

SIMPLE
Internet-Draft
Intended status: Experimental
Expires: January 28, 2009

R. Denis-Courmont
Nokia
July 27, 2008

Connection setup negotiation for the Message Session Relay Protocol
draft-denis-simple-msrp-comedia-02.txt

Status of This Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on January 28, 2009.

Abstract

This document extends the MSRP connection model to negotiate the direction of the TCP connection setup. This provides a partial yet simple solution for scenarios whereby either, but not both, party to an MSRP session is located behind a NAT or firewall, and cannot serve as the passive endpoint for TCP connection setup.

Internet-Draft

COMEDIA for MSRP

July 2008

Table of Contents

1.	Introduction	3
2.	Definitions	3
3.	Applicability statement	3
4.	MSRP COMEDIA Connection Model	4
4.1.	Offerer processing	4
4.1.1.	Sending the offer	4
4.1.2.	Receiving the answer	5
4.1.3.	Setting up the connection	5
4.2.	Answerer processing	6
4.2.1.	Receiving the offer	6
4.2.2.	Sending the answer	7
4.2.3.	Setting up the connection	7
5.	Interactions with MSRP relays	8
6.	NAT keep alives	8
7.	COMEDIA extensions	8
7.1.	Interactions with TLS	8
7.2.	Interactions with ICE	8
8.	Security Considerations	9
9.	IANA Considerations	9
10.	Acknowledgments	9
11.	References	9
11.1.	Normative References	9
11.2.	Informative References	10

1. Introduction

MSRP[RFC4975] allows transmission of byte streams (such as computer files) between two nodes using a SIP infrastructure. Because reliability and congestion control are required, MSRP uses TCP as its underlying transport protocol. Furthermore, MSRP specifies that the party initiating the session shall act as the active endpoint in establishing the connection-oriented transport session. The answering party shall wait for an incoming connection request, then check the MSRP path header in the first MSRP request, to bind the connection with the SIP dialog.

This poses a significant challenge if the answering party is located behind a NAT and/or a stateful firewall. To address these issues, MSRP defines relay nodes (in [RFC4976]), which MSRP clients can use as application-layer proxies.

However, deploying these relays bears a significant extra cost, especially as MSRP relays are limited to a single application-layer protocol (contrary to TURN[I-D.ietf-behave-turn] or SOCKS[RFC1928]). This also constitute a chicken-and-egg problem to MSRP deployment.

In addition, MSRP relaying affects the reliability of the data transmission, due to the lack of end-to-end congestion control and reliable end-to-end partial delivery acknowledgement mechanism (partial acknowledgment are optional for receiver to send).

This memo proposes an alternative connection model for MSRP. It avoids the use of any middlebox when either party to the MSRP session, is not behind a NAT or a firewall. It also brings reliability and congestion control to MSRP through to the use of an end-to-end TCP session.

2. Definitions

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](#)].

[3.](#) Applicability statement

Under some usage scenarios, the offerer of an MSRP[RFC4975] session description is more likely to be able to receive incoming transport-layer connection requests than the answerer. Some examples scenarios might be:

- o a MSRP chat server inviting an user to a chat session [[I-D.ietf-simple-chat](#)],

Denis-Courmont

Expires January 28, 2009

[Page 3]

Internet-Draft

COMEDIA for MSRP

July 2008

- o a file being pushed to the receiver [[I-D.ietf-mmusic-file-transfer-mech](#)] from a file server,
- o a SOCKS[RFC1928] proxy, or a TURN relay[I-D.ietf-behave-turn] available to the offerer but not the answerer,
- o adequate hole punching provision on the offerer side (e.g. with UPnP IGD profile, or manual configuration).

In these cases, it would be possible for the answerer to use an MSRP relay[RFC4976], if it cannot receive incoming connection requests, such as if it is located behind a NAT.

However, if the offerer can act as the passive side in the establishment of the media connection, the connection setup can be negotiated using COMEDIA[RFC4145]. This has the following advantages:

- o no need to deploy and provision a MSRP relay,
- o reliability and congestion control are transparently ensured, as the transport connection is end-to-end,

[4.](#) MSRP COMEDIA Connection Model

[4.1.](#) Offerer processing

[4.1.1.](#) Sending the offer

If the offerer of an MSRP session knows that it is prepared to handle transport-layer connection requests, it MUST include the "setup" SDP attribute, as defined in [\[RFC4145\]](#). It MAY also include the "connection" SDP attribute (to specify whether a transport connection may be re-used), as defined in the same document[RFC4145].

