Abstract

This document describes a combination and profiling of existing IETF protocols to provide a datagram service that is suitable as a generic transport substrate for the RTC-Web family of real-time audio/video applications.

Requirements Language

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].

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 May 14, 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 ....................................................... 3
2. Terminology ....................................................... 3
3. Service model ..................................................... 3
4. Channel types ..................................................... 4
   4.1. UDP channel .................................................. 4
   4.2. TCP channel .................................................. 4
   4.3. TLS channel .................................................. 4
   4.4. DTLS channel ............................................... 4
   4.5. Channels with relay ......................................... 4
5. Channel setup, teardown and usage .................................. 5
6. An URI scheme for datagram channels ............................. 5
7. IANA Considerations ............................................... 6
8. Security Considerations .......................................... 6
9. Acknowledgements ................................................. 6
10. References ....................................................... 6
    10.1. Normative References ...................................... 6
    10.2. Informative References .................................... 7
Author’s Address .................................................... 7
1. Introduction

When transporting audio / video data between participants on the current Internet, there are a number of obstacles to be faced.

Among them are NAT boxes, firewalls, connection interruptions, the availability of multiple paths between participants, and capacity issues.

This memo describes a combination of existing protocols that can be used to achieve a seamless datagram transport service across this very heterogenous environment.

An overview of the effort of which this is a part can be found in the overview document, [overview].

2. Terminology

This draft uses a couple of commonly used terms in quite specific ways. The reader is advised to study these definitions carefully.

(TODO: Agree on terminology to use)

Session  An association with two endpoints, between which datagrams flow.

Datagram  A sequence of octets, of a given length. In this specification, a datagram does not carry addressing information.

Channel  One means of transporting a datagram over a session. A session may have multiple channels at any time.

Endpoint  One end of a session. This document does not distinguish between an initiator and a responder endpoint.

Control channel  A means of communication between the endpoints of a session that does not require a transport to be active. Typically, authentication, authorization and negotiation is carried out over the control channel. The specification of the control channel is out of scope for this specification.

3. Service model

The basic model presented is a datagram model. On top of this one can layer various services, such as pseudoTCP (REF), RTP[RFC3550] or any other higher layer protocol that is capable of running across a
The datagram service.

The addressing model departs from the traditional Internet model in that end point addresses are not used for endpoint identification, only for channel establishment; instead, an initial packet exchange, using ICE [RFC5245], is used to bind a channel to a prenegotiated session.

The datagram service is not completely transparent; in particular, it is not possible to carry a datagram where the two highest bits of the first octet are zero and octet 5 to 8 contain the value 0x2112A442, since these datagrams are reserved for use of the STUN protocol (RFC 5389 section 6).

4. Channel types

4.1. UDP channel

An UDP channel is negotiated using ICE. Each datagram is simply carried as the content of an UDP packet.

4.2. TCP channel

A TCP channel consists of a TCP connection, over which are sent datagrams packaged according to (REF). The binding of a TCP channel is done by executing an ICE negotiation over the first few packets passed across the TCP channel.

4.3. TLS channel

A TLS channel consists of a standard TLS negotiation, followed by passing datagrams over the TLS record layer; the length fields of (REF) are not used. A TLS channel is bound to its session by <insert process description>.

4.4. DTLS channel

A DTLS channel is created by executing a DTLS connection negotiation, followed by datagram exchange, where the datagrams are protected by DTLS mechanisms. The DTLS channel is bound to its session by <insert process>.

4.5. Channels with relay

If there is no possibility of setting up a direct connection, a relay must be used. The specification from TURN [RFC5766]is used.
5. Channel setup, teardown and usage

The service model envisioned here is that all datagrams arriving on a session are considered equally valid. The session gives no guarantees against duplication, loss or reordering; such concerns are left to the higher protocol layers.

The expected normal usage is that two endpoints will exchange addressing information that can be used for a series of potential channels, that the endpoints will probe for working channels using ICE (RFC 5245), and use the "best" candidate, while using the STUN probing facilities to keep some number of "second best" candidates alive if the "best" candidate stops working.

A data-sending endpoint may unilaterally decide to start or stop using an established channel at any time. No negotiation is necessary.

A receiving endpoint will learn that a channel has been removed by not seeing any more STUN keepalive messages on that channel within <timeout>.

A session is considered closed when all channels that have been successfully established have timed out.

6. An URI scheme for datagram channels

This URI scheme is mainly included in order to make it easy for APIs that normally use URIs as what they use to refer to objects.

The DGSESSION URI scheme specifies the information required for a session; it consists of two parts:

- An absolute reference, which includes the user name and password used to establish the connection.
- A series of addressing hints, which include the data necessary to establish a channel.

Example:


The sequence of addressing hints is an indication of the preference
of the URL constructor for the sequence in which to try these candidates; the most preferred address is the one to the left.

Note that a DGSESSION URI is a capability; anyone with the URI will be able to connect to the entity. They should therefore be handled in the same way as (short-term) passwords, and never passed in the clear.

7. IANA Considerations

This document registers the URI scheme from section Paragraph 1.

Note to RFC Editor: this section may be removed on publication as an RFC.

8. Security Considerations

As with all layered protocols, it is a matter for the application to decide which level security should be provided at. For instance, an RTP session protected using SRTP <ref> can be considered to not need any further safeguards against interception, modification or replay, so can be passed "in the clear" across any channel type here. For data without such protection, adequate measures need to be taken; in particular, it is trivially easy for someone with the ability to snoop and insert packets to insert fake packets into an established UDP channel.

The main defense against denial-of-service attacks is the fact that the ICE mechanisms were designed for low cost refusal of unauthorized connections.

9. Acknowledgements

10. References

10.1. Normative References


10.2. Informative References


Author’s Address

Harald Tveit Alvestrand
Google
Kungsbron 2
Stockholm, 11122
Sweden

Email: harald@alvestrand.no