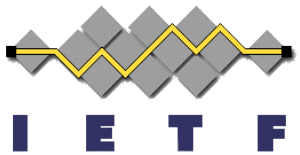
Group Communication for CoAP

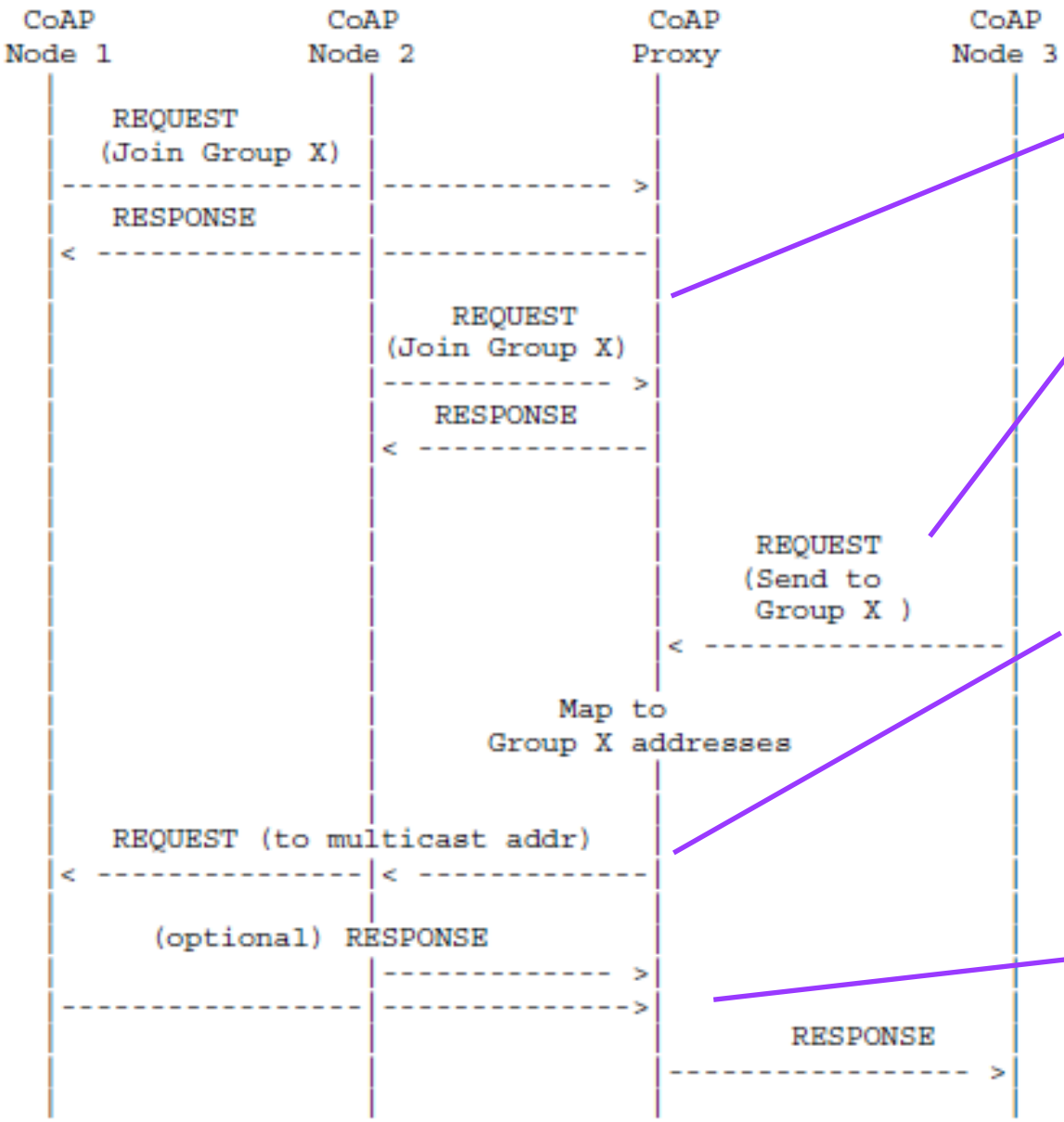


Akbar Rahman
Esko Dijk

IETF 81, July 2011

http://tools.ietf.org/html/draft-rahman-core-groupcomm-06

CoAP Group Communications Concept



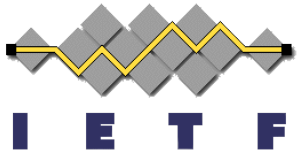
1) Multiple receiver nodes form a group

2) Source (sender) sends a single message with content to the group address

3) Content is distributed to all members of group (e.g. multicast, series of multicast, or serial unicast)

