DDoS Open Threat Signaling (DOTS)

https://datatracker.ietf.org/wg/dots/

T. Reddy & M. Boucadair

July 2020

Overall Context

- DDoS attacks are increasing
  - Enterprises, Content providers and ISPs are among top targets
- Attack are larger (volume) and complex
- Generalized because of the advent of "DDoS as a Service" offerings
  - Bots are ready to serve you

Overall Context

- DDoS attacks exacerbated with the massive deployment of vulnerable IoT devices
  - Many recent attacks rely on these devices

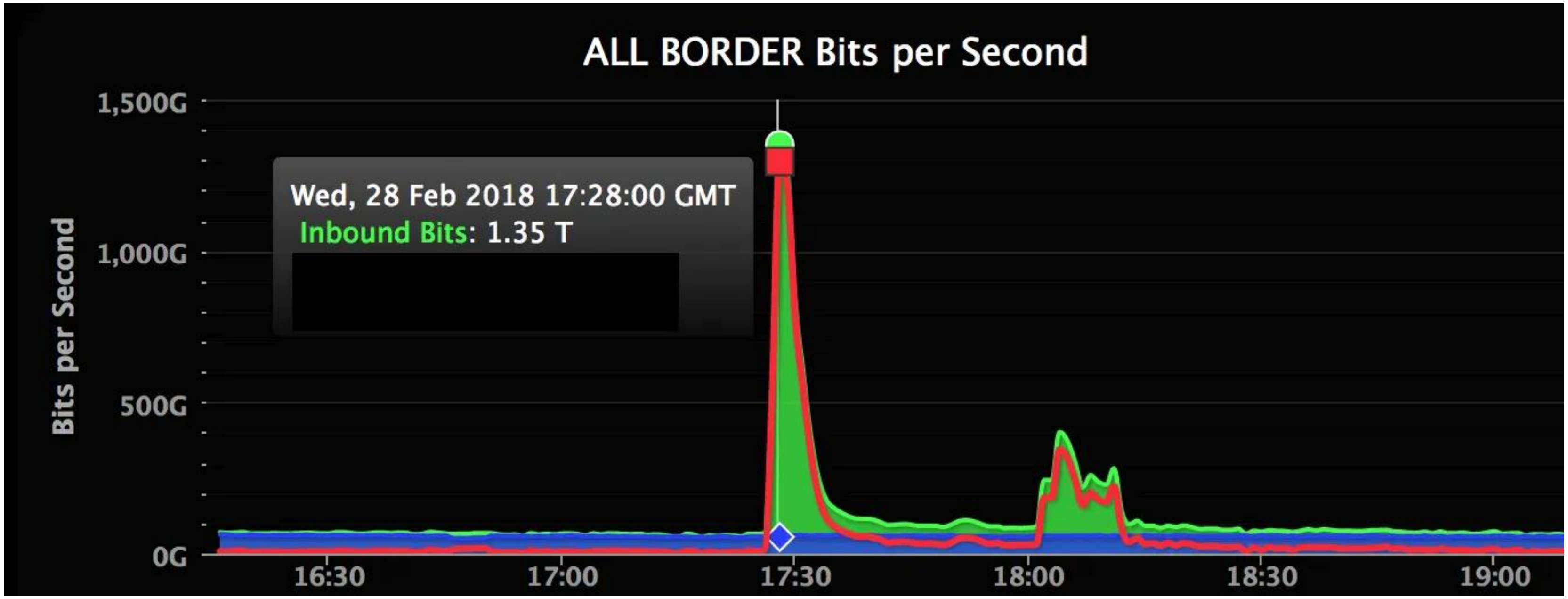
> *“OVH CTO Octave Klaba said the attacks OVH suffered were “close to 1 Tbps” and noted that the flood of traffic was a botnet made up of nearly 150,000 digital video recorders and IP cameras capable of sending 1.5 Tbps in DDoS traffic.”*

- Attack sources (owners) are not aware that they are participating in attacks
  - Impacts on the reputation of networks hosting these devices

Types of DDoS

- Amplification attacks (DNS)
- SYN flood
- Garbage data after TLS handshake
- Re-negotiating the cryptographic parameters
- Partial requests (Slowloris).

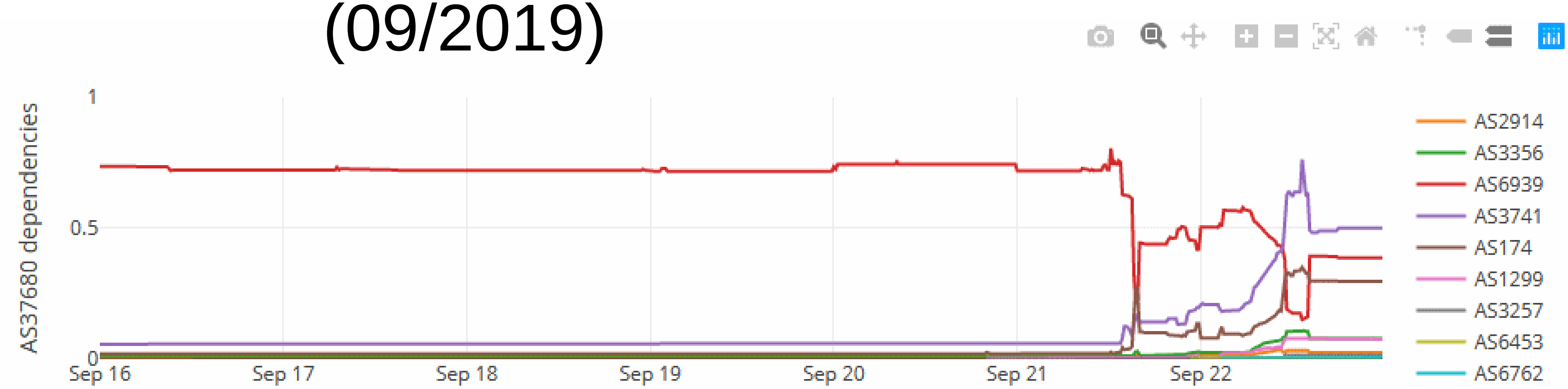
Automate DDoS Signaling: Case 1



“Making GitHub’s edge infrastructure more resilient to current and future conditions of the internet and less dependent upon human involvement requires better automated intervention. ***<u>We’re investigating the use of our monitoring infrastructure to automate enabling DDoS mitigation providers</u>*** *and will continue to measure our response times to incidents like this with a goal of reducing mean time to recovery (MTTR).”*

