DCCP Extensions for Multipath Operation with Multiple Addresses

draft-amend-tsvwg-multipath-dccp-03

Abstract

DCCP communication is currently restricted to a single path per connection, yet multiple paths often exist between peers. The simultaneous use of these multiple paths for a DCCP session could improve resource usage within the network and, thus, improve user experience through higher throughput and improved resilience to network failure.

Multipath DCCP provides the ability to simultaneously use multiple paths between peers. This document presents a set of extensions to traditional DCCP to support multipath operation. The protocol offers the same type of service to applications as DCCP and it provides the components necessary to establish and use multiple DCCP flows across potentially disjoint paths.

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 https://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 7, 2020.
Copyright Notice

Copyright (c) 2019 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 (https://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
   1.1. Multipath DCCP in the Networking Stack ......... 3
   1.2. Terminology ..................................... 3
   1.3. MP-DCCP Concept ................................ 3
   1.4. Differences from Multipath TCP ................. 4
   1.5. Requirements Language .............................. 7
2. Operation Overview ................................. 7
3. MP-DCCP Protocol ................................... 7
   3.1. Multipath Capable Feature ....................... 8
   3.2. Multipath Option ................................ 9
      3.2.1. MP_CONFIRM .................................. 9
      3.2.2. MP_JOIN ...................................... 9
      3.2.3. MP_FAST_CLOSE ................................. 10
      3.2.4. MP_KEY ...................................... 10
      3.2.5. MP_SEQ ..................................... 11
      3.2.6. MP_HMAC .................................... 11
      3.2.7. MP_RTT ..................................... 11
      3.2.8. MP_ADDADDR ................................ 12
      3.2.9. MP_REMOVEADDR ............................... 12
      3.2.10. MP_PRIO .................................... 12
   3.3. MP-DCCP Handshaking Procedure .................... 12
4. Security Considerations .......................... 13
5. Interactions with Middleboxes ..................... 13
6. Acknowledgments ..................................... 13
7. IANA Considerations ............................... 14
8. Informative References ............................ 14
Authors’ Addresses ....................................... 15
1. Introduction

Multipath DCCP (MP-DCCP) is a set of extensions to regular DCCP [RFC4340], which enables a transport connection to operate across multiple paths simultaneously. DCCP multipath operations is suggested in the context of ongoing 3GPP work on 5G multi-access solutions [I-D.amend-tsvwg-multipath-framework-mpdccp] and for hybrid access networks [I-D.lhwxz-hybrid-access-network-architecture][I-D.muelle-network-based-bonding-hybrid-access]. It can be applied for load-balancing, seamless session handover and aggregation purposes (referred to as steering, switching and splitting in 3GPP terminology [TR23.793]).

This document presents the protocol changes required to add multipath capability to DCCP; specifically, those for signaling and setting up multiple paths ("subflows"), managing these subflows, reassembly of data, and termination of sessions.

1.1. Multipath DCCP in the Networking Stack

MP-DCCP operates at the transport layer and aims to be transparent to both higher and lower layers. It is a set of additional features on top of standard DCCP; Figure 1 illustrates this layering. MP-DCCP is designed to be used by applications in the same way as DCCP with no changes.

```
+-------------------------------+     +-------------------------------+
|           Application         |     |            MP-DCCP            |
|-------------------------------+     |            + - - - - - - + - - - - - - | |
| Application                  |     | MP-DCCP                  |
|-------------------------------+     | Subflow (DCCP) | Subflow (DCCP) |
| DCCP                         |     +-------------------------------+ |
|-------------------------------+     | IP | IP |
| IP                           |     +-------------------------------+ |
|-------------------------------+     +-------------------------------+ |
```

Figure 1: Comparison of Standard DCCP and MP-DCCP Protocol Stacks

1.2. Terminology

[Tbd], could be similar to [RFC6824]

1.3. MP-DCCP Concept
1.4. Differences from Multipath TCP

Multipath DCCP is similar to Multipath TCP [RFC6824], in that it extends the related basic DCCP transport protocol [RFC4340] with multipath capabilities in the same way as Multipath TCP extends TCP [RFC0793]. However, mainly dominated by the basic protocols TCP and DCCP, the transport characteristics are different.

