
module: ietf-udp-client

  grouping udp-client-grouping:
    +-- remote-address    inet:ip-address-no-zone
    +-- remote-port       inet:port-number
```

2.2. The "udp-dtls-client-grouping" Grouping

The following tree diagram [RFC8340] illustrates the "udp-dtls-client-grouping" grouping:

```
module: ietf-udp-client

  grouping udp-dtls-client-grouping:
    +-- remote-address    inet:ip-address-no-zone
    +-- remote-port       inet:port-number
    +-- dtls! {dtls13}?
       +-- client-identity!
       |  +-- (auth-type)
       |     +--:(certificate) {client-ident-x509-cert}?
       |     |  +-- certificate
       |     |     +-- (local-or-keystore)
       |     |           ...
       |     +--:(raw-public-key) {client-ident-raw-public-key}?
       |     |  +-- raw-private-key
       |     |     +-- (local-or-keystore)
       |     |           ...
       |     +--:(tls12-psk)
       |     |        {client-ident-tls12-psk,not tlsc:client-ident-tls1
       |     |  +-- tls12-psk
       |     |     +-- (local-or-keystore)
       |     |     |     ...
       |     |     +-- id?                          string
       |     +--:(tls13-epsk) {client-ident-tls13-epsk}?
       |        +-- tls13-epsk
       |           +-- (local-or-keystore)
       |           |     ...
       |           +-- external-identity           string
       |           +-- hash
       |           |       tlscmn:epsk-supported-hash
       |           +-- context?                    string
       |           +-- target-protocol?            uint16
       |           +-- target-kdf?                 uint16
       +-- server-authentication
       |  +-- ca-certs! {server-auth-x509-cert}?
       |  |  +-- (local-or-truststore)
       |  |     +--:(local) {local-definitions-supported}?
       |  |     |  +-- local-definition
       |  |     |        ...
       |  |     +--:(truststore)
       |  |              {central-truststore-supported,certificates}?
       |  |        +-- truststore-reference?   ts:certificate-bag-ref
       |  +-- ee-certs! {server-auth-x509-cert}?
       |  |  +-- (local-or-truststore)
       |  |     +--:(local) {local-definitions-supported}?
       |  |     |  +-- local-definition
       |  |     |        ...
       |  |     +--:(truststore)
       |  |              {central-truststore-supported,certificates}?
       |  |        +-- truststore-reference?   ts:certificate-bag-ref
```

```
|  +-- raw-public-keys! {server-auth-raw-public-key}?
|  |  +-- (local-or-truststore)
|  |     +--:(local) {local-definitions-supported}?
|  |     |  +-- local-definition
|  |     |        ...
|  |     +--:(truststore)
|  |              {central-truststore-supported,public-keys}?
|  |        +-- truststore-reference?   ts:public-key-bag-ref
|  +-- tls12-psks?        empty
|  |       {server-auth-tls12-psk,not tlsc:server-auth-tls12-psk}
|  +-- tls13-epsks?       empty {server-auth-tls13-epsk}?
+-- hello-params {tlscmn:hello-params}?
|  +-- tls-versions
|  |  +-- tls-version*   identityref
|  +-- cipher-suites
|     +-- cipher-suite*   identityref
+-- keepalives {tls-client-keepalives}?
   +-- peer-allowed-to-send?   empty
   +-- test-peer-aliveness!
      +-- max-wait?       uint16
      +-- max-attempts?   uint8
```

2.3. YANG Module

The "ietf-udp-client" YANG module uses the groupings defined in [I-D.ietf-netconf-tls-client-server] for configuring the DTLS 1.3 encryption.

```
<CODE BEGINS> file "ietf-udp-client@2023-10-16.yang"

module ietf-udp-client {
  yang-version 1.1;
  namespace
    "urn:ietf:params:xml:ns:yang:ietf-udp-client";
  prefix udpc;
  import ietf-inet-types {
    prefix inet;
    reference
      "RFC 6991: Common YANG Data Types";
  }
  import ietf-tls-client {
    prefix tlsc;
    reference
      "RFC TTTT: YANG Groupings for TLS Clients and TLS Servers";
  }

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

     Authors:  Alex Huang Feng
               <mailto:alex.huang-feng@insa-lyon.fr>
               Pierre Francois
               <mailto:pierre.francois@insa-lyon.fr>";

  description
    "Defines a generic grouping for UDP-based client applications.
    Supports groupings for UDP clients and UDP clients with DTLS encrypt

    Copyright (c) 2023 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
    (https://trustee.ietf.org/license-info).

