           MIME Type Registration for RTP Payload Format for H.224

Status of This Memo

Copyright Notice

Abstract

   In conversational video applications, far-end camera control protocol
   is used by participants to control the remote camera. The protocol
   that is commonly used is ITU H.281 over H.224. The document
   registers the H224 media type. It defines the syntax and the
   semantics of the Session Description Protocol (SDP) parameters needed
   to support far-end camera control protocol using H.224.

Table of Contents

1. Introduction

The document registers the H224 media type, which may be used by systems that use SDP [RFC4566].

This media type is used for supporting the simple far-end camera control protocol on SDP-based systems. The media type helps signaling gateways between H.323 [ITU.H323] and SDP-based systems to use far-end camera control, end to end, without any protocol translation in the middle.

The document defines the H224 media type since the RTP packets in H.323 annex Q [ITU.H323] carry H.224 frames [ITU.H224]. The far-end camera control protocol (FECC) is internal to the H.224 frame and is identified by the client ID field of the H.224 packet.

The document will define the SDP [RFC4566] parameters needed to support the above far-end camera control protocol in systems that use SDP.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC2119 [RFC2119] and indicate requirement levels for compliant RTP implementations.

3. Far-End Camera Control Protocol

This simple protocol is based on ITU-T H.281[ITU.281] frames carried in ITU-T H.224 packets in an RTP/UDP channel. H.323 annex Q specifies how to build the RTP packets from the H.224 packets.

Using far end camera control protocol in point-to-point calls and multipoint calls for packet-switch networks is described in H.323, annex Q.

4. IANA Considerations

4.1. Media Type Registration

This section describes the media types and names associated with this payload format. The registration uses the templates defined in RFC 4288 [RFC4288]. It follows RFC 3555 [RFC3555].

4.1.1. Registration of MIME Media Type application/h224

   MIME media type name: application

   MIME subtype name: H224

   Required parameters: None

   Optional parameters: None

   Encoding considerations:

      This media type is framed (see H.323, Annex Q [ITU.H323]) and
      contains binary data; see Section 4.8 of [RFC4288]

   Security considerations: See Section 6 of RFC 4573.

   Interoperability considerations:

      Terminals sending simple far-end camera control commands should
      use this MIME type. Receivers who cannot support the protocol
      will reject the channel.

   Published specification: RFC 4573

   Applications that use this media type:

      Video conferencing applications.

   Additional information: None

   Person and email address to contact for further information:

      Roni Even: roni.even@polycom.co.il

   Intended usage: COMMON

   Restrictions on usage:

      This media type depends on RTP framing and thus is only defined
      for transfer via RTP [RFC3550]. Transport within other framing
      protocols is not defined at this time.

   Author: Roni Even

   Change controller:

      IETF Audio/Video Transport working group, delegated from the IESG.

5. SDP Parameters

The media type application/h224 string is mapped to fields in the
Session Description Protocol (SDP) as follows:

   o The media name in the "m=" line of SDP MUST be application. The
   transport SHALL be any applicable RTP profile (for example RFC
   3551 [RFC3551]), and the payload type is dynamic.

   o The encoding name in the "a=rtpmap" line of SDP MUST be h224
   (the MIME subtype).

   o The default clock rate in the "a=rtpmap" line MUST be 4800.

The recommended maximum bandwidth for this protocol is 6.4 kbit/sec.

5.1. Usage with the SDP Offer Answer Model

When offering FECC using SDP in an Offer/Answer model [RFC3264], the
following considerations are necessary.

Far-end camera control communication is uni-directional. H.224 is
bi-directional and can be used to learn the capabilities of the
remote video end point, e.g., how many cameras it has. The offer
answer exchange is dependent on the functionality of both sides.

The offerer offers a sendonly channel if its camera cannot be
remotely controlled and if the offerer does not intend to use H.224
to learn the capabilities of the remote video endpoints.

In all other cases, when the offerer's camera can be remotely
controlled and/or it intends to use H.224 capabilities negotiation,
the offerer offers a sendrecv channel.

The answerer behavior is as follows:

If it receives an offer with sendonly, it answers with a recvonly if
it supports far-end camera control; otherwise, it ignores/rejects the
offer.

If it receives an offer with sendrecv and its camera can be remotely
controlled, or it intends to use H.224 capabilities negotiation, it
answers with a sendrecv option. If its camera cannot be remotely
controlled, it can answer with a sendonly attribute. The answerer
may also reject the offer if he does not support FECC or does not
intend to use FECC at the moment.

