SIMPLE Working Group
Internet-Draft
Intended status: Standards Track
Expires: June 6, 2011

C. Holmberg
Ericsson
S. Blau
Ericsson AB

December 3, 2010

An Alternative Connection Model for the Message Session Relay Protocol (MSRP)
draft-ietf-simple-msrp-acm-10.txt

Abstract

This document defines an alternative connection model for Message Session Relay Protocol (MSRP) User Agents (UAs), which uses the connection-oriented media (COMEDIA) mechanism in order to create the MSRP transport connection. The model allows MSRP UAs behind Network Address Translators (NATs) to negotiate which endpoint initiates the establishment of the Transmission Control Protocol (TCP) connection, in order for MSRP messages to traverse the NAT.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on June 6, 2011.

Copyright Notice

Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect

to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction

The Message Session Relay Protocol (MSRP) core specification [RFC4975] defines that the MSRP User Agent (UA) which sends the Session Description Protocol (SDP) offer is "active", and it is responsible for creating the MSRP transport connection towards the remote UA if a new connection is required. The core specification also allows, but does not define, alternate mechanisms for MSRP UAs to create MSRP transport connections.

[RFC4145] defines a connection-oriented media (COMEDIA) mechanism, that endpoints can use to negotiate the endpoint which initiates the creation of media transport connection.

COMEDIA is especially useful when one of the endpoints is located behind a Network Address Translator (NAT). The endpoint can use the mechanism to indicate that it will create the media transport connection, in order for the media to traverse the NAT without the usage of relays, without being required to support more complex mechanisms (e.g. TCP Candidates with Interactive Connectivity Establishment (ICE) [I-D.ietf-mmusic-ice-tcp]). In addition, COMEDIA allows the usage of identical procedures in establishing Transmission Control Protocol (TCP) [RFC0793] connections for different types of media.

An example is the Open Mobile Alliance (OMA) defined "Instant Message using SIMPLE" [OMA-TS-SIMPLE_IM-V1_0-20090901-D], where one MSRP UA of every MSRP transport connection represents a media server, which is always located in the carrier network. The media server has a globally reachable IP address and handles application specific policy control as well as NAT traversal. The OMA IM (Instant Messenger) uses COMEDIA for NAT traversal, and all OMA IM MSRP clients support COMEDIA.

This document defines how an MSRP UA uses COMEDIA in order to negotiate which UA will create the MSRP transport TCP connection towards the other UA. The document also defines how an MSRP UA which uses COMEDIA can establish an MSRP transport connection with a remote UA that does not support COMEDIA.

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 RFC 2119 [RFC2119].

3. Applicability statement

Support of this specification is OPTIONAL for MSRP user agents in general. User Agents that are likely to be deployed in networks with NATs SHOULD support this specification. It will improve the odds of being able to make TCP connections successfully traverse NATs, since User Agents behind NATs can be requested to initiate the establishment of the TCP connections.

4. COMEDIA for MSRP

4.1. General

This section defines how an MSRP UA that supports this specification uses the COMEDIA SDP attributes defined in [RFC4145].

4.2. a=setup

4.2.1. General

An MSRP UA uses the SDP a=setup attribute [RFC4145], in order to negotiate which endpoint will create the MSRP transport connection towards the other UA.

An MSRP UA MUST always include an explicit a=setup attribute in its SDP offers and answers, since it might be useful for the other endpoint, or for entities in the network, to know whether the UA supports COMEDIA or not.

An MSRP UA MUST support the a=setup "active", "actpass" and "passive" attribute values. An MSRP UA MUST NOT send the "holdconn" attribute value. If MSRP UA receives the "holdconn" attribute value it MUST ignore it and process the message as if it did not contain an a=setup attribute.

4.2.2. Attribute usage

When the a=setup attribute value is "actpass" or "passive", the IP address and port values in the MSRP URI of the SDP a=path attribute MUST contain the actual address and port values on which the UA can receive a TCP connection for the MSRP transport connection.

In accordance with [RFC4145], if the a=setup attribute value is "active", the port number value should be 9.