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

  revision 2023-10-16 {
    description
      "Initial revision";
    reference
      "RFC-to-be: YANG Grouping for UDP Clients and UDP Servers";
  }
```

```
/*
 * FEATURES
 */
 feature dtls13 {
   description
     "This feature indicates that DTLS 1.3 encryption of UDP
      packets is supported.";
 }

 grouping udp-client-grouping {
   description
     "Provides a reusable grouping for configuring a UDP client.";

   leaf remote-address {
     type inet:ip-address-no-zone;
     mandatory true;
     description
       "IP address of the UDP client, which can be an
       IPv4 address or an IPV6 address.";
   }

   leaf remote-port {
     type inet:port-number;
     mandatory true;
     description
       "Port number of the UDP client.";
   }
 }

 grouping udp-dtls-client-grouping {
   description
     "Provides a reusable grouping for configuring a UDP client with
     DTLS encryption.";

   uses udp-client-grouping;
   container dtls {
     if-feature dtls13;
     presence dtls;
     uses tlsc:tls-client-grouping {
       // Using tls-client-grouping without TLS1.2 parameters
       // allowing only DTLS 1.3
       refine "client-identity/auth-type/tls12-psk" {
         // create the logical impossibility of enabling TLS1.2
         if-feature "not tlsc:client-ident-tls12-psk";
       }
       refine "server-authentication/tls12-psks" {
         // create the logical impossibility of enabling TLS1.2
         if-feature "not tlsc:server-auth-tls12-psk";
```

```
        }
      }
      description
        "Container for configuring DTLS 1.3 parameters.";
    }
  }
}

<CODE ENDS>
```

3. The "ietf-udp-server" Module

The "ietf-udp-server" YANG module defines two groupings for configuring UDP servers: the "udp-server-grouping" for UDP servers and the "udp-dtls-server-grouping" for UDP servers with DTLS 1.3 [RFC9147] enryption.

3.1. The "udp-server-grouping" Grouping

The following tree diagram [RFC8340] illustrates the "udp-server-grouping" grouping:

```
module: ietf-udp-server

  grouping udp-server-grouping:
    +-- local-address    inet:ip-address-no-zone
    +-- local-port       inet:port-number
```

3.2. The "udp-dtls-server-grouping" Grouping

The following tree diagram [RFC8340] illustrates the "udp-dtls-server-grouping" grouping:

```
module: ietf-udp-server

  grouping udp-dtls-server-grouping:
    +-- local-address    inet:ip-address-no-zone
    +-- local-port       inet:port-number
    +-- dtls! {dtls13}?
       +-- server-identity
       |  +-- (auth-type)
       |     +--:(certificate) {server-ident-x509-cert}?
       |     |  +-- certificate
       |     |     +-- (local-or-keystore)
       |     |           ...
       |     +--:(raw-private-key) {server-ident-raw-public-key}?
       |     |  +-- raw-private-key
       |     |     +-- (local-or-keystore)
       |     |           ...
       |     +--:(tls12-psk)
       |     |        {server-ident-tls12-psk,not tlss:server-ident-tls1
       |     |  +-- tls12-psk
       |     |     +-- (local-or-keystore)
       |     |     |     ...
       |     |     +-- id_hint?                    string
       |     +--:(tls13-epsk) {server-ident-tls13-epsk}?
       |        +-- tls13-epsk
       |           +-- (local-or-keystore)
       |           |     ...
       |           +-- external-identity          string
       |           +-- hash
       |           |       tlscmn:epsk-supported-hash
       |           +-- context?                   string
       |           +-- target-protocol?           uint16
       |           +-- target-kdf?                uint16
       +-- client-authentication! {client-auth-supported}?
       |  +-- ca-certs! {client-auth-x509-cert}?
       |  |  +-- (local-or-truststore)
       |  |     +--:(local) {local-definitions-supported}?
       |  |     |  +-- local-definition
       |  |     |        ...
       |  |     +--:(truststore)
       |  |              {central-truststore-supported,certificates}?
       |  |        +-- truststore-reference?   ts:certificate-bag-ref
       |  +-- ee-certs! {client-auth-x509-cert}?
       |  |  +-- (local-or-truststore)
       |  |     +--:(local) {local-definitions-supported}?
       |  |     |  +-- local-definition
       |  |     |        ...
       |  |     +--:(truststore)
       |  |              {central-truststore-supported,certificates}?
       |  |        +-- truststore-reference?   ts:certificate-bag-ref
```

```
|  +-- raw-public-keys! {client-auth-raw-public-key}?
|  |  +-- (local-or-truststore)
|  |     +--:(local) {local-definitions-supported}?
|  |     |  +-- local-definition
|  |     |        ...
|  |     +--:(truststore)
|  |              {central-truststore-supported,public-keys}?
|  |        +-- truststore-reference?   ts:public-key-bag-ref
|  +-- tls12-psks?        empty
|  |       {client-auth-tls12-psk,not tlss:client-auth-tls12-psk}
|  +-- tls13-epsks?       empty {client-auth-tls13-epsk}?
+-- hello-params {tlscmn:hello-params}?
|  +-- tls-versions
|  |  +-- tls-version*   identityref
|  +-- cipher-suites
|     +-- cipher-suite*   identityref
+-- keepalives {tls-server-keepalives}?
   +-- peer-allowed-to-send?   empty
   +-- test-peer-aliveness!
      +-- max-wait?       uint16
      +-- max-attempts?   uint8
```

3.3. YANG Module

The "ietf-udp-server" YANG module uses the groupings defined in [I-D.ietf-netconf-tls-client-server] for configuring the DTLS 1.3 encryption.

