

Group Communication for the Constrained Application Protocol (CoAP)

draft-ietf-core-groupcomm-bis-07

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

IETF 114 meeting – Philadelphia – July 26th, 2022

Following IETF 113 ...

› Working Group Last Call started on version -06

- Thanks for the comments!

› Review from Carsten Bormann

- Main points archived at [1]; further detailed comments sent to the authors

› More comments

- From Jon Shallow [2]: concurring with Carsten's points; pointer to *libcoap* implementation
- From Rikard Höglund [3]: the document looks good
- From John Mattson: ongoing PR #38 [4]; editorial fixes; more comments expected

[1] https://mailarchive.ietf.org/arch/msg/core/PtqtDE_3PWR-n-o_z9h0HxW2vDI/

[2] https://mailarchive.ietf.org/arch/msg/core/Z3978VEUvS3sJ5DPI2Pk0Qea_00/

[3] <https://mailarchive.ietf.org/arch/msg/core/5jvhR9JIfWpmLhmxAcUqpAy-zfM/>

[4] <https://github.com/core-wg/groupcomm-bis/pull/38>

Updates since version -06

- › **Submitted version -07, addressing the WGLC comments**

- › **Extended list of changes to other documents (Section 1.3)**
 - RFC 7390 (obsoleted) → Text on transport protocols and protocol interworking
 - RFC 7252 (updated) → Congestion control; newly admitted multicast scopes

- › **Real-life context added to deployment example in Figure 2**
 - Mapping of CoAP/Application/Security groups with one another
 - Building automation use case, with lighting devices, HVAC devices, temperature/humidity sensors and control panels

Updates since version -06

- › **Possible name aliasing for CoAP groups (with examples)**
 - Hostname or IP address literal in URI authority component
 - Default port number present or not in URI authority component
- › **Detailed examples about application group naming and group discovery**
 - Application group naming → Moved to new Appendix B
 - Group discovery → Moved to new Appendix C
- › **Security groups – Name not used in messages between group members**
 - Used as identifier when performing related side tasks
 - › Setup and configuration of a security group
 - › Authorization request for joining a security group
 - › Discovery of the security group and of means to join it
 - Don't use the name "NoSec" (or its variations), not even to signal that no security is used

Updates since version -06

› Using proxies

- Clarified limitations, addressed by the method in *-core-groupcomm-proxy*
- Expanded on different granularities of "standing in" for a reverse-proxy
- Pointer to *-core-groupcomm-proxy* for an HTTP-to-CoAP forwarding method
- Discussed case of group request sent at once to multiple proxies (e.g., over multicast)

› Limited use of reliable transports

- Individual unicast Block-wise requests, after the first one-to-many request
- Servers can advertise support for multiple transports as in *-core-transport-indication*

› Revised sections on interworking with other protocols

- MLD/MLDv2/IGMP/IGMPv3, RPL, MPL
- Reference to *-6lo-multicast-registration*

Updates since version -06

- › **Clearer description and discouragement of NoSec mode, as NOT RECOMMENDED**
 - Consistently and highly discouraged; possible in particular cases (e.g., early discovery)
 - Discussed implications and impact on security
 - Written with no quotes, as in RFC 7252
- › **Security considerations**
 - Group OSCORE: clearer split between replay-check and verifying source authentication
 - 6LoWPAN: fragment handling and loss of fragments for large IPv6 packets
 - More on pervasive monitoring; mitigate by using security and smallest scope possible
- › **Several minor clarifications and editorial improvements**

Summary and next steps

- › **Version -07 addresses all WGLC comments received so far**
- › **Plan to submit version -08, addressing:**
 - Any further comments from Carsten, following-up on his WGLC review
 - Further comments from John, expected under PR #38 [4]
 - Additional comments, if any
- › **Reminder – Francesca recommended to request publication together with:**
 - *draft-core-oscore-groupcomm* : Waiting for Shepherd Write-Up
 - *draft-ace-key-groupcomm-oscore* : in WGLC (processed 1st wave of comments in v-14)
 - › Some more changes are already planned and to be made soon
 - › They first require updates to *draft-ace-key-groupcomm*, which is in AD Review

Thank you!

Comments/questions?

<https://github.com/core-wg/groupcomm-bis/>

Goal

- › Normative successor of experimental RFC 7390
 - Obsoletes RFC 7390; Updates RFC 7252 and RFC 7641
- › New standard reference for implementations now based on RFC 7390
- › Scope
 - CoAP group communication, including latest features: Observe/Blockwise/Security ...
 - Unsecured and Group-OSCORE-secured
 - Definition of group types and Secure group configuration

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 used to normatively build on RFC 7390
 - However, it could properly refer to RFC 7390 only informationally