Connection Migration

January 2018, Melbourne

What's Covered: Implicit and Explicit Migration

When new IP is available, endpoint explicitly migrates

When NAT rebinding occurs, endpoint implicitly migrates

NAT rebinding is seen as migration by peer

- Cannot be privacy preserving
- Peer may choose to not validate new address

Peer cannot *know* NAT rebinding from explicit migration

- Cannot punish endpoint for not preserving privacy

What's Not Covered

Sending data from/to multiple IPs at the same time

Maintaining multiple congestion control and loss recovery contexts

Key Principles

1. Probing and Committing are separable events
   a. Committing: sending data from/to an IP address

2. Interface use is a local policy decision
   a. When possible, support peer's ability to choose.

3. Endpoint MUST validate peer ownership of new IP
   a. MUST limit traffic while validating

4. Endpoints SHOULD verify PMTU over new path

Building Blocks

1. PATH_CHALLENGE / PATH_RESPONSE frames
   a. Carries/echoes 12 bytes of random
   b. Not reliable, but sender may send new ones (perhaps using timer)

2. New Address Validation
   a. Endpoint sends PATH_CHALLENGE frame to peer's new IP
   b. Not retransmitted, but sender may send new PATH_CHALLENGE
   c. Peer responds with PATH_RESPONSE

3. PMTU verification
   a. Both directions should carry full-sized packets for verification
   b. Send PATH_CHALLENGE / PATH_RESPONSE in full-sized packets

Connection Migration Process Overview

1. Endpoint wishes to use new local IP
   a. Sends PATH_CHALLENGE or new data from new IP
   b. May send PATH_CHALLENGE to “prime” new IP and data later
   c. When data is acked, endpoint considers migration complete

2. Peer commits when data is received from new IP
   a. When peer receives probe packet, responds with probe, but continues sending data to old address
   b. When peer receives data packet, commits to this address
   c. (caveat: packet number must be largest seen)

Connection Migration Process Overview

3. Peer initiates validation at its earliest since rate limited
   a. If validation does not complete within *n* RTOs, *peer MUST return to previous validated address*
   b. When validation is complete, peer considers migration complete

4. PMTU verification happens along with probe packets
   a. Initiating endpoint need not verify PMTU, since peer will validate

Congestion control / loss recovery

- Single congestion controller and loss recovery context
  - Congestion control and RTT params reset on use of new IP
- All data and PATH_CHALLENGE / RESPONSE frames are subject to congestion control limits
- Reordering of probe frames with data, due to different path latencies, may cause spurious loss detection
  - May cause cwnd reduction during probing, but reset imminent
  - Proposed fix: Call this a potential perf issue during migration. Implementations may do something smarter.