DOTS Signal Channel

https://tools.ietf.org/html/draft-ietf-dots-signal-channel

DOTS Interim Meeting, February 2018

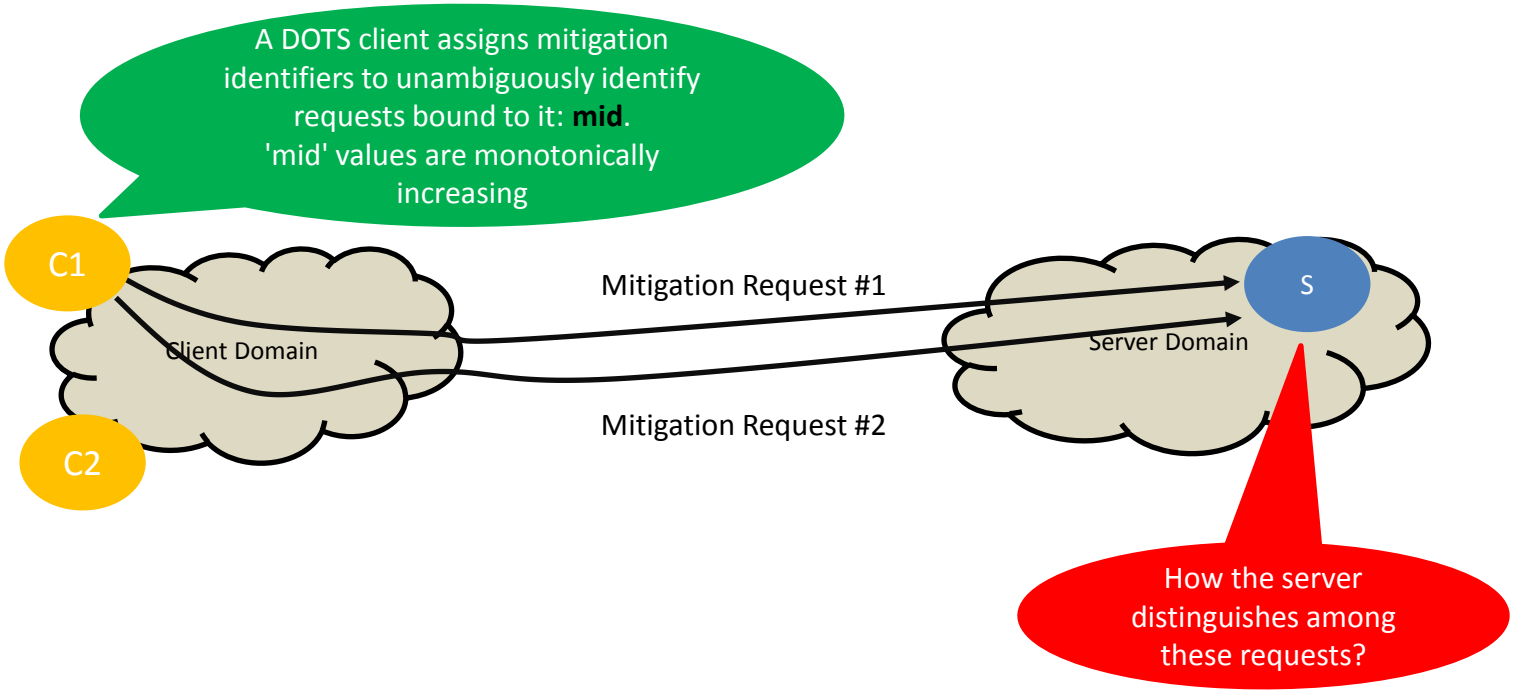
Presenter: Mohamed Boucadair

Agenda

- Quick walk through the protocol
- List of main changes since IETF#100
- Next steps