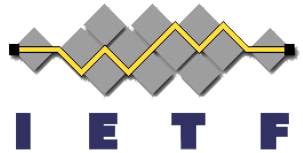
4) Optional Response

Requirements for Group Comm (1/4)



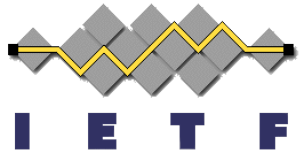
- REQ1: Selectable Reliability:
  - At least unreliable group communication supported, but preferably reliable group communications as well if possible
- REQ2: Efficiency:
  - Delivers messages more efficiently than a "serial unicast only" solution. Also, it should provide a right balance between group data traffic and control overhead
- REQ3: Low Latency:
  - Deliver a message (preferably) as fast as possible
- REQ4: Synchrony:
  - Allows near-simultaneous modification of a resource on all devices in a group, providing to users a perceived effect of synchrony or simultaneity
  - It can be expressed as a time span "D" such that message "m" is delivered to all destinations in a time interval [t, t+D] for arbitrary "t"

Requirements for Group Comm (2/4)



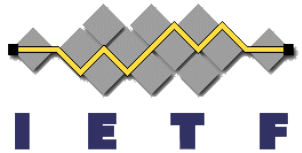
- REQ5: Ordering
  - [TBD to check what use cases require in terms of message ordering especially in multi-source situations]
- REQ6: Security
  - See Backup slides for 7 security requirements (reviewed in IETF Prague)
- REQ7: Flexibility:
  - Support for one or many source(s), for dense and sparse networks, for high or low listener density, one or many group(s), and multi-group membership
- REQ8: Robust Group Management:
  - Includes functionality to join groups, leave groups, view group membership, and persistent group membership in failing node or sleeping node situations

Requirements for Group Comm (3/4)



- REQ9: Network Layer Independence
  - A solution should be specified independent from specific unicast and/or IP multicast routing protocols
  - It should support different routing protocols and implementations thereof
- REQ10: Minimal Specification Overhead
  - A group communication solution should preferably re-use existing/established (IETF) protocols that are suitable for Low Power Lossy Network (LLN) and standard backbone deployments, instead of defining new protocols from scratch
- REQ11: Minimal Implementation Overhead
  - E.G. A solution allows to re-use existing (software) components that are already present on constrained nodes such as (typical) 6LoWPAN/CoAP nodes

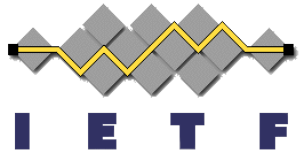
Requirements for Group Comm (4/4)



- REQ12: Mixed backbone/LLN Topology Support
  - A solution should work within a single LLN, and in combined LLN/backbone network topologies, including multi-LLN topologies
  - Both the senders and receivers of CoAP group messages may be attached to different network links or be part of different LLNs, possibly with routers or switches in between group members
  - In addition, different routing protocols may operate on the LLN and backbone networks. Preferably a solution also works with existing, common backbone IP infrastructure (e.g. switches or routers)

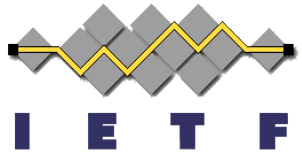
- REQ13: CoAP Proxying Support
  - A CoAP proxy can handle distribution of a message to a group on behalf of a (constrained) CoAP client

Potential Approaches for Group Communication



- There are three alternative approaches possible for CoAP group communications each with associated pros/cons:
  - IP Multicast
    - Routers must support multicast protocols
  - Overlay Multicast
    - CoAP Proxy nodes must support hybrid multicast functionality
  - CoAP Application level Group Management
    - CoAP application layer must support multicast functionality
- (See backup slides for more details - reviewed in previous IETFs)

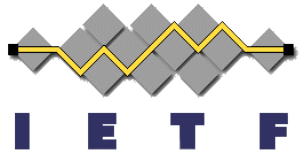
Recommended Solution (1/2)



- We recommend that IP Multicast be adopted as the base solution for CoAP Group Communication
  - This approach requires no standards changes to the IP Multicast suite of protocols
  - It does, however, require carfully implementing pieces of IP Multicast functionality in an LLN, in a backbone network, or in both

