Co-operative DDoS Mitigation

draft-reddy-dots-transport-05
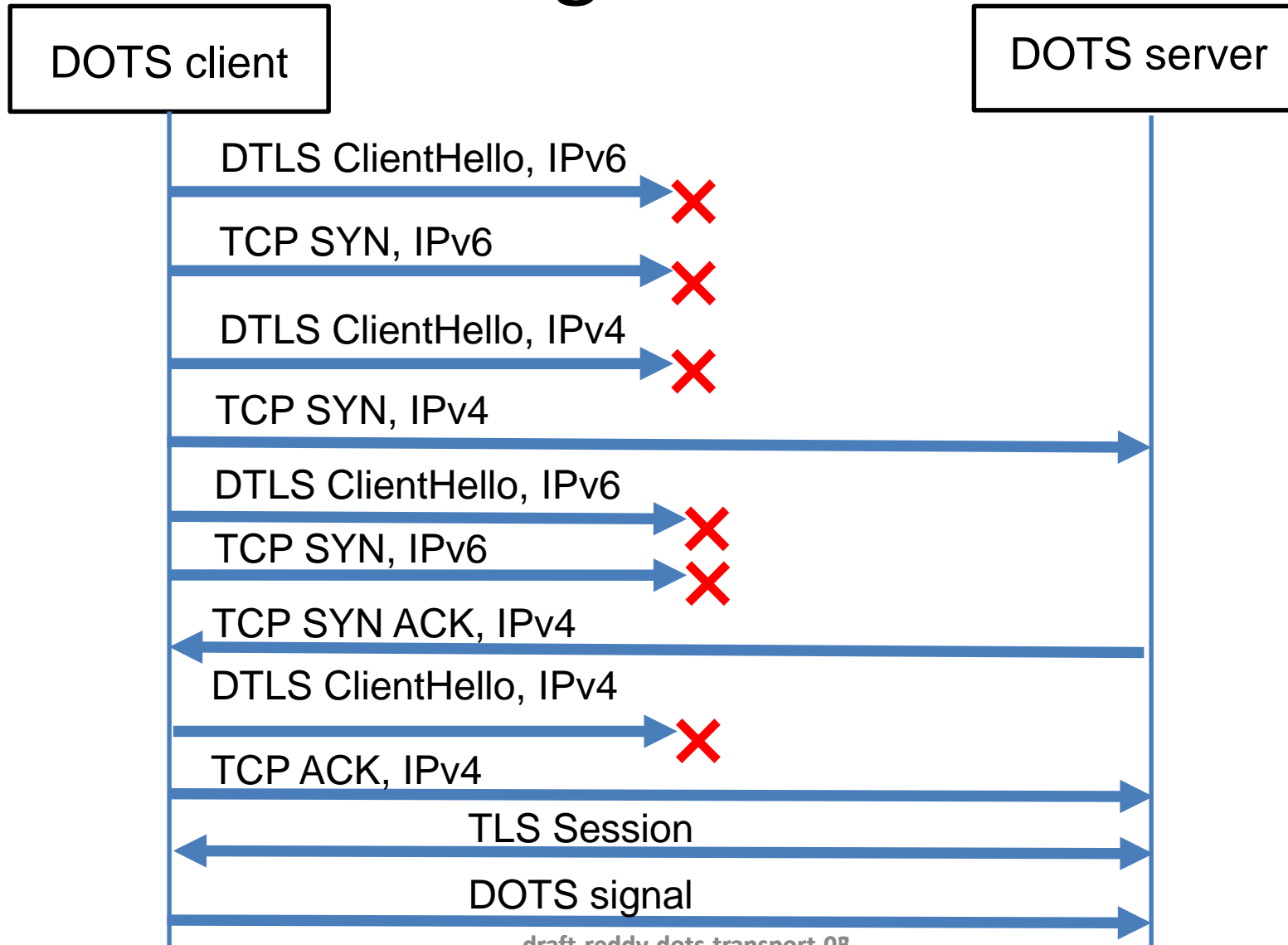
July 2016

IETF 96

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

Presenter : Tirumaleswar Reddy

Changes to draft

- Meets most of the requirements in draft-ietf-dots-requirements-02
