# ICE

is nice

Jonathan Rosenberg

Cisco Systems

# Much has transpired since last meeting

- ICE-10 with massive rewrite and simplification in August
- Formation of a design team to review and complete work
  - Myself, the chairs, Philip Matthews, Eric Cooper, Francois Audet, Rohan Mahy, Eric Rescorla, Tim Moore, Derek MacDonald, Cullen Jennings
- List and weekly conference calls
- ICE-11 and ICE-12 released with results of consensus

# Changes from -11 to -12

- Passive and controlling modes for sessions
  - STUN USE-CANDIDATE flag to signal when checks are done
  - Set by controlling agent
  - When done, passive side ceases checks and uses selected candidates
- “Passive-Only” mode
  - Signaled in SDP
  - ICE aborts when both sides are passive

# Changes from -11 to -12

- Updated offer sent by controlling agent
  - Only if selected candidate pairs don't match m/c-lines
- ICE restarts defined
  - Change in username
  - Can change role
- Media Transmission Rules
  - Bidirectional media allowed once ICE checks complete
- No recommendations on behavior when ICE checks fail

# Changes from -11 to -12

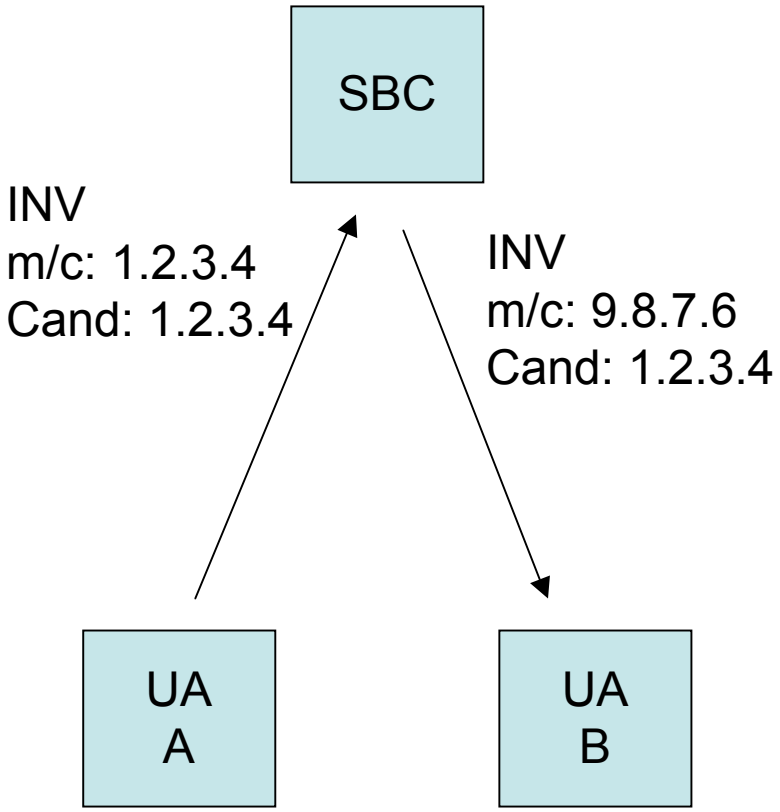
- ICE works with 3pcc flow III now
- DSCP markings in ICE match media

# Remaining Open Issues

- Biggest one: SBC and ALG considerations
- To some degree there is a new requirement lurking here
  - Allow calls to work through broken ALGs
  - Allow SBCs to be bypassed when ICE is on both sides

# Current ICE Behavior

- If ICE “detects” an ALG or SBC
  - m/c-line doesn’t match a candidate line
- ICE aborts, and acts as if one side doesn’t support ICE
- If ALG is “broken” call won’t work



# Whats the Alternative?

- ICE endpoint can ignore m/c-line and proceed with ICE negotiation
- Two cases
  - SBC
    - Some SBC will hang up call if they don't see media
    - Some SBC will block STUN on the RTP ports
    - So ignoring the m/c-line is dangerous
  - ALG
    - Fewer issues with ignoring their m/c-line
    - But TLS also fixes their issues
  - Problem: don't know which case you are in

