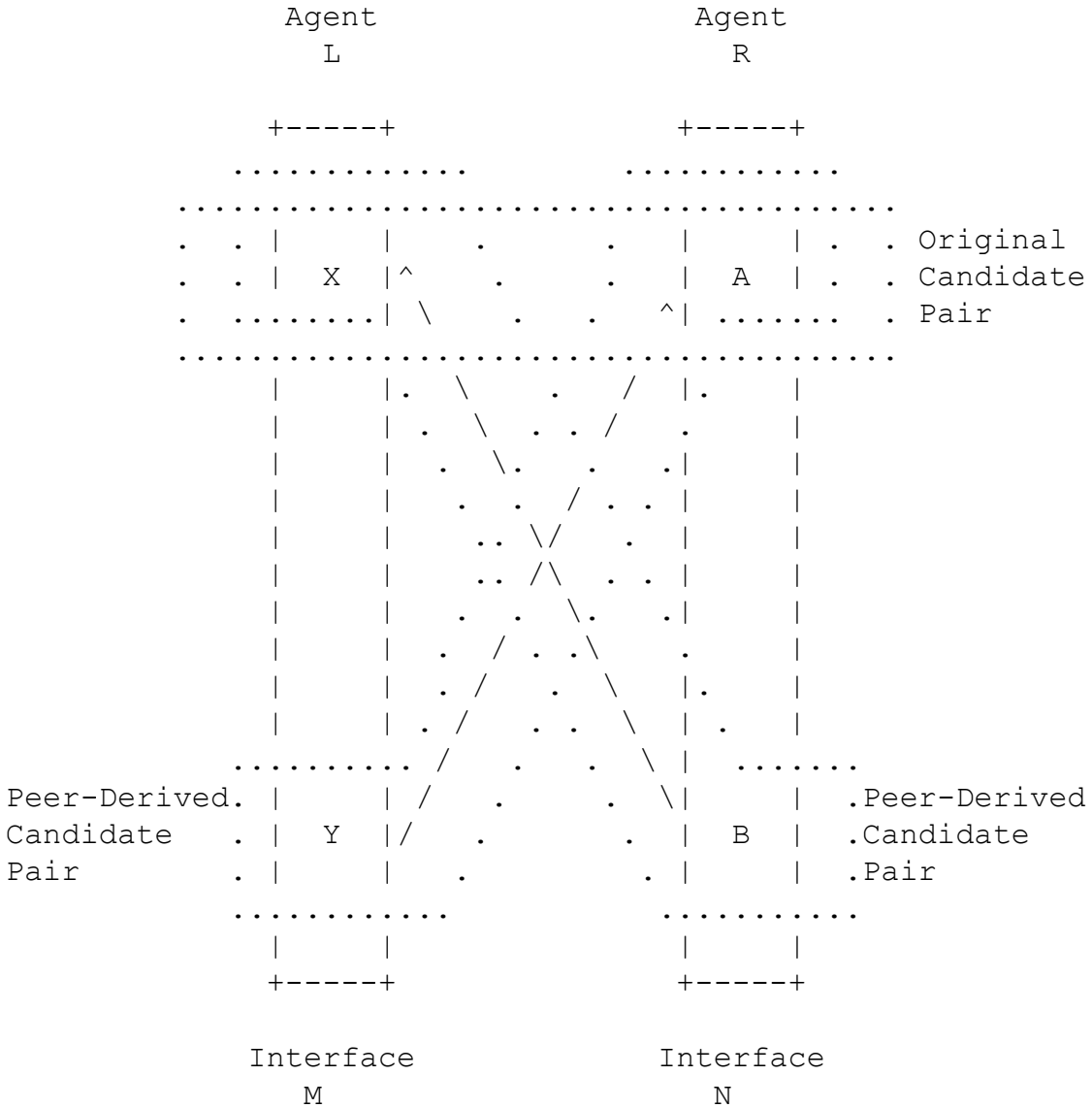
ICE

Jonathan Rosenberg
Cisco Systems

Changes since -05

- A lot of blood, sweat and tears
- Split out tcp into separate draft
- Call out processing that is transport specific and where new transport protocols need to say something
- ICE-tcp fits in much more naturally – transport address pair = connection (next slide)
- Added password component back into a=candidate
- Added a=candidate extensibility
- Added large call flow example
- Added complete security considerations section
- Improved state machine diagram
- Added terminology, consistent use of it