If an MSRP UA can provide a globally reachable IP address that the other endpoint can use as destination for a TCP connection, the UA

MUST use the a=setup "actpass" attribute value in SDP offers. This is in order to allow the remote UA to send an SDP answer with an a=setup "active" attribute value if the UA is located behind NAT, and in order to be compatible with UAs that do not support COMEDIA and thus always will act as passive endpoints. If an MSRP UA cannot provide the actual transport address, the UA MUST use the a=setup "active" attribute value.

The UA MUST NOT use the a=setup "passive" attribute value in an SDP offer.

The MSRP UA can determine that it provides a globally reachable IP address in the following scenarios:

- the UA can determine that it is not located behind a NAT;

- the UA relays its MSRP transport connections via a relay (e.g. MSRP relay or TURN server); or

- the UA has used Session Traversal Utilities for NAT (STUN) [RFC5389] signaling to retrieve NAT address and port through the local port to be used for the eventual transport connection, while also having determined that the NAT has endpoint independent mapping and filtering behavior [RFC5382], e.g. using the mechanism defined in [RFC5780].

Some UAs can determine whether the SIP [RFC3261] signaling has traversed a NAT by inspecting the SIP Via header field in the 200 (OK) response to the initial SIP REGISTER request, and comparing the IP addresses in the Via sent-by and the received header field parameters. If the IP addresses are not the same then the UA can determine that there is a NAT in the path. Even though the media transport might not traverse the NAT, it is safe to assume that it will, and set the a=setup attribute accordingly. This comparing mechanism does not work in all scenarios, though. For example, if SIP a requests crosses a SIP proxy before crossing a NAT, the UA will not be able to detect the NAT by comparing the IP addresses.

If an SDP offer includes an a=setup "actpass" attribute value, the SDP answerer MAY include an a=setup "active" attribute value in the SDP answer, but SHOULD include a=setup "passive" attribute value if it knows that it is not located behind a NAT.

Once the active UA has established the MSRP transport connection, the UA must immediately send an MSRP SEND request, as defined in [RFC4975].

NOTE: According to [RFC4975] the initiating UA is always active, but

when COMEDIA is used the a=setup attribute is used to negotiate which UA becomes active.

4.3. TLS

If an MSRP UA conformant to this document uses TLS, it MUST use the TLS mechanisms defined in [RFC4975] and [RFC4976].

According to [RFC4975], the connection can be established with or without TLS mutual authentication. In case mutual authentication is not used, the listening device waits until it receives a request on the connection, at which time it infers the identity of the connecting device from the associated session description. From TLS authentication point of view it is thus irrelevant whether an endpoint takes the active or passive role.

If an MSRP UA uses a self-signed TLS certificate to authenticate itself to MSRP peers it also includes its certificate fingerprint in the SDP.

Note that fingerprints can only be exchanged in peer-to-peer communication, as MSRP relays [RFC4976] will not receive the SDP payloads containing the fingerprint attributes.

4.4. a=connection

MSRP UAs MUST NOT use the SDP a=connection attribute. [RFC4975] defines connection reuse procedures for MSRP, and this document does not modify those procedures.

If an MSRP UA receives an a=connection attribute, the UA MUST ignore it.

4.5. MSRP relay connection

If an MSRP UA is located behind an MSRP relay [RFC4976], the UA MUST always initiate a transport connection towards the relay, no matter what value the client has provided in the a=setup attribute.

NOTE: Even if an MSRP UA initiates the TCP connection towards its relay, the UA will only send a SEND request if the UA is active, based on the COMEDIA negotiation.

5. Interoperability with connection model defined in RFC 4975

An MSRP UA conformant to this document can interoperate with a UA that follows the connection model defined in [RFC4975]. However, if

an MSRP UA conformant to this document is located behind NAT, and does not proxy its MSRP communication via an MSRP relay, and the UA receives an SDP offer from a remote UA that follows the connection model defined in [RFC4975], NAT traversal can only be achieved if the MSRP UA supports ICE [I.D.ietf-mmusic-ice-tcp], or if the network supports Session Border Controller (SBC) assisted NAT traversal for TCP.

6. Security Considerations

According to the connection model defined in [RFC4975], the MSRP UA that sends the SDP offer becomes the active party, and it is responsible for creating the MSRP transport connection towards the remote UA if a new connection is required.

