DOTS signal channel

draft-reddy-dots-signal-channel-02

Nov 2016

IETF 97

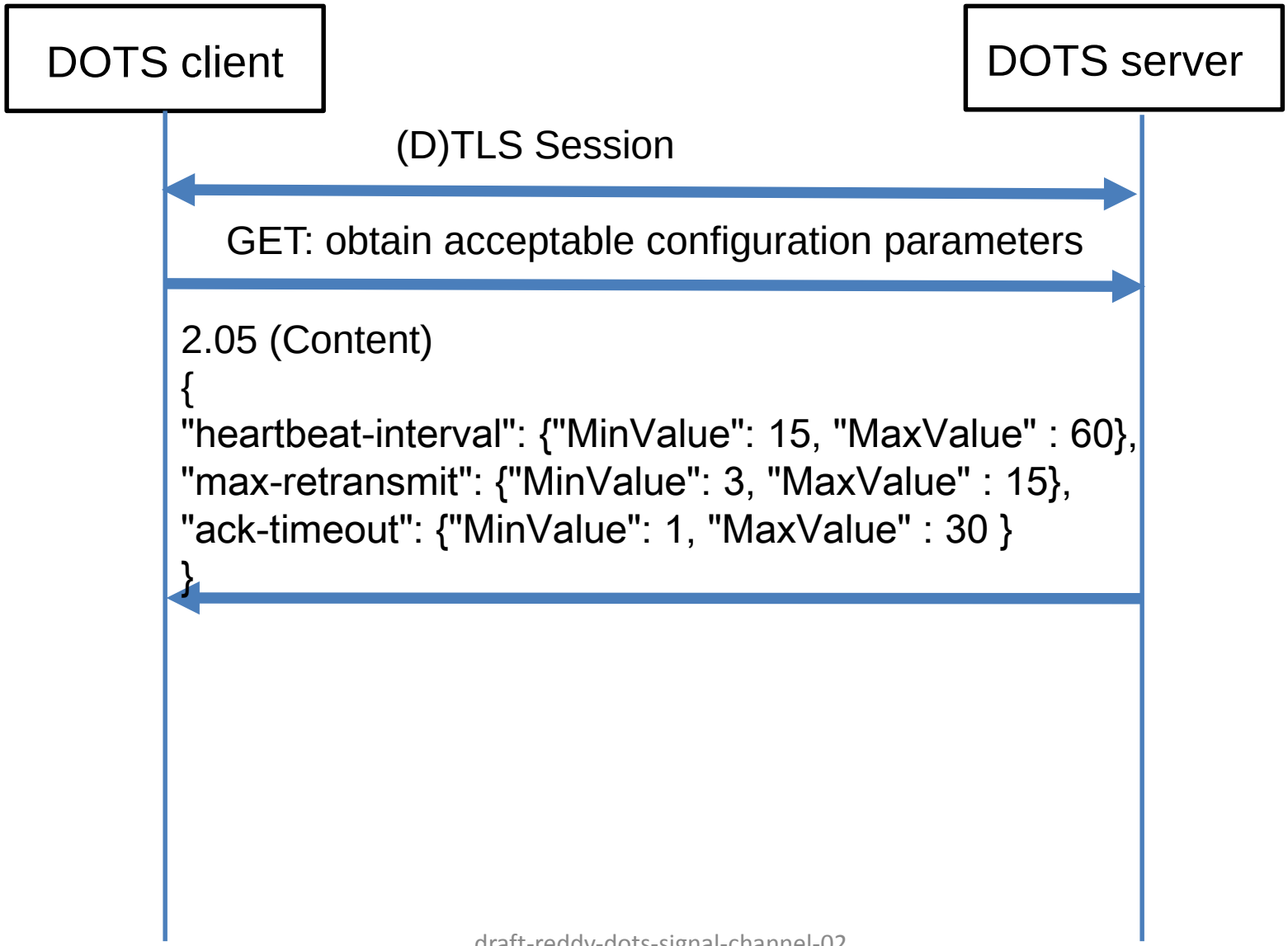
Authors: T. Reddy, D. Wing, P. Patil, M. Boucadair

