Update of RTSP

draft-ietf-mmusic-rfc2326bis-03.txt

Authors:

Henning Schulzrinne / Columbia University
Robert Lanphier / Real Networks
Magnus Westerlund / Ericsson (Presenting)
Anup Rao / Cisco

Outline

- Goals of work
- Work since Atlanta
- Extensions
- Updates Made
- Open Issues
- Ad-hoc meeting & Next Teleconference
- Links

Goals

- Update RTSP so that it is:
  - Works and is implementable
  - Interoperable
  - Has clear rules for extensions.
- Go to draft standard
  - May require a new proposed standard (Not decided)
  - Perform Interoperability tests of all functionality in updated specification.
- Have finished the core specification by October.

Worked performed since Atlanta

- Restarted the teleconferences
  - 5 telephone conferences since December.
  - Covered substantial amount of issues.
  - Participants volunteer to provide updated text on issue basis.
  - Decisions and proposed updates has been sent to MMUSIC list in form of minutes and proposals.
- Published an update draft, version 03.
  - Updates will be presented on following slides.
  - Still not consistency checked enough.
  - Needs update of most examples.
  - Lack of editor time. Volunteer needed.

RTSP and Extensions

- Minimal Core Specification:
  - Definition of the protocol idea.
  - Play-back of media support
  - Rules for how to extend RTSP
- Existing extension proposals
  - NAT traversal for RTSP (draft-ietf-mmusic-rtsp-nat-00.txt)
  - MUTE and UNMUTE (draft-sergent-rtsp-mute-00.txt, expired!)
- Proposed extensions
  - RTSP MIB
  - Record functionality
  - RTSP message transport security, i.e. rtsps
  - Unreliable transport of RTSP messages, i.e. rtspu

RTSP Updates in -03, part 1/5

- Non-persistent connection support a requirement.
  - Reliability issue
  - If client is disconnected server can't reach client.
- IPv6 support in protocol.
- Accept-Ranges as proposed in core spec.
- Byte ranges will be allowed.
  - Not edited in yet.
- Via header will not be changed to include client address.
- Use of 304 “Not Modified” clarified:
  - Does not work as the other 3rr codes.
  - Applies only to the resource that method deliver.

RTSP Updates in -03, part 2/5

- Redirect clarified:
  - Inclusion of session header in request makes difference to scope. Without session header, request is single-hop and all sessions on that connection is affected.
  - Use of Location clarified.
  - Can be used to inform clients that a live session has ended.
  - Can be sent any time as long as a transport connection exist.
- Agreed on feature extension mechanism:
  - Require, Unsupported as in RFC 2326.
  - Proxy-Require changed to only apply to proxies.
  - Supported header added.

RTSP Updates in -03, part 3/5

- Destination header:
  - Strengthen language. Requires knowledge by server that client are allowed to send to this address if different then RTSP connection address.
  - Is a security issue due to Denial of Service attacks.
- Added two parameters to Transport header:
  - “dst_addresses” and “src_addresses”
  - General usage for any media transport.
  - Allows for explicit addressing of any number of addresses. Depends on media transport on how to interpret.
- RTP-Info’s Base URL is PLAY request URL.

RTSP Updates in -03, part 4/5

- Interleaved usage has been clarified:
  - Server sets the channels to use.
  - Client suggests, but will mostly be ignored.
  - Proxy may renumber
  - Each channel is symmetric
  - Resolution edited in only partially.
- A SETUP to change transport parameters leaves the previous state intact if request fails, i.e. unless a 2xx reply is received. (Not edited in yet)
- Clarification that RTSP URLs are cases sensitive. (Not edited in yet)

RTSP Updates in -03, part 5/5

- Range header now required in all PLAY responses
- Range is formulated as start point (inclusive) to stop point (non-inclusive).
  - For "Scale=-1" the start point will be larger/later than stop point.
  - For positive scales start point may not be larger/later than stop point.
  - Clarification needed (not edited in yet).
- Use of PAUSE when in Ready state (not yet edited in)
  - Is allowed and shall result in 200 responses if request otherwise OK.
  - Solves backwards compatibility problems.
  - Does not have any effect of state as already in target state.