    - Happy Eyeballs-like technique for DOTS Signal Channel (v6/v4, UDP/TCP)
    - CoAP for lightweight communication
        - DOTS Signal Channel, UDP/TCP
        - DOTS Data Channel, TCP
    - Mutual Authentication of DOTS Agents & Authorization of DOTS Clients
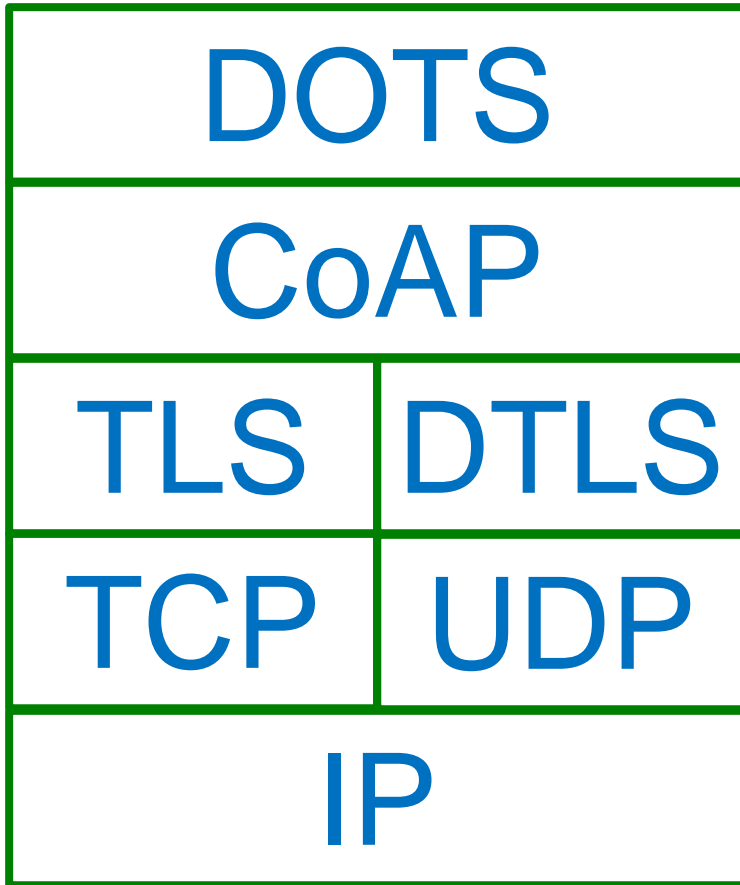   - (D)TLS protocol profile and Performance Considerations