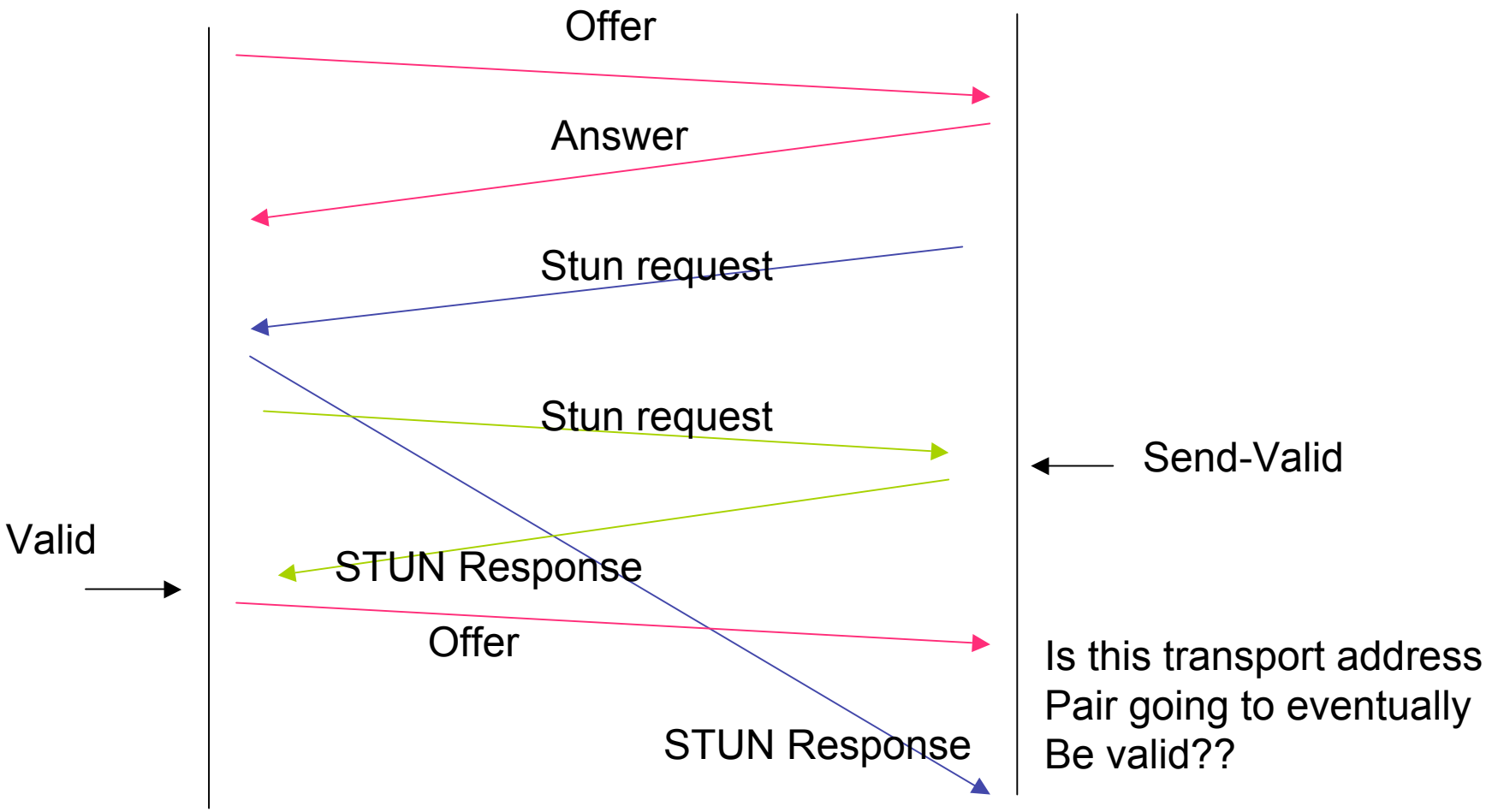
ICE-TCP Model



Changes since -05

- Removed extra SP at end of candidate grammar
- More general keepalive behavior – have to send something your peer understands
- Remove normative no-op, silence references
- Added notion of a component (Magnus' transport group)
- Different number of components in a pair is allowed
- RTP/RTCP recommendations on components
- Major change: rate limiting
  - TURN allocations only from one interface
  - Allocations paced 1 every 50ms, sequenced by priority
  - A=remote-candidate to solve race condition (next slide)
  - Connectivity checks paced out 1/50ms, in priority order
  - Priority determination algorithm