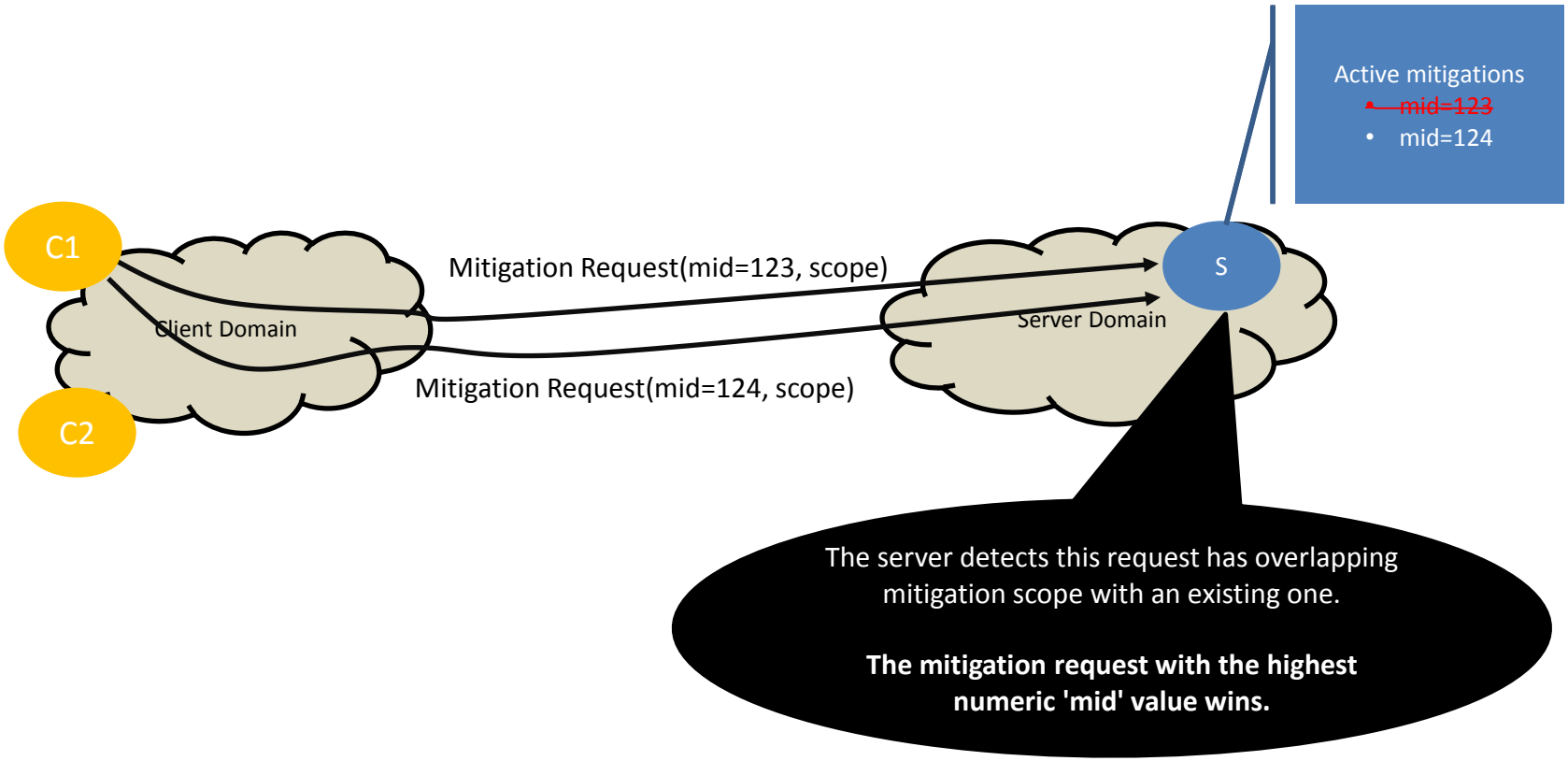
Design Walk Through

Handling Requests with Overlapping Scopes (incl. Out-of-Order Requests)