When COMEDIA is used, either the sender or the receiver of the SDP offer can become the active party. [RFC4975] requires that the active party immediately issues an MSRP SEND request once the connection has been established. This allows the passive party to bind the inbound TCP connection to the message session identified by the session id part of its MSRP URI. The use of COMEDIA does not change this requirement, but the sender of the SDP offer is no longer assumed to always become the active party.

The active party also takes the role as TLS client, if TLS is used to protect the MSRP messages. However, there are no procedures in [RFC4975] that would break in case the receiver of the SDP offer takes the role as TLS client, and the level of security provided by TLS is not affected.

7. IANA Considerations

This document has no actions for IANA.

8. Acknowledgements

Thanks to Ben Campbell, Remi Denis-Courmont, Nancy Greene, Hadriel Kaplan, Adam Roach, Robert Sparks, Salvatore Loreto and Shida Schubert for their guidance and input in order to produce this document.

9. Change Log

[RFC EDITOR NOTE: Please remove this section when publishing]

Changes from draft-ietf-simple-msrp-acm-09
- Changes based on IESG comments.
- 30.11.2012: Sean Turner
- 30.11.2010: Lars Eggert
- 02.12.2012: Adrian Farrel
- 03.12.2012: Jari Arkko
- TCP reference added.

Changes from draft-ietf-simple-msrp-acm-08
- Changes based on comments from Gonzalo Camarillo.

Changes from draft-ietf-simple-msrp-acm-07
- WGLC editorial changes.

Changes from draft-ietf-simple-msrp-acm-06
- WGLC changes.

Changes from draft-ietf-simple-msrp-acm-05
- TLS section modified.

Changes from draft-ietf-simple-msrp-acm-04
- TLS section modified.
- Security considerations section modified.

Changes from draft-ietf-simple-msrp-acm-03
- Changes based on WGLC comments from Adam Roach and Ben Campbell.
- New section added related to interoperability with connection model defined in RFC 4975.
- Text related to a=setup "holdconn" attribute value removed.
- NAT keepalive section removed.
- Usage of COMEDIA-TLS removed.

Changes from draft-ietf-simple-msrp-acm-02
- Changes based on WGLC comments from Salvatore Loreto and Shida Schubert.

Changes from draft-ietf-simple-msrp-acm-01
- Procedures for using SDP c/m for routing of MSRP messages removed.
- Procedures related to modification of MSRP address information by intermediates moved to separate document.
- Solution to open issue on usage of the SDP a=connection implemented.

10. References

10.1. Normative References

[RFC0793] Postel, J., "Transmission Control Protocol", STD 7, RFC 793, September 1981.

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

[RFC4145] Yon, D. and G. Camarillo, "TCP-Based Media Transport in the Session Description Protocol (SDP)", RFC 4145, September 2005.

[RFC4975] Campbell, B., Mahy, R., and C. Jennings, "The Message Session Relay Protocol (MSRP)", RFC 4975, September 2007.

[RFC4976] Jennings, C., Mahy, R., and A. Roach, "Relay Extensions for the Message Sessions Relay Protocol (MSRP)", RFC 4976, September 2007.

10.2. Informative References

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[RFC5382] Guha, S., Biswas, K., Ford, B., Sivakumar, S., and P. Srisuresh, "NAT Behavioral Requirements for TCP", BCP 142, RFC 5382, October 2008.

[RFC5389] Rosenberg, J., Mahy, R., Matthews, P., and D. Wing, "Session Traversal Utilities for NAT (STUN)", RFC 5389, October 2008.

[RFC5780] MacDonald, D. and B. Lowekamp, "NAT Behavior Discovery Using Session Traversal Utilities for NAT (STUN)", RFC 5780, May 2010.

[I-D.ietf-mmusic-ice-tcp] Rosenberg, J., Keranen, A., Lowekamp, B., and A. Roach, "TCP Candidates with Interactive Connectivity Establishment (ICE)", draft-ietf-mmusic-ice-tcp-11 (work in progress), November 2010.

Authors' Addresses

Christer Holmberg
Ericsson
Hirsalantie 11
Jorvas 02420
Finland

Email: christer.holmberg@ericsson.com

Staffan Blau
Ericsson AB
P.O Box 407
Sweden

Email: staffan.blau@ericsson.com