Table 1 compares the protocol characteristics of TCP and DCCP, which are by nature inherited by their respective multipath extensions. A major difference lies in the delivery of payload, which is for TCP an exact copy of the generated byte-stream. DCCP behaves contrary and does not guarantee to transmit any payload nor the order of delivery. Since this is mainly affecting the receiving endpoint of a TCP or DCCP communication, many similarities on sender side can be stated. Both transport protocols share the 3-way initiation of a communication and both exploit a congestion control to adapt to path characteristics.
<table>
<thead>
<tr>
<th>Feature</th>
<th>TCP</th>
<th>DCCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full-Duplex</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Connection- Oriented</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Header option space</td>
<td>40 bytes</td>
<td>&lt; 1008 bytes or PMTU</td>
</tr>
<tr>
<td>Data transfer</td>
<td>reliable</td>
<td>unreliable</td>
</tr>
</tbody>
</table>
| Packet-loss handling          | re-
transmission | report only          |
| Ordered data delivery         | yes       | no                    |
| Sequence numbers              | one per
byte | one per PDU           |
| Flow control                  | yes       | no                    |
| Congestion control            | yes       | yes                   |
| ECN support                   | yes       | yes                   |
| Selective ACK                 | yes       | depends on congestion control |
| Fix message boundaries        | no        | yes                   |
| Path MTU discovery            | yes       | yes                   |
| Fragmentation                 | yes       | no                    |
| SYN flood protection          | yes       | no                    |
| Half-open connections         | yes       | no                    |

Table 1: TCP and DCCP protocol comparison

Consequently, the multipath features, shown in Table 2, are the same, supporting volatile paths, session handover and path aggregation capabilities. All of them profit by the existence of congestion control.
Therefore the sender logic is not much different between MP-DCCP and MPTCP, even if the multipath session initiation differs. MP-DCCP inherits a robust session establishment feature, which guarantees communication establishment if at least one functional path is available. MP-TCP relies on an initial path, which has to work; otherwise no communication can be established.

The receiver side for MP-DCCP has to deal with the unreliable transport character of DCCP and a possible re-assembly of the data stream. In practice, it is assumed that some sort of re-assembly has to be applied, even if DCCP and the order of delivery is unreliable by nature. Such re-assembly mechanisms have to account for the fact that packet loss may occur for any of the DCCP subflows. Another issue is the packet reordering introduced when a DCCP communication is split across paths with disjoint latencies. In theory, applications using DCCP certainly have to deal with packet reordering, since DCCP has no mechanisms to prevent it. However, in practice, without any multipath extension, packet reordering can be assumed to be very limited. Therefore most services on top of DCCP are not expecting massive packet reordering and degrades their performance if it happens anyway.

The receiving process for MP-TCP is on the other hand a simple "just wait" approach, since TCP guarantees reliable delivery.

<table>
<thead>
<tr>
<th>Feature</th>
<th>MP-TCP</th>
<th>MP-DCCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volatile paths</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Robust session establishment</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Data reassembly</td>
<td>yes</td>
<td>optional / modular</td>
</tr>
<tr>
<td>Expandability</td>
<td>limited by TCP header</td>
<td>flexible</td>
</tr>
<tr>
<td>Session handover</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Path aggregation</td>
<td>yes</td>
<td>yes</td>
</tr>
</tbody>
</table>

Table 2: MPTCP and MP-DCCP protocol comparison
1.5. 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 [RFC2119].

2. Operation Overview

[Tbd], could be similar to [RFC6824]

The Multipath Capability for MP-DCCP can be negotiated with a new DCCP feature, as described in Section 3. Once negotiated, all subsequent MP-DCCP operations are signalled with a variable length multipath-related option, as described in Section 3.1.

3. MP-DCCP Protocol

The DCCP protocol feature list ([RFC4340] section 6.4) will be enhanced by a new Multipath related feature with Feature number 10, as shown in Figure 3.

<table>
<thead>
<tr>
<th>Number</th>
<th>Meaning</th>
<th>Rule</th>
<th>Value</th>
<th>Req'd</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Reserved</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Congestion Control ID (CCID)</td>
<td>SP</td>
<td>2</td>
<td>Y</td>
</tr>
<tr>
<td>2</td>
<td>Allow Short Seqnos</td>
<td>SP</td>
<td>0</td>
<td>Y</td>
</tr>
<tr>
<td>3</td>
<td>Sequence Window</td>
<td>NN</td>
<td>100</td>
<td>Y</td>
</tr>
<tr>
<td>4</td>
<td>ECN Incapable</td>
<td>SP</td>
<td>0</td>
<td>N</td>
</tr>
<tr>
<td>5</td>
<td>Ack Ratio</td>
<td>NN</td>
<td>2</td>
<td>N</td>
</tr>
<tr>
<td>6</td>
<td>Send Ack Vector</td>
<td>SP</td>
<td>0</td>
<td>N</td>
</tr>
<tr>
<td>7</td>
<td>Send NDP Count</td>
<td>SP</td>
<td>0</td>
<td>N</td>
</tr>
<tr>
<td>8</td>
<td>Minimum Checksum Coverage</td>
<td>SP</td>
<td>0</td>
<td>N</td>
</tr>
<tr>
<td>9</td>
<td>Check Data Checksum</td>
<td>SP</td>
<td>0</td>
<td>N</td>
</tr>
<tr>
<td>10</td>
<td>Multipath Capable</td>
<td>SP</td>
<td>0</td>
<td>N</td>
</tr>
<tr>
<td>11-127</td>
<td>Reserved</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>128-255</td>
<td>CCID-specific features</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 3: Proposed Feature Set