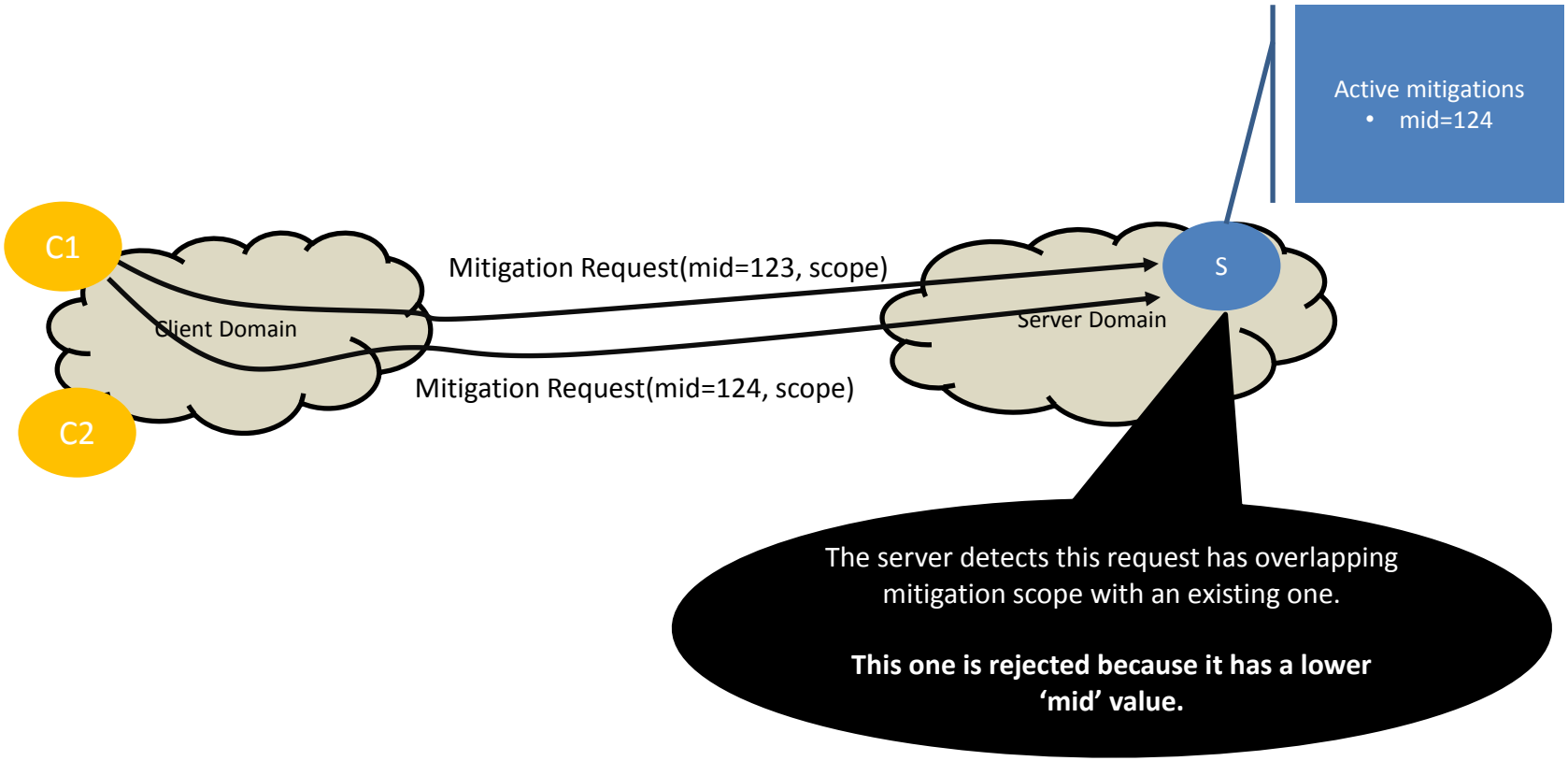
Design Walk Through

Handling Requests with Overlapping Scopes



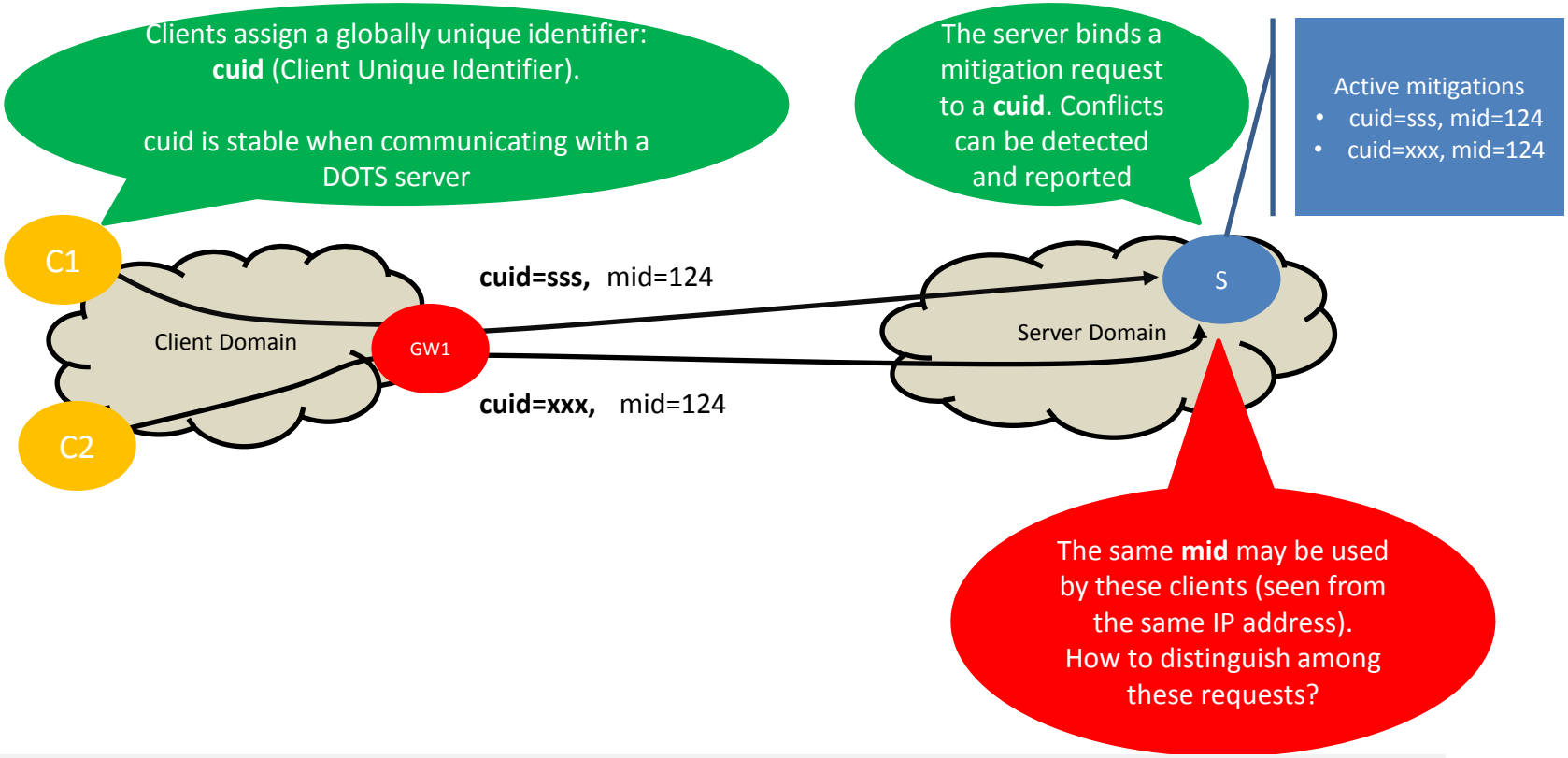
Design Walk Through

Handling Out-of-Order Requests



Design Walk Through

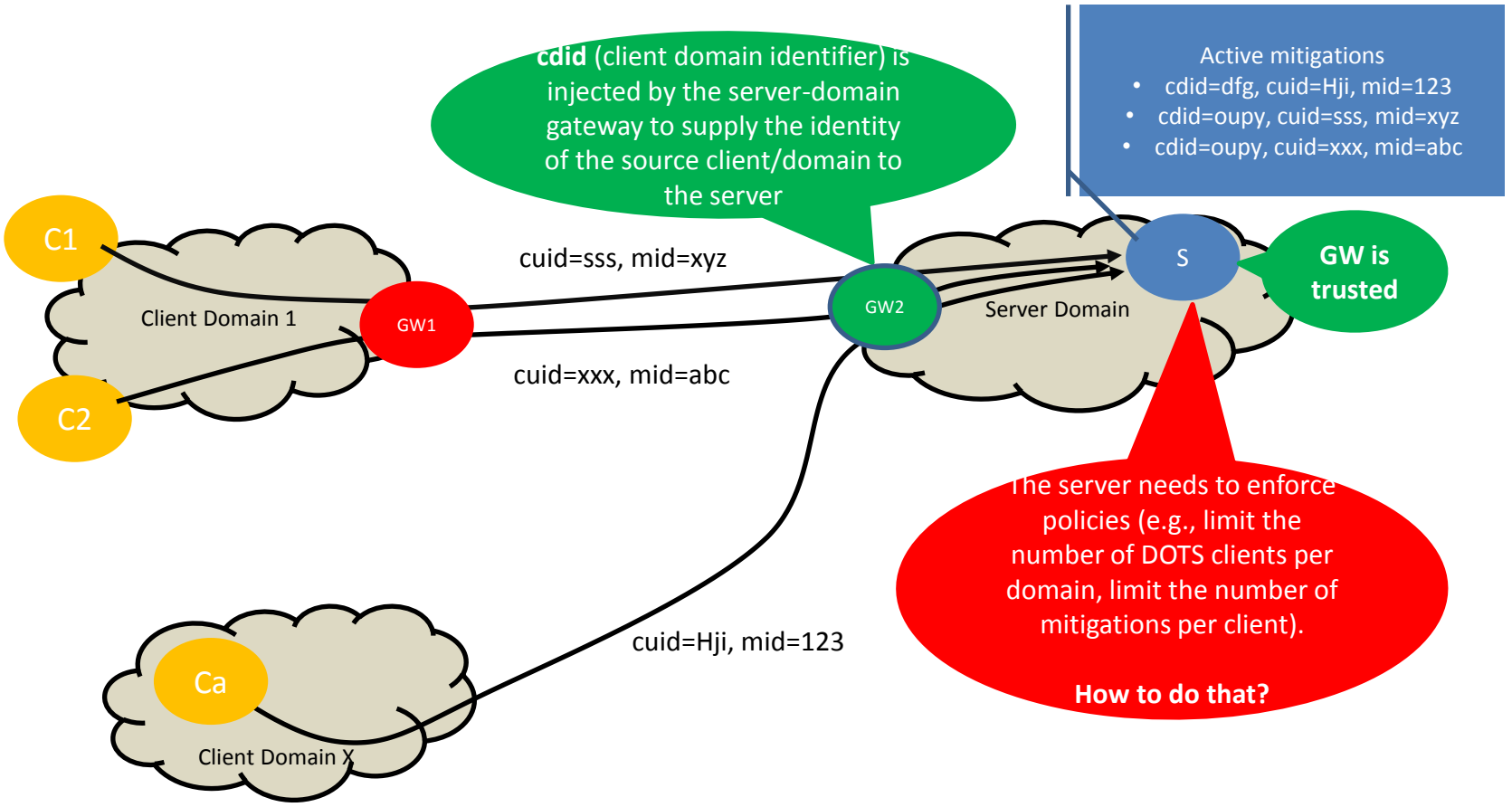
Collision Avoidance



- cuid is the output of a cryptographic hash algorithm
- The cryptographic hash algorithm is SHA-256
- Input:
  - The SPKI of the DOTS client X.509 certificate, the DOTS client raw public key, or the "PSK identity" used by the DOTS client in the TLS ClientKeyExchange message
- The output of the cryptographic hash algorithm is truncated to 16 bytes

Design Walk Through

Policy enforcement



Design Walk Through

Operations & Parameters

Operation	Method
Request mitigation	PUT
Adjust the scope of a mitigation	PUT
Refresh a mitigation	PUT
Retrieve mitigations	GET
Report efficacy update	PUT
Delete mitigations	DELETE

