New Revision of the Interactive Connectivity Establishment (ICE)

draft-ietf-mmusic-rfc5245bis-00

IETF 88, Vancouver
November 4th, 2013

Ari Keränen
ari.keranen@ericsson.com

Updates in -00 WG docs

- Updated (IPv6) address selection
  - MUST NOT use loopback or deprecated candidates
  - MUST pair link-locals only with link-locals
  - SHOULD use OS API if available for priorities
- Clarified short-term credential usage
- SDP (still) split from the main spec

Open Issues

- Username fragment length
- Connectivity check pacing
- Extensibility
- Aggressive nomination bug
- Updated offer

ICE username fragment length

- Off-by-one issue: ice-ufrag up to 256 chars, STUN username max length 512, ufrag1:ufrag2 up to 513 chars
- Proposal: offer ice-ufrag with max len 255 chars, but accept 256 chars too

Check Pacing (Background)

- For non-RTP traffic, current min 500ms
  - (Overly) “safe choice” -> poor performance
  - Implementations seem to ignore the MUST
- Concerns
  - Should not create NAT bindings too fast (20ms seems to be limit; ongoing research)
  - Congestion control (checks should not consume more bandwidth than data)

Check Pacing Proposal

- MUST NOT set lower than 20ms
- RECOMMEND 50ms if no better knowledge
  - This is for congestion control, not NAT bindings
- MAY use information of the network and/or ensuing traffic to go lower than 50ms
  - Appendix of guidelines on this topic
  - Note: this is traffic type/application agnostic; giving formula for RTP but just as an example
- Negotiate pacing value in offer/answer: pick higher of the two (for concurrent checks)

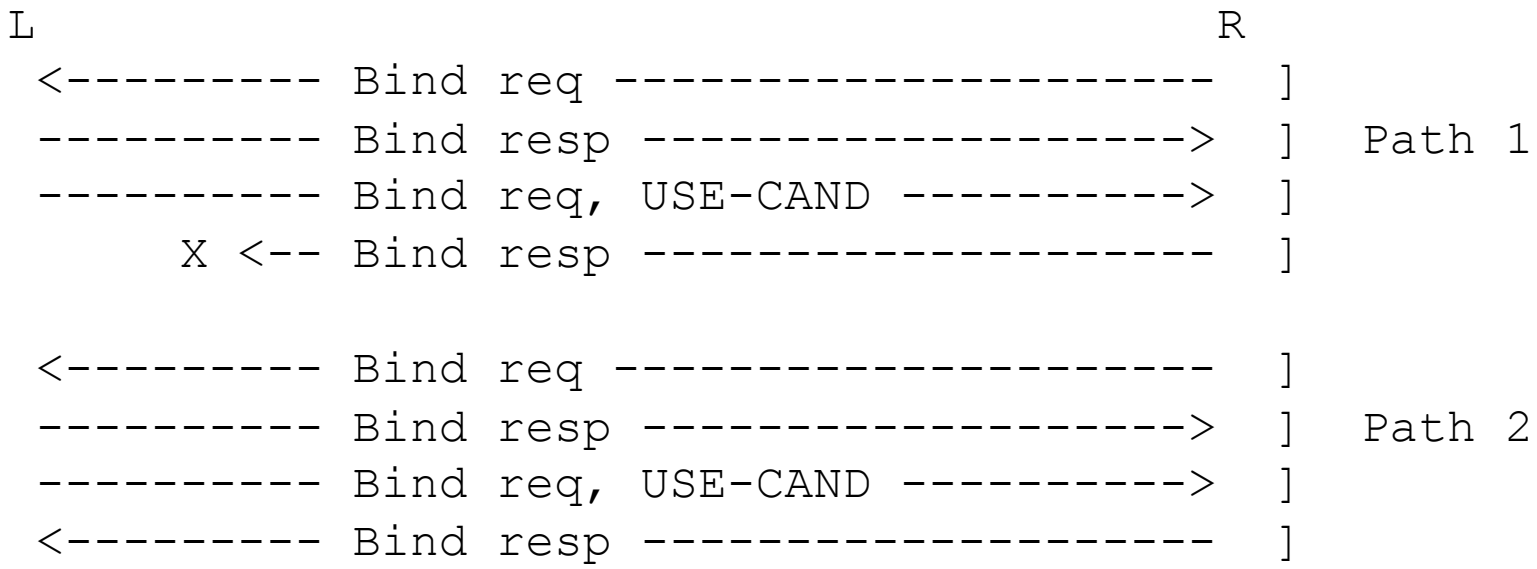
Extensibility

- Plenty of extensions to ICE discussed
  - Trickle ICE
  - Happy eyeballs
  - Mobility with ICE
  - MALICE
  - etc.
- Main way of extending ICE: ice-options
- Is this sufficient? Need something more in the base spec?

Aggressive Nomination Bug

- Two possible paths between L & R
- L controlling & using aggressive nomination; checking both paths concurrently
- Binding response for the first (higher priority) path does not make it back to L
- When L's check on 2nd path succeeds, L stops ICE processing and uses that pair
- R thinks the first path is being used

Aggressive Nomination Bug



Aggressive Nomination Bug Proposal

- Possible fixes
  - Keep re-transmitting checks on selected pair
  - Updated offer (if MUST always)
  - Detect application data or keepalives on wrong pair: update to that pair
    - allows attacker to select pair?

Updated Offer

- When ICE is finished, send new SDP offer/ answer with the selected candidates?
- Currently: only if different from default
  - i.e., the one in SDP m- and c-lines
- Pros for always
  - More consistent behavior for middle boxes
  - Helps with aggressive nomination
- Pros for never
  - Issues with 3rd Party Call Control and fax (draft-elwell-ice-updated-offer)

Updated Offer Proposals

- Proposal #1: always
- Proposal #2: never
- (#3 need more work?)