

**Use of CLUE with PERC**  
**draft-groves-perc-clue-00**  
**IETF 94, Yokohama**

**Christian Groves, Tommy Yang, Roni Even**



# Introduction

- Draft is initial thoughts around the PERC charter item:

PERC should:

“be implementable by both SIP (RFC3261) and WebRTC endpoints [I-D.ietf-rtcweb-overview]. How telepresence endpoints using the protocols defined in the CLUE working group could utilize the defined security solution needs to be considered. However, it is acknowledged that limitations may exist, resulting in restricted functionality or need for additional adaptations of the CLUE protocols.”

- The draft seeks to identify the restrictions and potential adaptations and to trigger further discussion.
- Draft assumes MDD terminates CLUE and acts as reduced function MCU.

# Basic CLUE flow

- SDP carries encoding information.
- CLUE carries metadata in Advertisements
- Capture Encodings selected by CLUE configures
- BOTH SDP and CLUE signalling are required to establish RTP media flow
- BUNDLE, SRTP can be used with CLUE

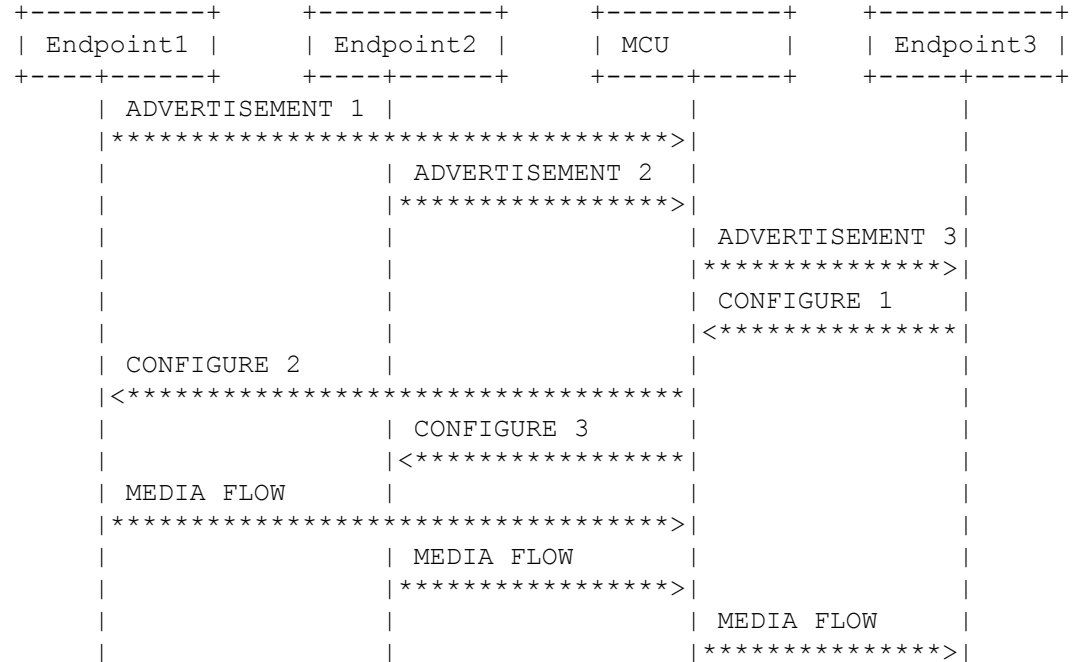
```

+-----+
| Endpoint1 |
+-----+
| INVITE (BASIC SDP+CLUECHANNEL) |
|----->
| 200 OK (BASIC SDP+CLUECHANNEL) |
|<-----|
| ACK |
|----->
|<#####>
| BASIC SDP MEDIA SESSION |
|<#####>
| CONNECT (CLUE CTRL CHANNEL) |
|=====|
| ... |
|<=====|
| CLUE CTRL CHANNEL ESTABLISHED |
|<=====|
| ADVERTISEMENT 1 |
|*****|
| ADVERTISEMENT 2 |
|<*****|
| CONFIGURE 1 |
|<*****|
| CONFIGURE 2 |
|*****|
| REINVITE (UPDATED SDP) |
|----->
| 200 OK (UPDATED SDP) |
|<-----|
| ACK |
|----->
|<#####>
| UPDATED SDP MEDIA SESSION |
|<#####>
|
v v

```

# CLUE MCU flow

- CLUE Hop-by-hop
- MCU acts as an aggregation point
- MCU modifies/combines CLUE Advertisements according to capabilities
- MCU generates CLUE configures based on received configures



# CLUE relation to PERC

- **PERC Charter:**

“...The meta information provided to the central device is to be limited to the minimal required for it to perform **its function to preserve the conference participant's privacy...**”

- Therefore CLUE metadata available to MDD needs to be minimized
- However, “enough” information is still required to be able to offer a telepresence experience

# CLUE relation to PERC: issues 1

- **Topology**

- MDD can only provide switching topologies, composition not supported. Implications on CLUE MaxCapture attribute and multi-content captures
- MCC policy attribute value “SoundLevel” can only be used with unencrypted end to end (can be hop by hop) sound level indication (e.g. RFC6464)

- **Media Manipulation**

- MDD cannot access encrypted media therefore cannot verify or filter out embedded text. Not possible to transform images etc.
- CLUE MDD can add own captures. PERC consumers need to ensure correct authentication before configuring these captures

- **Privacy**

- CLUE contains XCARD information about participants within captures. Advertisers may not want MDD to have access to this information.
- CLUE may contain proprietary extensions. May contain information not for MDD

# CLUE relation to PERC: issues 2

- **Encodings**
  - CLUE only has encodingID (used for correlation to SDP) and max bitrate
  - No need foreseen to add PERC specific encoding info
- **RTP stream to CLUE media capture mapping**
  - RTP/RTCP carry CLUE captureID.
  - MDD will need to modify RTP/RTCP and CLUE signalling to correlate the CaptureIDs
  - Therefore CaptureID needs to be unencrypted end to end.
- **Others?**

# Potential CLUE updates

- **Partially encrypt CLUE Advertisements**
  - Basic Structure of CLUE Advertisements remains
  - Only potential sensitive information is encrypted end to end
  - E.g. Information within CaptureScenes, Simultaneous Sets, People, mediaCapture (after encGroupIDREF) is encrypted
  - CLUE Configures unaffected
  - CLUE Options unaffected?
- **Others?**



# Discussion

- **Thoughts?**