QUIC WG   L. Tan
Internet-Draft   Beijing Jiaotong University
Intended status: Informational   X. Gao
Expires: April 18, 2021   China Unicom
                                                           W. Su
                                      Beijing Jiaotong University
                                                           N. Li
                                                       CNCERT/SD
                                                        W. Zhang
                               Shandong Computing Science Center
                                               October 15, 2020

                     Connection Migration in QUIC
                 draft-tan-quic-connection-migration-00

Abstract

   This document explores and classifies QUIC connection migration, and
   suggests possible improvements.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

   This document explores and classifies QUIC connection migration in
   detail.

2. Terminology

2.1. Terms Used In This Document

   This document uses the terminology and concepts established in
   [QUIC-TRANSPORT]. It is assumed that the reader is familiar with the
   above document and the terms defines there.

   The following terms used in this document:

   Endpoint   An entity that can participate in a QUIC connection by
                  generating, receiving, and processing QUIC packets.
                  There are only two types of endpoint in QUIC: client
                  and server.
   QUIC Client   The endpoint that initiates a QUIC connection.
   QUIC Server   The endpoint that accepts a QUIC connection.
   Connection ID An identifier that is used to identify a QUIC
                  connection at an endpoint. Each endpoint selects one
                  or more Connection IDs for its peer to include in
                  packets sent towards the endpoint. This value is
                  opaque to the peer.
   Connection migration The QUIC endpoint uses the connection ID to
                  make connections to survive changes to endpoint
                  addresses.
   Connection migration initiator The endpoint that initiated the
                  connection migration.
   Connection migration responder The peer communicating with the
                  connection migration initiator.
   Path validation Endpoints test reachability between a specific local
                  address and a specific peer address.
   Probing frame A Frame with probing function, such as PATH_CHALLENGE,
                  PATH_RESPONSE, NEW_CONNECTION_ID, and PADDING frame.
   Non-probing frame A frame except the probing frame.
   Probing packet A packet containing only probing frame.
   Non-probing packet A packet containing any other non-probing frame.
   Application   An entity that uses QUIC to send and receive data.

2.2. Abbreviations

The following abbreviations used in this document:

```
CM          Connection Migration.
ACM         Active Connection Migration.
PCM         Passive Connection Migration.
VCM         Vertical Connection Migration.
HCM         Horizontal Connection Migration.
CCM         Client Connection Migration.
SCM         Server Connection Migration.
SPCM        Single-path Connection Migration.
MPCM        Multi-path Connection Migration.
```

3. Connection Migration

QUIC connections are not strictly bound to a single network path.
Connection migration is one of the important features of QUIC.

The QUIC endpoint that initiates the connection migration is called
the connection migration initiator (CM Initiator). The peer is the
connection migration responder (CM Responder).

Connection migration uses connection ID to allow connections to
transfer to a new network path. The use of a connection ID allows
connections to survive changes to endpoint addresses (IP address and
port), such as those caused by an endpoint migrating to a new
network, as shown in Figure Figure 1.

