Inter-Domain DOTS Use Cases

draft-nishizuka-dots-inter-domain-usecases-01

Kaname Nishizuka, NTT Communications

Apr. 2016 IETF95@Buenos Aires

Diff from -00 to -01

Revised Points:

1. Aligned with terminology of existing WG draft
2. Added studies about DDoS protection methods
3. Clarified the usecases
   - based on the feedback at the last IETF meeting and discussions given on the ML and direct messages

Categorization of usecases

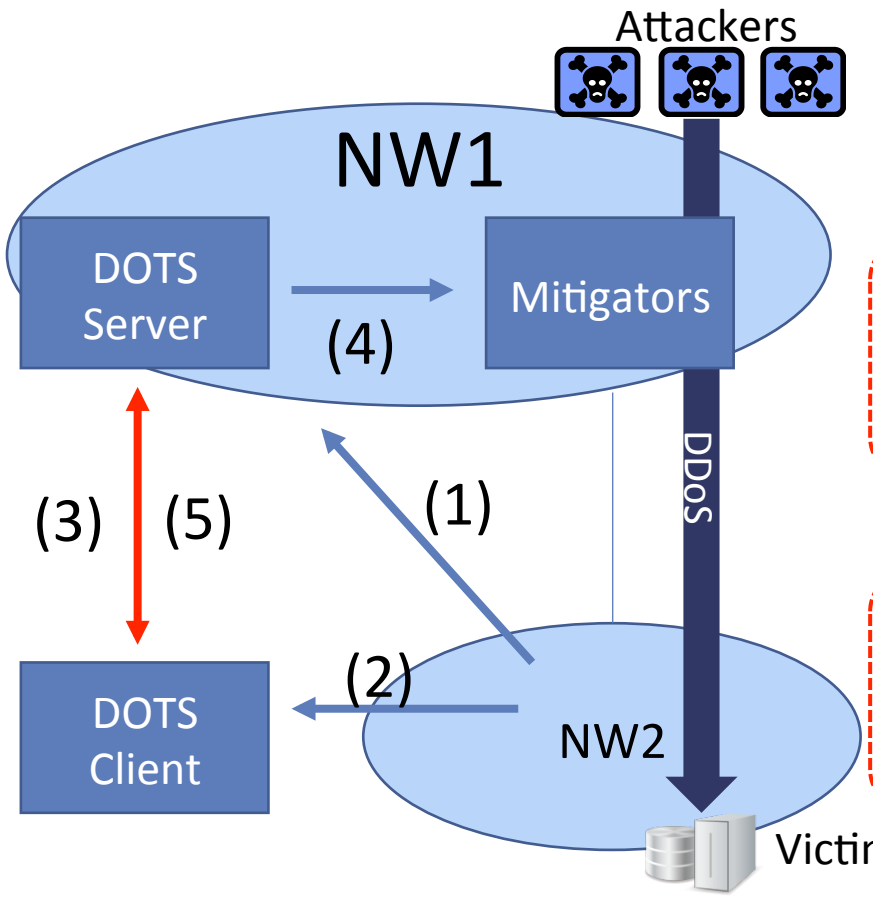
1. intra-domain use cases

- a DOTS client, a DOTS server and mitigators are in the same organization

2. inter-domain use cases

- a DOTS server and mitigators are in a different organization from a DOTS client
  - 2-1. customer-to-provider(c2p)
  - 2-2. provider-to-provider(p2p)

Scenario of Inter-domain usecases



(1)Provisioning of DDoS protection capability(if needed)

(2) Attack Detection

Scope of DOTS

(3) DOTS Signaling

DOTS signaling from a DOTS client to a DOTS server in different organization

(4)DDoS protection by mitigators

(5) Protection Status

Status update from the DOTS server to the DOTS client

Protection methods

- For protection, these information should be provided from a DOTS client to a DOTS server

