Changes in coap-02

• Sending an error on a critical option clarified (#18)
• Clarification on behavior of PUT and idempotent operations (#19)
• Use of Uri-Authority clarified along with server processing rules. Uri-Scheme option removed. (#20, #23)
• Resource discovery section removed to a separate CoRE Link
• Format draft (#21)
• Initial security section outline added.
Finishing the Security Section

• coap-02 has security section placeholders
• Proposed outline
  – 10.1 Securing CoAP with IPSec
  – 10.2 Securing CoAP with DTLS
  – 10.3 Threat analysis and protocol limitations
• What more is needed?
  – Section mentioning payload encryption (S/MIME or CMS?)
  – How much more DTLS detail is needed?
    • Default port for DTLS secured CoAP
Threat Analysis

• Current threat analysis based on RFC2616
• Threats in outline
  – Processing URIs
  – Proxying and Caching
  – Attacks on TIDs
  – Risk of amplification using multicast
  – Asynchronous responses
• Help needed to flesh out analysis
• Other threats?
core-link-format-00

- Link format spun out of coap-01
- The link format ABNF from draft-nottingham-http-link-header was completely re-used
- Quoted strings were added for string attributes
- Explanation of the target/context URI was added along with use of the relation attribute
- References to DNS-SD and mDNS were completely removed as this was found to be misleading in Maastricht
- Well-known URI changed to /.well-known/core to make registration possible (/r was too short)
- Filtering was changed to a MAY
- Proper IANA section was created