

INTAREA
Internet-Draft
Intended status: Standards Track
Expires: January 4, 2018

S. Kanugovi
S. Vasudevan
Nokia
J. Zhu
Intel
F. Baboescu
Broadcom
S. Peng
Huawei
S. Seo
Korea Telecom
J. Mueller
AT&T
July 3, 2017

Control Plane Protocols and Procedures for Multiple Access Management
Services
draft-zhu-intarea-mams-control-protocol-02

Abstract

Today, a device can be simultaneously connected to multiple communication networks based on different technology implementations and network architectures like WiFi, LTE, DSL. In such multi-connectivity scenario, it is desirable to combine multiple access networks or select the best one to improve quality of experience for a user and improve overall network utilization and efficiency. This document presents the control plane protocols, as well as describes control plane procedures for configuring the user plane in a multi access management services (MAMS) framework that can be used to flexibly select the combination of uplink and downlink access and core network paths, and user plane treatment for improving network efficiency and enhanced application quality of experience.

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 January 4, 2018.

Copyright Notice

Copyright (c) 2017 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. Conventions used in this document	3
2. Introduction	3
3. Terminology	3
4. MAMS Control-Plane Protocol	4
5. MAMS User Plane Protocol	4
6. MAMS Control Plane Procedures	6
6.1. Overview	6
6.2. Common fields in MAMS Control Messages	7
6.3. Common procedures for MAMS Control Messages	7
6.3.1. Message Timeout	8
6.3.2. Keep Alive Procedure	8
6.4. Discovery & Capability Exchange	8
6.5. User Plane Configuration	12
6.6. MAMS Path Quality Estimation	14
6.7. MAMS Traffic Steering	16
6.8. MAMS Network ID Indication	17
6.9. MAMS Client Measurement Configuration and Reporting	17
6.10. MAMS Session Termination Procedure	19
7. Applying MAMS Control Procedures with MPTCP Proxy as User Plane	20
8. Applying MAMS Control Procedures for Network Assisted Traffic Steering when there is no convergence layer	25
9. Co-existence of MX Adaptation and MX Convergence Layers	27
10. Security Considerations	27
10.1. MAMS Control plane security	27
10.2. MAMS User plane security	28

11. Contributing Authors	28
12. References	28
12.1. Normative References	28
12.2. Informative References	28
Appendix A. MAMS Control Plane Optimization over Secure Connections	29
Authors' Addresses	30

1. Conventions used in this document

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. Introduction

Multi Access Management Service (MAMS)

[I-D.kanugovi-intarea-mams-protocol] is a framework to select and configure network paths when multiple connections can serve a client device. It allows the path selection and configuration to adapt to dynamic network conditions. It is based on principles of user plane interworking that enables the solution to be deployed as an overlay without impacting the underlying networks.

This document presents the control plane protocols for the MAMS framework. It co-exists and complements user plane protocols (e.g. MPTCP [RFC6824], MPTCP Proxy [I-D.boucadair-mptcp-plain-mode], [I-D.wei-mptcp-proxy-mechanism], GRE [I-D.zhu-intarea-mams-user-protocol]) by providing a way to negotiate and configure them based on client and network capabilities. It allows exchange of network state information and leverages network intelligence to optimize the performance of such protocols.

3. Terminology

"Anchor Connection": Refers to the network path from the N-MADP to the Application Server that corresponds to a specific IP anchor that has assigned an IP address to the client.

"Delivery Connection": Refers to the network path from the N-MADP to the client.

"Network Connection Manager" (NCM), "Client Connection Manager" (CCM), "Network Multi Access Data Proxy" (N-MADP), and "Client Multi Access Data Proxy" (C-MADP) in this document are to be interpreted as described in [I-D.kanugovi-intarea-mams-protocol].

4. MAMS Control-Plane Protocol

The MAMS architecture [I-D.kanugovi-intarea-mams-protocol] introduces the following functional elements,

- o Network Connection Manager (NCM) and Client Connection Manager (CCM) in the control plane, and
- o Network Multi Access Data Proxy (N-MADP) and Client Multi Access Data Proxy (C-MADP) handling the user plane.

Figure 1 shows the default MAMS control plane protocol stack. WebSocket is used for transporting management and control messages between NCM and CCM.

