# Encrypted Key Transport for SRTP draft-mcgrew-srtp-ekt-06

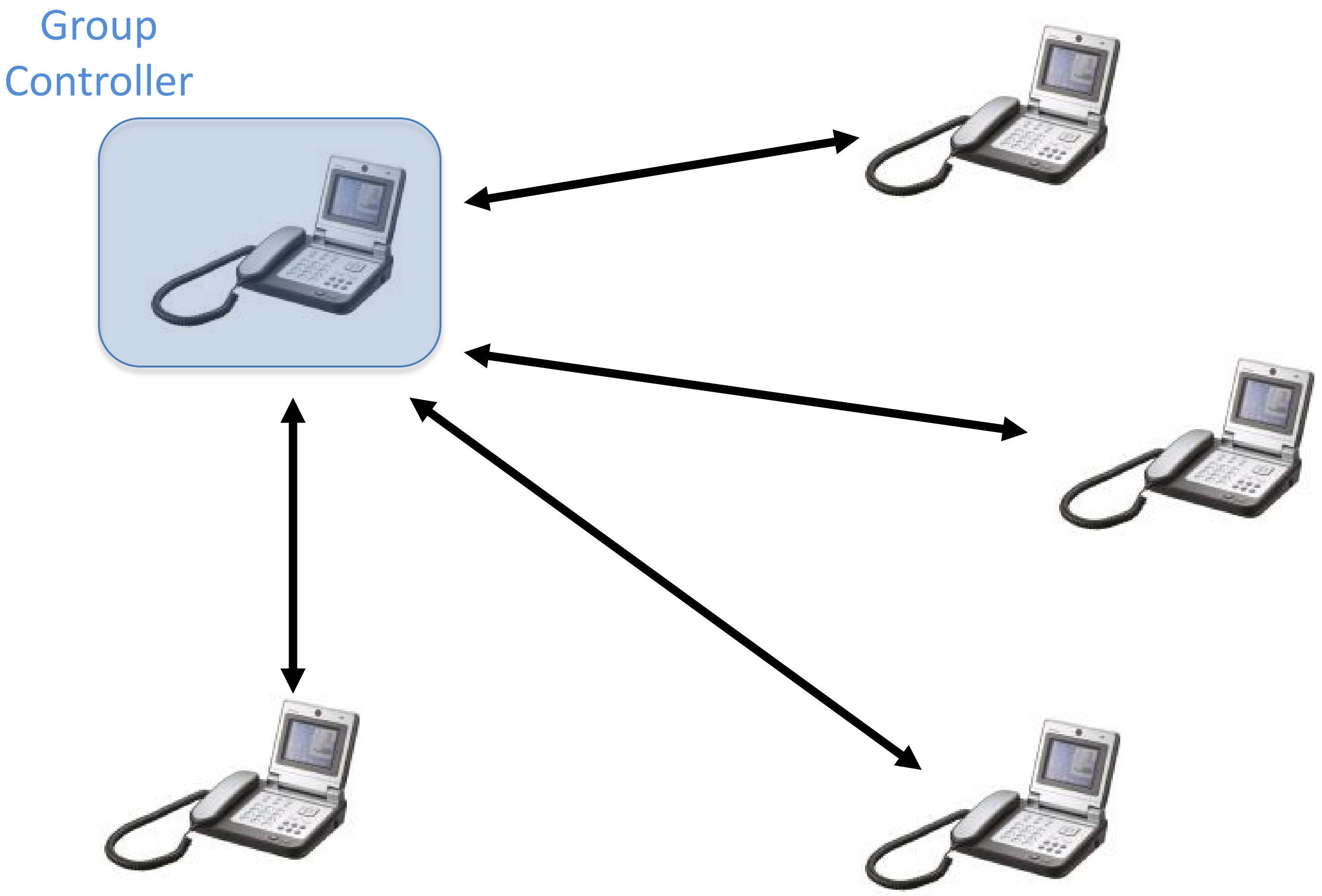
David McGrew, mcgrew@cisco.com

Dan Wing, dwing@cisco.com

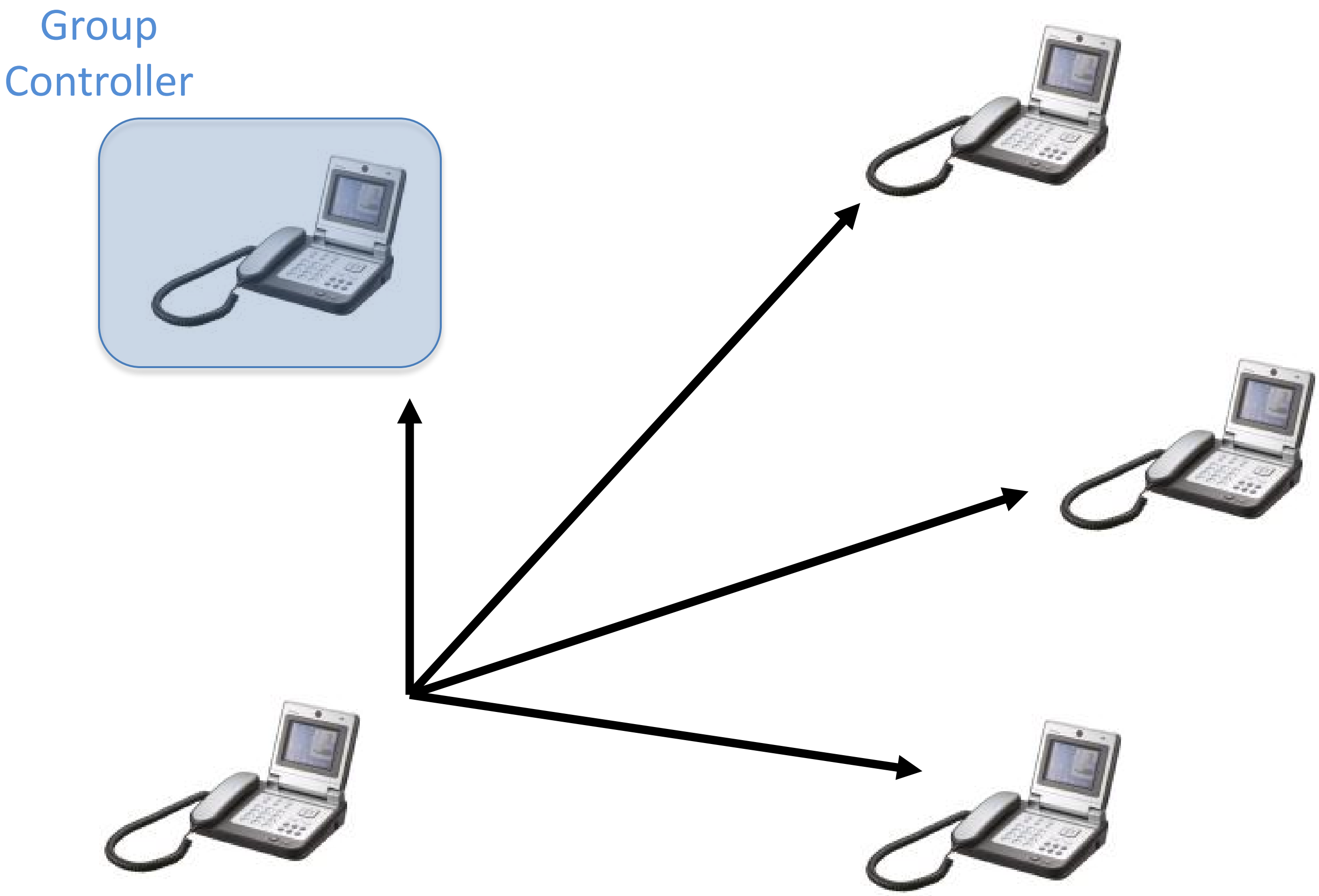
# Encrypted Key Transport for SRTP

- In-band key transport protected by separate RTP session-level key
  - Conveys SRTP master key and ROC
- Layer of indirection between Key Management and SRTP
  - Avoids layer violation
  - Key management should be oblivious to RTP Sources, SSRCs, Seq Nums, Rollover Counter
  - Indirection is important for large groups

# 1. DTLS-SRTP-KTR (1:1)



# 2. EKT (1:Many)



Group Controller

# Looking back and forward

- EKT defined 2006-2007
  - Expired pending implementation and interest
  - We now have both!
- EKT is only way to avoid layer violations
  - Essential for scalability to large groups

# EKT Changes

- Now fully described using DTLS-SRTP
  - DTLS-SRTP has better security than SDESC
  - DTLS-SRTP is IETF standard for SRTP keying
- EKT in an SRTP packet no longer an Appendix
  - Provides key and data for new speaker
  - Fate-sharing of key and data encrypted with that key
- WG item?