Happy Eyeballs-like technique for DOTS Signal Channel

DOTS client

DOTS server

DTLS ClientHello, IPv6 ✗

TCP SYN, IPv6 ✗

DTLS ClientHello, IPv4 ✗

TCP SYN, IPv4

DTLS ClientHello, IPv6 ✗

TCP SYN, IPv6 ✗

TCP SYN ACK, IPv4

DTLS ClientHello, IPv4 ✗

TCP ACK, IPv4

TLS Session

DOTS signal
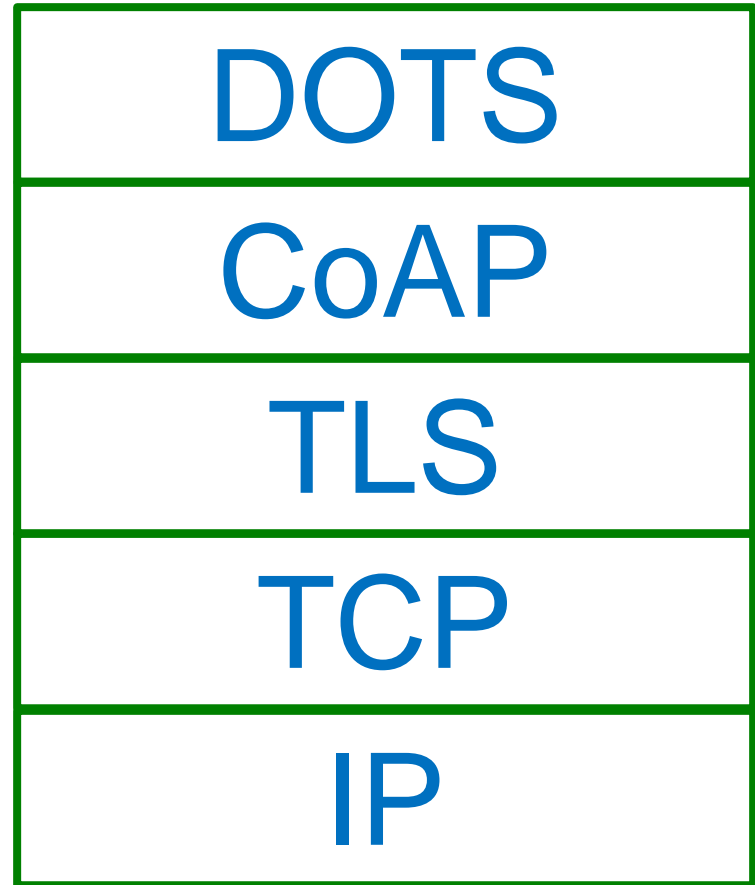
