Connecting Mobile Phones to the Internet Simply (CoMPIS)

IETF London
DISPATCH WG

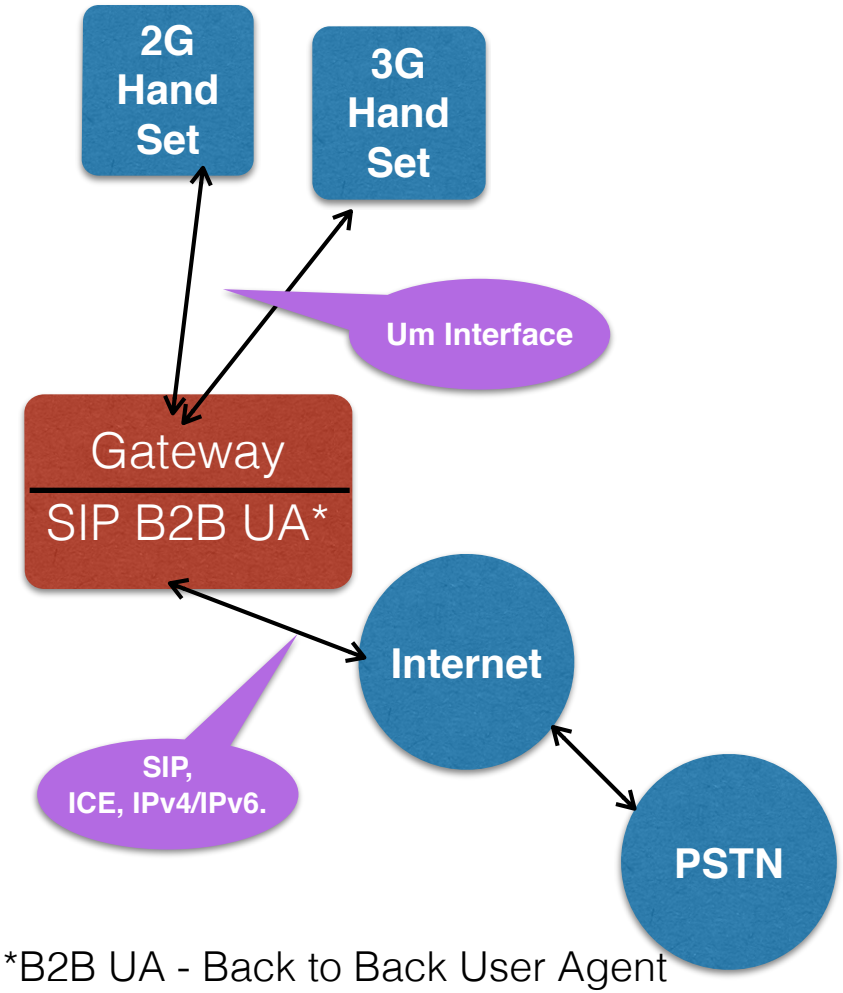
Jim Forster, Mike Iedema, Harvind Samra - Range Networks
Tim Panton

Problem Statement

- Many people have no mobile service. Cost of required infrastructure is apparently one barrier.
- Many of these are in locations with smaller user base than is typically sustainably served by existing architecture (BSC, MSC, HLR, VLR, Circuit mode L1,….)
- Can we just connect 2G/3G phones to the Internet?
  - Yes, OpenBTS & other solutions do this
  - Um, the Air Interface, is preserved. 1-2 Billion phones are supported
- Existing Code (OpenBTS) addresses this need, but is not documented outside of the running code
- We seek to document and improve on this in the IETF Community

Current OpenBTS Implementations

- Web Site: openbts.org
- Mailing list: openbts-discuss@lists.sourceforge.net
- Wiki: http://wush.net/trac/rangepublic/wiki
- Various Software Defined Radio (SDR) boards and systems