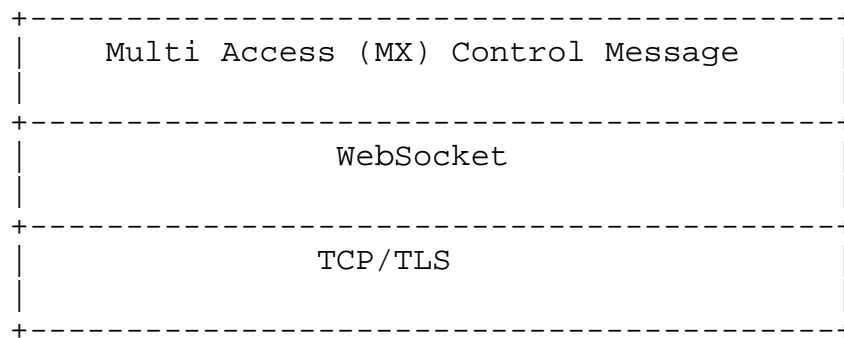


Figure 1: TCP-based MAMS Control Plane Protocol Stack

5. MAMS User Plane Protocol

Figure 2 shows the MAMS user plane protocol stack.

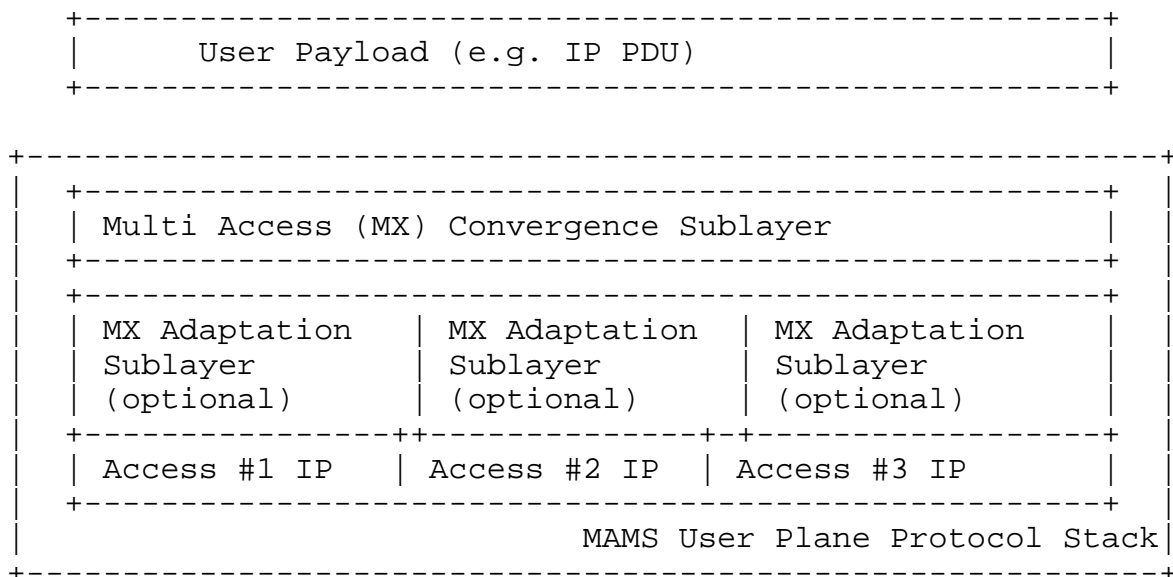


Figure 2: MAMS User Plane Protocol Stack

It consists of the following two Sublayers:

- o Multi-Access (MX) Convergence Sublayer: This layer performs multi-access specific tasks, e.g. access (path) selection, multi-link (path) aggregation, splitting/reordering, lossless switching, fragmentation, concatenation, etc. For example, MX Convergence layer can be implemented using existing user plane protocols like MPTCP or by adapting encapsulating header/trailer schemes (e.g. Trailer Based MX Convergence as specified in [I-D.zhu-intarea-mams-user-protocol]).
- o Multi-Access (MX) Adaptation Sublayer: This layer performs functions to handle tunnelling, network layer security, and NAT. For example, MX Adaptation can be implemented using IPsec, DTLS or Client NAT (Source NAT at Client with inverse mapping at N-MADP [I-D.zhu-intarea-mams-user-protocol]). The MX Adaptation Layer is optional and can be independently configured for each of the Access Links, e.g. in a deployment with LTE (assumed secure) and Wi-Fi (assumed not secure), the MX Adaptation Sublayer can be omitted for the LTE link but MX Adaptation Sublayer is configured as IPsec for the Wi-Fi link.