draft-reddy-dots-transport-03

3

Happy Eyeballs for DOTS Signal Channel

- Order of preference (aligns with RFC6724)
  - IPv6 over DTLS over UDP
  - IPv6 over TLS over TCP
  - IPv4 over DTLS over UDP
  - IPv4 over TLS over TCP
- DNS lookup during peacetime.
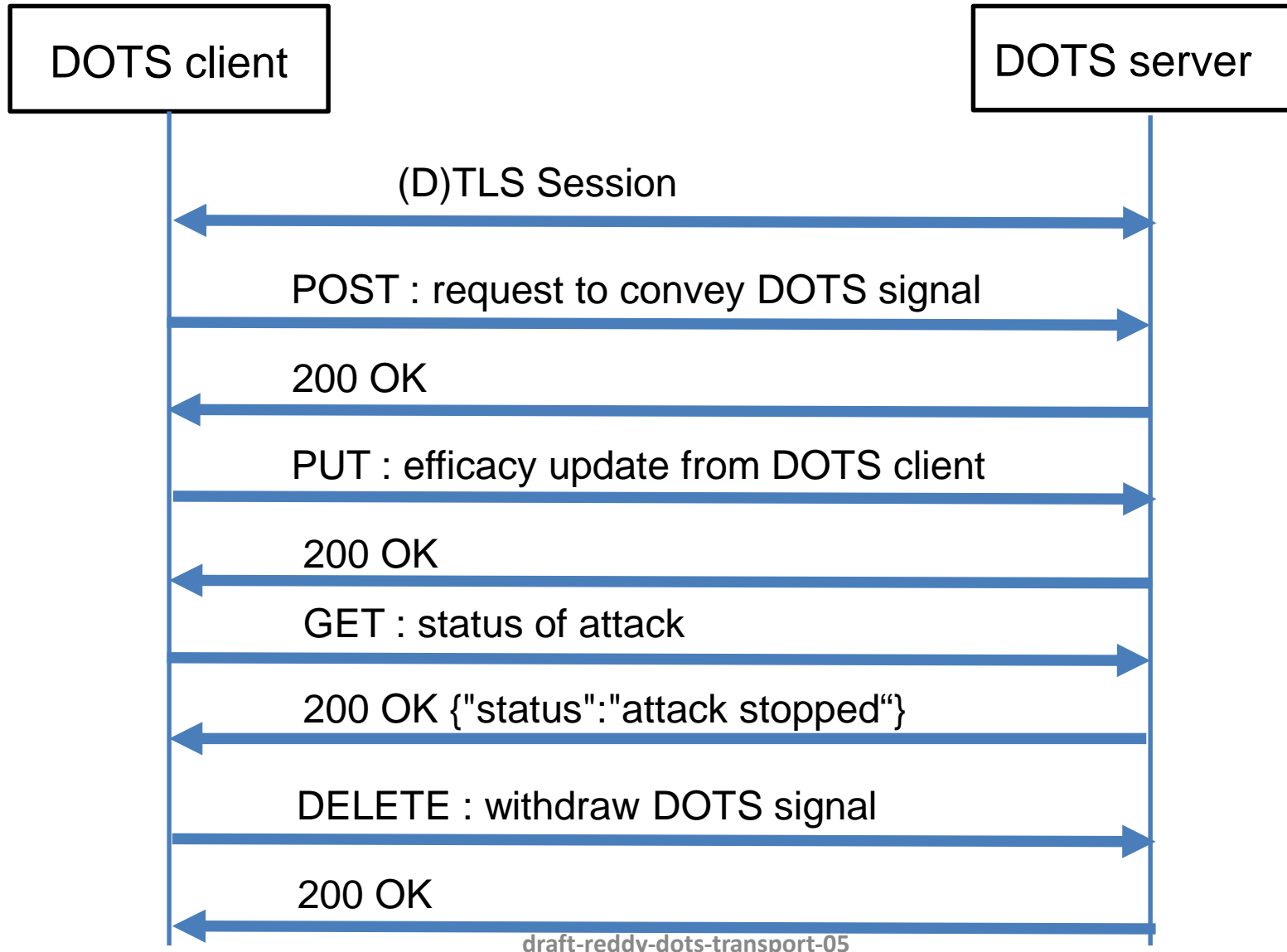
DOTS signal and data channel

