Negotiation and Extensibility

Cullen Jennings
fluffy@cisco.com
IETF 80

Why Negotiation of Algorithms and Extensions

- Addition of features, innovation, and fixes later
  - Example crypto agility: MD5 -> SHA1 -> SHA256
- Better Codecs over time
- Product differentiation

Negotiation Failures

- Client server allows the server to implement A and B then client to choose A or B (or visa versa)
  - Example: Email client does IMAP and POP, then server can choose to use either
- Peer to Peer has no client/server differentiation of capabilities
  - If two peers do not have at least one common capability, you do not have interoperability
  - Examples of problems:
    - XMPP File transfer: XEP 65, 95, 96, 47, 234
    - SIP DTMF: RTP (RFC4733), Info (many versions) , KPML
    - IPv4, IPv6

Probable Extension Points for RTCWeb

- Relay protocols: STUN, TURN, The Next Thing
- RTP Profile
- RTP Header extensions
- SRTP Crypto profiles
- Codecs
- Codec parameters
- Network Statistics: Packet statistics, RTCP,…
- Non audio/video media
- Possibly media signaling protocols (active discussion but no agreement)

Legacy VOIP Equipment

- Ideally new stuff would work with 100% of old stuff
  - This is not going to happen
  - Old stuff has less than 100% interoperability with other old stuff
  - Browser security will impose constraints
- Goal should be to
  - Find right balance of working with significant fraction of modern VoIP equipment
  - Minimize cost of interoperation gateways

Summary

- The solution will allow negotiation of extensions
- Working group will identify what parts of the solution need to allow for extensibility
- Working group will determine a balance between ease of interoperation with legacy VoIP equipment and practicality of browser deployment
- Working group will choose (to the best of its ability) enough of a baseline to ensure we do not have negotiation failures