ICE

Jonathan Rosenberg
Cisco Systems
Changes since -08

• Connectivity preconditions to informative reference
• Removed remnants of ICE meta-protocol from intro – its about offer/answer protocols
• New terminology – server reflexive and relayed replace STUN-derived and TURN-derived

• Username randomness reduced to 24 bit minimum – not for security, for conflicts
• Password in separate a=ice-pwd attribute, shared for all candidates of all sessions
  – Reduces message entropy and size – more sigcomp friendly
Changes since -08

- Changed references to rfc3489bis from RFC3489
- Using behave terminology, not ‘symmetric’, ‘full-cone’, etc.
- Added diagram for explaining justification for a=remote-candidate

- Answerer can now use a candidate once validated, in anticipation of upcoming offer
  - Must revert to actual one in m/c line if timer fires after next expected offer
  - Only answerer can send – not offerer

- Still need to reliably deliver 183 w/ SDP – retransmit until STUN trick described
Why 183 needs to be reliable

INV (offer)

No permission yet!!

183 (early answer)

STUN check

Permission opened to UAS

UAC  NAT  UAS

183 needed to send STUN request to create permission

STUN check

STUN check

STUN check

RTP
Changes in -06

• Role of offerer vs. answer for derived candidates now inherited from generating candidate
  – Role dictates who sends updated offer (offerer)
  – Role dictates who can send early media (answerer)

• Previously, role was defined as
  – Agent sending STUN request that lead to discovery of new peer-derived candidate was offerer
  – Agent sending STUN response was answerer

• Why – see next slide
Case 1: UAC Behind APD Binding
NAT

INV (offer A-priv)

183 (early answer B-pub)

STUN check pair 1
A-pub

STUN check pair 2

RTP

(offerer,answerer)

(A-priv,B-pub) pair 1

(A-pub,B-pub) pair 2

A would be offerer from old defn

Media flows since B is the answerer for pair 2

UAC (A) NAT UAS (B)
Case 2: UAS Behind APD Binding

NAT

INV (offer A-pub)

183 (early answer B-priv)

STUN check pair 1

B-pub

STUN check pair 2

RTP

UAC (A)  NAT  UAS (B)

(offerer,answerer)

(A-pub,B-priv) pair 1

(A-pub,B-pub) pair 2

B would be offerer from old defn

Media flows since B is the answerer for pair 2
Changes since -08

• Agent must be prepared to receive RTP and STUN on each candidate
  – Not just one in m/c-line
  – Consequence of early promotion – no way to signal that STUN only can be received

• Incoming STUN request processed if prefix matches existing username
  – Deals with race condition – next slide
Username Race Condition

INV (offer A-priv, cid=U)

183 (early answer B-pub, cid=V)

STUN check pair 1 uname=V:1:U:1

A-pub

STUN resp pair 1

STUN check pair 2 uname=UV:1:V:1

UAC doesn’t know UV as a valid cid yet. But it accepts stun request since prefix is “U”

UAC (A)  NAT  UAS (B)
Changes since -08

- Added simpler example and updated larger example to use just TURN
- Jitter buffer adaptation triggered on receipt of marker bit or change in source IP
- Retransmit your STUN request when you get a STUN request
  - Speeds up convergence – see call flow next slide
Retransmit condition

INV (offer A-priv)

183 (early answer B-pub)

STUN check pair 1

A-pub

Permission opened to UAS

STUN check pair 1

Permission open – retransmit will succeed

UAC (A)  NAT  UAS (B)
Changes since -08

• If address gathering yields same derived address from different local address, then keep it
  – Complicated corner case, but it’s a real case
  – Impacts where you send STUN checks from – will send from both

• Next slide
Redundant Address Elimination

UAC Addresses
- 192.168.1.1:3344 from local i/f
- 10.0.1.1:2498 from other local i/f
- 10.0.1.1:2498 from stun server through 192.168.1.1
Open Issues

• None I am aware of
• Document ready for WGLC!
ICE-tcp Changes

• Defined three types of tcp candidates – active, passive, actpass
• Type of candidate is signaled in a=candidate line
• Local interfaces produce actpass and active
• STUN produces passive
  – Yes – for TCP!
• Relayed both active and actpass
  – With TURN – you obtain one candidate for actpass, separate one for active
• Pairings go as one would expect
  – Active with passive or actpass
  – Passive with active or actpass
  – Actpass with anything
• Why have actpass and active from local interface?
  – Simultaneous open can fail miserably
• With active candidates, port 9 and local interface are signaled
  – Discovered by p2p stun checks
ICE-tcp Changes

- TURN can provide both relayed and server reflexive TCP address
- Actpass candidates preferred over active and passive
- m/c-line contains native IP/port of candidate
  - Ephemeral IP/port for peer derived
- FSM for pairing states driven by STUN, not connection attempts
- For pairs where one side is active, actual pair goes into invalid and peer derived pair goes to active
- STUN-based keepalives used for TCP
- Generic demux algorithm defined
ICE-tcp Status

• No known issues – needs review
• Ready for WGLC?
  – Should ideally go jointly with ICE to make sure its all in sync