DOTS
CoAP
TLS / DTLS
TCP / UDP
IP

DOTS signal channel

DOTS
CoAP
TLS
TCP
IP

DOTS data channel

DOTS signal channel

DOTS client   DOTS server

(D)TLS Session

POST : request to convey DOTS signal

200 OK

PUT : efficacy update from DOTS client

200 OK

GET : status of attack

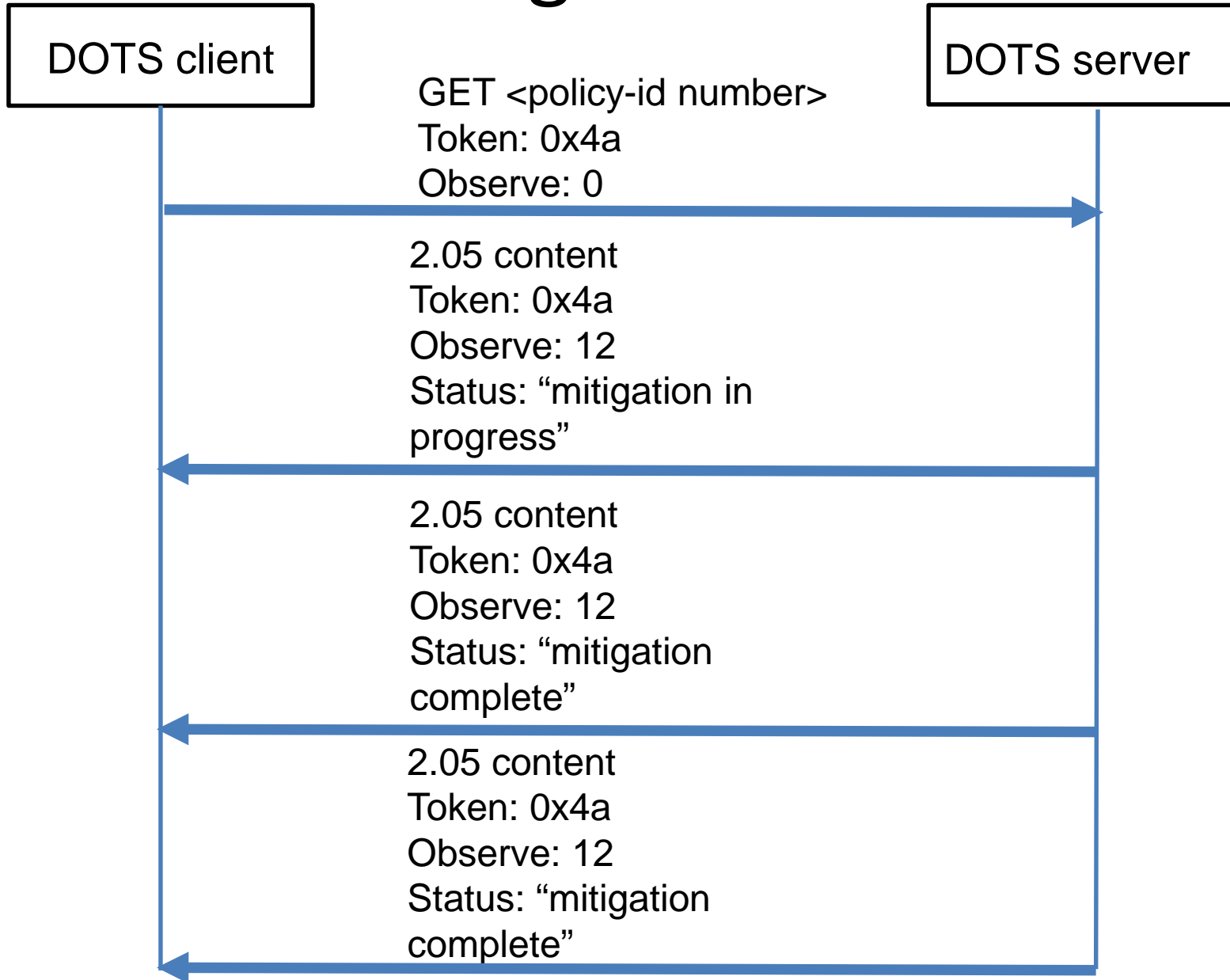200 OK {"status":"attack stopped"}

DELETE : withdraw DOTS signal

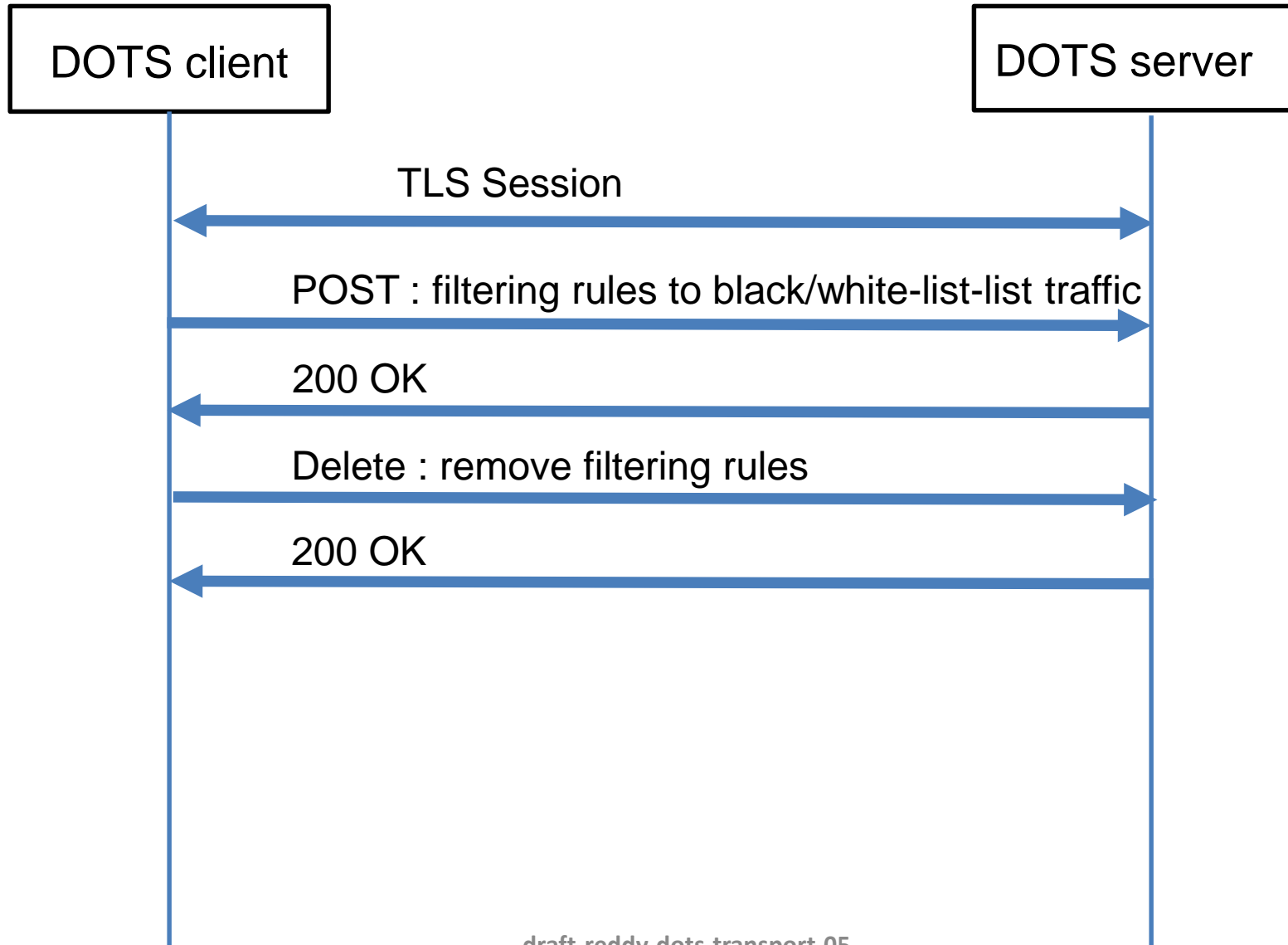200 OK

6

DOTS signal channel

- POST, DELETE, GET, and PUT requests are marked as COAP confirmable messages.

- Asynchronous message exchanges for DDOS mitigation status.

