IETF-60 MMUSIC WG

RTSP NAT Traversal Update

draft-ietf-mmusic-rtsp-nat-03.txt

Magnus Westlund (Ericsson)
Thomas Zeng (PVNS, an Alcatel company)

Update Since Last Version (-02)

1. Removed dependency on New RTSP CORE (RFC2326bis)
2. Added 5th candidate NAT Solution: variation of Symmetric RTP
3. Added comparison of five NAT solutions against the requirements that have been agreed upon during IETF-58
4. Added the reference to the newer STUN spec (RFC3489bis)
5. Added text on the threat of dual-hosted client using RTSP servers for DDOS attacks
6. As agreed in IETF-58, the first proriority is the NAT solution for RTSP servers in the open

Recap: Requirements On RTSP NAT Solutions

1. MUST work for all flavors of NATs, including symmetric NATs
2. MUST work for firewalls (subject to pertinent FW admin policies), including those with ALGs
3. SHOULD have minimal impact on clients in the open and not dual-hosted
   - For instance, no extra delay from RTSP connection till arrival of media
4. SHOULD be simple to implement and administer that people actually turn them on
5. SHOULD authenticate dual-hosted client transport handler to prevent DDOS attacks

New Candidate: A Variation of Symmetric RTP

- Based on already deployed RTSP services
- The procedures are very similar to Symmetric RTP:
  1. **RTSP client behind NAT initiates UDP traffic with one or more NAT probing packets to the server's UDP send port pair (RTP and RTCP)**
  2. **RTSP server performs address and port translations using the received probing packets**
     - Identify client based on the SSRC in the probing packet
  3. **RTSP server sends RTP and RTCP streams to the translated address and port pairs**
  4. **For keep-alive, probing packets are sent periodically even during RTSP PAUSE**
  5. **Probing packets DO NOT use RTP header**
  - Hence this scheme is NOT symmetric RTP
  - Probing packet can be extended (e.g., version 2) to carry digital signatures to perform receiver challenge/response so as to meet requirement 5

Overview of 5 Candidate NAT Solutions

1. **STUN (Simple Traversal of UDP thru NATs, rfc3489)**
   - Not designed for Symmetric NATs
2. **ICE (Interactive Connectivity Establishment)**
   - ICE implementation MUST implement STUN and TURN
3. **Symmetric RTP**
   - No RTP payload number and payload format available, unless negotiated via RTSP
4. **Variation of Symmetric RTP**
   - Doesn't require payload number
   - Still needs a format for probing packet
5. **TURN (Traversal Using Relay NATs)**
   - Is necessary if both RTSP server and client are behind NATs

Disadvantage of Symmetric RTP

1. Need new payload format (rtp-noop?)
2. Need to negotiate dynamic PT number
    1. Unless a static number can be found

Pros and Cons of ICE

1. Pro:
   1. Solves general problem where RTSP server can also be behind NATs
   2. Solves also receiver media transport handler authentication
   3. Line up well with SIP: one “framework” kills two (or more?) birds
2. Cons:
   1. Depends on TURN: potential long delay before TURN becomes a standard
   2. Need more signaling extensions to RTSP
      - ¬ Need new parameters in RTSP Transport header
   3. Potentially complex to implement
      - ¬ Has anyone implemented ICE?

Comments on ICE

For ICE to be a viable RTSP NAT solution the following needs to be done:

- Remove the “MUST” dependency on TURN
  - So that timing is more accommodating to market demand
  - So that the requirement 4 (easy to implement and administer) is met
  - Since TURN is not needed when RTSP server is in the open

Moving Forward

1. At some point, IETF MMUSIC WG needs to recommend a common RTSP-NAT solution in order to meet market demand
   - ¬ The sooner, the better, otherwise de-facto standards will take hold
2. To-do:
   - ¬ Coordinate with the author of ICE to ensure timing
   - ¬ Work on mapping ICE to RTSP
     - Magnus has started the work