*B2B UA - Back to Back User Agent
- draft-ietf-straw-b2bua-taxonomy

Use Cases

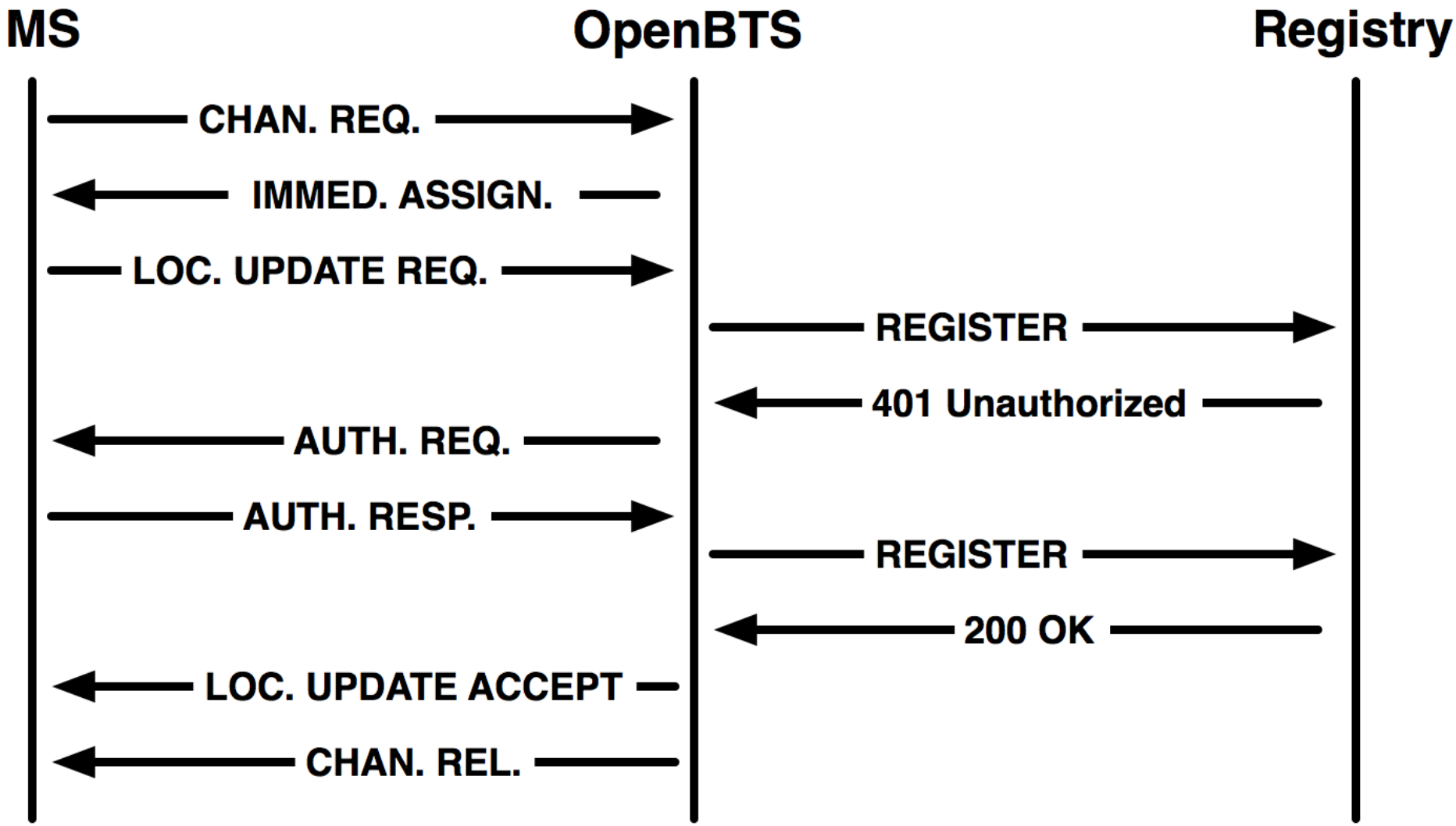
- Isolated locations w/ thin backhaul
- Disaster Response
- Private GSM Nets (licensed or non)

MIT Tech Review Article

GSM <-> SIP Mapping

- GSM Location Update Requests -> SIP REGISTER
- GSM Mobile Originated Call -> SIP INVITE
- GSM Mobile Terminated Call -> SIP INVITE
- GSM Emergency Call -> SIP INVITE
- GSM Mobile Originated SMS -> SIP MESSAGE
- GSM Mobile Terminated SMS -> SIP MESSAGE

