Abstract

This document describes how 5G session continuity can affect MPTCP. For now only potential performance issues are identified. This document aims to document discussions that took place at the IETF on this subject, to facilitate future deployment of MPTCP over 5G.

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 August 17, 2019.

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 and Goal .................................. 2
2. Problem Statement ........................................ 2
   2.1. 5G Will Not Hide Session Continuity from MPTCP Any Longer 2
   2.2. Detailed Issues ...................................... 3
3. Potential Solutions ....................................... 4
   3.1. Alternative #1: No Change to MPTCP Protocol .......... 4
   3.2. Alternative #2: Explicit signaling of Session Continuity Type .......................... 5
   3.3. Alternative #3: Client-Driven Handling .............. 6
4. IANA Considerations ...................................... 7
5. Security Considerations ................................... 7
6. Acknowledgements ......................................... 7
7. Informative References ................................... 7
Appendix A. IP Address Session Continuity Service Type .... 8
Appendix B. Overview of 5G Session and Service Continuity ... 8
   B.1. SSC mode 1 ........................................... 9
   B.2. SSC mode 2 ........................................... 9
   B.3. SSC mode 3 ........................................... 10
Appendix C. Example of MPTCP Client Implementations Behavior with 5G SSC .......................... 10
Authors’ Addresses ......................................... 12

1. Introduction and Goal

MPTCP [RFC6824] is being deployed and widely adopted in today’s smart devices, which typically have multiple network interfaces such as Cellular and Wifi. It provides reliability, bandwidth aggregation capability, and handover efficiency.

This document describes how 5G session continuity can affect MPTCP. For now only potential performance issues are identified. This document aims to document discussions that took place at the IETF on this subject, to facilitate future deployment of MPTCP over 5G.

2. Problem Statement

2.1. 5G Will Not Hide Session Continuity from MPTCP Any Longer

In 4G [3GPP.23.401], a single long-term IP address was provided to the end device. Session continuity was performed through a fixed anchor, and effectively hidden from MPTCP.
In 5G, session continuity won’t always be hidden from MPTCP. 3 session continuity modes are defined in [3GPP.23.501]: in some cases, what used to be a single IP address will now be visible by MPTCP as multiple successive and possibly concurrent IP addresses.

More details on session continuity in 5G are provided in Appendix B. In particular, the 5G term for session continuity is Session and Service Continuity (SSC), and the 3 SSC modes correspond to: fixed anchor (mode 1), distributed anchor with break-before-make (mode 2), and distributed anchor with make-before-break (mode 3).

While it could be possible to hide 5G session continuity to MPTCP by limiting its usage to SSC mode 1, it would limit the range of applications that can benefit from MPTCP, since SSC modes 2 and 3 enable low-latency mobility. In the rest of this document, we will study how MPTCP can deal with any SSC mode.

An MPTCP proxy function will be integrated with the 5G network in 3GPP Release-16, enabling a 5G device to use MPTCP over multiple access technologies (e.g. cellular and WiFi) even if the server does not support MPTCP. The normative phase for this feature has recently started and is based on the concluded study [3GPP.23.793].

Potential issues raised in this document may apply to 5G devices directly using MPTCP without a proxy. Assuming that session continuity modes 2 and 3 are available when using the MPTCP proxy (which is possible but not yet established in the standard), these issues may apply to 5G devices making use of the proxy as well.

2.2. Detailed Issues

Overall we don’t expect SSC modes 2 and 3 will cause MPTCP to break, but we do expect inefficiencies in some scenarios. The following potential inefficiencies have been identified:

- Supporting make-before-break (MBB) without wasting resources*: the old IP address should be released shortly after a MBB handover has been performed. Not too early (wait for traffic using the new IP address to ramp up), and not too late (to release resources to the mobile network). Today’s MPTCP implementations are likely to keep using the old IP address as long as it is available, which will prevent the network from releasing the resources early.

- Supporting break-before-make (BBM) without temporarily switching to backup*: if there is a backup IP address, MPTCP peers should not switch to using this backup IP address immediately, and instead should wait for a new replacement IP address to be used after BBM handover. Today’s MPTCP implementations are likely to
switch back-and-forth between active and backup IP addresses, which can lead to network and power consumption inefficiencies.