Protection Method	Mandatory Information	Optional Information
Blackholing	Destination Address	
Selective Blackholing	Destination Address	BGP Community Next-hop Address
RTBH with uRPF	Source Address	
BGP flowspec	Flow Type Action Rule	
Filtering(ACL)	Match Rule Action Rule	
DDoS mitigation Appliances	Destination Address	(Desired)Countermeasures Attack Telemetry
Detouring Technologies	Destination Address Next-Hop	Tunnel Information

Attack telemetry

- a set of summarized traffic information which characterizes the feature of the DDoS attack
- utilized by each protection methods

Mandatory:	Dst IP
Optional:	Attack ID Dst Port Src IP/Port TCP Flag Type of Attack (Average/Maximum/Current)Traffic Volume[bps/pps] Severity Attack Start Time Duration

DDoS Protection Status

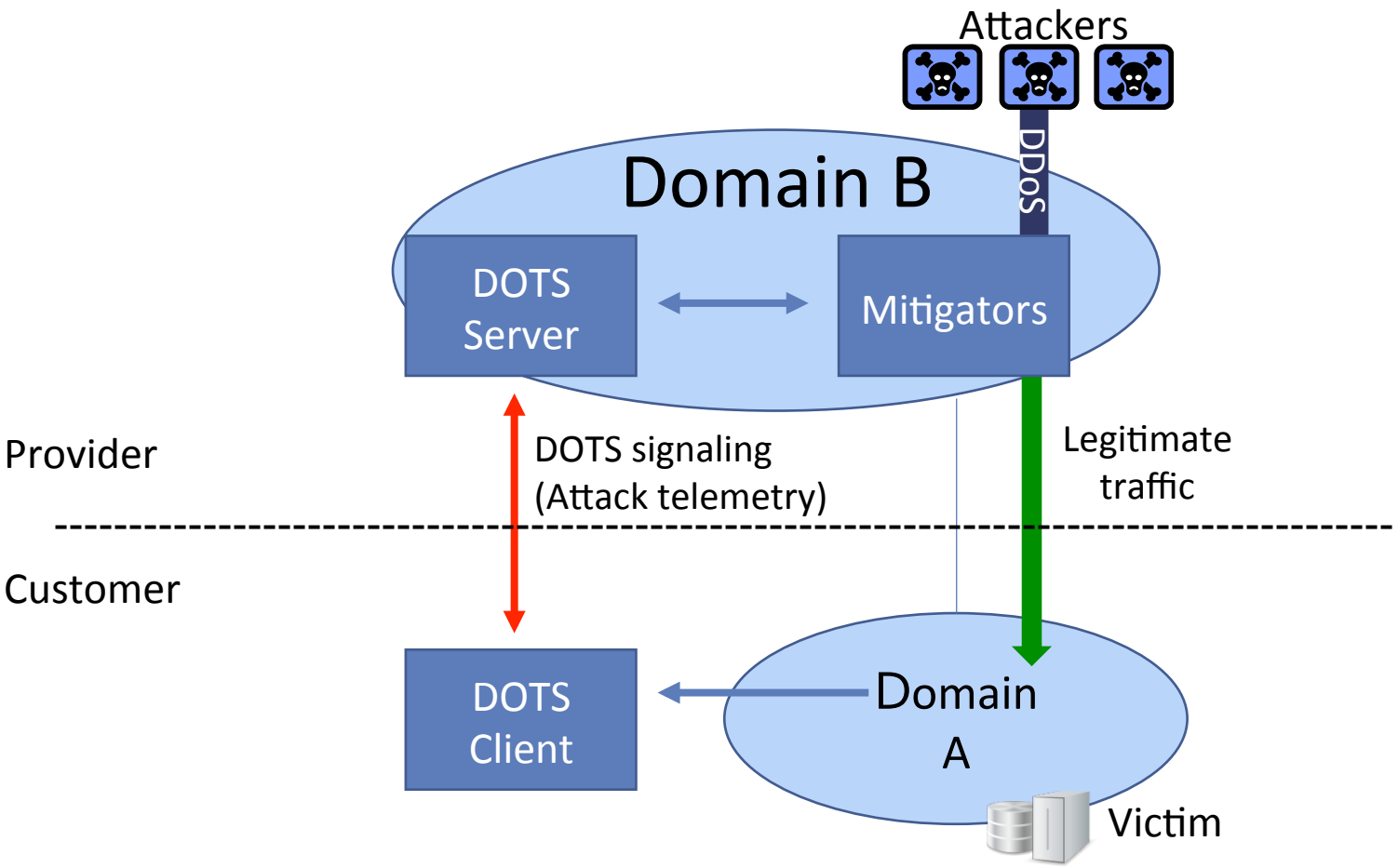
- difficult to know whether the DDoS attack has ended or not from the monitoring point of the DOTS client especially if it is inter-domain
- Information from DOTS server to client
  - Attack telemetry
  - Status of protection
  - Data for billing