Presenter : Flemming Andreasen

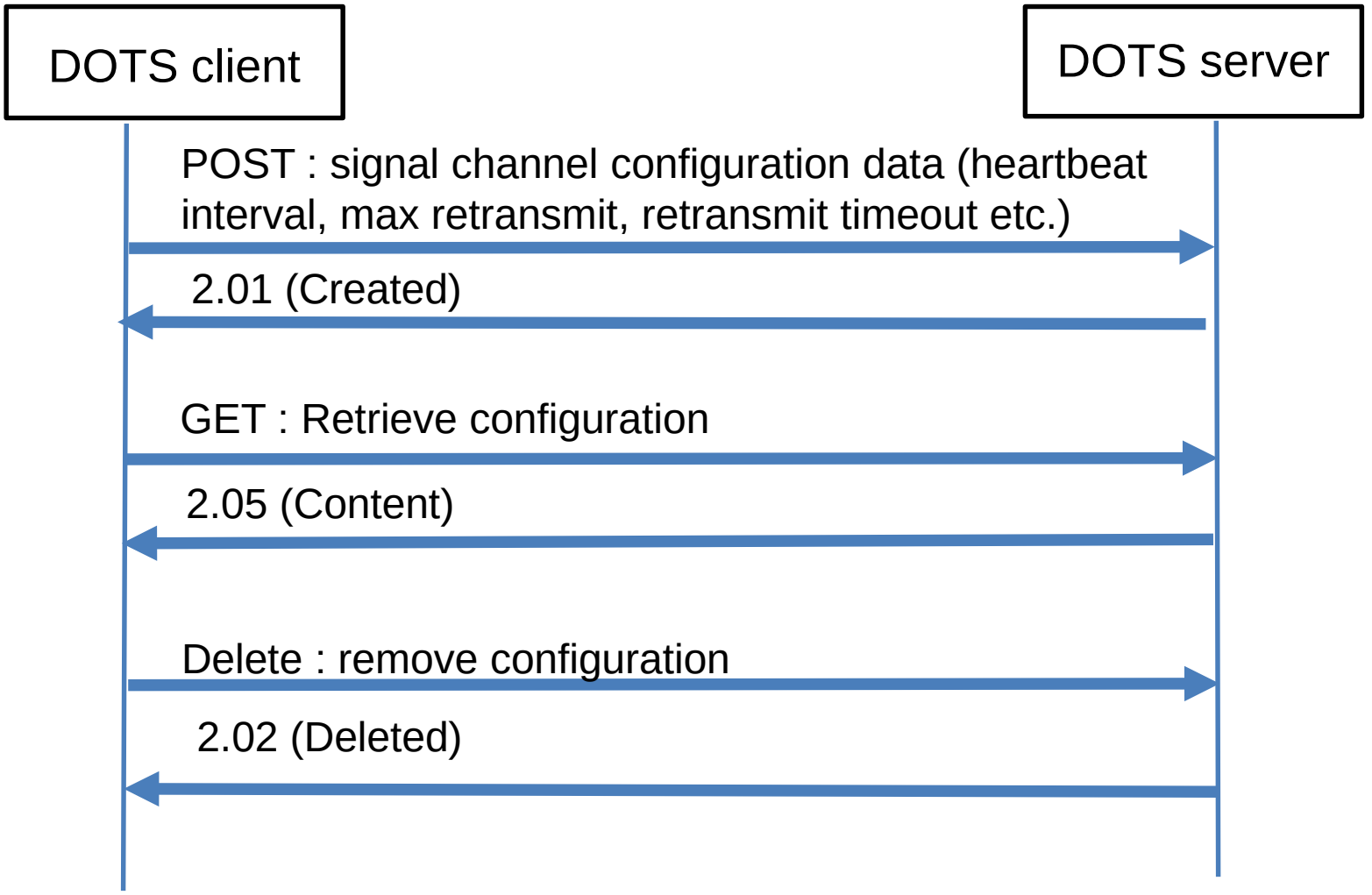
Agenda

- DOTS signal channel session configuration
  - Discover
  - Configure/Retrieve/Delete
- Redirected signaling
- Proof of concept
- (D)TLS 1.3