6. Security Considerations

   H.224 payload format, defined in H.323, annex Q defines packet
   structure based on RTP using the RTP header structure from RFC 3550.
   Those packets are subject to the security considerations discussed in
   the RTP specification [RFC3550]. This implies that confidentiality
   of the media streams is achieved by encryption. Secure Realtime
   Transport Protocol (SRTP) [RFC3711] may be used to provide both
   encryption and integrity protection of RTP flow.

   A potential denial-of-service threat exists for data that causes
   application behavior like camera movement. The attacker can inject
   pathological datagrams into the stream that cause the receiver to
   change the camera position. Therefore, the usage of data origin
   authentication and data integrity protection of at least the H.323
   annex Q packet is RECOMMENDED; for example, with SRTP.

   Note that the appropriate mechanism to ensure confidentiality and
   integrity of H.323 annex Q packets and their payloads is very
   dependent on the application and on the transport and signaling
   protocols employed. Thus, although SRTP is given as an example
   above, other possible choices exist.

7. References

7.1. Normative References

   [ITU.281]   International Telecommunications Union, "A far end camera
               control protocol for videoconferences using H.224", ITU- T
               Recommendation H.281, November 1994.

   [ITU.H224] International Telecommunications Union, "A real time
               control protocol for simplex applications using the H.221
               LSD/HSD/HLP channels.", ITU-T Recommendation H.224,
               February 2000.

   [ITU.H323] International Telecommunications Union, "Visual telephone
               systems and equipment for local area networks which
               provide a non-guaranteed quality of service", ITU-T
               Recommendation H.323, July 2003.

   [RFC2119]   Bradner, S., "Key words for use in RFCs to Indicate
               Requirement Levels", BCP 14, RFC 2119, March 1997.

   [RFC3264]   Rosenberg, J. and H. Schulzrinne, "An Offer/Answer Model
               with Session Description Protocol (SDP)", RFC 3264, June
               2002.

   [RFC3550] Schulzrinne, H., Casner, S., Frederick, R., and V.
              Jacobson, "RTP: A Transport Protocol for Real-Time
              Applications", STD 64, RFC 3550, July 2003.

   [RFC4566] Handley, M., Jacobson, V., and C. Perkins, "SDP: Session
              Description Protocol", RFC 4566, July 2006.

7.2. Informative References

   [RFC3551] Schulzrinne, H. and S. Casner, "RTP Profile for Audio and
              Video Conferences with Minimal Control", STD 65, RFC 3551,
              July 2003.

   [RFC3555] Casner, S. and P. Hoschka, "MIME Type Registration of RTP
              Payload Formats", RFC 3555, July 2003.

   [RFC3711] Baugher, M., McGrew, D., Naslund, M., Carrara, E., and K.
              Norrman, "The Secure Real-time Transport Protocol (SRTP)",
              RFC 3711, March 2004.

   [RFC4288] Freed, N. and J. Klensin, "Media Type Specifications and
              Registration Procedures", BCP 13, RFC 4288, December 2005.

Authors' Addresses

   Roni Even
   Polycom
   94 Derech Em Hamoshavot
   Petach Tikva 49130
   Israel

   EMail: roni.even@polycom.co.il

   Andrew Lochbaum
   Polycom
   6500 River Place Blvd, Building 6
   Austin, TX 78730
   USA

   EMail: alochbaum@polycom.com

Intellectual Property

   The IETF takes no position regarding the validity or scope of any
   Intellectual Property Rights or other rights that might be claimed to
   pertain to the implementation or use of the technology described in
   this document or the extent to which any license under such rights
   might or might not be available; nor does it represent that it has
   made any independent effort to identify any such rights. Information
   on the procedures with respect to rights in RFC documents can be
   found in BCP 78 and BCP 79.

   Copies of IPR disclosures made to the IETF Secretariat and any
   assurances of licenses to be made available, or the result of an
   attempt made to obtain a general license or permission for the use of
   such proprietary rights by implementers or users of this
   specification can be obtained from the IETF on-line IPR repository at
   http://www.ietf.org/ipr.

   The IETF invites any interested party to bring to its attention any
   copyrights, patents or patent applications, or other proprietary
   rights that may cover technology that may be required to implement
   this standard. Please address the information to the IETF at
   ietf-ipr@ietf.org.