Automate DDoS Signaling:
Case 2

- An ISP was down for almost one day (09/2019)



"Preston also said that, nowadays, most ISPs have the tools to mitigate such attacks. **For example, *they can deploy the DOTS protocol on DDoS mitigation platforms and work together to sinkhole bad traffic*** *aimed at one of the participating members long before it reaches the target's network*".

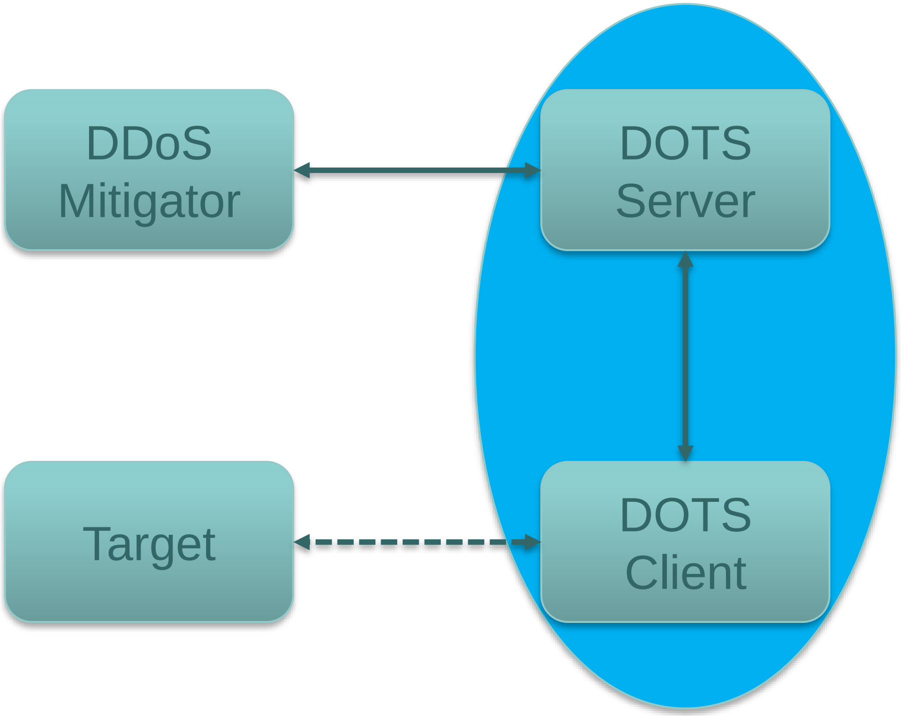
Lack of Interoperability

- No vendor-agnostic signaling
  - The existing protocols are **proprietary** and the only way to get things to work is to fall back to exporting flows
  - Vendor lock-in.
  - There are other methods used, e.g., Syslog export… but this is a hack
    - The signaling be resilient under extremely hostile network conditions

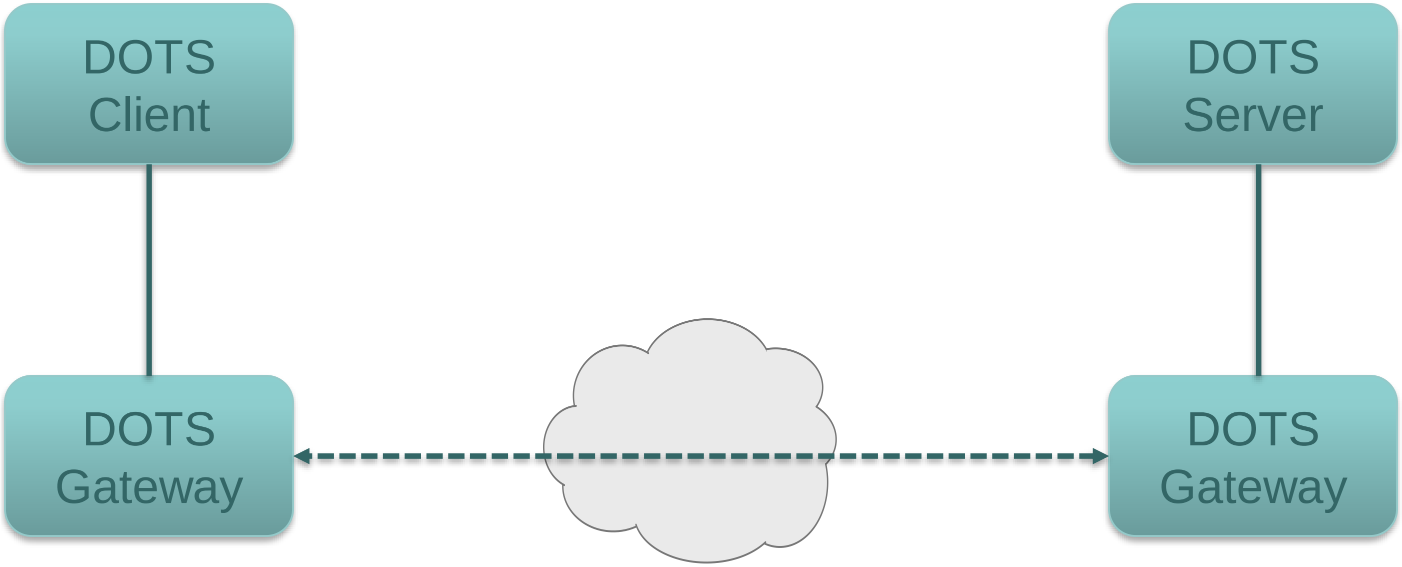
What is DOTS?