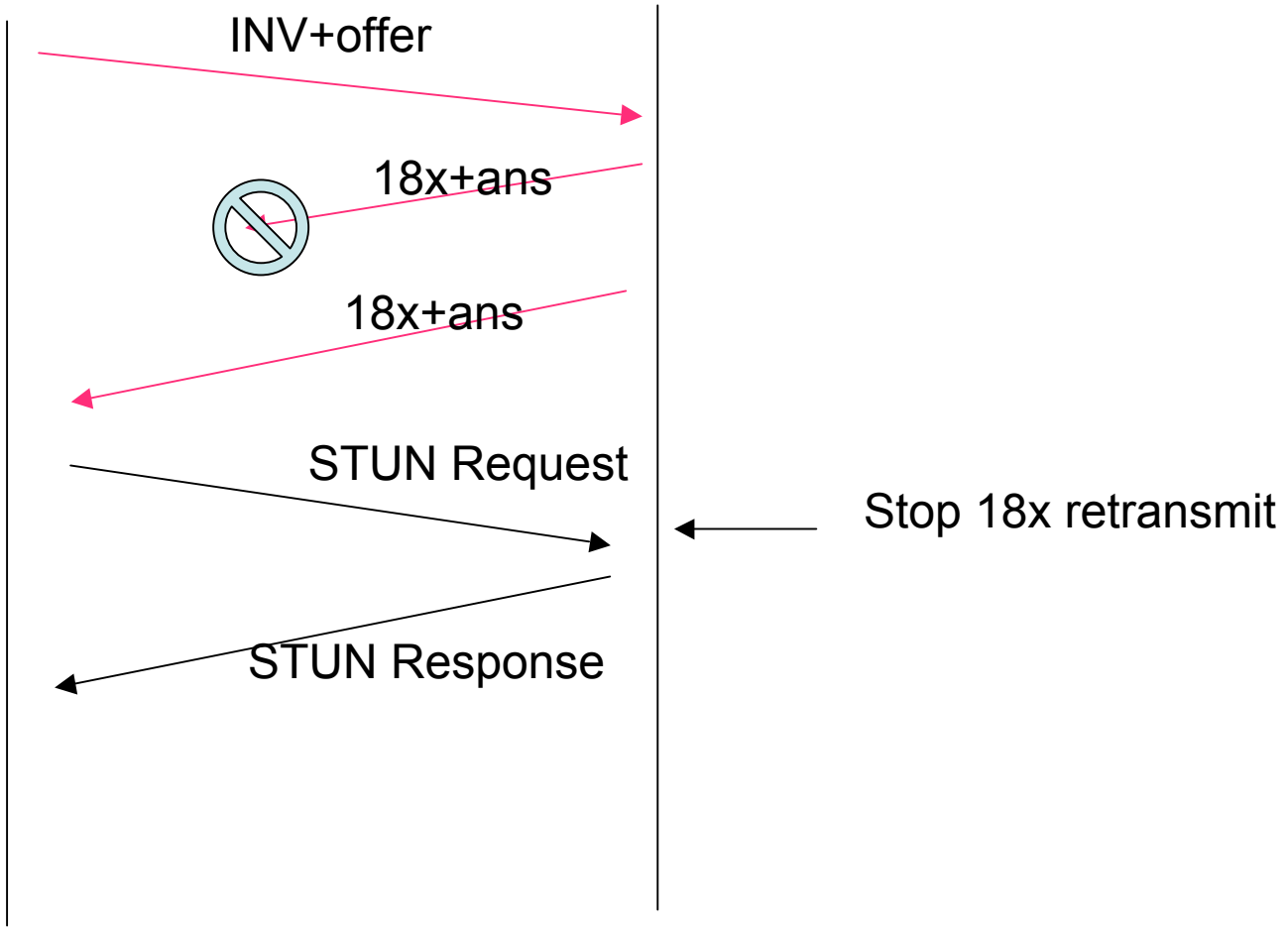
Race Condition



Changes since -05

- Addr production based on 3266 for v6
- Candidate-id to base64
- Removed connectivity preconditions discussion
- SIP Mapping discussed
  - PRACK and UPDATE recommended
  - Mechanisms for non-PRACk/UPDATE implementations – retransmit 18x until Binding Response