3. Potential Solutions

Locally on the mobile node itself, a MPTCP implementation will need some information to support session continuity. For each local IP address "IP_A", MPTCP should be aware of the following information:

- Is IP_A provided by a mobile network, and, if applicable, what is its session continuity type? Session continuity type overview and references are listed in Appendix A.
- The original local IP address of the session (if it is not IP_A).

The client can use the tuple (address type, original IP address) to locally support session continuity. An example of implementation behavior is given in Appendix C. For example, a local MPTCP client implementation can use this tuple to appropriately mark new subflows as "backup", when they replace original subflows marked as "backup".

With regard to the behavior of the remote MPTCP peer, three alternatives are identified at this point:

- In alternative #1, we do not implement any specific support in the MPTCP protocol.
- In alternative #2, the MPTCP client sends to its remote peer, over MPTCP signaling, the tuple (address type, original IP address) for each IP address.
- In alternative #3, we use an hybrid solution, where the tuple (address type, original IP address) is not sent to the remote peer; instead, the local MPTCP client influences the remote peer using modified MPTCP signaling.

Some enhancements to the MPTCP protocol are proposed in alternatives #2 and #3. Further discussions and analysis are expected to determine which alternative is best suited for MPTCP.

3.1. Alternative #1: No Change to MPTCP Protocol

This section evaluates the impact of not implementing any specific support in the MPTCP protocol, for the issues mentioned earlier (although the MPTCP client implementation on a 5G device should still be updated to be session continuity-aware, as in all 3 alternatives, to implement client-side behavior such as properly assigning the "backup" property).
*Supporting make-before-break (MBB) without wasting resources*: MBB can impact unmodified MPTCP (1) in term of network resource usage and (2) in term of performances.

Resource usage: unmodified MPTCP will keep using the old IP address until the network physically reclaims the network resources when the lifetime of the old IP address is over. This lifetime is not specified and may be implementation specific. In the worst case, the network operator chooses a long lifetime, with the option to remove the old IP address after sensing it stopped being used, which would not happen with MPTCP.

Performances: when the old IP address is brought down by the network, some in-flight segments will need to be re-sent on other subflows. While the client will be aware of the IP address lifetime, and may therefore stop sending segments on the associated subflow before reaching the end of the address lifetime, the server may continue using this subflow until the address is removed. The impact may therefore vary depending on throughput and the nature of the application.

*Supporting break-before-make (BBM) without temporarily switching to backup*: even if this issue is not addressed in the MPTCP protocol, some applications, e.g. applications generating bursts of traffic, may not be strongly impacted when temporarily switching back and forth between radios, especially if the occurrence is rare enough.

### 3.2. Alternative #2: Explicit signaling of Session Continuity Type

In this case, options that implicitly or explicitly add a new IP address (MP_CAPABLE, ADD_ADDR, MP_JOIN) are associated with additional fields (address type, original IP address index). This way, both MPTCP peers share the same information about the IP address, with regards to session continuity.

*Supporting make-before-break (MBB) without wasting resources*: after the local client creates a new subflow using the new IP address, local client and remote peer both start using it. They continue sending traffic on the old subflow (i.e. subflow using the old IP address), until the traffic usage ramps up on the new subflow. At this point, both peers stop sending new segments on the old subflow. Once in-flight segments are received and acked, the local client resets the old subflow and then remove the old IP address, which makes it possible for the network to ultimately reclaim the network resources.
*Supporting break-before-make (BBM) without temporarily switching to backup*: remote peer and local client are both aware that a BBM is a normal occurrence for IP addresses associated with a "non persistent" type. Therefore, remote peer and local client should both wait for a given time before using a backup subflow. This "BBM timeout" parameter may for example be sent in a new field by the local client to the remote peer, when adding the original "non persistent" IP address.

3.3. Alternative #3: Client-Driven Handling

In this case, session continuity type is not sent over MPTCP signaling. The local client uses non-session-continuity-specific MPTCP signaling to control the behavior of the remote peer. Some minor modifications of the MPTCP protocol may be needed.

*Supporting make-before-break (MBB) without wasting resources*: the local client creates a new subflow using the new IP address. After enough time passed for traffic to ramp up on the new subflow, the local client instructs the remote peer to stop using the old subflow (i.e. subflow using the old IP address), without abruptly closing the subflow, to avoid re-sending segments on the new subflow and affect performance. To do this, the local client sets the priority of the old subflow to "backup", and then waits until in-flight segments are received and acked. At this point, the local client resets the old, now unused subflow. Once no more subflows are using the old IP address, the local client removes it using REMOVE_ADDR.

