

YANG Grouping for UDP Clients and UDP Servers

draft-ahuang-netconf-udp-client-server-00

A. Huang Feng, INSA-Lyon
P. Francois, INSA-Lyon
K. Watsen, Watsen Networks

29 October 2023

YANG Grouping for UDP Clients and UDP Servers

Context

- Based on UDP-notif draft feedback
 - Interest on having a dedicated draft for generic groupings
- Definition of Generic Groupings for UDP clients and servers
 - UDP client
 - UDP DTLS client
 - UDP server
 - UDP DTLS server
- To be used standalone or in combination with other protocol stacks

YANG model for NETCONF Event Notifications

UDP client and UDP DTLS client

```
module: ietf-udp-client

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

Observations:

- IP-address defined as **ip-address-no-zone** (feedback on UDP-notif)
- DTLS container based on “ietf-tls-client” generic grouping
- DTLS container support DTLS 1.3 (DTLS 1.2 are removed)
- “feature dtls13” is defined within this YANG module

```
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 tls:client-ident-tls12-psk}?
            +-- 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 tls: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
```

YANG model for NETCONF Event Notifications

UDP server and UDP DTLS server

```
module: ietf-udp-server

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

Observations:

- IP-address defined as **ip-address-no-zone** (feedback on UDP-notif)
- DTLS container based on “ietf-tls-server” generic grouping
- DTLS container support DTLS 1.3 (DTLS 1.2 are removed)
- “feature dtls13” is defined within this YANG module

```
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-tls12-psk}?
              +-- 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
```

YANG model for NETCONF Event Notifications

Next steps

- Request more feedback from the WG
- Will send the draft to QUIC WG
- **Working group adoption**