The DCCP protocol options ([RFC4340] section 5.8) will be enhanced by a new Multipath related variable-length option with option type 45, as shown in Figure 4.
<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
<th>Meaning</th>
<th>Data?</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>Padding</td>
<td>Y</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>Mandatory</td>
<td>N</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>Slow Receiver</td>
<td>Y</td>
</tr>
<tr>
<td>3-31</td>
<td>1</td>
<td>Reserved</td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>variable</td>
<td>Change L</td>
<td>N</td>
</tr>
<tr>
<td>33</td>
<td>variable</td>
<td>Confirm L</td>
<td>N</td>
</tr>
<tr>
<td>34</td>
<td>variable</td>
<td>Change R</td>
<td>N</td>
</tr>
<tr>
<td>35</td>
<td>variable</td>
<td>Confirm R</td>
<td>N</td>
</tr>
<tr>
<td>36</td>
<td>variable</td>
<td>Init Cookie</td>
<td>N</td>
</tr>
<tr>
<td>37</td>
<td>3-8</td>
<td>NDP Count</td>
<td>Y</td>
</tr>
<tr>
<td>38</td>
<td>variable</td>
<td>Ack Vector [Nonce 0]</td>
<td>N</td>
</tr>
<tr>
<td>39</td>
<td>variable</td>
<td>Ack Vector [Nonce 1]</td>
<td>N</td>
</tr>
<tr>
<td>40</td>
<td>variable</td>
<td>Data Dropped</td>
<td>N</td>
</tr>
<tr>
<td>41</td>
<td>6</td>
<td>Timestamp</td>
<td>Y</td>
</tr>
<tr>
<td>42</td>
<td>6/8/10</td>
<td>Timestamp Echo</td>
<td>Y</td>
</tr>
<tr>
<td>43</td>
<td>4/6</td>
<td>Elapsed Time</td>
<td>N</td>
</tr>
<tr>
<td>44</td>
<td>6</td>
<td>Data Checksum</td>
<td>Y</td>
</tr>
<tr>
<td>45</td>
<td>variable</td>
<td>Multipath</td>
<td>Y</td>
</tr>
<tr>
<td>46-127</td>
<td>variable</td>
<td>Reserved</td>
<td></td>
</tr>
<tr>
<td>128-255</td>
<td>variable</td>
<td>CCID-specific options</td>
<td>-</td>
</tr>
</tbody>
</table>

Figure 4: Proposed Option Set

[Tbd] On top it requires particular considerations for:

- The minimum PMTU of the individual paths must be selected to announce to the application. Changes of individual path PMTUs must be re-announced to the application if they are lower than the current announced PMTU.

- Overall sequencing for optional reassembly procedure

- Congestion control

- Robust MP-DCCP session establishment (no dependency on an initial path setup)

### 3.1. Multipath Capable Feature

DCCP endpoints are multipath-disabled by default and multipath capability can be negotiated with the Multipath Capable Feature.

Multipath Capable has feature number 10 and is server-priority. It takes one-byte values. The first four bits are used to specify
compatible versions of the MP-DCCP implementation. The following four bits are reserved for further use.

3.2. Multipath Option

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>00101101</td>
<td>Length</td>
<td>MP_OPT</td>
<td>Value(s)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>------------------</td>
<td>------------------</td>
<td>------------------</td>
<td>------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>----------</td>
<td>------------------</td>
<td>------------------</td>
<td>------------------</td>
<td>------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Type=45</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Option Type Length MP_OPT Meaning
---- ------ ------- ----- 45 7 0 =MP_CONFIRM Confirm reception and processing of an MP_OPT option
45 7 1 =MP_JOIN Join path to an existing MP-DCCP flow
45 3 2 =MP_FAST_CLOSE Close MP-DCCP flow
45 var 3 =MP_KEY Exchange key material for MP_HMAC
45 7 4 =MP_SEQ Multipath Sequence Number
45 23 5 =MP_HMAC HMA Code for authentication
45 12 6 =MP_RTT Transmit RTT values
45 TBD 7 =MP_ADDADDR TBD
45 TBD 8 =MP_REMOVEADDR TBD
45 TBD 9 =MP_PRIO TBD