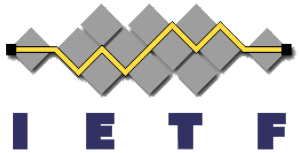
- Implementation strategies for the following target network topologies are outlined in the I-D:
  - Single LLN topology
  - Single LLN with backbone topology
  - Multiple LLNs with backbone topology

Recommended Solution (2/2)



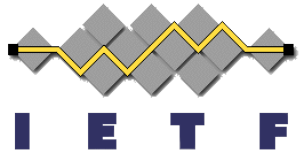
- For all network topologies that were evaluated, CoAP group communication can in principle be supported with IP Multicast, making use of existing protocols

- Also potential (but optional) optimizations were identified for an “MLD-like” or “MLD-lightweight” protocol specifically for LLNs, which would interwork with regular MLD on the backbone network
  - E.G: A subset of MLD could be defined for an “MLD for 6LowPAN” to minimize complexity for constrained nodes



BACKUP

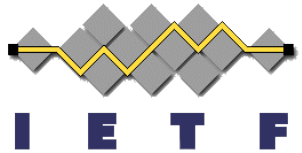
Background



- This draft is a follow up to our previous draft on “Sleeping and Multicast Considerations for CoAP” which was in a problem statement format:
  - http://tools.ietf.org/html/draft-rahman-core-sleeping-00

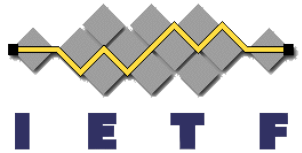
- During the previous CORE Webex calls, we were asked to produce satellite drafts to more precisely identify the problems and provide some initial solution proposals for:
  - Group Communications (as the more general problem of multicast) – This draft
  - Sleeping Nodes – TBD draft (but in progress)

IP Multicast



- Concept:
  - CoAP sub-networks to be connected directly to IP multicast enabled routers (e.g. running PIM-SM [RFC4601]).
  - Sending CoAP node can directly transmit group messages by setting IP address to selected multicast IP group address
  - Receiver CoAP nodes use MLD [RFC3810] to subscribe (listen) to any messages sent to selected IP multicast group
- Pros
  - Most efficient solution since done at IP layer
  - ROLL [draft-ietf-roll-rpl-14] assumes IP multicast supported
  - CoAP-03 draft [section 4.1] assumes IP multicast supported
- Cons
  - IP multicast is not generally deployed outside of corporate LANs and a few ISPs. So we may specify IP multicast support but practically it may often not be deployed

Overlay (Proxy based) Multicast (1/2)

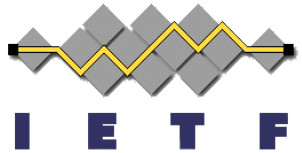


- Concept:
  - We define overlay multicast as one that utilizes an infrastructure based on proxies (rather than an IP router based multicast backbone) to deliver IP multicast packets to an end device
  - Since ROLL and CoAP drafts already support MLD (see pg. 4), we propose MLD Proxy [RFC3810] to be used as the overlay multicast approach
  - Specifically, the CoAP proxy node will also support Proxy MLD
  - Receiver CoAP nodes use MLD Proxy signaling to subscribe (listen) to any messages sent to selected IP multicast group
  - The CoAP (MLD) proxy node would be responsible for delivering any IP multicast message to the subscribed CoAP devices
  - Note that the CoAP (MLD) proxy need not necessarily be connected to an external multicast backbone

Overlay (Proxy based) Multicast (2/2)

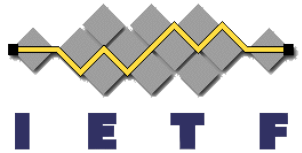
- Pros
  - Ties well into existing CoAP proxy concept
- Cons
  - It is not obvious that existing MLD Proxy [RFC 3810] allows the specific scenario we are proposing. Further investigation required.

CoAP Application level Group Mgmt



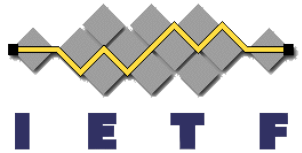
- Concept:
  - Perform all group communications at the CoAP application level
  - Expand CoAP headers to allow simple group mgmt functions (Join, Leave, etc.)
  - The CoAP proxy node would be responsible for group mgmt
  - Any CoAP node that wanted to send a message to a CoAP group would first send the CoAP message to the proxy. The proxy would then explode it out to the group
- Pros
  - Functionality fully within the CoAP protocol (and CORE WG control)
  - Analogous approach as Email group management (and other Apps)
- Cons
  - Has high overhead compared to lower layer solutions

