IETF 121, IPPM draft-ietf-ippm-capacity-protocol

IP Capacity Measurement Protocol, draft version -10

Changes after presentation & comments on crypto approach by CFRG:

Partial Encryption is still optional. The approach on encryption in combination with authentication is new and follows advice given by CFRG:

- First, add a randomised Initialization Vector (IV) which is
  - Independent from the Auth Digest
  - Set newly with each message (IV size still 128 Bit)
- Then, encrypt the parts of the message to be encrypted (still 128 Bit AES-CBC),
- And finally authenticate the entire header and add the Auth Digest (still HMAC-256SHA)

Initial feedback from Brian Weis, early SecDir rev: “This looks good!“

IETF 121, IPPM draft-ietf-ippm-capacity-protocol

Introduced an optional UDP checksum
Intended for environments where UDP data integrity may be uncertain (if, e.g., standard UDP checksum is disabled to improve performance by a low-end device).

Removed security related text which doesn't specify or discuss features applied by the Test Protocol for One-way IP Capacity Measurement

- E.g., section "OPTIONAL Fully Encrypted mode - For Information Only"

....and got positive feedback from Brian Weis too, who felt the removed text to be "a bit confusing and unnecessary".