UDP-based Transport for Configured Subscriptions

draft-ietf-netconf-udp-notif-06/-07

G. Zheng, Huawei
T. Zhou, Huawei
T. Graf, Swisscom
P. Francois, INSA-Lyon
A. Huang Feng, INSA-Lyon
P. Lucente, NTT
Draft-ietf-netconf-udp-notif-07

Agenda

- Context
- Diffs between -05 and -07
- Planned changes
3.2. Format of the UDP-Notif Message Header

The UDP-Notif Message Header contains information that facilitate the message transmission before deserializing the notification message. The data format is shown in Figure 2.

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----------+-----------+-----------+-----------+
| Ver | S | MT | Header Len | Message Length |
| +-----------+-----------+-----------+-----------|
| | +-----------+-----------+-----------+-----------|
| | | Observation-Domain-ID |
| | +-----------+-----------+-----------+-----------|
| | | Message-ID |
| | +-----------+-----------+-----------+-----------|
| | | Options |
| ~ +-----------+-----------+-----------+-----------|
```

Figure 2: UDP-Notif Message Header Format
Draft-ietf-netconf-udp-notif-07

Context

- Designed to be deployed in secured networks
- For unsecured networks, a DTLS layer is proposed in section 6

6.1. Transport

As shown in Figure 6, the DTLS is layered next to the UDP transport providing reusable security and authentication functions over UDP. No DTLS extension is required to enable UDP-notif messages over DTLS.

Figure 6: Protocol Stack for DTLS secured UDP-notif
How can we configure DTLS from Netconf?
- Add DTLS parameters into the YANG Module
- Examples of configuration
module: ietf-udp-notif

augment /sn:subscriptions/sn:subscription/sn:receivers/sn:receiver:
  +--rw address inet:ip-address
  +--rw port inet:port-number
  +--rw enable-segmentation? boolean {segmentation}?
  +--rw max-segment-size? uint32 {segmentation}?
  +--rw enable-dtls? boolean {dtls-supported}?
  +--rw dtls {dtls-supported}?

    +--rw client-identity!
      |  +--rw (auth-type)
      |      +--:(certificate) {client-ident-x509-cert}?
      |      |      ... ...
      |      +--:(raw-public-key) {client-ident-raw-public-key}?
      |      |      ... ...
      |      +--:(tls12-psk) {client-ident-tls12-psk}?
      |      |      ... ...
      |      +--:(tls13-epsk) {client-ident-tls13-epsk}?
      |      ...

    +--rw server-authentication
      |  +--rw ca-certs! {server-auth-x509-cert}?
      |  |  +--rw (local-or-truststore)
      |  |  |  ... ...
      |  |  +--rw ee-certs! {server-auth-x509-cert}?
      |  |  |  +--rw (local-or-truststore)
      |  |  |  ... ...
      |  |  +--rw raw-public-keys! {server-auth-raw-public-key}?
      |  |  |  +--rw (local-or-truststore)
      |  |  |  ... ...
      |  |  +--rw tls12-psks? empty {server-auth-tls12-psk}?
      |  |  +--rw tls13-epsks? empty {server-auth-tls13-epsk}?
      |  +--rw hello-params {tlscmm:hello-params}?
      |      +--rw tls-versions
      |      |  |  +--rw tls-version* identityref
      |      |  |  +--rw cipher-suites
      |      |  |  |  +--rw cipher-suite* identityref
      |      |  +--rw keepalives {tls-client-keepalives}?
      |      |  +--rw peer-allowed-to-send? empty
      |      |  +--rw test-peer-aliveness!
      |      |  +--rw max-wait? uint16
      |      +--rw max-attempts? uint8

changes between -05 and -06
grouping target-receiver udp-receiver-grouping {
  description
  "Provides a reusable description of a UDP-Notif target receiver."
}

leaf address {
  type inet:ip-address;
  mandatory true;
  description
  "IP address of target UDP-Notif receiver, which can be an IPv4 address or an IPV6 address."
}

leaf port {
  type inet:port-number;
  mandatory true;
  description
  "Port number of target UDP-Notif receiver, if not specified, the system should use default port number."
}
leaf max-segmentation-size {  
  when "./enable-segmentation = 'true'";  
  if-feature segmentation;  
  type uint32;  
  description  
    "UDP-Notif provides a configurable  
    max-segmentation-size to  
    control the size of each message;"; segment (UDP-Notif header, with  
    options, included);";  
}  
leaf enable-dtls {  
  if-feature dtls-supported;  
  type boolean;  
  default false;  
  description  
    "The switch for the DTLS encryption feature. When disabled, the  
    publisher will not encrypt UDP-Notif messages;";  
}  
container dtls {  
  when "./enable-dtls = 'true'";  
  if-feature dtls-supported;  
  uses tlsc:tls-client-grouping;  
  description  
    "Container for configuring DTLS parameters if DTLS is enabled;";  
}  
}
Figure 2: UDP-Notif Message Header Format

The Message Header contains the following field:

* Ver represents the PDU (Protocol Data Unit) encoding version. The current version value is 0 or 1.
Planned changes

**YANG module example**

- Add example for the defined YANG Module
Thanks !
Subscription to Distributed Notifications

draft-ietf-netconf-distributed-notif-04

G. Zheng, Huawei
T. Zhou, Huawei
E. Voit, Cisco
T. Graf, Swisscom
P. Francois, INSA-Lyon
Update
  • Corrected some nits on -04 version

Planned
  • Last Call when draft-ietf-netconf-udp-notif-0X is Last Called
Thanks !