	URI Parameters		
Method	**cdid**	**cuid**	**mid**
PUT	MUST NOT	Mandatory	Mandatory
GET	MUST NOT	Mandatory	Optional
DELETE	MUST NOT	Mandatory	Mandatory

DOTS clients & client-domain gateways

	URI Parameters		
Method	**cdid**	**cuid**	**mid**
PUT	Optional	Mandatory	Mandatory
GET	Optional	Mandatory	Optional
DELETE	Optional	Mandatory	Mandatory

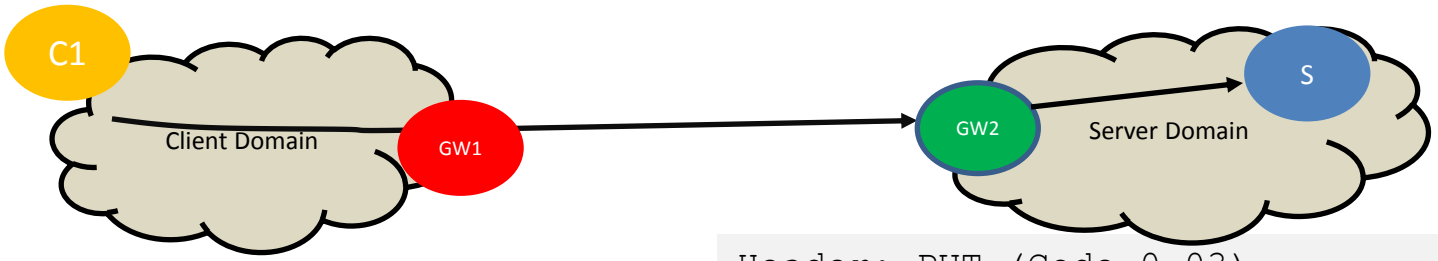
DOTS servers & server-domain gateways

Design Walk Through

Sample Mitigation Request Message

```
Header: PUT (Code=0.03)
Uri-Host: "host"
Uri-Path: ".well-known"
Uri-Path: "dots"
Uri-Path: "v1"
Uri-Path: "mitigate"
Uri-Path: "cuid=dz6pHjaADkaFTbjr0JGBpw"
Uri-Path: "mid=123"
Content-Type: "application/cbor"
```