Figure 5: MP_OPT Option Types

3.2.1. MP_CONFIRM

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>00101101</td>
<td>Length</td>
<td>00000000</td>
<td>List of options</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>------------------</td>
<td>------------------</td>
<td>------------------</td>
<td>------------------</td>
<td>------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>----------</td>
<td>------------------</td>
<td>------------------</td>
<td>------------------</td>
<td>------------------</td>
<td>------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Type=45</td>
<td>MP_OPT=0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

MP_CONFIRM can be used to send confirmation of received and processed options. Confirmed options are copied verbatim and appended as List of options.

3.2.2. MP_JOIN

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>00101101</td>
<td>00001011</td>
<td>00000001</td>
<td>Path Token</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>------------------</td>
<td>------------------</td>
<td>------------------</td>
<td>------------------</td>
<td>------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>----------</td>
<td>------------------</td>
<td>------------------</td>
<td>------------------</td>
<td>------------------</td>
<td>------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Type=45</td>
<td>Length=11</td>
<td>MP_OPT=1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The MP_JOIN option is used to add a new path to an existing MP-DCCP flow. The Path Token is the SHA-1 HASH of the derived key (d-key), which was previously exchanged with the MP_KEY option. MP_HMAC MUST be set when using MP_JOIN to provide authentication (See MP_HMAC for details). Also MP_KEY must be set to provide key material for authentication purposes.

### 3.2.3. MP_FAST_CLOSE

```
+--------+--------+--------+
|00101101|00000011|00000010|
+--------+--------+--------+
```

Type=45  Length=3 MP_OPT=2

MP_FAST_CLOSE terminates the MP-DCCP flow and all corresponding subflows.

### 3.2.4. MP_KEY

```
+--------+--------+--------+--------+--------+--------+--------+
|00101101| Length |00000011|Key Type| Key Data +--------+--------+--------+--------+--------+--------+
|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|
```

Type=45           MP_OPT=3

The MP_KEY suboption is used to exchange key material between hosts. The Key Type field is used to specify the key type. Key types are shown in table Figure 6.

<table>
<thead>
<tr>
<th>Option</th>
<th>Key Type</th>
<th>Key Length</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>=Plain Text</td>
<td>8</td>
<td>Plain Text Key</td>
</tr>
<tr>
<td>1</td>
<td>=ECDHE-C25519-SHA256</td>
<td>32</td>
<td>ECDHE with SHA256 and Curve25519</td>
</tr>
<tr>
<td>2</td>
<td>=ECDHE-C25519-SHA512</td>
<td>32</td>
<td>ECDHE with SHA512 and Curve25519</td>
</tr>
<tr>
<td>3-255</td>
<td></td>
<td>Reserved</td>
<td></td>
</tr>
</tbody>
</table>

Figure 6: MP_KEY Key Types

Plain Text

Key Material is exchanged in plain text between hosts and the key parts (key-a, key-b) are concatenated to form the derived key (d-key).

ECDHE-SHA256-C25519

Key Material is exchanged via ECDHE key exchange with SHA256 and Curve 25519 to generate the derived key (d-key).

ECDHE-SHA512-C25519
Key Material is exchanged via ECDHE key exchange with SHA512 and Curve 25519 to generate the derived key (d-key).

3.2.5. MP_SEQ

+--------+--------+--------+--------+--------+--------+--------+
|00101101|00000111|00000100| Multipath Sequence Number         |
+--------+--------+--------+--------+--------+--------+--------+
  Type=45 Length=7 MP_OPT=4

The MP_SEQ option is used for end-to-end datagram-based sequence numbers of an MP-DCCP connection. The initial data sequence number (IDSN) SHOULD be set randomly.

3.2.6. MP_HMAC

+--------+--------+--------+--------+--------+--------+--------+
|00101101|00000111|00000101| HMAC-SHA1 (20 bytes) ... |
+--------+--------+--------+--------+--------+--------+
  Type=45 Length=23 MP_OPT=5

The MP_HMAC option is used to provide authentication for the MP_JOIN option. The HMAC is built using the derived key (d-key) calculated previously from the handshake key material exchanged with the MP_KEY option. The Message for the HMAC is the header of the MP_JOIN for which authentication shall be performed. By including a nonce in these datagrams, possible replay-attacks are remedied.

