Group Communication for the Constrained Application Protocol (CoAP)

draft-ietf-core-groupcomm-bis-00

Esko Dijk, IoTconsultancy.nl
Chonggang Wang, InterDigital
Marco Tiloca, RISE

IETF CoRE WG virtual interim, April 8th, 2020

Goal

- Intended normative successor of experimental RFC 7390 (if approved)
  - As a Standards Track document
  - Obsoletes RFC 7390, Updates RFC 7252 / 7641
- Be standard reference for implementations that are now based on RFC 7390, e.g.:
  - “Eclipse Californium 2.0.x” (Eclipse Foundation)
  - “Implementation of CoAP Server & Client in Go” (OCF)
- What’s in scope?
  - CoAP group communication over UDP/IP, including latest developments (Observe/Blockwise/Security …)
  - Unsecured CoAP or group-OSCORE-secured communication
  - Principles for secure group configuration
  - Use cases (appendix)

Groupcomm-bis-03/00: process view

- Updated with reviewers' comments (Jim [1], Thomas [2])
- Adopted as CoRE WG document
  - draft-dijk-core-groupcomm-bis-03 (March 9) is now draft-ietf-core-groupcomm-bis-00

[1] https://mailarchive.ietf.org/arch/msg/core/fme0kaeiiroi6ETKxD3yoD_MiyE/

[2] https://mailarchive.ietf.org/arch/msg/core/TgmEmwhDB2EokFkMCh8UWgOxO8E/

Groupcomm-bis-00: content view

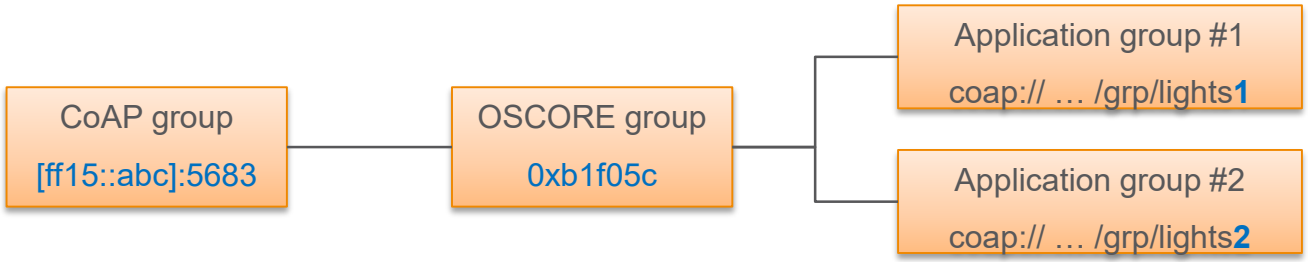
- Improved definition (2.1) of application/CoAP/security groups
  - including two new figures
- Added group discovery (2.2.3) with reference to RD.
- Security section on countering attacks (5.2.3) rewritten with more details
- Fixes & clarifications
  - improved description of RFCs that are obsoleted/updated
  - many others!

Groupcomm-bis-00 “Group” concepts

› **Distinguish *types* of groups**
  – CoAP group: network level
  – OSCORE group (‘security group’)
  – Application group: application level

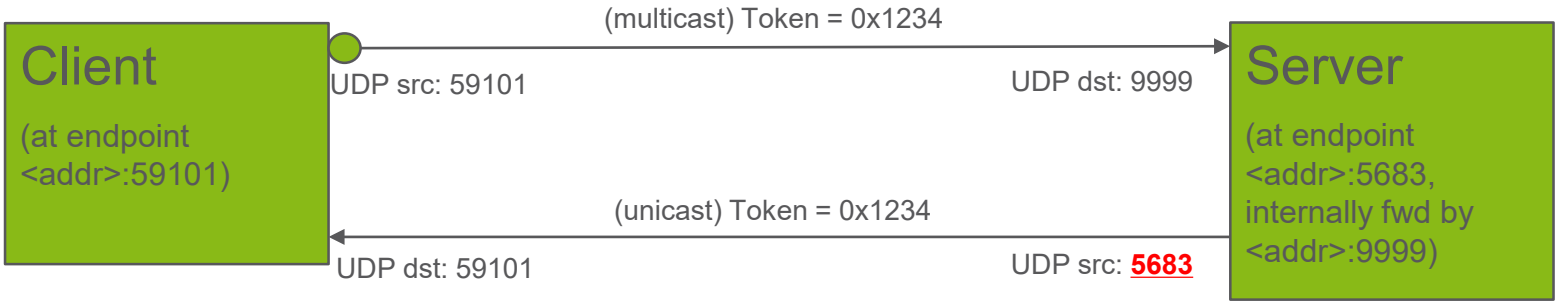
(identifiers for group type:)
→ multicast-address + port
→ Group name (invariant string)
→ <any application-specific ID>

› Example of group relations:



Open Issues in Github / Gitlab

- See groupcomm-bis issues page and previous page
- #1 Clarify multicast endpoint concept and messaging model - UDP port may change
  - based on email thread [core] RFC 7252 - 8.2 - Multicast - Request / Response Layer, page 67, top



Open Issues in Github / Gitlab

- See groupcomm-bis GitHub issues page and previous GitLab page

- #26 Section 2.1.2 - URI-Host for naming application groups

- #35 Consider if consistency requirement for "response suppression" should operate on Response Code class or not

Next steps

- Work on issues in -00
- Process the latest review comments by Jim
- Test selected functions in CoAP implementations
  - E.g. “Observe + multicast” extension of RFC 7641 (first tests done successfully with Californium)

Thank you!

Comments/questions?

Motivation (backup slide)

- RFC 7390 was published in 2014
  - CoAP functionalities available by then were covered
  - No group security solution was available to indicate
  - It is an Experimental document (started as Informational)
- What has changed?
  - More CoAP functionalities have been developed (Block-Wise, Observe)
  - RESTful interface for membership configuration is not really used
  - Group OSCORE provides group end-to-end security for CoAP
- Practical considerations
  - Group OSCORE clearly builds on RFC 7390 normatively
  - However, it can refer RFC 7390 only informationally