Inter-domain usecases

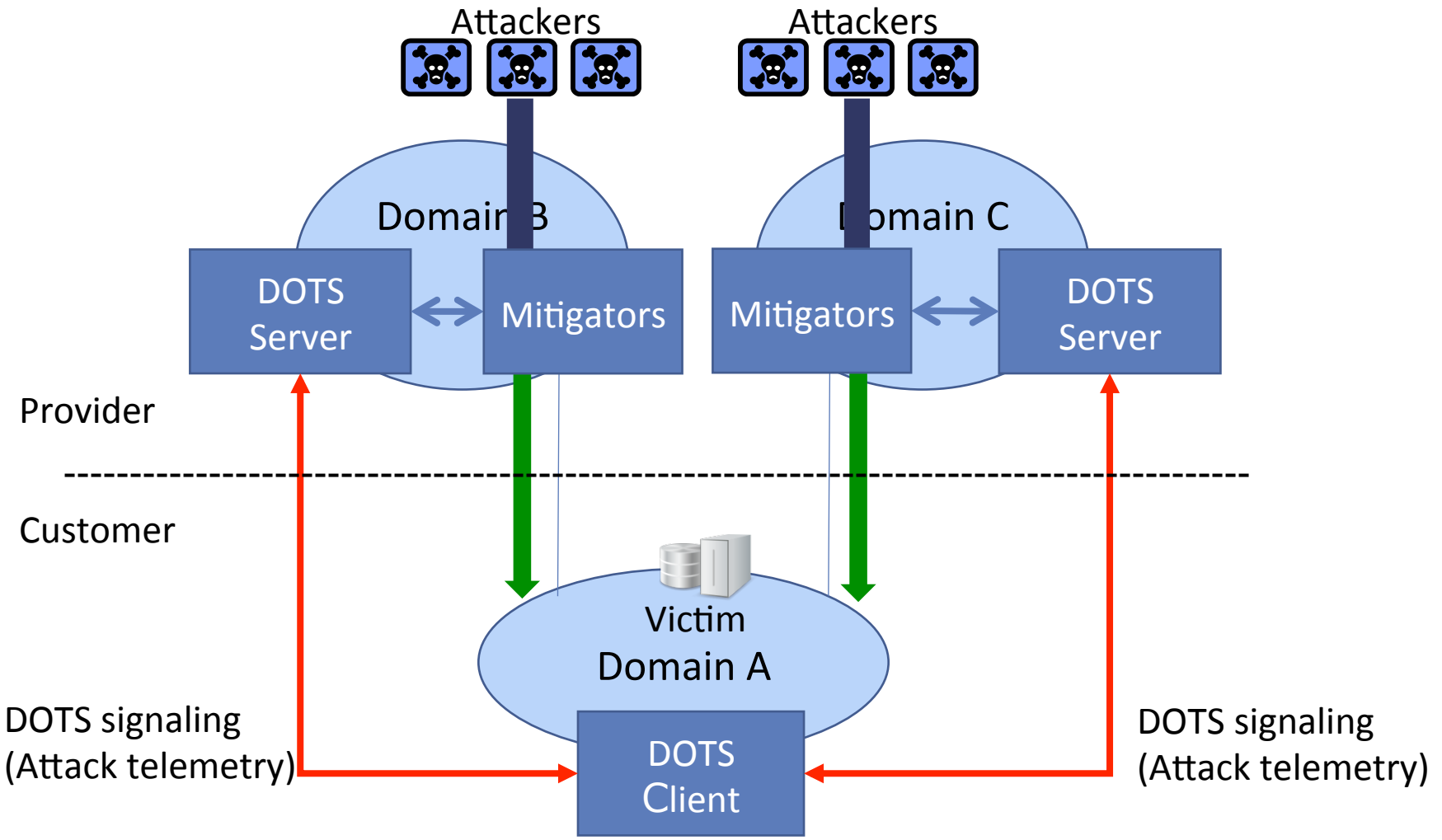
- Customer to Provider(c2p)
  - Usecase 1: Single-home Model
  - Usecase 2: Multi-home Model
- Provider to Provider(p2p)
  - Usecase 3: Delegation Model
  - Usecase 4: Distributed Architecture Model
  - Usecase 5: Centralized Architecture Model