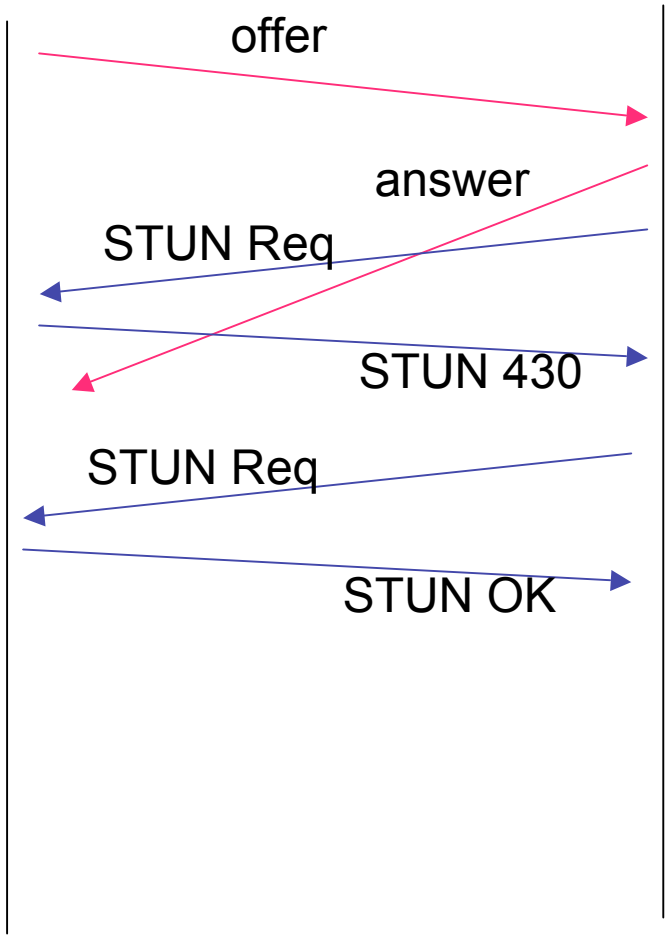
Non-PRACK Solution



Changes since -05

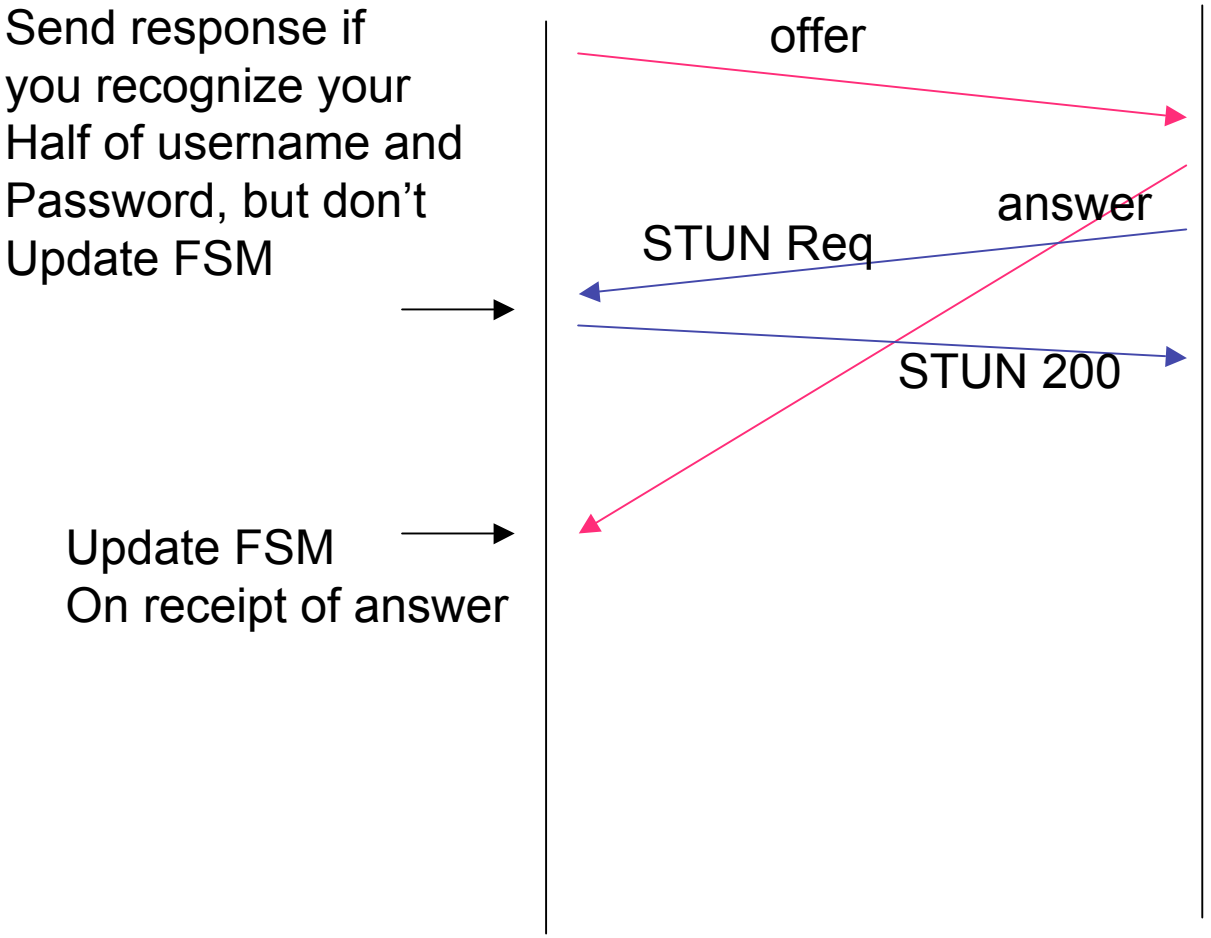
- STUN Binding Request received over TURN – MAPPED-ADDRESS is the one on the relay
- Usage of a=inactive to skip active candidate described
- Prefer peer-derived over STUN-derived addresses of equal priority - security
- Elimintated 430 response to STUN Binding Response and race condition

ICE-05 430 Case



Drawbacks:
- Wasteful bandwidth
- Doesn't differentiate case where stray Request is received

ICE-06 Solution



Open Issues

- RFC3489bis dependency change
  - Will result in some terminology shift
  - Removal of text recommending against including CHANGED-RESPONSE
- RTCP Optimizations
  - Lots of call flow messages to test RTCP, because we include it
  - Can do better by omitting it, once candidate is selected, add it as another candidate of the same type, then promote
    - May add another round trip in symmetric nat case

Magnus' Issues

- T1: Different local transport addresses yield the same derived transport address – should use that candidate
  - Can this happen?
  - If it does, not clear its helpful to keep them
- T2: Do we REALLY need 128 bits of randomness? Will yield candidate IDs and passwords of 22 characters
  - Three things we need candidate ID uniqueness for
    - Identifier for candidates from same peer
    - Handles connectivity checks sent to wrong UA
    - Resolve conflicts in prioritization algorithm
  - Password requires randomness for security
  - Proposal
    - Reduce bits in candidate to 32(?)
    - Share password across candidates – separate attribute

Magnus' Issues

- T3: Is TURN allocation done from same local transport address as STUN?
  - YES. This used to be different, but no longer
- E3: Definition of lexicographic order
  - Anyone know a good reference for this?