In that case, the setup attribute MUST be set to either "passive" or "actpass". However, for the sake of compatibility with MSRP client which do not implement this specification, it is RECOMMENDED:

- o that "actpass" be used, rather than "passive",
- o that the offerer be ready to establish an active connection, as per the basic MSRP connection model.

The following example shows an excerpt of an SDP offer using COMEDIA:

```
v=0
o=alice 8459831645 4643536435 IN IP4 alice.example.com
s= -
c=IN IP4 alice.example.com
t=0 0
m=message 4535 TCP/MSRP *
a=setup:actpass
a=connection:new
... other session attributes ...
```

Offer example

If the offerer is not willing or capable of handling incoming connection requests, it MAY set the setup attribute to "active". If not specified, this is assumed to be the default. For backward compatibility with MSRP endpoints that do not support the extension specified in this memo, it SHOULD include its actual transport-layer source port number in the offer m= line, rather than specify the port number 9 (discard).

The "holdconn" setup type is not defined, and MUST NOT be used. It is left for future specification.

4.1.2. Receiving the answer

When the offerer receives a successful answer, it looks for the setup attribute in the SDP for each media:

- o If the setup attribute is absent from the answer, and if the offerer had included a setup attribute with the value "passive", the answerer does not support this specification, and the media establishment MUST be considered as failed.
- o Otherwise, if the setup attribute is absent from the answer, even though the answerer might not support this specification, the COMEDIA connection model can be used (because it is then compatible with the baseline MSRP connection model).
- o Otherwise, the answerer supports the COMEDIA connection model described in this specification.

4.1.3. Setting up the connection

If it has been determined that the connection can be established according to the model described in this memo, the offerer MUST establish the media connection according to [[RFC4145](#)], with the following exception:

The source address of the active connection endpoint would normally be found in the relevant c= line, as well as in MSRP path line from the SDP. However, if a NAT device is present on the media path, these addresses might not match the IP address and port numbers of the actual TCP packets. To compensate for this inconsistency, the passive endpoint MUST ignore the address found in the c= and a=path: SDP lines, and accept incoming TCP connection requests from any remote peer.

To protect against a potential denial of service, the passive peer might need to process multiple incoming TCP sessions, until one of them has been authenticated. The legitimate TCP session MUST be authenticated by checking the From-Path and To-Path fields from MSRP requests received through that TCP session.

As specified in [[RFC4145](#)], the active endpoint MUST use the host/ address and ports as found in the SDP m= and c= line. It SHOULD not match the MSRP path in the SDP a=path: attribute with the m= and c= line. That should allow interoperating with COMEDIA-aware application layer gateways if there is one on the signaling path.

[4.2.](#) Answerer processing

[4.2.1.](#) Receiving the offer

When a MSRP client receives a MSRP session offer, and determines that it will accept the offer, it looks for the setup attribute.

- o If it is absent, or its value is active, the client MUST follow the normal MSRP connection model.
- o If the value is "passive", the answerer MUST initiate the TCP connection to the offerer, as specified in [[RFC4145](#)]. It will still need to process other SDP parameters (such as "a=accept-bytes") as specified in [[RFC4975](#)]. In particular, it needs to cross-match the MSRP a=path SDP attribute with the From-Path headers used in the received MSRP messages.
- o If the value is "actpass", it MUST choose either of two above connection models, and send format its answer accordingly as specified above. In particular, if it is known that connection requests cannot be processed by the answerer, it SHOULD act as the active endpoint. Similarly, if it is known that connection requests can be processed efficiently (i.e. not using any relaying protocol), it SHOULD act as the passive endpoint.

[4.2.2.](#) Sending the answer

If the answerer is to initiate the TCP connection (as per the rules set above), it MUST include a COMEDIA setup attribute with a value of "active" in the answer SDP which it sends back to the offerer (see example below). It MUST also format the c= and m= line as specified in [[RFC4145](#)].

```
v=0
o=alice 3245439832 1457605654 IN IP4 bob.example.com
s= -
c=IN IP4 bob.example.com
t=0 0
m=message 9 TCP/MSRP *
a=setup:active
a=connection:new
... other session attributes ...
```

Active setup answer example

Otherwise, the answerer MAY include a COMEDIA setup attribute with a value of "passive", as in the following example:

```
v=0
o=alice 3245439832 1457605654 IN IP4 bob.example.com
s= -
c=IN IP4 bob.example.com
t=0 0
m=message 34567 TCP/MSRP *
a=setup:active
a=connection:new
... other session attributes ...
```

Passive setup answer example

[4.2.3.](#) Setting up the connection

Once the TCP session is established, and if the answerer was the active connection endpoint, it MUST send an MSRP request. In particular, if it has no pending data to send, it MUST send an empty MSRP SEND request. That is necessary for the other endpoint to authenticate this TCP session.