- DDoS Open Threat Signaling https://datatracker.ietf.org/wg/dots/about/
- A standards-based approach for the real-time signaling of DDoS related telemetry and threat handling requests and data between elements concerned with DDoS attack detection, classification, traceback, and mitigation/

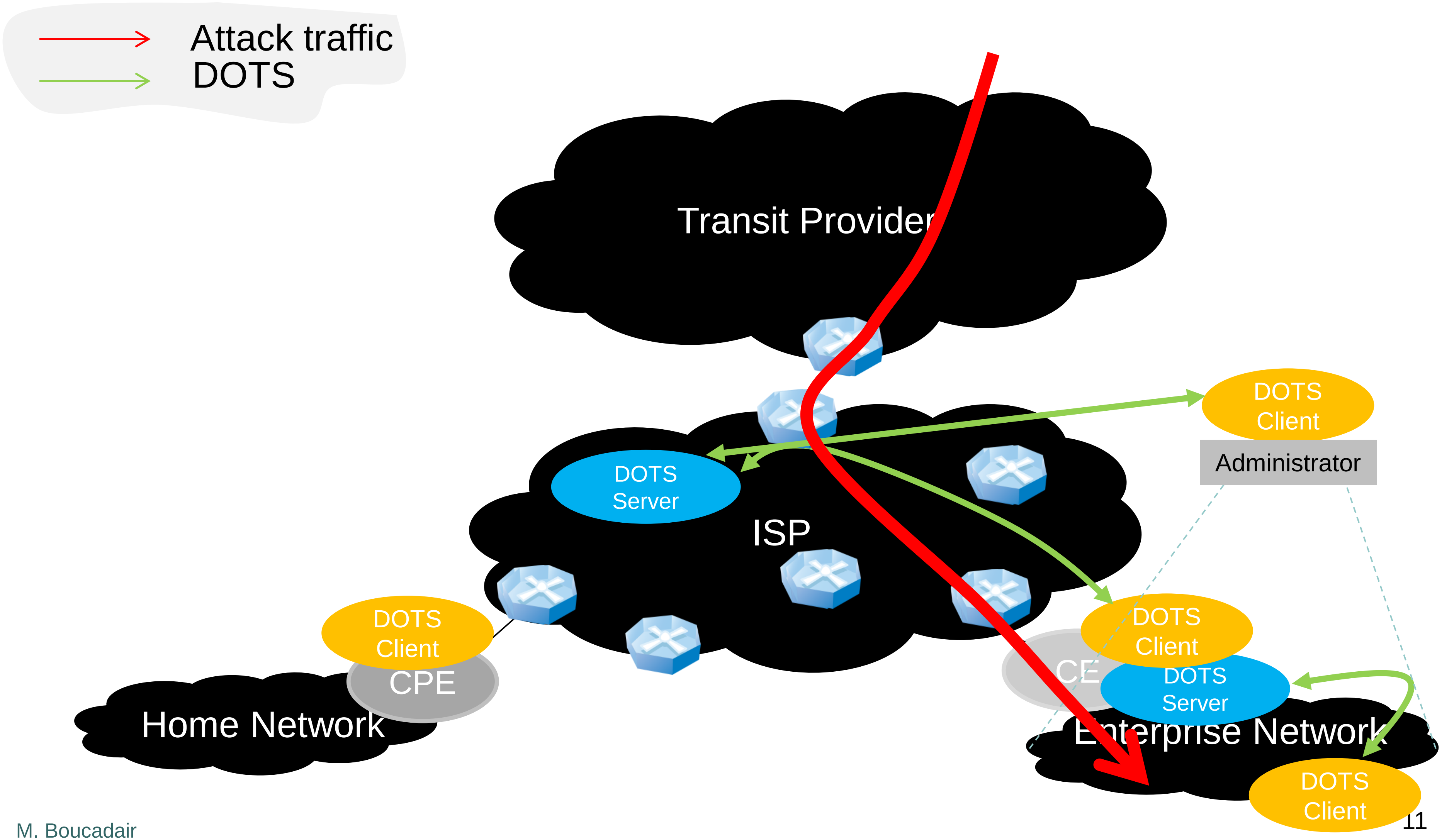
Basic DOTS architecture



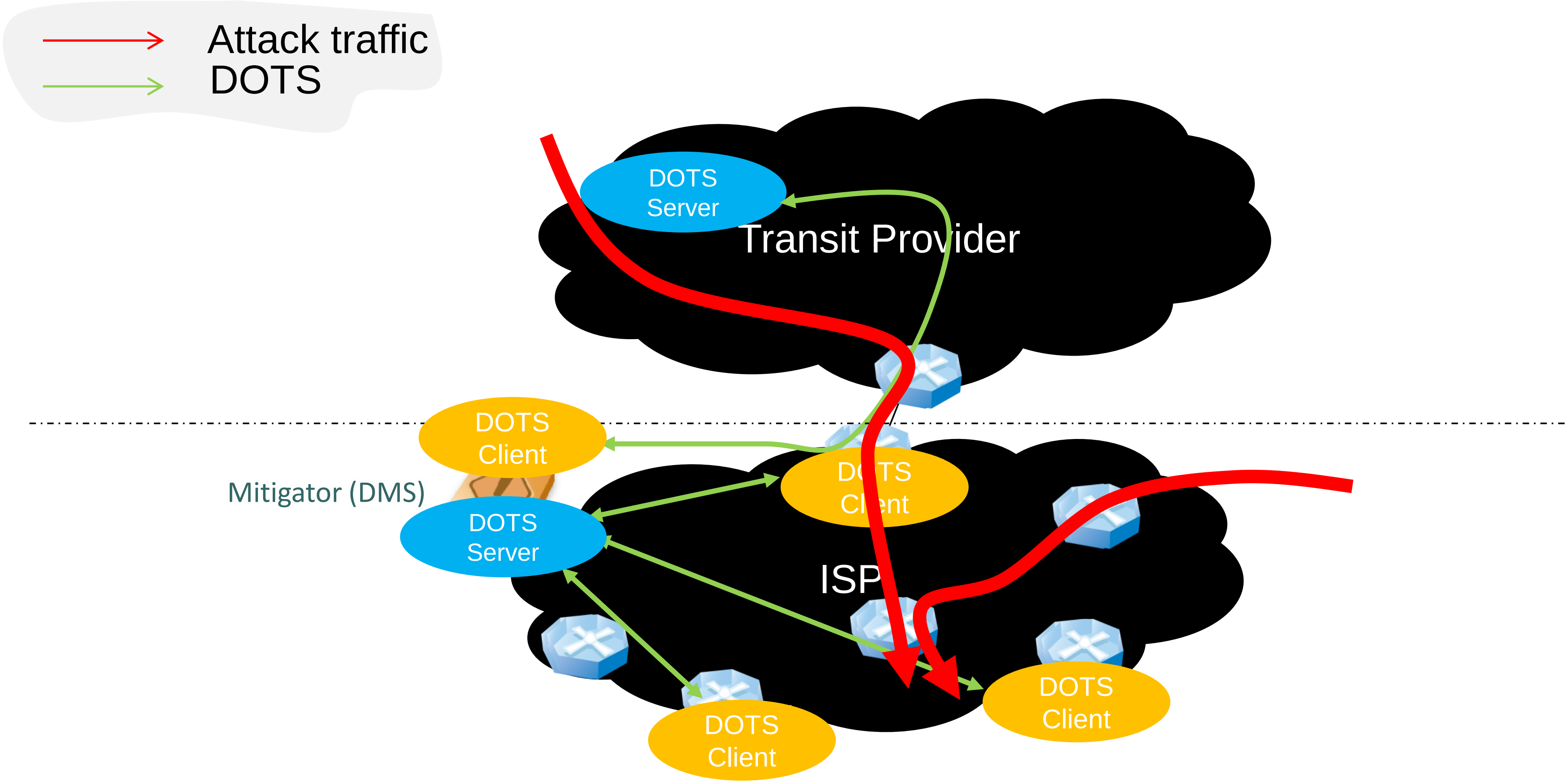
Relayed signaling



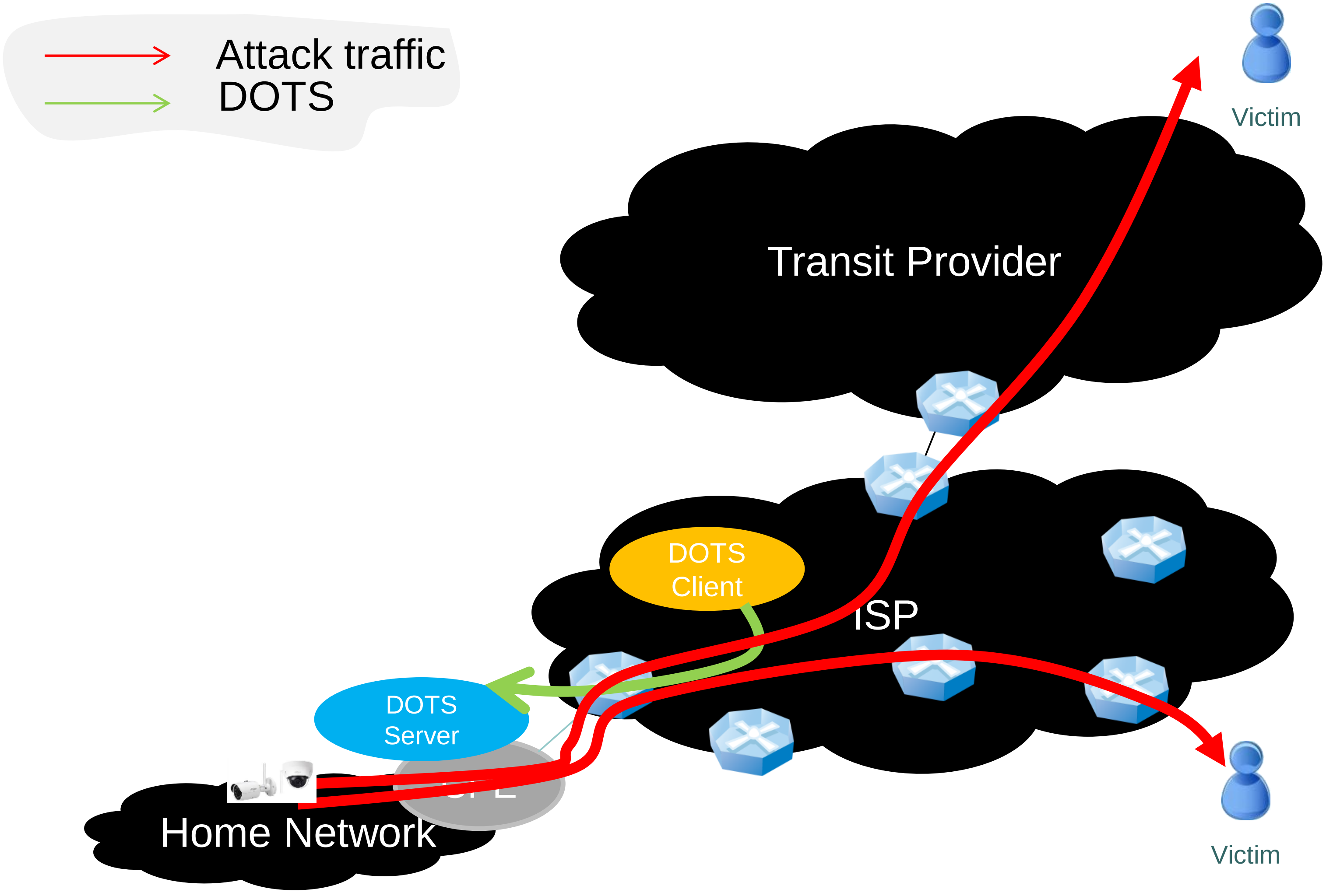
Inbound DDoS



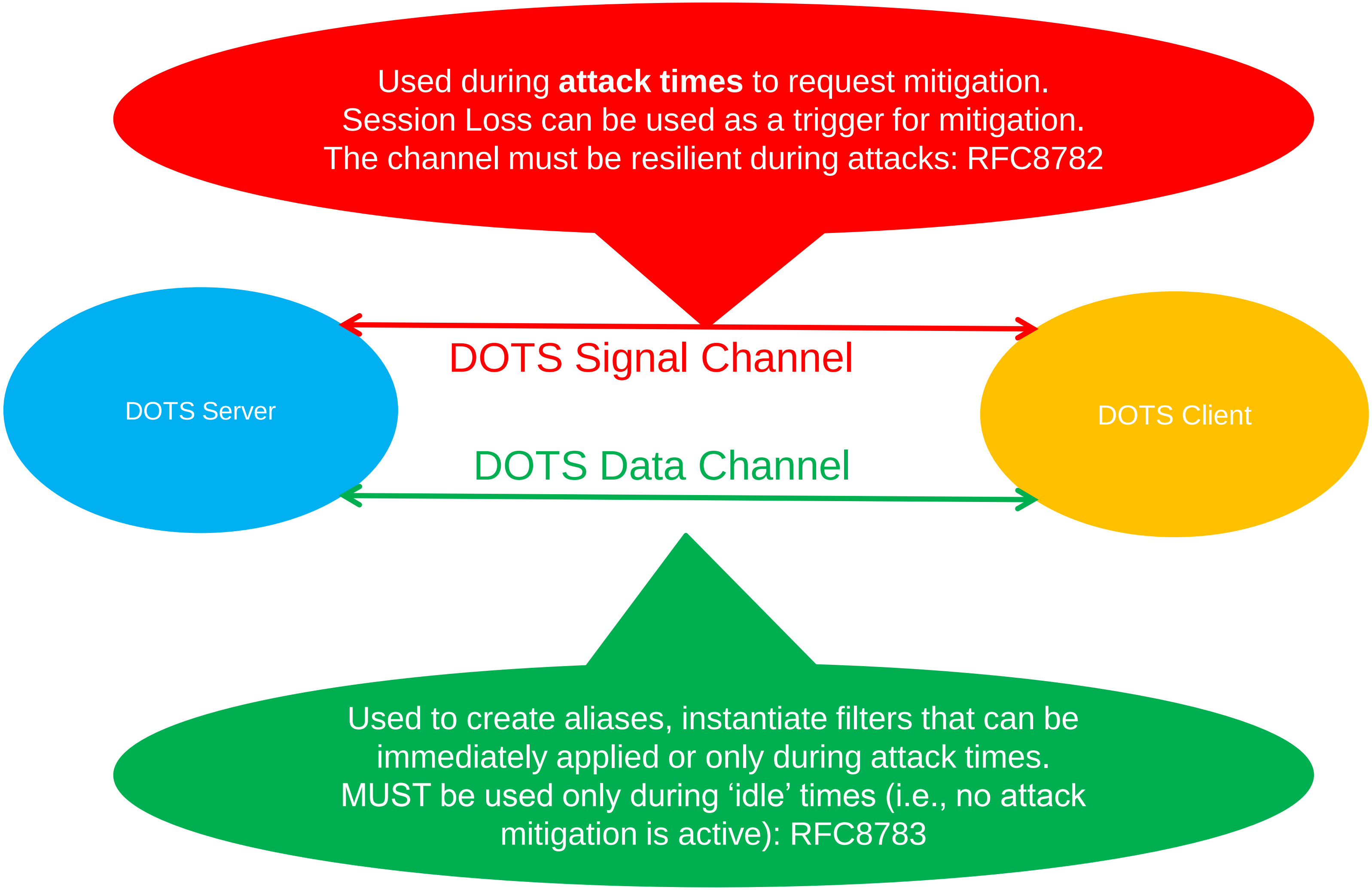
Recursive Mitigation



Filter Close to Sources



