

# UDP-based Transport for Configured Subscriptions

## draft-ietf-netconf-udp-notif-08

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-08

## Agenda

- Diffs between -07 and -08
- Feedback from ML
- Planned changes for -09
- YANG Push gap

# Draft-ietf-netconf-udp-notif-08

## Changes between -07 and -08

- Requirements language has been updated
- Secured layer for UDP-notif section has been updated
  - 0-RTT data as defined in [RFC9147] **MUST NOT** be used
  - In unsecured networks DTLS layer **MUST** be used instead of **SHOULD**
  - YANG module: dtls container made presence container and removed DTLS 1.2 parameters
- Third IANA registry to manage UDP-notif SHIM header version
- Security considerations have been moved to the end of the draft and “limited domains” reference has been added

# Draft-ietf-netconf-udp-notif-08

## Feedback from ML : YANG Module

- YANG Module prefix
  - Currently: un
  - Feedback from Tom Petch :
    - “Should have a common pattern for the family [...] base spec uses sn”
    - snun?
    - What about the rest (HTTPS-notif hnt, YANG push yp...)?
- Why ip-address (with zone)?
  - Ok to change to ip-address-no-zone?
- YANG module based on Subscribed Notifications example
  - Inconsistent with HTTPS-notif
  - Shall we use ietf-subscribed-notif-receivers from HTTPS-notif?

# Draft-ietf-netconf-udp-notif-08

## YANG Module for configuration

### Current

```
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 dtls! {dtls-supported}?
  +--rw client-identity!
  | +--rw (auth-type)
  | | +--:(certificate) {client-ident-x509-cert}?
  | | | ...
  | | +--:(raw-public-key) {client-ident-raw-public-key}?
  | | | ...
  | | +--:(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 tls13-epsks? empty {server-auth-tls13-epsk}?
  +--rw hello-params {tlscmn: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
```

### HTTPS-notif

```
module: ietf-subscribed-notif-receivers

augment /sn:subscriptions:
  +--rw receiver-instances
  | +--rw receiver-instance* [name]
  | | +--rw name string
  | | +--rw (transport-type)
  +--rw receiver-instance-ref? leafref

module: ietf-https-notif-transport

augment /sn:subscriptions/snr:receiver-instances
  /snr:receiver-instance/snr:transport-type:
  +--:(https)
  | +--rw https-receiver
  | | +--rw (transport)
  | | | +--:(tls) {tls-supported}?
  | | | +--rw tls
  | | | | +--rw tcp-client-parameters
  | | | | | +--rw remote-address inet:host
  | | | | | +--rw remote-port? inet:port-number
  | | | | | +--rw local-address? inet:ip-address
  | | | | | | {local-binding-supported}?
  | | | | | +--rw local-port? inet:port-number
  | | | | | | {local-binding-supported}?
  | | | | | +--rw proxy-server! {proxy-connect}?
  | | | | | | ...
  | | | | | +--rw keepalives! {keepalives-supported}?
  | | | | | | ...
  | | | | +--rw tls-client-parameters
  | | | | | +--rw client-identity!
  | | | | | | ...
```

# Draft-ietf-netconf-udp-notif-08

## Feedback from ML : DTLS

- Operations considerations section saying that DTLS might impact performance
  - Necessary?

# Draft-ietf-netconf-udp-notif-08

## Proposed changes for next iteration

- What to do with messages with unordered options?
  - Suggested text: “Messages with unordered options MAY be dropped”
- Example for configuration
- Example for a message notification
- Message-id unicity text (feedback from dev)
  - “A publisher MUST use different Message-ID values for different messages generated with the same Observation-Domain-ID.”
  - Email sent to the ML
- Ready for SECDIR review

# YANG push gap on notification message model definition

```
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2022-09-02T10:59:55.32Z</eventTime>
  <push-update xmlns="urn:ietf:params:xml:ns:yang:ietf-yang-push">
    <id>101</id>
    <datastore-contents>
      <interfaces xmlns="urn:ietf:params:xml:ns:yang:ietf-interfaces">
        <interface>
          <name>eth0</name>
          <oper-status>up</oper-status>
        </interface>
      </interfaces>
    </datastore-contents>
  </push-update>
</notification>
```

RFC 5277 - Netconf Event Notifications

RFC 8641 - YANG Push

RFC 7951 - YANG JSON

RFC 9254 - YANG CBOR

```
{
  "ietf-notification:notification": {
    "eventTime": "2017-10-25T08:00:11.22Z",
    "ietf-yang-push:push-update": {
      "id": 1011,
      "datastore-contents": {
        "ietf-interfaces:interfaces": [
          "interface": {
            "name": "eth0",
            "oper-status": "up"
          }
        ]
      }
    }
  }
}
```

No YANG module for “ietf-notification”  
New draft for IETF116



# **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

# Draft-ietf-netconf-distributed-notif-04

- No updates on this draft
- To be last called when UDP-notif draft is last called

Thanks !