The connection ID MUST be non-zero.

```
            (Before connection migration)
            +--------------+   Non-probing Packet   +--------------+
            | CM Initiator |   ------------------>  |              |
            |(Source IP: 1)|   <------------------  |              |
            +--------------+    Non-probing Packet  |              |
                   |                                |              |
                   |                                |              |
                   |                                |              |
                   v            Probing Packet      |              |
            +--------------+   (PATH_CHALLENGE)      |              |
            |              |   ------------------>   |              |
            |              |   <------------------   |              |
            |              |      Probing Packet     |              |
            |              |     (PATH_RESPONSE)      |              |
            |              |                         | CM Responder |
            |              |      Probing Packet     |              |
            |              |     (PATH_CHALLENGE)     |              |
            | CM Initiator |   <------------------    |              |
            |(Source IP: 2)|   ------------------>   |              |
            |              |      Probing Packet     |              |
            |              |     (PATH_RESPONSE)      |              |
            |              |                         |              |
```

```
|             |   Non-probing Packet  |            |
|             |   ------------------>  |            |
|             |   <------------------  |            |
|             |   Non-probing Packet  |            |
+-------------+                        +-------------+
      (After connection migration)
```
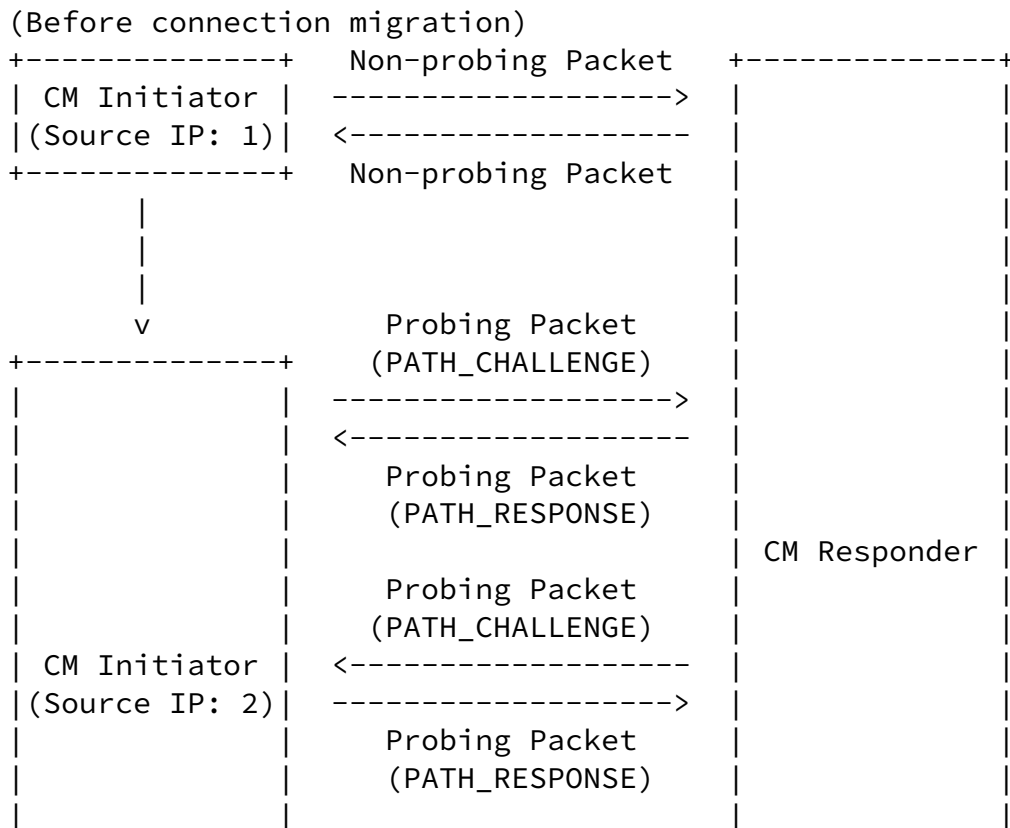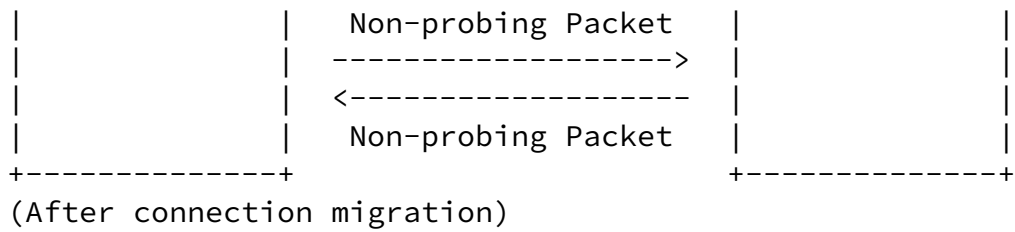
Figure 1: The connection migration

3.1. Initiating Connection Migration

An CM Initiator can migrate a connection to a new local address by
sending packets containing non-probing frames from that address.

3.2. Path Verification

The endpoint sends a PATH_CHALLENGE frame containing a random number
to initialize path verification. Each endpoint validates its peer's
address during connection establishment. Therefore, a migrating
endpoint can send to its peer knowing that the peer is willing to
receive at the peer's current address.

Path verification MUST be performed for most connection migrations,
unless the endpoints have verified the path, the reason is to verify
the reachability and security of the path. But in some special

cases, the connection migration initiator should be allowed to send
data packets directly without path confirmation from the peer. The
condition is to ensure that the packet received by connection
migration responder does not carry a spoofed source address.

Endpoints can use PATH_CHALLENGE frames (type=0x1a) to check
reachability to the peer and for path validation during connection
migration.

PATH_CHALLENGE frames are formatted as shown in Figure Figure 2.

A PATH_RESPONSE frame (type=0x1b) is sent in response to a
PATH_CHALLENGE frame.