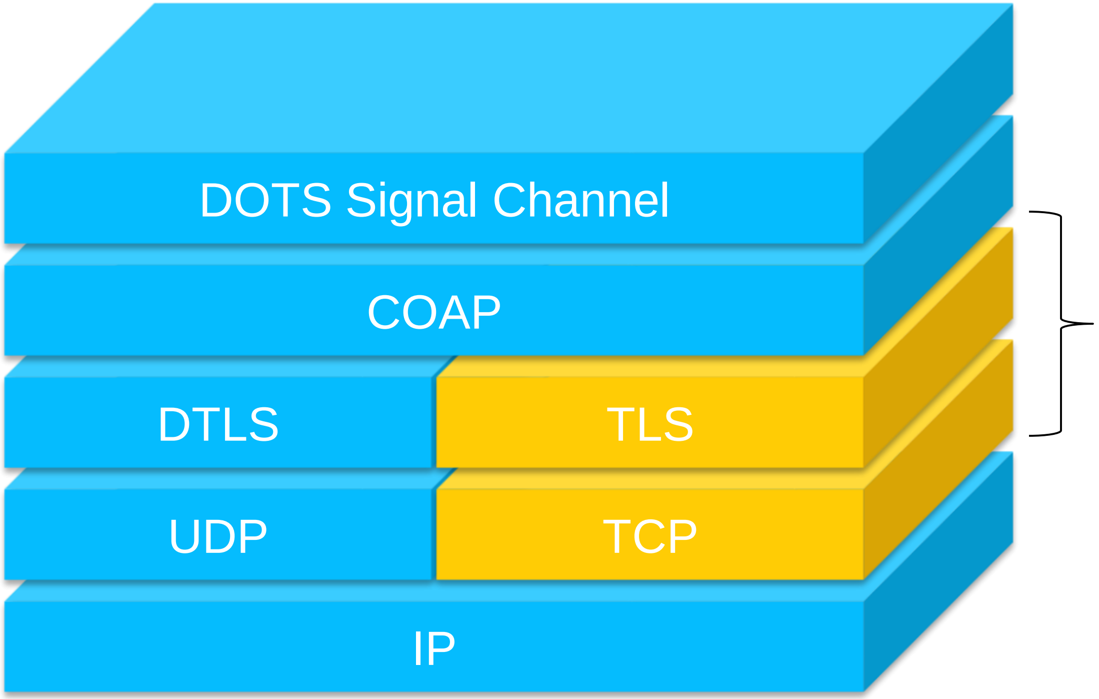
DOTS Channels



Used during **attack times** to request mitigation.
Session Loss can be used as a trigger for mitigation.
The channel must be resilient during attacks: RFC8782

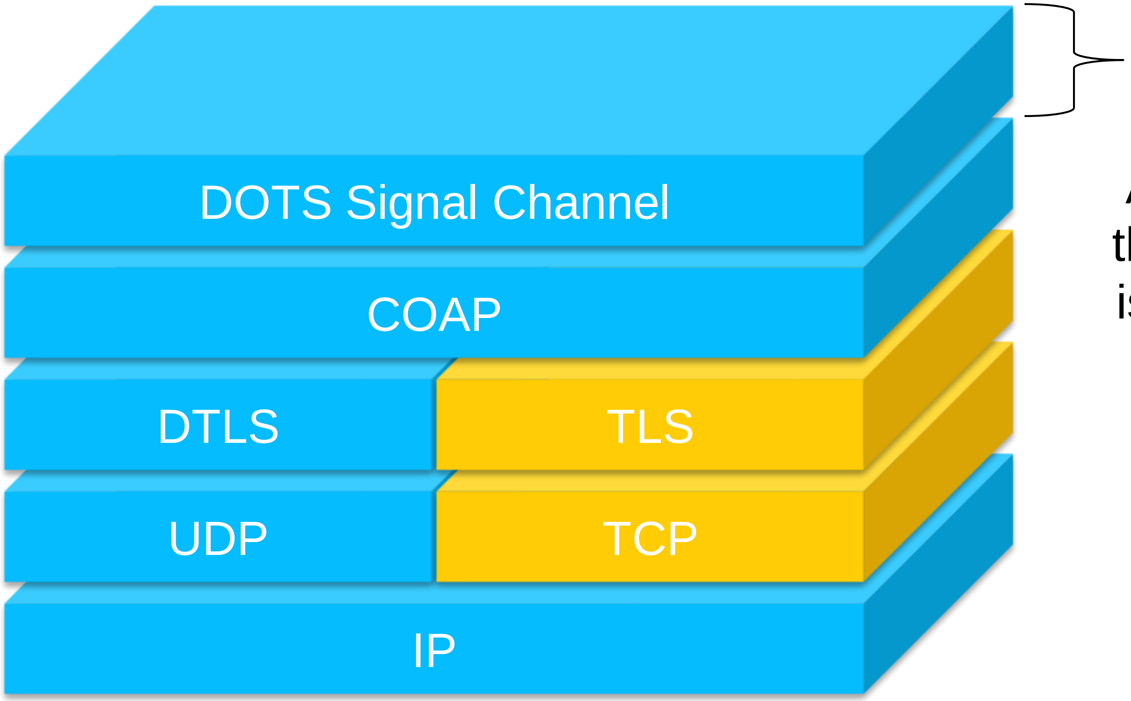
Used to create aliases, instantiate filters that can be immediately applied or only during attack times.
MUST be used only during ‘idle’ times (i.e., no attack mitigation is active): RFC8783

Protocol Stack: Signal Channel



Not Recommended but the protocol covers how to use signal channel in deployments where UDP is blocked