Group Resource Manipulation (1/3)



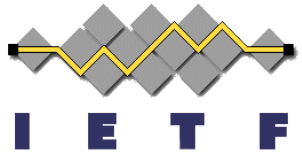
- Needed to replicate functionality of existing standards, e.g. BACnet's Alarm and Event Notification service
- Two forms of group resource manipulation should be supported:
  - Push (PUT or MPUT) as for example "turn off all lights simultaneously"
  - Pull (GET or MGET) as for example "return all the resources matching a well known URI"
- Conceptually, the result of a MGET or MPUT should be the same as if the client had unicast them serially

Group Resource Manipulation (2/3)



- Limit manipulation to idempotent methods (PUT/GET/DEL)
  - Repeat requests can then be used to increase reliability of receipt
- Requires a consistent naming and addressing scheme for groups
  - Multicast is the easy case; can use DNS to resolve FQDN in authority to multicast or unicast address
- Can a group be represented by a list of addresses as well?
  - If so, perhaps this argues for a group scheme, e.g. “coapm” to signal a proxy to do fan-out task

Group Resource Manipulation (3/3)



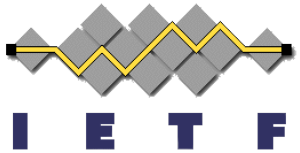
- Target resource must be located at same port and path for all group members
  - Suggests a need to advertise path, port or have a priori agreement

Security Considerations

- As per major comment from IETF79 (Beijing), reviewed output of:
  - IETF MSEC (Multicast Security)
    - In particular, [RFC3740], [RFC5374] and [RFC4046] are very instructive
  - IRTF SAMRG (Scalable Adaptive Multicast Research Group)

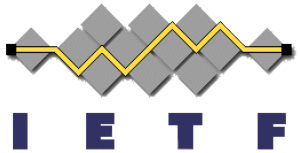
- And derived the following requirements for securing group communications in CoAP

Group Security Requirements for CoAP (1/3)



- REQ1: Group communications data encryption:
  - Important CoAP group communications shall be encrypted (using a group key) to preserve confidentiality. It shall also be possible to send CoAP group communications in the clear (i.e. unencrypted) for low value data.
- REQ2: Group communications source data authentication:
  - Important CoAP group communications shall be authenticated by verifying the source of the data (i.e. that it was generated by a given and trusted group member). It shall also be possible to send unauthenticated CoAP group communications for low value data.
- REQ3: Group communications limited data authentication:
  - Less important CoAP group communications shall be authenticated by simply verifying that it originated from one of the group members (i.e. without explicitly identifying the source node). This is a weaker requirement (but simpler to implement) than REQ2. It shall also be possible to send unauthenticated CoAP group communications for low value data.

Group Security Requirements for CoAP (2/3)

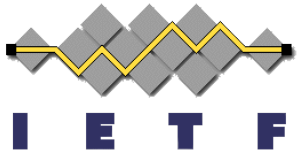


- REQ4: Group key management:
  - There shall be a secure mechanism to manage the cryptographic keys (e.g. generation and distribution) belonging to the group; the state (e.g. current membership) associated with the keys; and other security parameters.

- REQ5: Use of Multicast IPSec:
  - The CoAP protocol [I-D.ietf-core-coap] allows IPSec to be used as one option to secure CoAP. If IPSec is used at the CoAP level, then multicast IPSec [RFC5374] should be used for securing CoAP group communications.