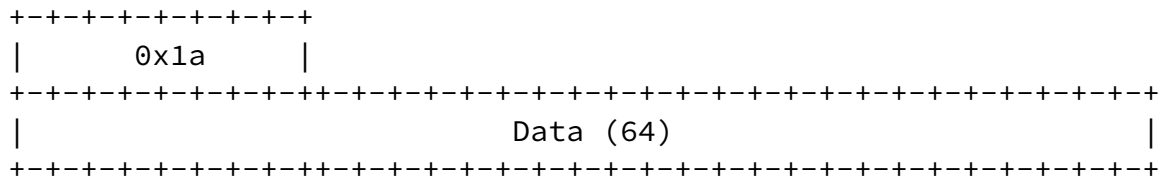PATH_RESPONSE frames are formatted as shown in Figure Figure 3.

```
+-+-+-+-+-+-+-+-+
|     0x1a      |
+-+-+-+-+-+-+-+-++-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Data (64)                           |
+-+-+-+-+-+-+-+-++-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2: PATH_CHALLENGE Frame Format


```
+-+-+-+-+-+-+-+-+
|     0x1b      |
+-+-+-+-+-+-+-+-++-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Data (64)                           |
+-+-+-+-+-+-+-+-++-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
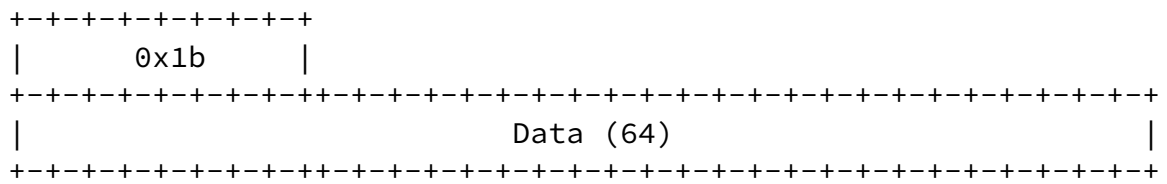
Figure 3: PATH_RESPONSE Frame Format

3.3. Completing Connection Migration

The endpoint receives a packet containing the new peer address of the
non-probing frame from the peer, indicating that the connection
migration initiator has migrated to this address.

After the connection is migrated, the endpoints need to reset the
congestion control parameters.

3.4. Special Cases

Some situations that do not allow connection migration:

1. An endpoint MUST NOT initiate connection migration before the
    handshake is confirmed, as defined in section 4.1.2 of
    [QUIC-TLS].
2. An endpoint MUST NOT initiate connection migration if the peer
```

sent the disable_active_migration transport parameter.

   The section 9.1 of [QUIC-TRANSPORT] analyzes several potential
   security problems and solutions in the process of connection
   migration.

4.  Classification of Connection Migration

   According to business scenarios, connection migration can be divided
   into multiple types, which involve different implementation
   technologies.

4.1.  Active Connection Migration and Passive Connection Migration

   According to different initiators, connection migration can be
   divided into Active Connection Migration (ACM) and Passive Connection
   Migration (PCM).

   From the perspective of the network model, ACM can be regarded as
   connection migration initiated by the application layer, and PCM can
   be regarded as connection migration initiated by the IP layer or
   lower layers.

   ACM requires the IP layer to present all available network
   connections to QUIC.  The application layer or QUIC designs an
   effective connection migration strategy according to the measurement
   results of different network connections to achieve better user
   experience, security and economy.  Available migration strategies
   include threshold-driven migration, polling migration, random
   migration, etc.

   The purpose of PCM is to maintain the connection between the QUIC
   client and the QUIC server in a mobile or weak network environment.
   QUIC is often forced to adapt to PCM.  In addition, NAT/NAPT will
   also cause QUIC endpoints to perform forced connection migration.

4.2.  Vertical Connection Migration and Horizontal Connection Migration

Due to the movement of QUIC terminals or access networks, QUIC needs
to support connection migration in a multi-network access
environment.  Therefore, connection migration in this situation can
be divided into Vertical Connection Migration (VCM) and Horizontal
Connection Migration (HCM).

VCM occurs between heterogeneous networks and HCM occurs in
homogeneous networks.  Due to temporal and spatial changes, VCM and
HCM MAY occur alternately or simultaneously.  Since the HCM occurs
under a homogeneous network, the network before migration MAY have
some similarities with the network after migration.  This guides QUIC
to better maintain connections by drawing on historical information.

4.3.  Client Connection Migration and Server Connection Migration

In most cases, the QUIC server is stationary.  QUIC connection
migration occurs on the QUIC client side.  However, in scenarios such
as P2P networks, mobile servers, and data center four-layer load
balancing, both endpoints of QUIC communication MAY undergo
connection migration.

According to the location, connection migration is divided into
Client Connection Migration (CCM) and Server Connection Migration
(SCM).

The section 9 of [QUIC-TRANSPORT] stipulates that only QUIC clients
can actively initiate connection migration.  The client MUST discard
packets from unknown servers.  The section 9.6 of [QUIC-TRANSPORT]
describes the scene when clients initially connect to an address
shared by multiple servers but would prefer to use a unicast address
to ensure connection stability.  So we believe that the client and
server should be equal, and SCM is necessary.

4.4.  Single-path Connection Migration and Multi-path Connection
      Migration

According to the number of connection paths maintained between the
client and the server during connection migration, connection
migration can be divided into single-path connection migration (SPCM)
and multi-path connection migration (MPCM).

SPCM is a simple and common form of connection migration.  However,
in the future, with the continuous development of heterogeneous
converged networks, it is also possible for endpoints to perform
connection migration while maintaining multi-path transmission.  It
is worth noting that there is a difference between MPCM and MPQUIC

[QUIC-MPQUIC].  MPCM is an event that MAY occur during MPQUIC
transmission.  Therefore, MPCM has more decision variables than SPCM.

## 5.  Connection Migration Strategy

In addition to the connection migration classification in Section 4,
QUIC can also consider connection migration from strategy.

### 5.1.  Failover Mode

In failover mode, the networking stack monitors the quality of the
connection or link, when they are not operating normally, the QUIC
connection is migrated to an alternative path.

QUIC doesn't require any packets to be exchanged before migrating to
a new path, so this migration is seamless.  However, if the new path
hasn't been validated, there's less confidence that it will work.  In
this mode, the QUIC connection MAY be temporarily interrupted.

### 5.2.  Standby Mode

In standby mode, the networking stack establishes and validates an
alternative path shortly after establishing a connection on the main
path.  When the link or the connection deteriorate, QUIC can switch
to the alternative path.

This means that there are two or more logical paths between the QUIC
client and the QUIC server.  In this mode, QUIC always uses only one
of these paths for communication at any time.

### 5.3.  Aggregation Mode

In the aggregation mode, the QUIC client (or QUIC server) can use
MPQUIC [QUIC-MPQUIC] technology to achieve greater network
throughput.  This means that multiple source IPs will share the same
connection ID.

### 5.4.  Load Balance Mode

The section 9.6 of [QUIC-TRANSPORT] detailed load balancing mode.

Servers MAY communicate a preferred address of two or more addresses
to allow clients to pick the one most suited to their network
attachment.  The client SHOULD select one of the two or more
addresses provided by the server and initiate path validation.  As
soon as path validation succeeds, the client SHOULD begin sending all

future packets to the new server address using the new connection ID
and discontinue use of the old server address.

_____

6.  Trigger Condition for Connection Migration

   Except for PCM, other connection migrations can be triggered by RTT,
   packet loss rate, timeout, ECN or application signals.

7.  Security Considerations

   TBD.

8.  IANA Considerations

   TBD.

9.  Acknowledgements

   None.

10.  Normative references

   [QUIC-MPQUIC]
              Coninck, Q. and O. Bonaventure, "Multipath Extensions for
              QUIC (MP-QUIC)", August 2020,
              <https://tools.ietf.org/html/draft-deconinck-quic-
              multipath-05>.

   [QUIC-TLS]
              Thomson, M. and S. Turner, "Using TLS to Secure QUIC",
              September 2020,
              <https://tools.ietf.org/html/draft-ietf-quic-tls-31>.

   [QUIC-TRANSPORT]
              Iyengar, J. and M. Thomson, "QUIC: A UDP-Based Multiplexed
              and Secure Transport", September 2020,
              <https://tools.ietf.org/html/draft-ietf-quic-transport-
              31>.

Authors' Addresses

   Lizhuang Tan

Beijing Jiaotong University
Shangyuan Cun. 3.
Haidian, Beijing  100044
China

Email: lzhtan@bjtu.edu.cn

Xiaochuan Gao
China Unicom
Zhonghe Street. 1.
Daxing, Beijing  100176
China

Email: gaoxc50@chinaunicom.cn


Wei Su
Beijing Jiaotong University
Shangyuan Cun. 3.
Haidian, Beijing  100044
China

Email: wsu@bjtu.edu.cn


Na Li
CNCERT/SD
Jingshiyi Road. 40.
Shizhong, Jinan  250002
China

Email: lina@cert.org.cn


Wei Zhang
Shandong Computing Science Center
Keyuan Road. 19.
Lixia, Jinan  250014
China

Email: wzhang@qlu.edu.cn