Network Working Group
Internet-Draft
Expires: April 20, 2006

C. Perkins
University of Glasgow
October 17, 2005

RTP and the Datagram Congestion Control Protocol (DCCP)
draft-perkins-dccp-rtp-00.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/1id-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 April 20, 2006.

Copyright Notice

Copyright (C) The Internet Society (2005).

Abstract

This memo specifies a mapping of RTP onto DCCP, along with associated signalling.

Table of Contents

1. Introduction 3
2. Rationale 3
3. Conventions Used in this Memo 3
4. RTP over DCCP: Framing 3
4.1. RTP Data Packets 3
4.2. RTP Control Packets 4
4.3. Multiplexing Data and Control 5
4.4. RTP Sessions and DCCP Connections 5
4.5. RTP Profiles 6
5. RTP over DCCP: Signalling using SDP 6
5.1. Protocol Identification 6
5.2. Service Codes 7
5.3. Connection Management 8
5.4. Example 8
6. Security Considerations 9
7. IANA Considerations 9
8. Acknowledgements 9
9. References 10
9.1. Normative References 10
9.2. Informative References 10
Author's Address 12
Intellectual Property and Copyright Statements 13

1. Introduction

The Real-time Transport Protocol (RTP) [1] is widely used in video streaming, telephony, and other real-time networked applications. RTP can run over a range of lower-layer transport protocols, and the performance of an application using RTP is heavily influenced by the lower-layer transport protocol. The Datagram Congestion Control Protocol (DCCP) [2] is a newly specified transport protocol which provides desirable properties for real-time applications running on unmanaged best-effort IP networks. This memo describes how RTP can be framed for transport using DCCP. It also describes how the Session Description Protocol (SDP) [3] can be used to signal such sessions.

The remainder of this memo is structured as follows: we begin with a rationale for the work in Section 2, describing why a mapping of RTP onto DCCP is needed. Following a description of the conventions used in this memo in Section 3, the specification begins in Section 4 with the definition of how RTP packets are framed within DCCP; associated signalling is described in Section 5. We conclude with a discussion of security considerations in Section 6, and IANA considerations in Section 7.

2. Rationale

TODO: rationale why RTP over DCCP is useful, referencing [13] and comparing with [14].

3. Conventions Used in this Memo

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 [4].

4. RTP over DCCP: Framing

The following section defines how RTP and RTCP packets are framed for transport using DCCP. It also describes the different between an RTP session and a DCCP connection, and the impact this has on application design.

4.1. RTP Data Packets

Each RTP data packet MUST be conveyed in a single DCCP datagram. Fields in the RTP header MUST be interpreted according to the RTP

specification, and any applicable RTP Profile and Payload Format. Header processing is not affected by DCCP framing (in particular, note that the semantics of the RTP sequence number and the DCCP sequence number are not compatible, and the value of one cannot be inferred from the other).

A DCCP connection is opened when an end system joins an RTP session and SHOULD remain open for the duration of the session. To ensure NAT bindings are kept open, an end system SHOULD send periodic low rate zero length DCCP-Data packets during periods when it has no RTP data to send. This removes the need for RTP no-op packets [15] when using RTP over DCCP.

RTP data packets MUST obey the dictates of DCCP congestion control. In some cases, the congestion control will require a sender to send at a rate below that which the payload format would otherwise use. To support this, an application should use either a rate adaptive payload format, or a range of payload formats (allowing it to switch to a lower rate format if necessary). Details of the rate adaptation policy for particular payload formats are outside the scope of this memo.

TODO: should we give more guidance here?

DCCP allows an application to choose the checksum coverage, using a partial checksum to allow an application to receive packets with corrupt payloads. Some RTP Payload Formats (e.g. [16]) can make use of this feature in conjunction with payload-specific mechanisms to improve performance when operating in environments with frequent non-congestive packet corruption. If such a payload format is used, an RTP end system MAY enable partial checksums at the DCCP layer, in which case the checksum should cover at least the DCCP and RTP headers. Partial checksums MUST NOT be used unless supported by mechanisms in the payload format.

4.2. RTP Control Packets

The RTP Control Protocol (RTCP) SHOULD be used in the usual manner with DCCP. RTCP packets MUST be grouped into compound packets, as described in Section 6.1 of [1]. Each compound RTCP packet MUST be transported in a single DCCP datagram.

The usual RTCP timing rules apply, subject to the constraint that RTCP packets MUST be subject to DCCP congestion control.

TODO: is the RTP "session bandwidth" affected by congestion control? Dynamically adapting the RTCP transmission interval based on DCCP is difficult, since it will involve frequent reconsideration of the next

RTCP send time. Also, might be a problem if the RTP session spans a range of links, with widely varying capacities.

As noted in Section 17.1 of [2], there is the potential for overlap between the information conveyed in RTCP report packets and that conveyed in DCCP acknowledgement options. In general this is not an issue: RTCP packets contain media-specific data that is not present in DCCP acknowledgements, and DCCP options contain network-level data that is not present in RTCP. There is no overlap between the RTCP packet types defined in [1] and the DCCP options defined in [2].