GSM Location Update Request



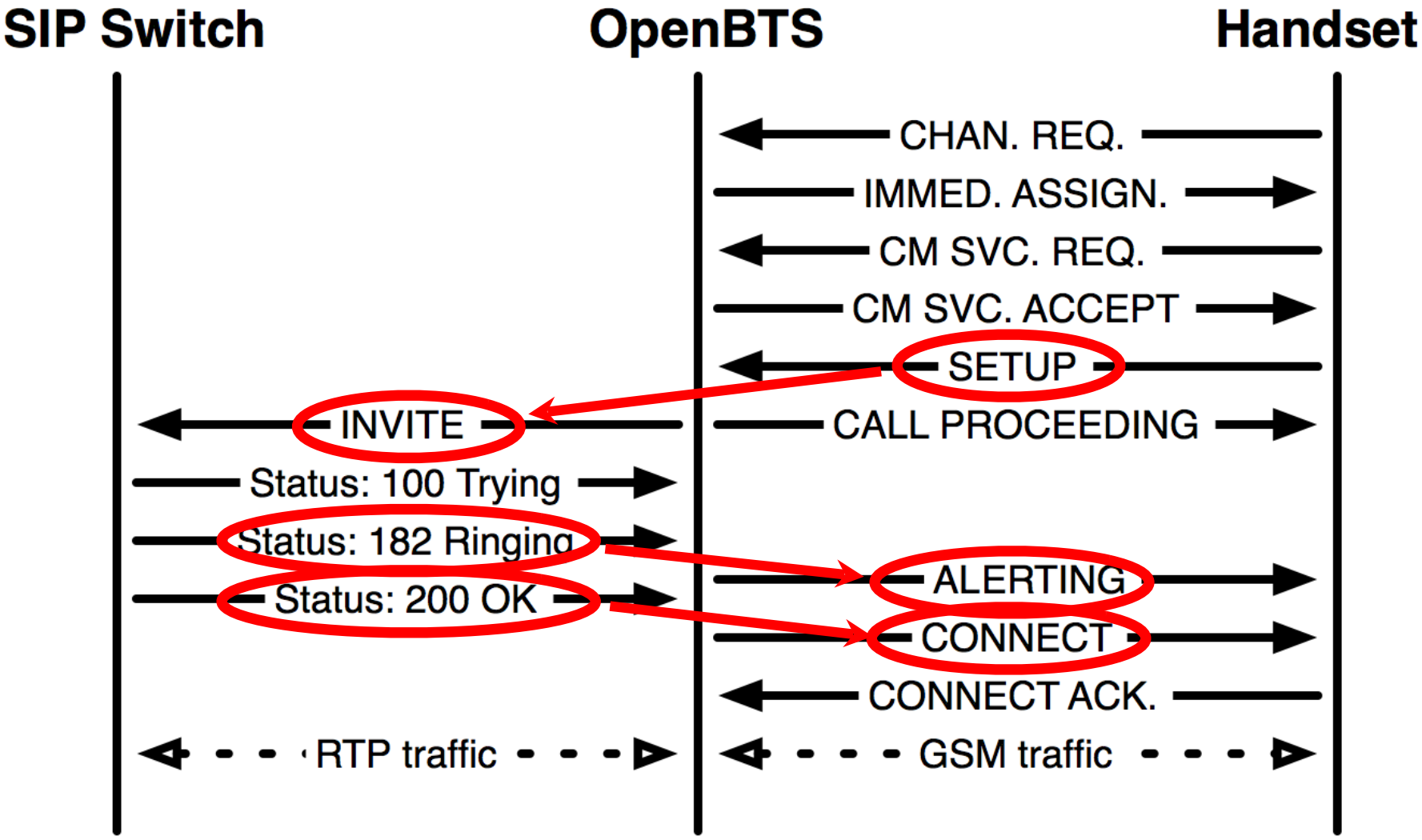
GSM Authentication

- SIMs given out for users
- Challenge-Response based on shared secret key Ki.
- Network generates 128-bit random string (RAND) to send to phone.
- Phone encrypts RAND with Ki and a hash function (A3) to produce SRES.
- Network performs identical SRES calculation with same RAND, Ki and A3.
- Phone returns SRES and network compares results.