A new subflow reset reason code "path management decision" may be defined to indicate that a peer took the decision to permanently remove a subflow.

As a minor improvement, a new priority "inactive" may also be defined. "Inactive" would be similar to backup, except that it would never become active, even if no other active subflow exist. This could avoid rare issues when losing active subflows while removing an old subflow.

*Supporting break-before-make (BBM) without temporarily switching to backup*: the local client associates a timer value to a backup priority on a subflow, e.g. using a new field in the MP_PRIO option. When all active subflows are lost, MPTCP peers must wait for the specified time before using the backup subflow. To avoid switching between backup and active subflows in BBM, the local client should ensure that all backup priority timers are set to a value that is higher that the maximum BBM transition time.
4. IANA Considerations

This document requests no IANA actions.

5. Security Considerations

No new security considerations are identified at this time.

6. Acknowledgements

Thanks to following people for contributing through discussions or reviews: Christoph Paasch, Michelle Perras, Debashish Purkayastha, Akbar Rahman, Sri Gundavelli, Philip Eardley, Yoshifumi Nishida.

7. Informative References


Appendix A.  IP Address Session Continuity Service Type

The "session continuity service type" (SCS type) characterises the session continuity properties an IP address allocated by a mobile network. It has been defined for on-demand mobility management [I-D.ietf-dmm-ondemand-mobility], as:

- FIXED IP address: valid for a very long time, for session continuity and IP address reachability.
- SESSION_LASTING IP address: valid for the lifetime of an IP session, even if the mobility host moves.
- NON_PERSISTENT IP address: which does not provide session continuity nor IP address reachability.
- GRACEFUL_REPLACEMENT IP address: similar to a non-persistent address, but adding a limited graceful period for the transition from one address to another.

This information can be conveyed to the device by the network that allocates the address: for example, as described in [I-D.feng-dmm-ra-prefixtype], the SCS type of an IP address may be conveyed through router advertisements.

Although the session continuity service types are not 3GPP-specific, they are planned to be used in the 5G specification from 3GPP, as properties of the IP addresses allocated by the network to mobile devices. There is a 1:1 relationship between the session continuity service type of the initial IP address of a session and the SSC mode of this session (SSC mode is a 3GPP concept discussed in the following section).

Appendix B.  Overview of 5G Session and Service Continuity

One of the goals of 5G systems, as outlined in [3GPP.23.501], is to enable low latency services and access to local data networks where mobility anchors can be deployed close to devices, thereby satisfying...
use cases with stringent transmission delay and high reliability. Mobility in 4G networks, as described at the architecture level in [3GPP.23.401], was based on a central mobility solution that made it difficult to relocate mobility anchors closer to the end user. In contrast, 5G uses a distributed mobility solution based on multiple anchors providing different IP addresses as the device moves from one area to another.

In 5G, every unit of a network connectivity service (PDU session) has a type which can be IP (IPv4 or IPv6), Ethernet or unstructured. Different PDU sessions will typically correspond to distinct network interfaces on the device (though this is not explicit in the standard, and some implementations may possibly behave differently).

In 4G networks, session continuity is enabled by anchoring a PDN Connection (as PDU Sessions are referred to in 4G networks) to a P-GW which allocates an IP address to the mobile device; PDN connection and IP address allocation are maintained as long as the device remains attached to the network, even when the device moves around. In 5G, different types of session continuity can be provided, and are indicated by a "Session and Service Continuity" (SSC) mode value of 1, 2 or 3 (defined in [3GPP.23.501] section 5.6.9). Every PDU session is associated with a single SSC mode, which cannot be changed on this PDU session. The following sub-sections will study how 5G handles each SSC mode, and potential effects on MPTCP.

B.1. SSC mode 1

In SSC mode 1 the same network anchor is kept regardless of device location. An application running on the device will therefore be able to keep using the same IP address on the same interface.

Additionally, in SSC mode 1, the network may decide to add and remove, dynamically, additional network anchors (and therefore IP addresses) to the PDU session, while always keeping the initial one. This would result in a second IP address being allocated on the network interface with which the long-term IP address is associated. This second IP address may be brought down at any time.

B.2. SSC mode 2

SSC mode 2 has a break-before-make behavior. When the device leaves the service area of its first network anchor, the network stops using it and starts using a second network anchor closer to the device. (Such service areas may have a highly variable size depending on network deployments.) On the device, this can result in the currently used network interface being brought down, and after a short time a new network interface being brought up. The time...
between these 2 events is not standardized and implementation dependent.

