

DISPATCH
Internet-Draft
Intended status: Standards Track
Expires: September 14, 2017

M. Petit-Huguenin
Impedance Mismatch
G. Salgueiro
Cisco
March 13, 2017

Path MTU Discovery (PMTUD) for RTP/RTCP
draft-petithuguenin-dispatch-rtp-pmtud-00

Abstract

This document describes an implementation of the Path MTU Discovery (PMTUD) protocol for RTP sessions.

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 September 14, 2017.

Copyright Notice

Copyright (c) 2017 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.

Internet-Draft

RTP PMTUD

March 2017

Table of Contents

1.	Introduction	2
2.	Overview of Operations	2
3.	Terminology	2
4.	Probe Support Signaling	3
5.	Path MTU Discovery Using the Simple Probing Mechanism	3
6.	Path MTU Discovery Using the Complete Probing Mechanism . . .	3
7.	Security Considerations	4
8.	IANA Considerations	4
9.	References	4
9.1.	Normative References	4
9.2.	Informative References	5
	Authors' Addresses	5

[1.](#) Introduction

The Guidelines for Writers of RTP Payload Formats ([RFC 2736](#), [BCP 36](#) [[RFC2736](#)]) states in [Section 4](#) that "[i]f a codec's frame size is larger than the MTU, the payload format must not rely on IP fragmentation." Similarly, [RFC 3550](#) [[RFC3550](#)] states that "...only the subset [of RR packets into one compound RTCP packet] that will fit into one MTU SHOULD be included in each interval."

These statements can be extended to the Path MTU, as fragmentation along the media path is no better than fragmentation on the first link-layer.

RTP and RTCP [[RFC3550](#)] were not designed with a mechanism to discover the Path MTU, so this document describes a way to add this capability by using the PMTUD protocol defined in [[I-D.ietf-tram-stun-pmtud](#)].

[2.](#) Overview of Operations

Multiplexing between RTP/RTCP packets and STUN packets is a well-known technique used for example to discover the IP address of a NAT [[RFC5389](#)] or to check connectivity [[RFC5245](#)].

The PMTUD mechanism for RTP/RTCP uses either the Simple Probing Mechanism described in Section 4.1 of [[I-D.ietf-tram-stun-pmtud](#)] or the Complete Probing Mechanism described in [Section 4.2](#).

[3.](#) 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](#)].

[4.](#) Probe Support Signaling

Real-time media protocols (SIP [[RFC3261](#)], Jingle [XEP-0166]) that are using the Offer/Answer protocol [[RFC3264](#)] signals their support of this specification by the usage of an "a:x-pmtud" attribute in the SDP. This attribute can be used at the session-level or at the media-level.

An Offerer indicates the support of this specification by adding an "a:x-pmtud" attribute in the SDP sent. An Answerer receiving an SDP containing an "a:x-pmtud" attribute and supporting this specification can immediately start probing for the PMTU, as described in Section 5.2 of [[I-D.ietf-tram-stun-pmtud](#)]. Even if the SDP received by an Answerer does not contain an "a:x-pmtud" attribute, an Answerer supporting this specification MUST insert an "a:x-pmtud" attribute in the SDP it will send.

Realtime media protocols that support ICE [[RFC5245](#)] (i.e. WebRTC, in addition to the protocols listed above) MAY signal that a specific candidate support for this specification differs from what is declared at the session-level or media-level of the SDP by inserting an extension attribute with values "pmtud on" or "pmtud off" in the candidate line.

[5.](#) Path MTU Discovery Using the Simple Probing Mechanism

When initiating the Probe transactions, as described in Section 4.1 of [[I-D.ietf-tram-stun-pmtud](#)], the RTP/RTCP client MUST use the same IP address and port destination that are used as the destination for the RTP or RTCP packets.

The server side MUST be prepared to demultiplex the Probe Requests from the RTP/RTCP packets and other STUN messages.

[6.](#) Path MTU Discovery Using the Complete Probing Mechanism

When sending the Probe Indications, the RTP/RTCP client MUST use the same source IP address and port and same IP address and port destination that are used for the RTP or RTCP packets.

Any STUN message sent along the RTP/RTCP packets, like ICE connectivity checks, media keep-alive, or consent packets MUST be used to populate the identifier list described in Section 4.2.3 of [[I-D.ietf-tram-stun-pmtud](#)].

For a STUN message, the identifier is made up of the first 12 bytes of the Transaction ID.

For an RTP packet, the identifier is made up of the SSRC concatenated with the Sequence Number, for a total of 12 bytes.

For an RTCP packet, the identifier is made up of the Reporter SSRC concatenated with the last 4 bytes of the Extended Highest Sequence Number Received, for a total of 12 bytes.

[7.](#) Security Considerations

TBD.

[8.](#) IANA Considerations

TBD

[9.](#) References

[9.1.](#) Normative References

[I-D.ietf-tram-stun-pmtud]

Petit-Huguenin, M. and G. Salgueiro, "Path MTU Discovery Using Session Traversal Utilities for NAT (STUN)", [draft-ietf-tram-stun-pmtud-05](#) (work in progress), February 2017.

[RFC2119]

Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.

- [RFC3264] Rosenberg, J. and H. Schulzrinne, "An Offer/Answer Model with Session Description Protocol (SDP)", [RFC 3264](#), DOI 10.17487/RFC3264, June 2002, <<http://www.rfc-editor.org/info/rfc3264>>.
- [RFC3550] Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", STD 64, [RFC 3550](#), DOI 10.17487/RFC3550, July 2003, <<http://www.rfc-editor.org/info/rfc3550>>.
- [RFC5245] Rosenberg, J., "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols", [RFC 5245](#), DOI 10.17487/RFC5245, April 2010, <<http://www.rfc-editor.org/info/rfc5245>>.

- [RFC5389] Rosenberg, J., Mahy, R., Matthews, P., and D. Wing, "Session Traversal Utilities for NAT (STUN)", [RFC 5389](#), DOI 10.17487/RFC5389, October 2008, <<http://www.rfc-editor.org/info/rfc5389>>.

[9.2](#). Informative References

- [RFC2736] Handley, M. and C. Perkins, "Guidelines for Writers of RTP Payload Format Specifications", [BCP 36](#), [RFC 2736](#), DOI 10.17487/RFC2736, December 1999, <<http://www.rfc-editor.org/info/rfc2736>>.
- [RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", [RFC 3261](#), DOI 10.17487/RFC3261, June 2002, <<http://www.rfc-editor.org/info/rfc3261>>.

Authors' Addresses

Marc Petit-Huguenin
Impedance Mismatch

Email: marc@petit-huguenin.org

Gonzalo Salgueiro
Cisco Systems, Inc.
7200-12 Kit Creek Road
Research Triangle Park, NC 27709
United States

Email: gsalguei@cisco.com