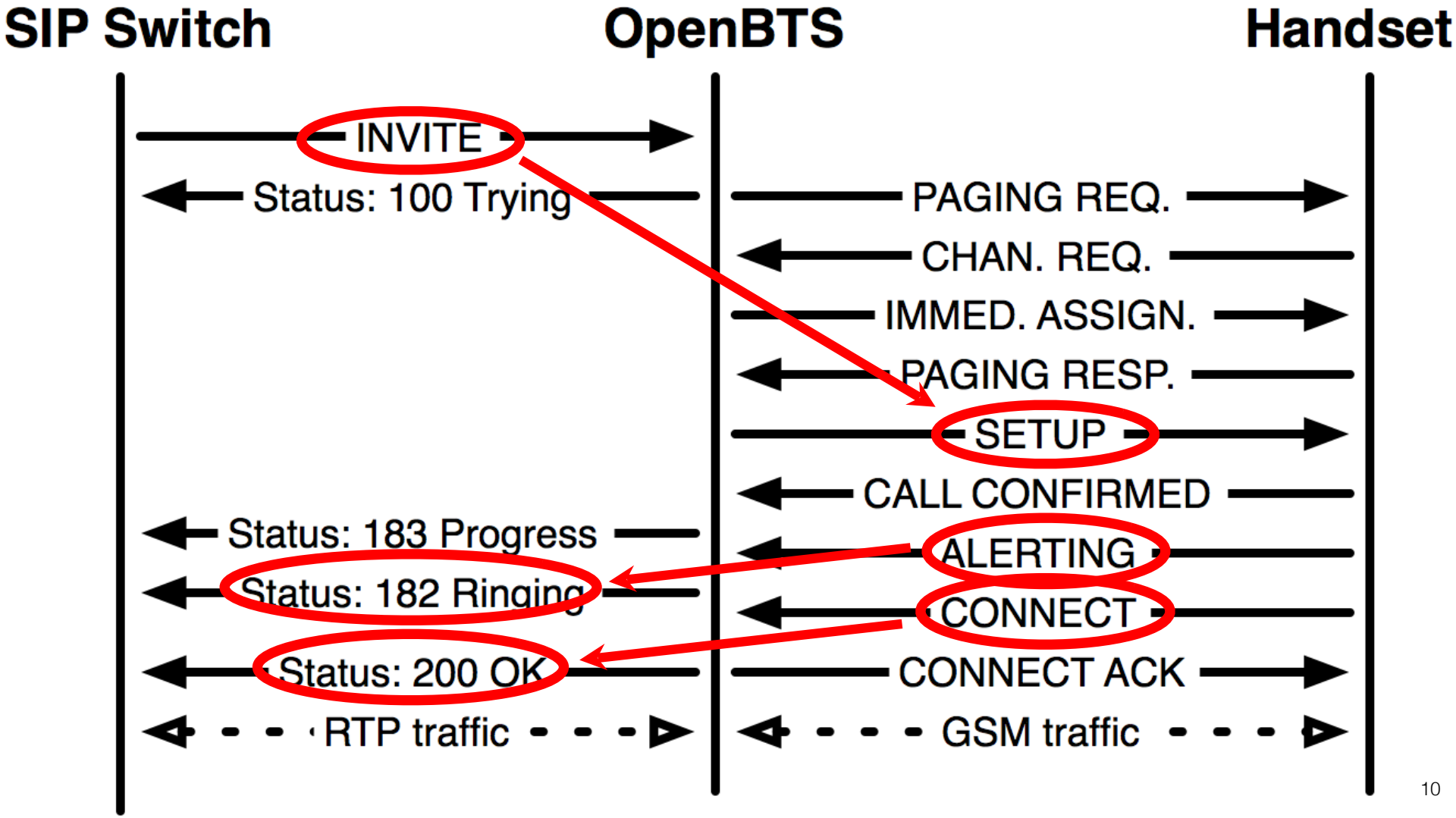
Mapped to SIP Authentication

- follows form of RFC-3261, Section 22 using:
- RAND as the NONCE
- A3 instead of MD5
- SRES as the RESPONSE

GSM Mobile Originated Call



GSM Mobile Terminated Call



Dealing With Network Issues

- OpenBTS is an IP endpoint. IP networks have different characteristics
- Current solution VPN – unsatisfactory extends core network trust to edge.
- Multiple NATS could be replaced by ICE/STUN/TURN
- Limited bandwidth -> long Ptimes or BUNDLE to cut header overhead
- Lossy Satellite or long range wifi link -> SIP over webSockets or TLS
- Insecure networks -> DTLS/SRTP
- Local browser endpoints on same wifi -> webRTC?
- Overall some common ground with WebRTC– scope for re-use ?
  (some deployments use RFC 5456)

What's not Being Proposed

- No Change to the Air Interface to Phones (Um)
- Not trying to replace IMS
- Not suggesting Rebel / Illegal operation
    - Usually licensed spectrum is required
    - Experimental licenses not so hard (.DE, .MX, .US..)
    - Unlicensed GSM bands in .SE; others?
    - Enterprise license (not public operator) licenses in .BR
    - Qualcomm advocating LTE in 5.8 unlicensed band
    - Existing GSM Bands are crowded in cities, but empty in un/underserved areas (white space)
- Not aimed to replace existing phone systems
    - For places without service

Work to be Done

- Document protocol used by existing code
  - Specify Call Control - SIP Mapping
  - Handover should be looked at closely
- Improve spec with IETF ICE for NAT traversal
- Security Review
- IPv6 Implementors Guide
- For further study
  - Invite contributions from WebRTC, etc.
  - How to convey other information, such as RRLP?
  - Roaming Interconnect Messages? MSRN Assignment, etc.