DOTS signal channel

DOTS client

DOTS server

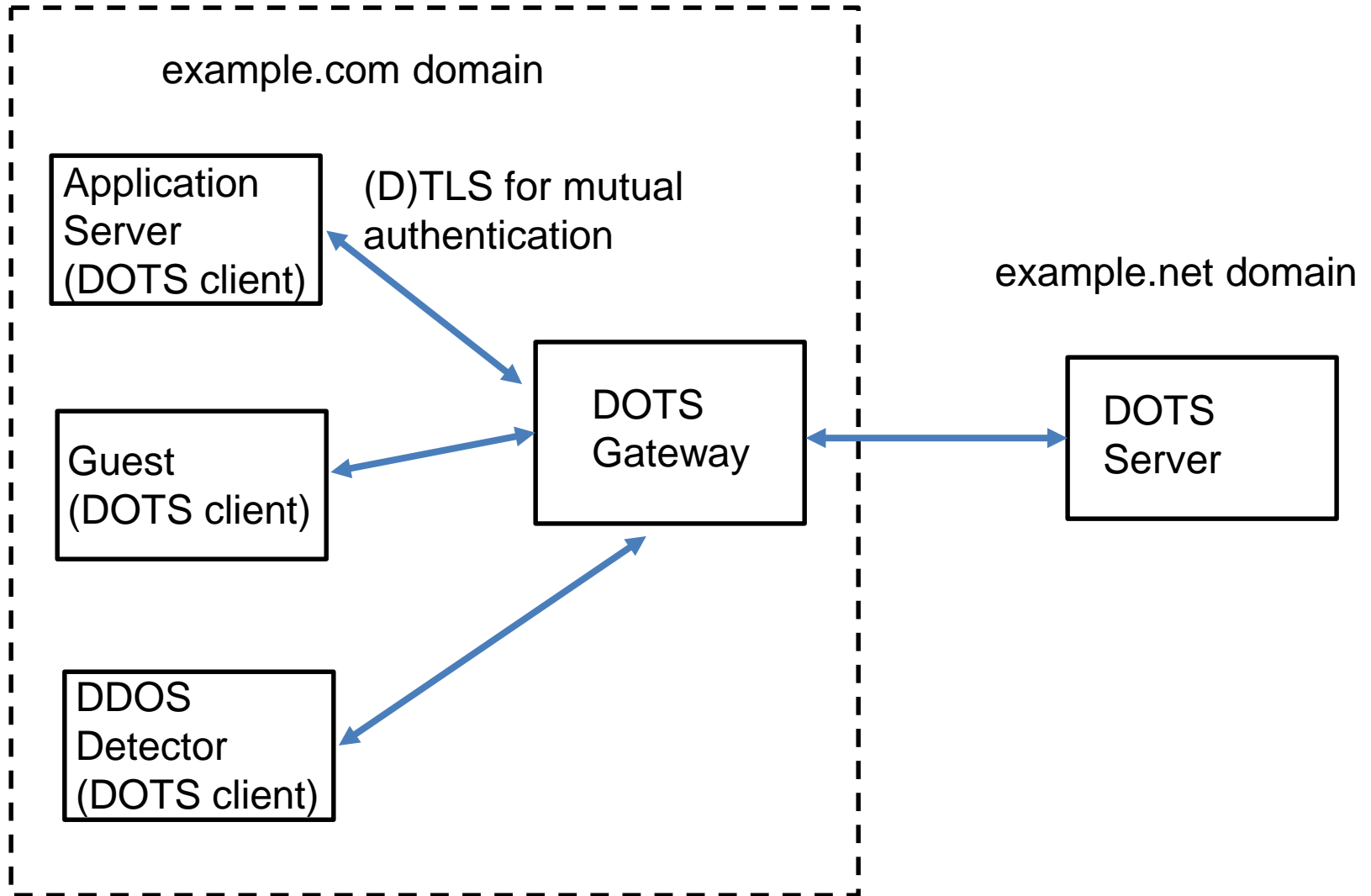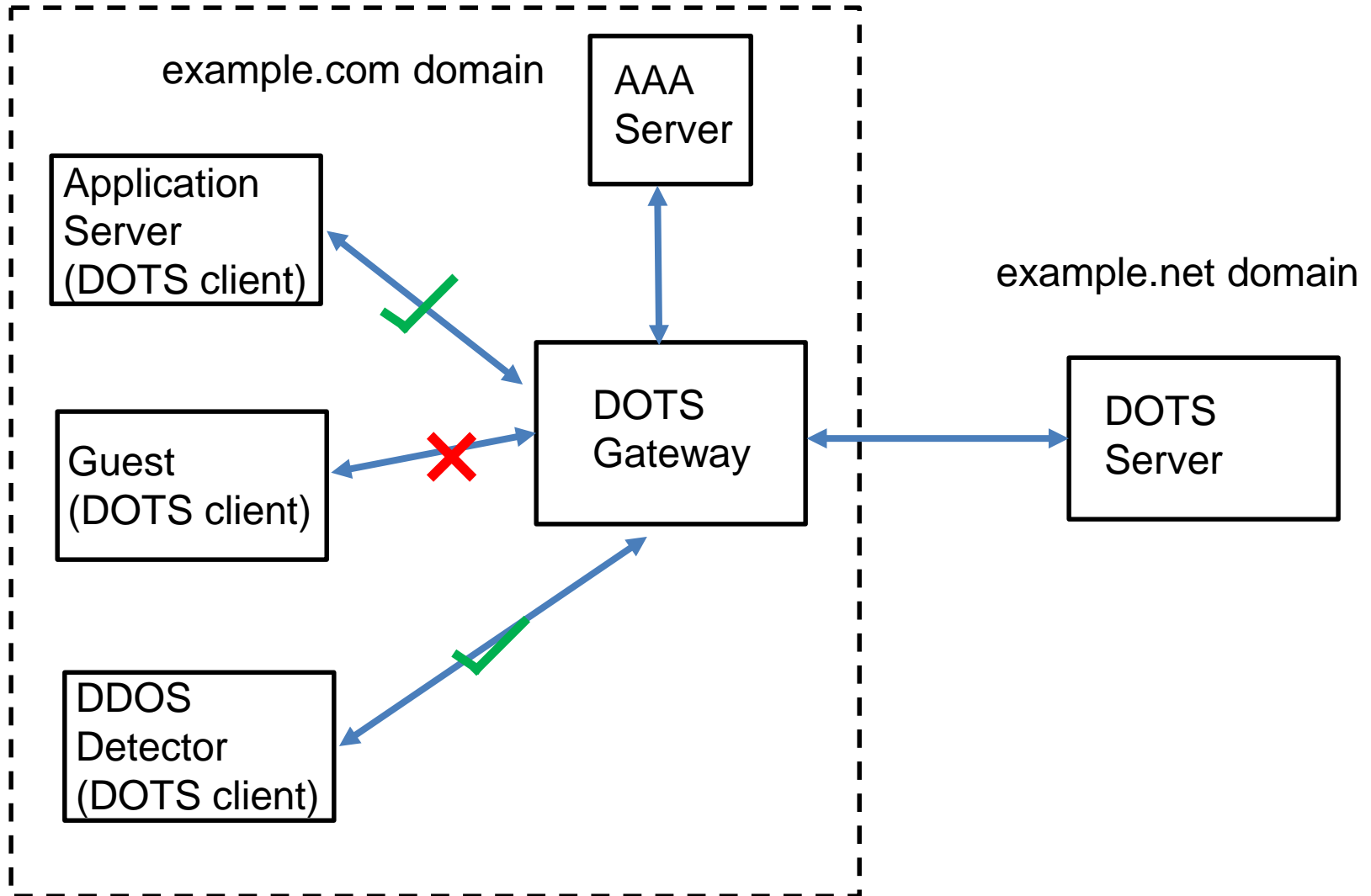GET <policy-id number>
Token: 0x4a
Observe: 0

2.05 content
Token: 0x4a
Observe: 12
Status: "mitigation in progress"

2.05 content
Token: 0x4a
Observe: 12
Status: "mitigation complete"

2.05 content
Token: 0x4a
Observe: 12
Status: "mitigation complete"

DOTS data channel

DOTS client

DOTS server

TLS Session

POST : filtering rules to black/white-list-list traffic

200 OK

Delete : remove filtering rules

200 OK

Mutual Authentication of DOTS agents

example.com domain

Application Server (DOTS client)

(D)TLS for mutual authentication

example.net domain

Guest (DOTS client)

DOTS Gateway

DOTS Server

DDOS Detector (DOTS client)

Authorization of DOTS client

(D)TLS profile

- (D)TLS session resumption without server-side state [RFC5077].

- Raw public keys [RFC7250].

- (D)TLS Heartbeat.

Performance considerations

- TLS False Start [I-D.ietf-tls-falsestart].
- Cached Information Extension [I-D.ietf-tls-cached-info].
- TCP FastOpen [RFC7413].

draft-reddy-dots-transport-05

- Comments and questions
- Consider adoption of this document as WG item.