# Proposed Path Forward

- It is not in our scope to fix problems with ALGs and SBCs
- The ill-defined behavior of these boxes makes working around them hard
- TLS is the best fix for the broken ALGs
- If you don’t want to always use TLS, then fallback to it only when ALG is detected
  - When answerer aborts because m/c-line doesn’t match, include an SDP attribute to flag that this has happened (a=ice-mismatch)
  - Offerer notices that answerer supported ICE but didn’t use it – probably because of ALG. Now revert to TLS.

# MacDonald-2

- Where to put text on ICE-for-gateways?
- Currently, its in two places
  - Throughout the normative text, different rules for passive-mode and regular mode
  - An appendix which summarizes
- This has not worked very well
  - Still need to read and understand whole document and extract ICE gateways processing
- Proposal
  - Separate behaviors on a section by section basis
  - Remove appendix – separate informative document that runs through it so you don't have to read ICE
    - We'll need to verify it doesn't conflict

# Issue #10: ICE Hammer

- ICE itself can cause a flood of packets in the form of checks
- They can come as fast as once transaction every 20ms
- What should we do about it?
- Possibilities
  - Limit number of candidates per stream
  - Candidates can’t share an IP address
  - Rate limit checks
  - Limit number of outstanding checks with no answer
- Proposal: Time limit ICE checks to 100 total checks by default (2 seconds in current timers)

# Issue #11: ICE Pacing

- Should we send ICE checks faster, at media rate?
- Proposal: no – leave these kinds of optimizations for the future

# Issue #12: Retransmits

- In ICE, retransmits fall into one of two modes
  - Never succeed because connectivity doesn't exist, so retransmits are needless
  - Eventually succeed because there was packet loss
- Consequently, number of retransmits is nearly bimodal
- Idea is, to reduce retransmits since they are ususally needless
- Proposal: don't do this

# Issue #15: Obfuscating ICE candidates

- Worries about generic ALGs modifying ASCII-coded IP addresses in body of SDP
- Can change encoding to replace the period with a comma (1,2,3,4 instead of 1.2.3.4)
- Proposal: this is ugly, rather run TLS

# Holmberg-1

- Some way of learning the STUN server from a REGISTER response
- I haven’t really understood this issue

# Holmberg-6: Reliable Provisionals

- The bit about retransmitting 1xx until STUN arrives is a hack
  - But helpful
- I think we have the following conclusion from the list:
  - SHOULD use PRACK if its available
  - Don’t hang up call of STUN never arrives
  - When you send 200 OK, stop 1xx retransmits

# Sinnreich-1

- Want to remove section on QoS, which motivates the related-address
- Have also been waiting for some additional text from Packetcable to help clarify it
- Propose to keep

# Keepalives

- DOCSIS and Wimax issue – can't send keepalives if there is media traffic – only do it during silence
  - Even then, can't be request/response in case the other guy has traffic in progress!
- Another issue – if you can explicitly control the bindings, the timing is different
- Proposal
  - Loosen requirement to only require keepalive when no other traffic has been sent
  - Use Binding Indication
  - Timer can change if you can control NATs

# ICE-TCP

- -02 is almost a complete rewrite based on the new algorithms introduced in -10 onwards
- Good news: ICE-TCP is now pretty much identical to regular ICE

# Functional Changes

- Added TLS support as well
- SDP/ICE transport protocols are “tcp-so”, “tcp-act” and “tcp-pass”

# Open Issues

- Treatment of TLS as a separate transport protocol is a bit odd
  - If TCP succeeds, you have connectivity and can run TLS (in theory)
  - Main concern is deep-packet inspecting devices
- Needs review!

# The Plan

- Issue ICE-13 next week or so with required changes
- Begin WGLC on ICE
- ICE-for-gateways comes out in a few weeks
- Really want to complete core ICE and send to IESG prior to the holidays next month
- ICE needs to be finished more than anything else!