```
<CODE BEGINS> file "ietf-udp-server@2023-10-16.yang"

module ietf-udp-server {
  yang-version 1.1;
  namespace
    "urn:ietf:params:xml:ns:yang:ietf-udp-server";
  prefix udps;
  import ietf-inet-types {
    prefix inet;
    reference
      "RFC 6991: Common YANG Data Types";
  }
  import ietf-tls-server {
    prefix tlss;
    reference
      "RFC FFFF: YANG Groupings for TLS Clients and TLS Servers";
  }

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

     Authors:  Alex Huang Feng
               <mailto:alex.huang-feng@insa-lyon.fr>
               Pierre Francois
               <mailto:pierre.francois@insa-lyon.fr>";

  description
    "Defines a generic grouping for UDP-based server applications.
    Supports groupings for UDP servers and UDP servers with DTLS encrypt

    Copyright (c) 2023 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
    (https://trustee.ietf.org/license-info).

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

  revision 2023-10-16 {
    description
      "Initial revision";
    reference
      "RFC-to-be: YANG Grouping for UDP Clients and UDP Servers";
  }
```

```
/*
 * FEATURES
 */
 feature dtls13 {
   description
     "This feature indicates that DTLS 1.3 encryption of UDP
      packets is supported.";
 }

 grouping udp-server-grouping {
   description
     "Provides a reusable grouping for configuring a UDP servers.";

   leaf local-address {
     type inet:ip-address-no-zone;
     mandatory true;
     description
       "IP address of the UDP server, which can be an
       IPv4 address or an IPV6 address.";
   }

   leaf local-port {
     type inet:port-number;
     mandatory true;
     description
       "Port number of the UDP server.";
   }
 }

 grouping udp-dtls-server-grouping {
   description
     "Provides a reusable grouping for configuring a UDP server with
     DTLS encryption.";

   uses udp-server-grouping;
   container dtls {
     if-feature dtls13;
     presence dtls;
     uses tlss:tls-server-grouping {
       // Using tls-server-grouping without TLS1.2 parameters
       // allowing only DTLS 1.3
       refine "server-identity/auth-type/tls12-psk" {
         // create the logical impossibility of enabling TLS1.2
         if-feature "not tlss:server-ident-tls12-psk";
       }
       refine "client-authentication/tls12-psks" {
         // create the logical impossibility of enabling TLS1.2
         if-feature "not tlss:client-auth-tls12-psk";
```

```
        }
      }
      description
        "Container for configuring DTLS 1.3 parameters.";
    }
  }
}

<CODE ENDS>
```

4. Security Considerations

TODO:

5. IANA Considerations

This document describes the URIs from IETF XML Registry and the registration of a two new YANG module names

5.1. URI

IANA is requested to assign two new URI from the IETF XML Registry [RFC3688]. The following two URIs are suggested:

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

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

5.2. YANG module name

This document also requests two new YANG module names in the YANG Module Names registry [RFC8342] with the following suggestions:

```
name: ietf-udp-client
namespace: urn:ietf:params:xml:ns:yang:ietf-udp-client
prefix: udpc
reference: RFC-to-be

name: ietf-udp-server
namespace: urn:ietf:params:xml:ns:yang:ietf-udp-server
prefix: udps
reference: RFC-to-be
```

6. Acknowledgements

The authors would like to thank xxx for their review and valuable comments.

7. References

7.1. Normative References

[I-D.ietf-netconf-tls-client-server]
Watsen, K., "YANG Groupings for TLS Clients and TLS Servers", Work in Progress, Internet-Draft, draft-ietf-netconf-tls-client-server-33, 17 April 2023, <https://

datatracker.ietf.org/doc/html/draft-ietf-netconf-tls-client-server-33>.

[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>.

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

[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>.

[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>.

[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>.

[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>.

[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>.

7.2. Informative References

Authors' Addresses

Alex Huang Feng
INSA-Lyon
Lyon
France

Email: alex.huang-feng@insa-lyon.fr

Pierre Francois
INSA-Lyon
Lyon
France

Email: pierre.francois@insa-lyon.fr

Kent Watsen
Watsen Networks

Email: kent+ietf@watsen.net