Request as sent by the client



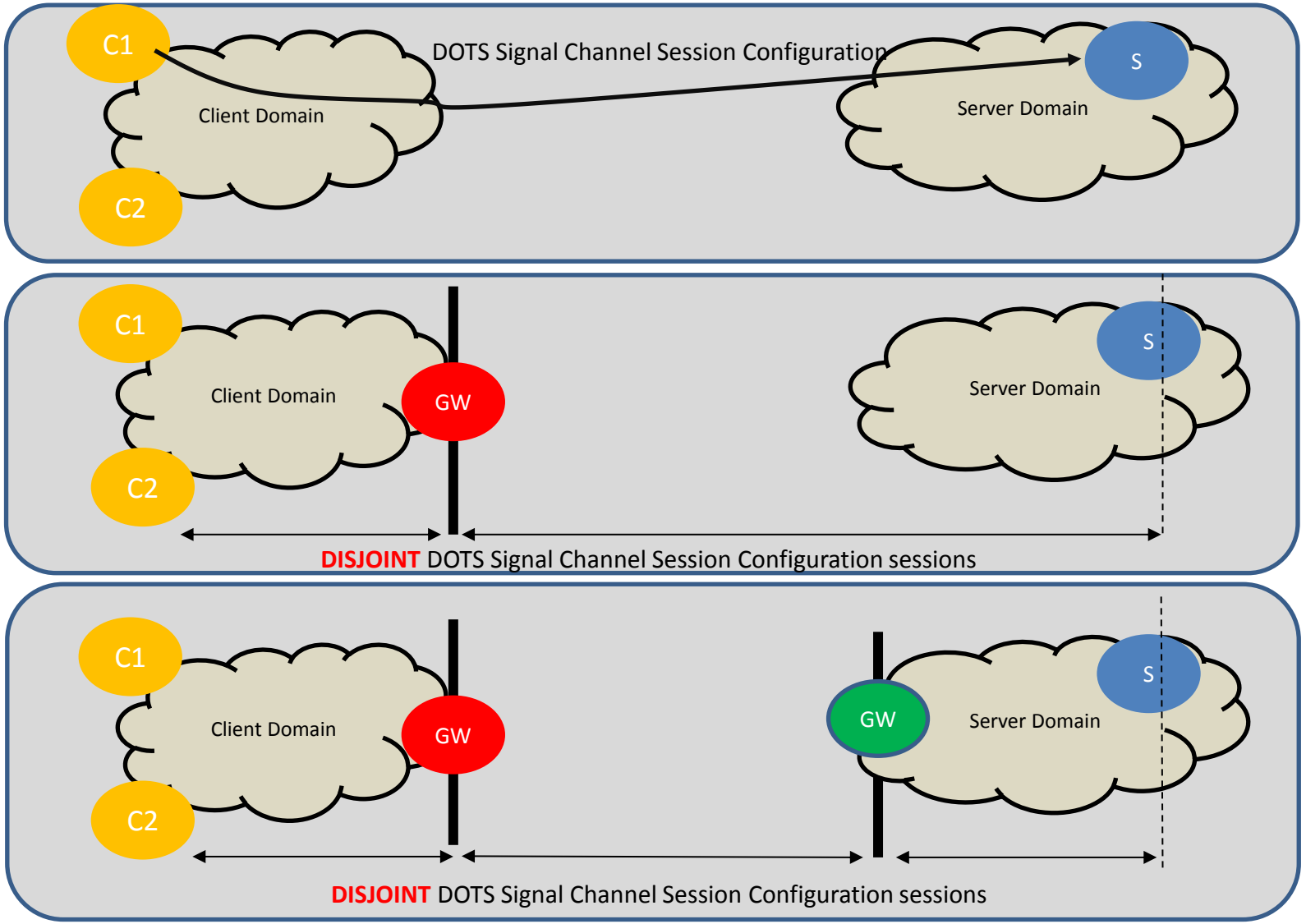
Request as relayed by the server-domain gateway

```
Header: PUT (Code=0.03)
Uri-Host: "host"
Uri-Path: ".well-known"
Uri-Path: "dots"
Uri-Path: "v1"
Uri-Path: "mitigate"
Uri-Path: "cdid=7eeaf349529eb55ed50113"
Uri-Path: "cuid=dz6pHjaADkaFTbjr0JGBpw"
Uri-Path: "mid=123"
Content-Type: "application/cbor"
```