3.2.7. MP_RTT

+--------+--------+--------+--------+--------+--------+--------+
|00101101|00000111|00000110|RTT Type| RTT         |
+--------+--------+--------+--------+--------+--------+--------+
  |        | Age                               |
+--------+--------+--------+--------+--------+
  Type=45 Length=12 MP_OPT=6

The MP_RTT option is used to transmit RTT values in milliseconds. Additionally, the age of the measurement is specified in milliseconds.

Raw RTT (=0)

Raw RTT value of the last Datagram Round-Trip. The Age parameter is set to the age of when the Ack for the datagram was received.

Min RTT (=1)

Min RTT value. The period for computing the Minimum can be specified by the Age parameter.
Max RTT (=2)
Max RTT value. The period for computing the Maximum can be specified by the Age parameter.

Smooth RTT (=3)
Averaged RTT value. The period for computing the Minimum can be specified by the Age parameter.

3.2.8. MP_ADDADDR

[TBD]

3.2.9. MP_REMOVEADDR

[TBD]

3.2.10. MP_PRIO

[TBD]

3.3. MP-DCCP Handshaking Procedure

<table>
<thead>
<tr>
<th>Host A</th>
<th>Host B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address A1</td>
<td>Address A2</td>
</tr>
<tr>
<td>Address B1</td>
<td></td>
</tr>
</tbody>
</table>

```
DCCP-Request + MP_CAPABLE
------- MP_KEY(Key-A) ---------------
---------- MP_KEY(Key-B) ---------------
DCCP-Response + MP_CAPABLE agreed

DCCP-Ack
------- MP_KEY(Key-A) + MP_KEY(Key-B) ---------------

DCCP-Request + MP_CAPABLE
--- MP_JOIN(TB,RA) ---------------

DCCP-Response

DCCP-Ack
------- MP_HMAC(B) ---------------

DCCP-ACK
```

Figure 7: Example MP-DCCP Handshake

The basic initial handshake for the first flow is as follows:
o Host A sends a DCCP-Request with the MP-Capable feature Change request and the MP_KEY option with Host-specific Key-A

o Host B sends a DCCP-Response with Confirm feature for MP-Capable and the MP_Key option with Host-specific Key-B

o Host A sends a DCCP-Ack with both Keys echoed to Host B

The handshake for subsequent flows based on a successful initial handshake is as follows:

o Host A sends a DCCP-Request with the MP-Capable feature Change request and the MP_JOIN option with Token TB, derived from the derived key by applying a SHA-1 hash and truncating to the first 32 bits. Additionally, a random nonce RA is transmitted with the MPJOIN.

o Host B computes the HMAC of the DCCP-Request and sends a DCCP-Response with Confirm feature option for MP-Capable and the MP_JOIN option with the Token TB and a random nonce RB together with the computed MP_HMAC.

o Host A sends a DCCP-Ack with the HMAC computed for the DCCP-Response.

o Host B sends a DCCP-Ack confirm the HMAC and to conclude the handshaking.

4. Security Considerations

[Tbd]

5. Interactions with Middleboxes

[Tbd], should mention standardized technologies like [RFC5597] or [RFC6773] and U-DCCP [I-D.amend-tsvwg-dccp-udp-header-conversion]

6. Acknowledgments

1. Notes

This document is inspired by Multipath TCP [RFC6824] and some text passages for the -00 version of the draft are copied almost unmodified.
7. IANA Considerations

[Tbd], must include options for:

- handshaking procedure to indicate MP support
- handshaking procedure to indicate JOINING of an existing MP connection
- signaling of new or changed addresses
- setting handover or aggregation mode
- setting reordering on/off

should include options carrying:

- overall sequence number for restoring purposes
- sender time measurements for restoring purposes
- scheduler preferences
- reordering preferences

8. Informative References

[I-D.amend-tsvwg-dccp-udp-header-conversion]

[I-D.amend-tsvwg-multipath-framework-mpdccp]

[I-D.lhwxz-hybrid-access-network-architecture]
[I-D.muley-network-based-bonding-hybrid-access]


Authors’ Addresses
Markus Amend
Deutsche Telekom
T-Online-Allee 1
64295 Darmstadt
Germany
Email: Markus.Amend@telekom.de

Eckard Bogenfeld
Deutsche Telekom
T-Online-Allee 1
64295 Darmstadt
Germany
Email: Eckard.Bogenfeld@telekom.de

Anna Brunstrom
Karlstad University
Universitetsgatan 2
651 88 Karlstad
Sweden
Email: anna.brunstrom@kau.se

Andreas Kassler
Karlstad University
Universitetsgatan 2
651 88 Karlstad
Sweden
Email: andreas.kassler@kau.se

Veselin Rakocevic
City University of London
Northampton Square
London
United Kingdom
Email: veselin.rakocevic.1@city.ac.uk