Discover acceptable configuration parameters



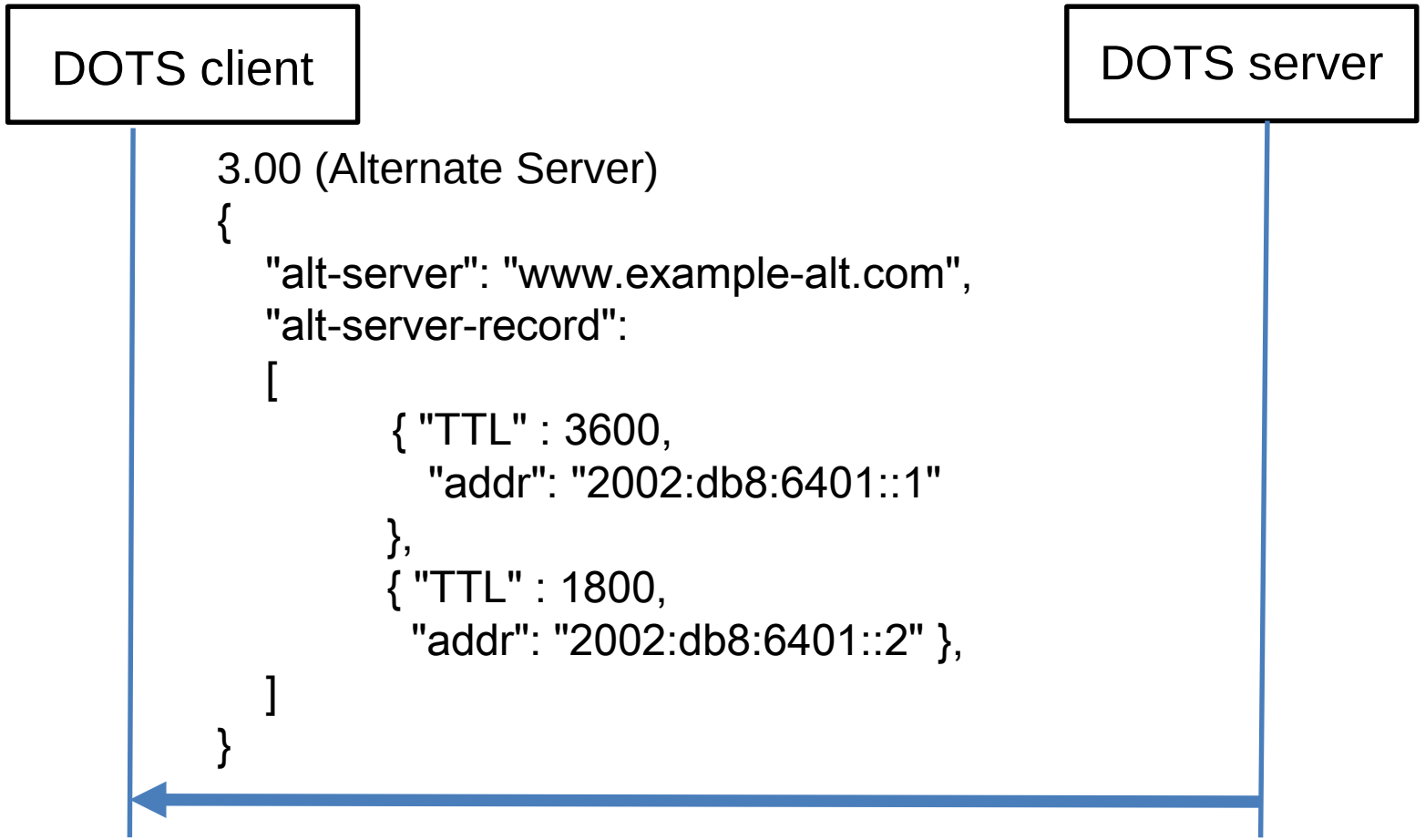
DOTS signal channel session configuration



DOTS signal channel session configuration

- If range not acceptable then DOTS server returns 422 (Unprocessable Entity) error response code.
- In the error response body conveys the minimum and maximum attribute values acceptable by the DOTS server.

Redirected signaling



Proof of concept

- Used californium framework (https://eclipse.org/californium/) to exchange DOTS messages using COAP over DTLS.
- Mozilla (with copper plugin ttps://addons.mozilla.org/en-US/firefox/addon/copper-270430/) to exchange DOTS messages to a test DOTS server.

Proof of concept

```
> Frame 225: 152 bytes on wire (1216 bits), 152 bytes captured (1216 bits) on interface 0
> Ethernet II, Src: IntelCor_64:78:c3 (44:85:00:64:78:c3), Dst: CiscoInc_9f:f0:03 (00:00:0c:9f:f0:03)
> Internet Protocol Version 4, Src: 10.142.109.78, Dst: 134.102.218.18
> User Datagram Protocol, Src Port: 51032, Dst Port: 5683
v Constrained Application Protocol, Confirmable, POST, MID:33751
    01.. .... = Version: 1
    ..00 .... = Type: Confirmable (0)
    .... 0011 = Token Length: 3
    Code: POST (2)
    Message ID: 33751
    Token: 3d6fce
  > Opt Name: #1: Uri-Host: www.example.com
  > Opt Name: #2: Uri-Path: .well-known
  > Opt Name: #3: Uri-Path: DOTS-signal
  > Opt Name: #4: Uri-Path: v1
  > Opt Name: #5: Content-Format: application/json
    End of options marker: 255
  v Payload: Payload Content-Format: application/json, Length: 56
      Payload Desc: application/json
      JavaScript Object Notation: application/json
    v Line-based text data: application/json
        "policy-id": 1000\n
        "alias": HTTPS server\n
        "lifetime": 3600
```

(D)TLS 1.3

- Reduced number of handshake messages.
- 0-RTT resumption using PSK.

- Recommend TLS 1.3 ?
  - Peace time: TLS handshake to receive PSK.
  - Attack time: If no response from server or session terminated then use 0-RTT resumption using PSK.

draft-reddy-dots-signal-channel-02

- Comments and questions.