Protocol Stack: Signal Channel

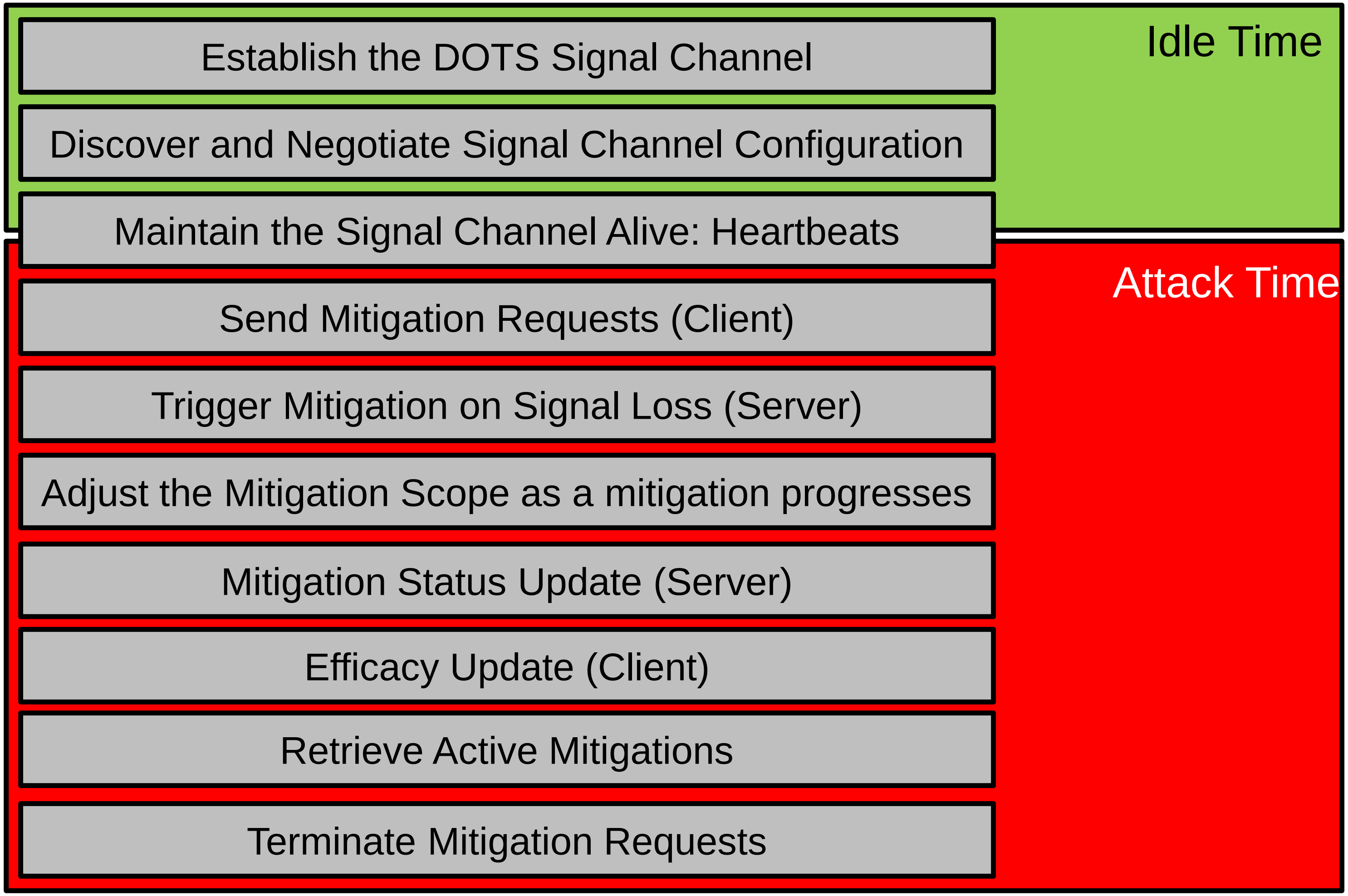


Application Encoding:
CBOR

An application determines that a CBOR data structure is a DOTS object by means of a new Content Type:

"application/dots+cbor"

Typical Signaling Steps



Idle Time

Establish the DOTS Signal Channel

Discover and Negotiate Signal Channel Configuration

Maintain the Signal Channel Alive: Heartbeats

Attack Time

Send Mitigation Requests (Client)

Trigger Mitigation on Signal Loss (Server)

Adjust the Mitigation Scope as a mitigation progresses

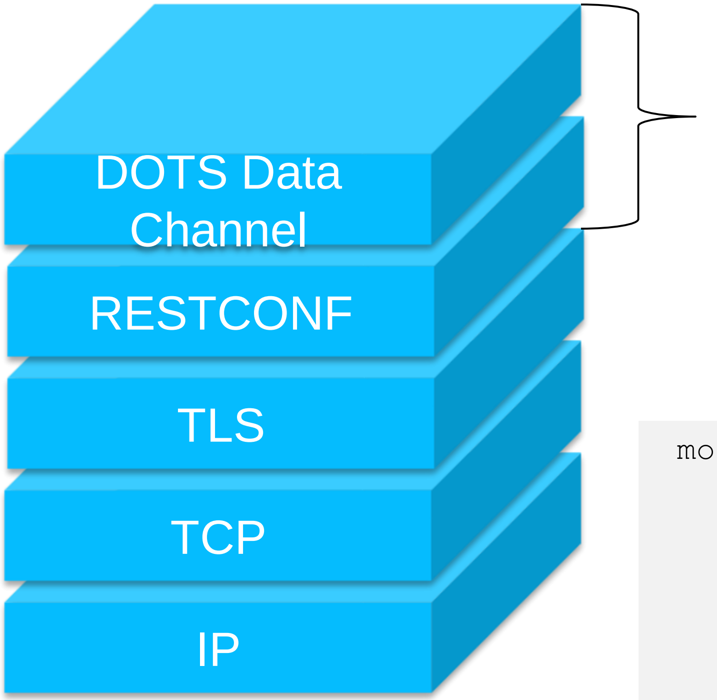
Mitigation Status Update (Server)

Efficacy Update (Client)