There are, however, other cases of overlap: most clearly between the optional RTCP Extended Reports Loss RLE Blocks [17] and DCCP Ack Vector options. If there is overlap between RTCP reports and DCCP acknowledgements, an application SHOULD either use RTCP feedback or request DCCP acknowledgements, but not both (use of both types of feedback will waste available network capacity, but is not otherwise harmful).

4.3. Multiplexing Data and Control

The obvious mapping of RTP onto DCCP creates two DCCP connections for each RTP flow: one for RTP data packets, one for RTP control packets. A frequent criticism of RTP relates to the number of ports it uses, since large telephony gateways can support more than 32768 RTP flows between pairs of gateways, and so run out of UDP ports. In addition, use of multiple ports complicates NAT traversal.

If care is taken in the choice of payload type used, it is possible to multiplex RTP and RTCP onto the same port. This requires care in the application, but the added complexity there might be worthwhile. Is it appropriate to encourage this for RTP-over-DCCP?

4.4. RTP Sessions and DCCP Connections

An end system SHOULD NOT assume that it will observe only a single RTP synchronisation source (SSRC) because it is using DCCP framing. An RTP session can span any number of transport connections, and can include RTP mixers or translators bringing other participants into a session. The use of a unicast DCCP connection does not imply that the RTP session will have only two participants, and RTP end systems SHOULD assume that multiple synchronisation sources may be observed when using RTP over DCCP.

A single RTP session may span multiple DCCP connections. The RTP translator bridging those DCCP connections MUST be aware of the congestion state of each connection, and MUST adapt the media to the available capacity of each. In general, transcoding is required to

adapt the media: this is computationally expensive, induces delay, and generally gives poor quality results. Depending on the payload, it might be possible to use some form of scalable coding. Scalable media coding formats are an active research area, and are not in widespread use at the time of this writing.

A single RTP session may also span a DCCP connection and some other type of transport connection. An example might be an RTP over DCCP connection from an RTP end system to an RTP translator, with an RTP over UDP/IP multicast group on the other side of the translator. A second example might be an RTP over DCCP connection that links PSTN gateways. The issues for such an RTP translator are similar to those when linking two DCCP connections, except that the congestion control algorithms on either side of the translator may not be compatible. Implementation of effective translators for such an environment is nontrivial.

4.5. RTP Profiles

In general, there is no conflict between new RTP Profiles and DCCP framing, and most RTP profiles MAY be negotiated for use over DCCP. The only potential for conflict occurs if an RTP profile changes the RTCP reporting interval or the RTP packet transmission rules, since this may conflict with DCCP congestion control. If an RTP profile conflicts with DCCP congestion control, that profile MUST NOT be used with DCCP.

The RTP Profile for TFRC [14] MUST NOT be used with DCCP, since it conflicts with DCCP congestion control by providing alternative congestion control semantics.

5. RTP over DCCP: Signalling using SDP

The Session Description Protocol (SDP) [3] and the offer/answer model [5] are widely used to negotiate RTP sessions (for example, using the Session Initiation Protocol [18]). This section describes how SDP is used to signal RTP sessions running over DCCP.

5.1. Protocol Identification

SDP uses a media ("m=") line to convey details of the media format and transport protocol used. The ABNF syntax of a media line is as follows (from [3]):

```
media-field = "m=" media SP port ["/" integer] SP proto
              1*(SP fmt) CRLF
```

The proto field denotes the transport protocol used for the media, while the port indicates the transport port to which the media is sent. Following [6] and [7] this memo defines the following five values of the proto field to indicate media transported using DCCP:

```
DCCP
DCCP/RTP/AVP
DCCP/RTP/SAVP
DCCP/RTP/AVPF
DCCP/RTP/SAVPF
```

The "DCCP" protocol identifier is similar to the "UDP" and "TCP" protocol identifiers and describes the transport protocol, but not the upper-layer protocol. An SDP "m=" line that specifies the "DCCP" protocol MUST further qualify the application layer protocol using a fmt identifier. A single DCCP port is used, as denoted by the port field in the media line. The "DCCP" protocol identifier MUST NOT be used to signal RTP sessions running over DCCP.

The "DCCP/RTP/AVP" protocol identifier refers to RTP using the RTP Profile for Audio and Video Conferences with Minimal Control [8] running over DCCP.

The "DCCP/RTP/SAVP" protocol identifier refers to RTP using the Secure Real-time Transport Protocol [9] running over DCCP.

The "DCCP/RTP/AVPF" protocol identifier refers to RTP using the Extended RTP Profile for RTCP-based Feedback [10] running over DCCP.

The "DCCP/RTP/SAVPF" protocol identifier refers to RTP using the Extended Secure RTP Profile for RTCP-based Feedback [11] running over DCCP.

5.2. Service Codes

In addition to the port number, specified on the SDP "m=" line, a DCCP connection has an associated service code. To signal the service code, one new SDP attribute is defined:

```
dccp-service-attr = "a=dccp-service-code:" 1x8HEXDIG
```

where HEXDIG is as defined in [12].

The "a=dccp-service-code:" attribute conveys the numeric value of the DCCP service code, in network byte order, expressed as a sequence of eight hexadecimal digits. This representation was chosen since DCCP services codes are not necessarily comprised of printable characters.