Order is important to ease identifying a resource

Design Walk Through

Session Configuration



Design Walk Through

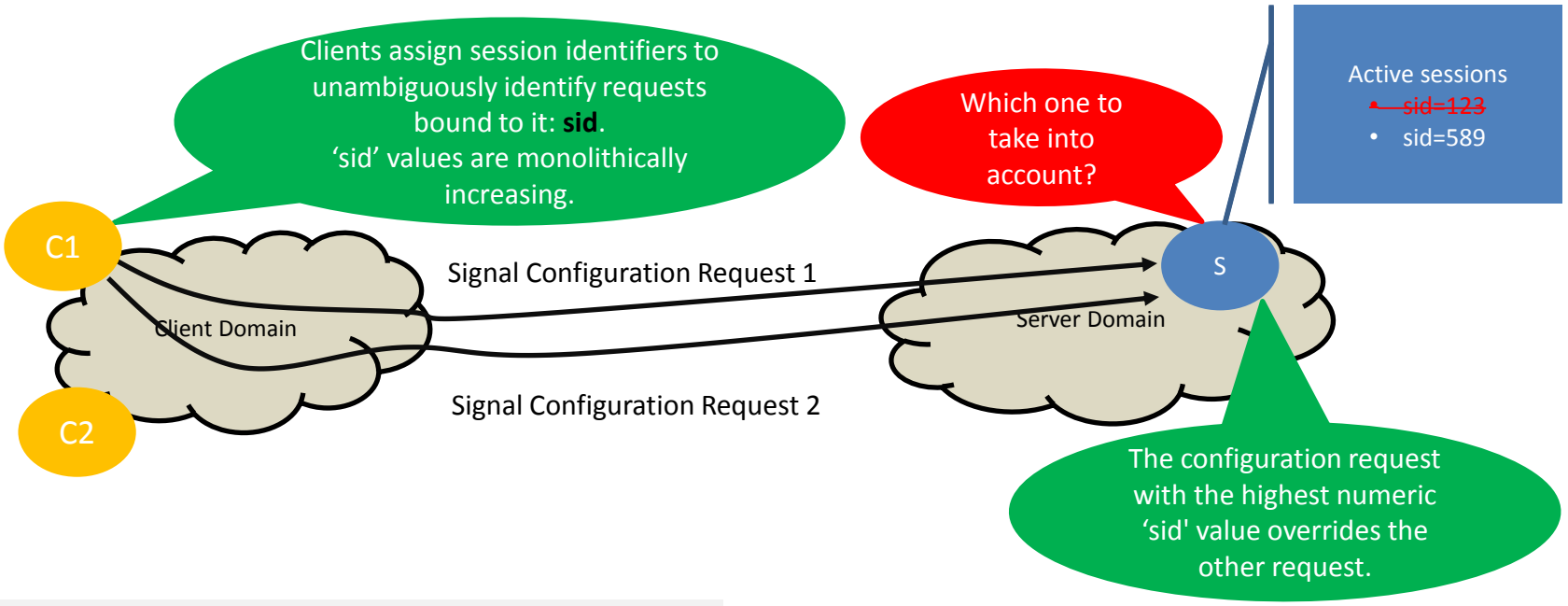
Session Configuration

- A DOTS client can negotiate, configure, and retrieve the DOTS signal channel session behavior with its DOTS peers
  - Heartbeat interval
  - Missing heartbeats allowed
  - Acceptable signal loss ratio
  - Automated mitigation on loss of signal (trigger-mitigation)
- The same or distinct configuration sets may be used during times when a mitigation is active and when no mitigation is active

Operation	Method	Description
Discover Configuration Parameters	GET	Obtain acceptable (e.g., minimum and maximum values) and current configuration parameters on the DOTS server
Convey Signal Channel Session Configuration	PUT	Convey the configuration parameters for the signal channel (e.g., heartbeat interval, maximum retransmissions).
Delete Signal Channel Configuration	DELETE	Set to default values

Design Walk Through

Out-of-Order Configuration Requests




```
Header: PUT (Code=0.03)
Uri-Host: "host"
Uri-Path: ".well-known"
Uri-Path: "dots"
Uri-Path: "v1"
Uri-Path: "config"
Uri-Path: "sid=123"
Content-Format: "application/cbor"
```

Method	'sid' URI Parameter
GET	MUST NOT
PUT	MUST
DELETE	Optional

Changes Since IETF#100

- Handling conflicts
- NAT considerations
- No list of client-identifiers but two identifiers instead (cuid and cdid)
- Fix and clarify request URIs to identify resources
- Multiple mitigations in the same request are forbidden
- Restructure the YANG module
- Update CBOR mapping table

Changes Since IETF#100

- Same or distinct configuration may be used during idle and mitigation-active times
- Config-interval to force a client to contact the server (changes may happen at the server side)
- SNI support
- Validation of target-prefix
- Rate-limit DOTS requests and cuid regeneration
- Clarify that signal configuration messages must not be relayed
- And many other edits to enhance the readability of the document

Early Port Allocation

- Request for 4646 was handed to the AD
- IANA suggested to apply for permanent allocation
- In progress

Pending Changes (github)

- Integrate hop-limit
- Fix some few typos

https://github.com/boucadair/draft-ietf-dots-signal-channel

Next Steps

- Publish -18 to integrate hop-limit
- Issue a WGLC on -18
- Questions?