Multi-provider cooperative DDoS protection
→draft-nishizuka-dots-inter-domain-mechanism

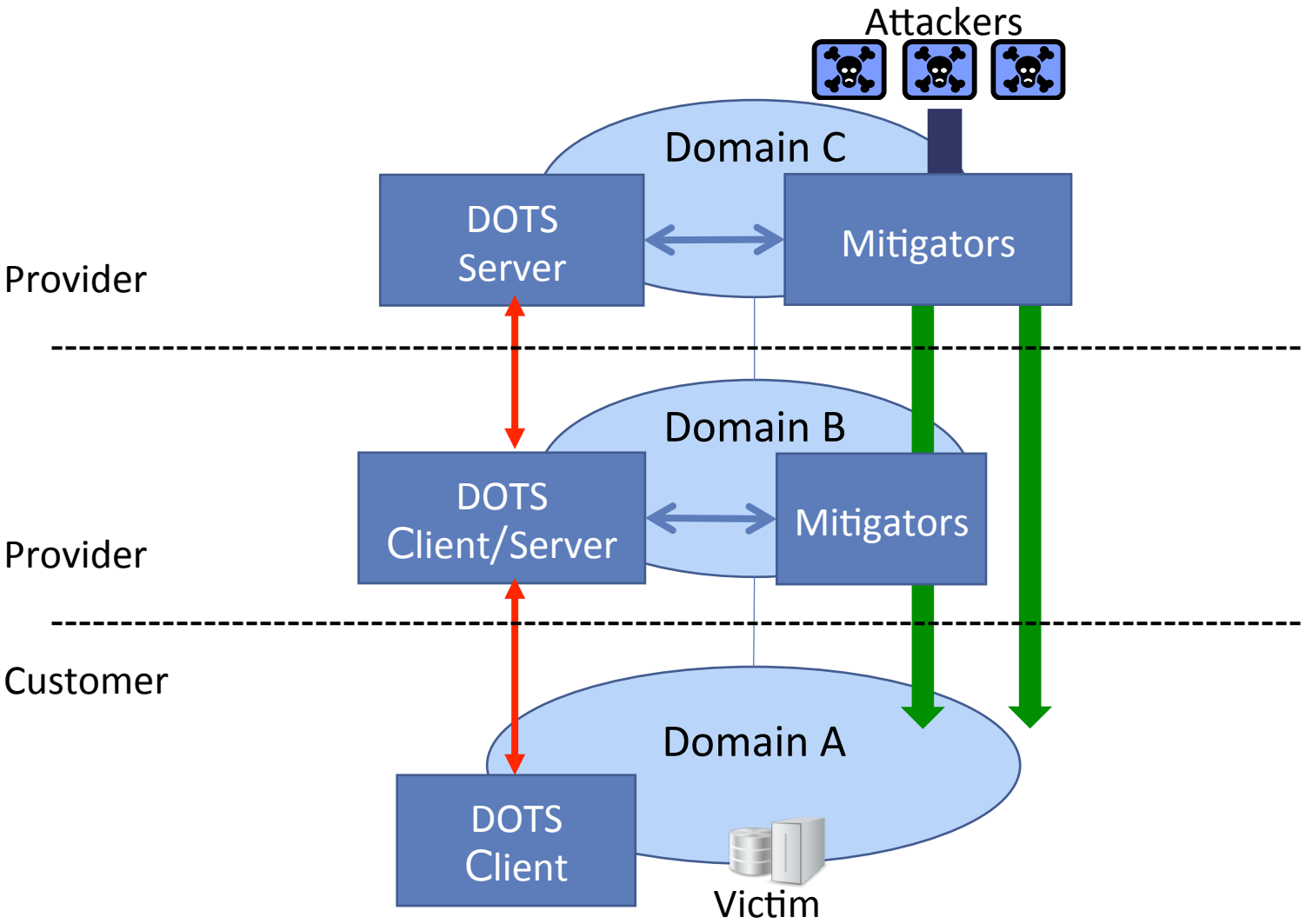
Inter-domain usecase1: Single-home model