Retrieve Active Mitigations

Terminate Mitigation Requests

Protocol Stack: Data Channel

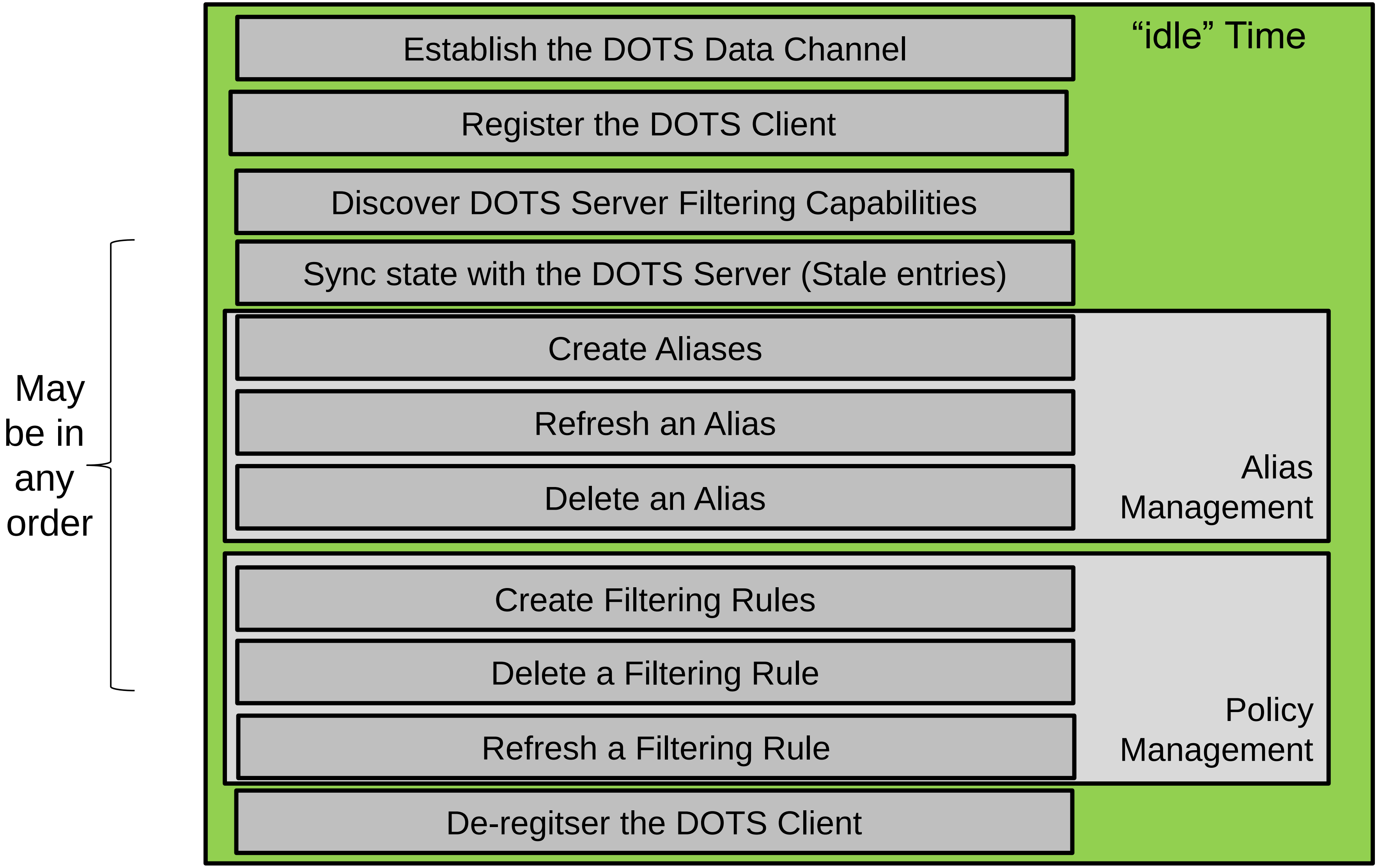


Application Encoding:
JSON

to represent the Data Channel
YANG modelled data

```
module: ietf-dots-data-channel
      +--rw dots-data
         +--rw dots-client* [cuid]
         |  +--rw cuid                  string
         |  +--rw cdid?                 string
         |  +--rw aliases
         |  |     ...
         |  +--rw acls
         |     ...
         +--ro capabilities
            ...
```

Typical Operations



“idle” Time

Establish the DOTS Data Channel

Register the DOTS Client

Discover DOTS Server Filtering Capabilities

Sync state with the DOTS Server (Stale entries)

Create Aliases

Refresh an Alias

Delete an Alias

Alias Management

Create Filtering Rules

Delete a Filtering Rule

Refresh a Filtering Rule

Policy Management

De-regitser the DOTS Client

May be in any order

DOTS Specifications

- Use Cases: draft-ietf-dots-use-cases
- Requirements: RFC 8612
- Architectures
  - DOTS Architecture (draft-ietf-dots-architecture)
  - Multi-homing Deployment Considerations for DOTS (draft-ietf-dots-multihoming)
- Protocol Specifications
  - **DOTS Signal Channel Specification (RFC8782)**
  - **DOTS Data Channel Specification (RFC8783)**
  - **Constrained Application Protocol (CoAP) Hop-Limit Option (RFC8768)**
  - Controlling Filtering Rules Using DOTS Signal Channel (draft-ietf-dots-signal-filter-control)
  - DOTS Signal Channel Call Home (draft-ietf-dots-signal-call-home)
  - DOTS Agent Discovery (draft-ietf-dots-server-discovery)
  - DOTS Telemetry (draft-ietf-dots-telemetry)
- **Open Source:** https://github.com/nttdots/go-dots

Questions?

Tirumaleswar Reddy (kondtir@gmail.com)
Mohamed Boucadair (mohamed.boucadair@orange.com)