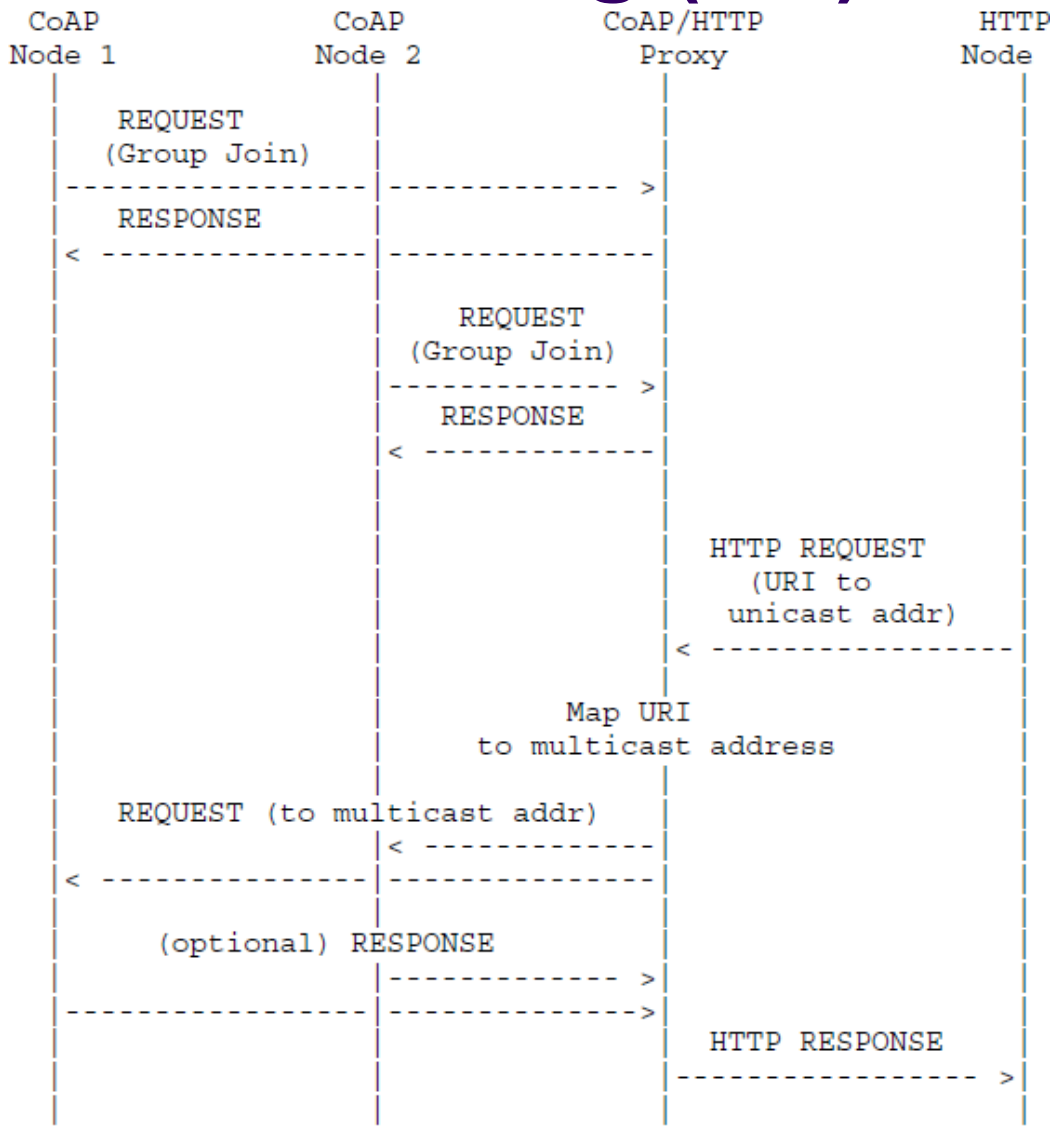
- REQ6: Independence from underlying routing security:
  - CoAP group communication security shall not be tied to the security of underlying routing and distribution protocols such as PIM [RFC4601] and ROLL [I-D.ietf-roll-rpl]. Insecure or inappropriate routing (including multicast routing) may cause loss of data to CoAP but will not affect the authenticity or secrecy of CoAP group communications.

Group Security Requirements for CoAP (3/3)

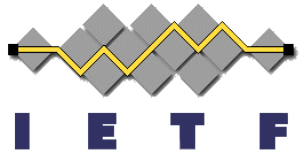


- REQ7: Interaction with HTTPS:
  - The security scheme for CoAP group communications shall account for the fact that it may need to interact with HTTPS (Hypertext Transfer Protocol Secure) when a transaction involves a node in the general Internet (non-constrained network).

CoAP Multicast and HTTP Unicast Interworking (1/2)



CoAP Multicast and HTTP Unicast Interworking (2/2)



- Proxy node needs to have the following functionalities to interwork CoAP/UDP (multicast) and HTTP/TCP (unicast):
  - Incoming HTTP Request will carry a URI (with HTTP scheme)
  - At the proxy node, the URI will then be again resolved (with CoAP scheme) to an IP multicast. This may be accomplished, for example, by using DNS-SD
  - The proxy node will then multicast the CoAP Request to the appropriate nodes

- CoAP proxy can be considered to be a "non-transparent" proxy according to [RFC2616]:
  - Specifically, [RFC2616] states that a "non-transparent proxy is a proxy that modifies the request or response in order to provide some added service to the user agent, such as group annotation services, media type transformation, protocol reduction or anonymity filtering."