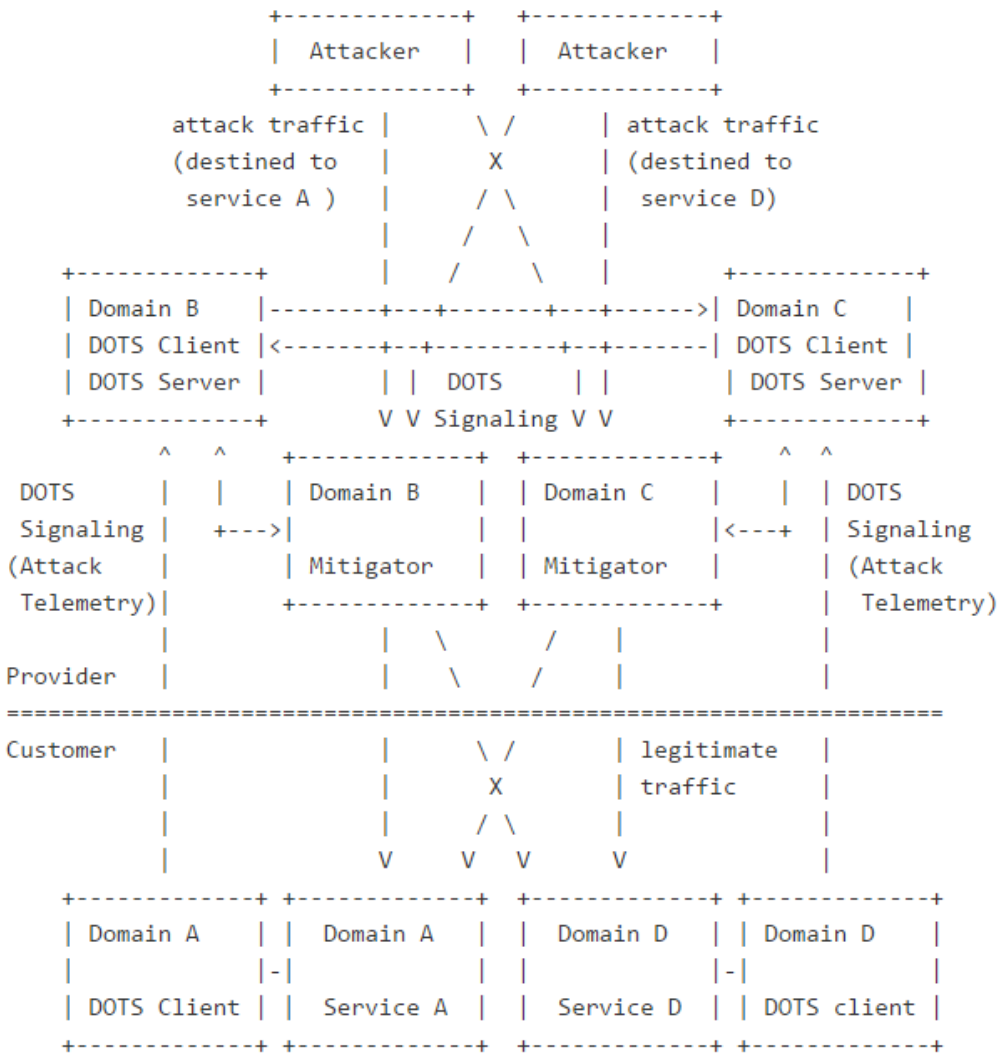
Inter-domain usecase2: Multi-home model



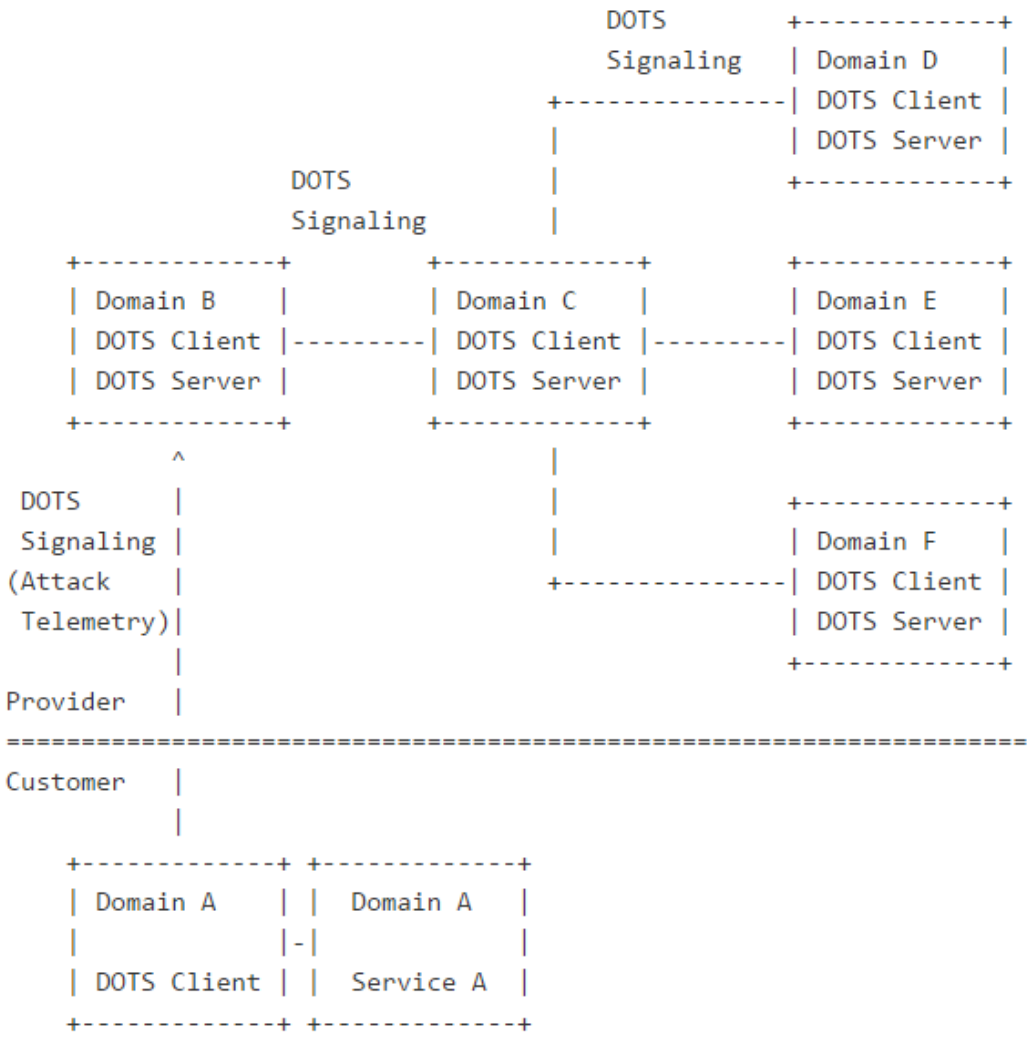
Inter-domain usecase3: Delegation model



Inter-domain usecase4: Distributed Architecture model



Inter-domain usecase5: Centralized Architecture model



Nextstep

- Consolidation with draft-ietf-dots-use-cases-01
  - Texts and contexts will be merged