The "a=dccp-service-code:" attribute is a media level attribute which is not subject to the charset attribute.

TODO: Should this memo register service codes for each RTP profile? Or should they be assigned to applications?

5.3. Connection Management

The "a=setup:" attribute indicates which of the end points should initiate the DCCP connection establishment (i.e. send the initial DCCP-Request packet). The "a=setup:" attribute MUST be used in a manner comparable with [7], except that DCCP connections are being initiated rather than TCP connections.

After the initial offer/answer exchange, the end points may decide to re-negotiate various parameters. The "a=connection:" attribute MUST be used in a manner compatible with [7] to decide whether a new DCCP connection needs to be established as a result of subsequent offer/answer exchanges, or if the existing connection should still be used.

5.4. Example

An offerer at 10.0.0.47 signals its availability for an H.261 video session, using RTP/AVP over DCCP with service code "RTP ":

```
v=0
o=alice 1129377363 1 IN IP4 10.0.0.47
s=-
c=IN IP4 10.0.0.47
t=0 0
m=video 51372 DCCP/RTP/AVP 99
a=rtpmap:99 h261/90000
a=dccp-service-code:52545020
a=setup:passive
a=connection:new
```

An answerer at 10.2.5.128 receives this offer and responds with the following answer:

```
v=0
o=bob 1129377364 1 IN IP4 10.2.5.128
s=-
c=IN IP4 10.2.5.128
t=0 0
m=video 9 DCCP/RTP/AVP 99
a=rtpmap:99 h261/90000
a=dccp-service-code:52545020
a=setup:active
```

```
a=connection:new
```

The end point at 10.2.5.128 then initiates a DCCP connection to port 51372 at 10.0.0.47.

TODO: is DCCP port 9 registered as discard?

6. Security Considerations

The security considerations in the RTP specification [1] and any applicable RTP profile (e.g. [8], [9], [10], or [11]) or payload format apply when transporting RTP over DCCP.

The security considerations in the DCCP specification [2] apply.

The SDP signalling described in Section 5 is subject to the security considerations of [3], [5], [7] and [6].

It is not believed that any additional security considerations are introduced as a result of combining these protocols. Indeed, the provision of effective congestion control for RTP will alleviate the potential for denial-of-service present when RTP flows ignore the advice in [1] to monitor packet loss and reduce their sending rate in the face of persistant congestion.

7. IANA Considerations

The following SDP "proto" field identifiers are registered: "DCCP", "DCCP/RTP/AVP", "DCCP/RTP/SAVP", "DCCP/RTP/AVPF" and "DCCP/RTP/SAVPF" (see Section 5.1 of this memo).

One new SDP attribute ("a=dccp-service-code:") is registered (see Section 5.2 of this memo).

8. Acknowledgements

This work was supported in part by the UK Engineering and Physical Sciences Research Council, under a GridNet2 award (administered by the UK National e-Science Centre).

9. References

9.1. Normative References

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

[2] Kohler, E., "Datagram Congestion Control Protocol (DCCP)", draft-ietf-dccp-spec-11 (work in progress), March 2005.

[3] Handley, M., "SDP: Session Description Protocol", draft-ietf-mmusic-sdp-new-25 (work in progress), July 2005.

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

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

[6] Lazzaro, J., "Framing RTP and RTCP Packets over Connection-Oriented Transport", draft-ietf-avt-rtp-framing-contrans-06 (work in progress), September 2005.

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

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

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

[10] Ott, J. and S. Wenger, "Extended RTP Profile for RTCP-based Feedback(RTP/AVPF)", draft-ietf-avt-rtcp-feedback-11 (work in progress), August 2004.

[11] Ott, J. and E. Carrara, "Extended Secure RTP Profile for RTCP-based Feedback (RTP/SAVPF)", draft-ietf-avt-profile-savpf-02 (work in progress), July 2005.

[12] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", RFC 2234, November 1997.

9.2. Informative References

[13] Floyd, S. and J. Kempf, "IAB Concerns Regarding Congestion Control for Voice Traffic in the Internet", RFC 3714, March 2004.

[14] Gharai, L., "RTP Profile for TCP Friendly Rate Control", draft-ietf-avt-tfrc-profile-04 (work in progress), July 2005.

[15] Andreasen, F., "A No-Op Payload Format for RTP", draft-wing-avt-rtp-noop-03 (work in progress), May 2005.

[16] Sjoberg, J., Westerlund, M., Lakaniemi, A., and Q. Xie, "Real-Time Transport Protocol (RTP) Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs", RFC 3267, June 2002.

[17] Friedman, T., Caceres, R., and A. Clark, "RTP Control Protocol Extended Reports (RTCP XR)", RFC 3611, November 2003.

[18] 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.

Author's Address

Colin Perkins
University of Glasgow
Department of Computing Science
17 Lilybank Gardens
Glasgow G12 8QQ
UK

Email: csp@csperkins.org

Intellectual Property Statement

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.

Disclaimer of Validity

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 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.

Copyright Statement

Copyright (C) The Internet Society (2005). 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.

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.