Open Issues 1/3

- RTSP extension registrations and requirement levels
  - Feature tags: First come, first served basis.
  - Methods: IETF Standards Action
  - Headers: Public Specification
  - Status Codes: IETF Standards Action
  - Transport header parameters (5 sub registries):
    - Transport protocol: Public Specification
    - Profile: Public Specification
    - Lower Transport: Public Specification
    - Transport Modes: IETF Standards Action
    - Parameter extension: Public Specification (Not in draft yet)
  - Cache directives: IETF Standards Action

Open Issues 2/3

- Removal of timed requests
  - Issuer of Request does not know at the time of execution if request succeed or fails.
  - Problem of producing response headers, e.g. RTP-Info a head of execution time.
  - Is it allowed to have multiple outstanding to create queued behavior?
  - Lack of implementations.

Open Issues 3/3

- Handling of multiple SSRC in RTSP.
  - To provide synchronization between different SSRC space other than RTCP extension to RTP-Info will be needed.
  - Multiple SSRC in Transport header?
  - Use cases are: RTP retransmission, Multiple sources for live transmissions.
- Include Warning header
  - Provides extended reporting on problems, both no fatal and fatal.
  - Exist in both HTTP and SIP.

Ad-hoc meeting

- Had one on yesterday evening (Sunday) at 21.00-23.15.
- Will have one more at:
  Monday (Today) 13.00-15.00, Lobby Bar.

Next Teleconference

- Wednesday, April 2, 18.00 CET.
- If you want to participate, send mail to:
  magnus.westerlund@era.ericsson.se
- We will discuss latest draft version.

Useful Links

- Read and log Bugs:
  http://rtspspec.sourceforge.net
- Teleconference minutes + more stuff:
  http://rtsp.org
- Discussion:
  MMUSIC mailing list mmusic@ietf.org

RTSP and NAT

draft-ietf-mmusic-rtsp-nat-00.txt

Magnus Westerlund

Ericsson

Introduction

- The draft covers potential ways of having RTSP traverse one or more NAT.
- The problem does not exist for the control signaling over TCP, but for the media streams.
- Media streams transport parameters signaled in “Transport” header.
- Media normally only goes from server to client.
- Client’s public address (from TCP connection) and given port numbers are not forwarded to client.
- Will also address Firewall cooperation.

Goals

- Provide tools that allow RTSP to Traverse NATs.
- Will not specify a single solution.
- Do not reduce the current security level of RTSP to accomplish traversal of NATs:
  - RTSP is not safe against man in the middle attacks. Requires RTSP message security and protection against interception of RTSP connection.
  - Looks like a NATed connections can never be made safe against man in the middle hi-jacking.
- To have this specification ready as updated RTSP goes to IESG.

Ways of traversing a NAT present in draft

- STUN
  - Requires server modifications.
  - Needs destination address field freely used = Security problem.
- Symmetric RTP
  - Requires server modifications.
  - Will require large port usage on server.
- Tunneled in TCP
  - Works out of the box as specified in RFC 2326.
  - Real-time issues.
- Application Layer Gateway
  - Works if correctly implemented.
  - Have issues with future extensions and deployment.

Open Issues

- Usage of STUN for symmetric NATs
  - Requires Server modifications to allow non-continuous RTP and RTCP ports.
  - Requires co-location of STUN server and Media Sender/RTCP sender & receiver, to same port. =>
    Require heuristics based demultiplexing.
  - Requires that “destination” is used, i.e. does not work if media stream gets different IP than RTSP transport connection.

Open Issues

- Symmetric RTP
  - Requires Server modifications for protocol extension to carry shared secret (RTP SSRC).
  - To guarantee session demultiplexing each media stream needs a separate server port. Also provides maximum security.
  - Binding packets can not be accepted unless address is same as RTSP transport connection’s:
    - Otherwise it can be used as a DOS attack tool.
    - Attacker can himself spoof the binding packet source IP.
  - Security against non “man in the middle” attacks are as strong as the size of shared secret, i.e. SSRC’s 32 random bits.

Open Issues

- Currently only TCP tunneling and ALG will work for NAT’s giving a client’s different packet flows, different IP addresses.
- Further possible solutions that should be covered:
  - TURN?
  - Others?
- Ways of resolving the DOS attack possibilities:
  - Other signaling to verify that destination accepts to receive media stream.
- Looking for co-author to help me!