Some extension to this specification MAY specify other methods to authenticate the peer, (see also [[I-D.niemi-simple-msrp-ice](#)]).

[5.](#) Interactions with MSRP relays

It is not possible to use the MSRP COMEDIA connection model as defined in this memo, and one or more MSRP relays[RFC4976] for a given MSRP session.

Whenever the offerer uses a MSRP relay, then it MUST NOT advertise support of the MSRP COMEDIA connection model. Instead, it MUST follow the baseline MSRP connection model.

Whenever the answerer detects a MSRP media with a COMEDIA "a=setup" SDP parameter within an offer, while it wants to use a MSRP relay, it MUST discard the "a=setup" attribute in the offer. Note that the discarded "a=setup" SDP attribute might still apply to any other media in the same offer, if there are more than one m= lines in the SDP offer.

[6.](#) NAT keep alives

The MSRP protocol does not allow leading CRLF (contrary to e.g., HTTP or SIP). If a keep-alive is required, a dummy MSRP SEND request SHOULD be sent, similar to when establishing a new MSRP connection.

It should be noted that sending frequent keep-alives may have very adverse effect when used with certain network access technologies (such as 3G cellular), such as dramatic increase of current drain. As TCP bindings tend to have much longer expiration timers than UDP, on middleboxes, sending of keep-alives might not be as critical as with a UDP-based protocol.

[7.](#) COMEDIA extensions

[7.1.](#) Interactions with TLS

If an MSRP connection that is negotiated using the mechanism described in section [Section 4](#), uses the Transport Layer Security protocol, the Client and Server TLS roles MUST negotiate the relevant parameter as specified per COMEDIA-TLS[RFC4572].

In addition, the MSRP "a=path" attribute MUST specify "msrps" as the URI scheme, consistent with [\[RFC4975\]](#). If TLS is not used, the URI scheme would be "msrp".

[7.2.](#) Interactions with ICE

ICE-TCP can be used as is with the MSRP COMEDIA, as it is an extension to COMEDIA.

[8.](#) Security Considerations

TBD.

[9.](#) IANA Considerations

This document raises no new IANA considerations.

[10.](#) Acknowledgments

The authors would like to thank Christian Schmidt, Bernhard Boehmer, Miguel Garcia, Thomas Theimer, Ivo Sedlacek, Markku Vimpari and Thomas Belling for their comments on this document.

[11.](#) References

[11.1.](#) Normative References

- | | |
|-----------|---|
| [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. |
| [RFC4572] | Lennox, J., "Connection-Oriented Media Transport over the Transport Layer Security (TLS) Protocol in the Session Description Protocol (SDP)", RFC 4572 , July 2006. |
| [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. |

[11.2](#). Informative References

- [I-D.ietf-behave-turn] Rosenberg, J., Mahy, R., and P. Matthews, "Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)", [draft-ietf-behave-turn-09](#) (work in progress), July 2008.
- [I-D.ietf-mmusic-file-transfer-mech] Garcia-Martin, M., Isomaki, M., Camarillo, G., Loreto, S., and P. Kyzivat, "A Session Description Protocol (SDP) Offer/Answer Mechanism to Enable File Transfer", [draft-ietf-mmusic-file-transfer-mech-08](#) (work in progress), May 2008.
- [I-D.ietf-simple-chat] Niemi, A., Garcia-Martin, M., and G. Sandbakken, "Multi-party Instant Message (IM) Sessions Using the Message Session Relay Protocol (MSRP)", [draft-ietf-simple-chat-02](#) (work in progress), February 2008.
- [I-D.niemi-simple-msrp-ice] Niemi, A., "Message Session Relay Protocol Adaptation for Interactive Connectivity Establishment (ICE)", [draft-niemi-simple-msrp-ice-00](#) (work in progress), February 2007.
- [RFC1928] Leech, M., Ganis, M., Lee, Y., Kuris, R., Koblas, D., and L.

Denis-Courmont Expires January 28, 2009 [Page 10]

Internet-Draft COMEDIA for MSRP July 2008

Author's Address

Remi Denis-Courmont
Nokia Technology Platforms
P.O. Box 407
Nokia Group FIN-00045
Finland

Phone: +358 50 487 6315
EMail: remi.denis-courmont@nokia.com

Full Copyright Statement

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

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.