B.3. SSC mode 3

SSC mode 3 has a make-before-break behavior. When the device leaves the service area of its first network anchor, the network selects a second network anchor closer to the device, and either creates a new PDU session (i.e. new IP address on new network interface) or share the existing PDU session (i.e. new IP address on same network interface). The first network anchor keeps being used for a given time period, which is communicated to the device by the network using the "valid lifetime" field of a prefix information option in a router advertisement ([RFC4861], [RFC4862]). 5G specifications does not mandate a specific range for this valid lifetime. The first/older IP address should not be used to create any new traffic ([RFC4862] section 5.5.4). In some implementations, the network (SMF) may decide to release the first network anchor as soon as it stops carrying traffic.

There is no limit set by the 5G standard for the number of concurrently used network anchors. We expect that in usual cases the first network anchor will be released before a third network anchor starts being used. Nevertheless, to our knowledge nothing prevents a 5G system deployment to allow a third network anchor to be selected while the first one is still in use.

On the 5G device, when using SSC mode 3, mobility will therefore result in a new IP address being configured, either on the same network interface initially used, or on a different network interface. In general, an application will see a single cellular-facing IP address, and during transient phase it will see 2 IP addresses (with a possibility for more than 2 concurrent IP addresses on some 5G system implementations).

Appendix C. Example of MPTCP Client Implementations Behavior with 5G SCC

The following describes at high level how a MPTCP implementation could be modified to on the client to support 5G session continuity. If the solution alternative #2 is used, this behavior can be extended to the MPTCP server as well.

For simplicity, we consider a case where MPTCP is used in a client with 2 IP addresses, one of them being provided by a mobile network. The behaviors described here depend on the session continuity type of the initial mobile network-provided IP address, which has a 1:1 mapping to the 5G SCC mode used.
When the initial IP address session continuity type is FIXED or SESSION_LASTING (i.e. in SCC mode 1):

MPTCP should not close all subflows originated from this original IP address at any point during the session, since this IP address is the only one that is guaranteed, under normal circumstances, to be maintained over time for this application.

At any time during the session, a new IP address of SCS type NON_PERSISTENT may become available. MPTCP may create new subflows for the application, using this IP address (this IP address is likely to provide shorter path subflows, but may disappear at any time).

When the initial IP address session continuity type is NON_PERSISTENT (i.e. in SCC mode 2):

At any point in time, the current NON_PERSISTENT IP address may be taken down by the network stack. The MPTCP implementation should wait for another NON_PERSISTENT IP address to be made available by the network stack. If such an address is made available within a given time limit, the MPTCP stack should create new subflows using this new address (effectively following the existing break-before-make behavior present in MPTCP).

Additionally, if an initial backup IP address is a NON_PERSISTENT address, the MPTCP implementation should consider any subsequent NON_PERSISTENT IP address as a backup IP address in replacement of the initial NON_PERSISTENT address.

When the initial IP address session continuity type is GRACEFUL_REPLACEMENT (i.e. in SCC mode 3):

At any point in time, a new GRACEFUL_REPLACEMENT IP address may be made available by the network stack. The MPTCP implementation must create new subflows using this new address, gracefully transfer traffic to these new subflow(s), and close subflow(s) using the previous GRACEFUL_REPLACEMENT IP address before its scheduled closing (known by obtaining the valid lifetime of the IP address from the operating system).

Additionally, if an initial backup IP address is a GRACEFUL_REPLACEMENT address, the MPTCP implementation should consider any subsequent GRACEFUL_REPLACEMENT IP address as the new backup IP address, in replacement of the first GRACEFUL_REPLACEMENT IP address.
Authors’ Addresses

Xavier de Foy  
InterDigital Communications, LLC  
1000 Sherbrooke West  
Montreal H3A 3G4  
Canada  
Email: Xavier.Defoy@InterDigital.com

Ulises Olvera-Hernandez  
InterDigital Communications, LLC  
64 Great Eastern Street  
London EC2A 3QR  
England  
Email: Ulises.Olvera-Hernandez@InterDigital.com

Uma Chunduri  
Huawei USA  
2330 Central Expressway  
Santa Clara, CA 95050  
USA  
Email: uma.chunduri@huawei.com