6. MAMS Control Plane Procedures

6.1. Overview

CCM and NCM exchange signaling messages to configure the user plane functions, C-MADP and N-MADP, at the client and network respectively. The means for CCM to obtain the NCM credentials (FQDN or IP Address) for sending the initial discovery messages are out of the scope of MAMS document, e.g. using methods like provisioning, DNS query. Once the discovery process is successful, the (initial) NCM can update and assign additional NCM addresses for sending subsequent control plane messages.

CCM discovers and exchanges capabilities with the NCM. NCM provides the credentials of the N-MADP end-point and negotiates the parameters for user plane with the CCM. CCM configures C-MADP to setup the user plane path (e.g. MPTCP/UDP Proxy Connection) with the N-MADP based on the credentials (e.g. (MPTCP/UDP) Proxy IP address and port, Associated Core Network Path), and the parameters exchanged with the NCM. The key procedures are described in details in the following sub-sections.

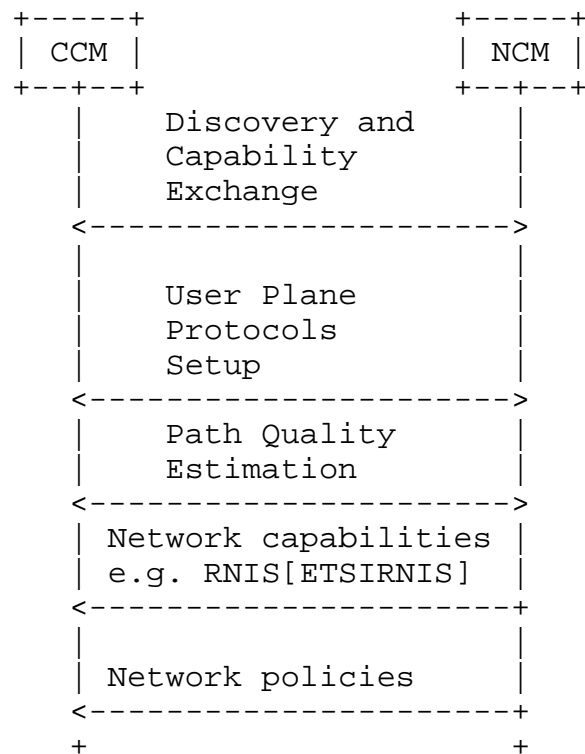


Figure 3: MAMS Control Plane Procedures

6.2. Common fields in MAMS Control Messages

Each MAMS control message consists of the following common fields:

- o Version: indicates the version of MAMS control protocol.
- o Message Type: indicates the type of the message, e.g. MX Discovery, MX Capability REQ/RSP etc.
- o Sequence Number: auto-incremented integer to uniquely identify a transaction of message exchange, e.g. MX Capability REQ/RSP.

6.3. Common procedures for MAMS Control Messages

This section describes the common procedures for MAMS Control Messages.

6.3.1. Message Timeout

MAMS Control plane peer (NCM or CCM) waits for a duration of MAMS_TIMEOUT ms, after sending a MAMS control message, before timing out when expecting a response. The sender of the message will retransmit the message for MAMS_RETRY times before declaring failure. A failure implies that the MAMS peer is dead. CCM may initiate the MAMS discovery procedure for re-establishment of the MAMS session.

6.3.2. Keep Alive Procedure

MAMS Control plane peers execute the keep alive procedures to ensure that peers are reachable and to recover from dead-peer scenarios. Each MAMS control plane end-point maintains a MAMS_KEEP_ALIVE timer that is set for duration MAMS_KEEP_ALIVE_TIMEOUT. MAMS_KEEP_ALIVE timer is reset whenever the peer receives a MAMS Control message. When MAMS_KEEP_ALIVE timer expires, MAMS KEEP ALIVE REQ message is sent. On reception of a MAMS KEEP ALIVE REQ message, the receiver responds with a MAMS KEEP ALIVE RSP message. If the sender does not receive a MAMS Control message in response to MAMS_RETRY number of retries of MAMS KEEP ALIVE REQ message, the MAMS peer declares that the peer is dead. CCM may initiate MAMS Discovery procedure for re-establishment of the MAMS session.

CCM shall additionally send MX KEEP ALIVE REQ message immediately to NCM whenever it detects a handover from one base station/access point to another. During this time the user equipment shall stop using MAMS user plane functionality in uplink direction till it receives a MX KEEP ALIVE RSP from NCM.

MX KEEP ALIVE REQ includes following information:

- o Reason: Can be 'Timeout' or 'Handover'. Reason 'Handover' shall be used by CCM only on detection of handover.
- o Unique Session Identifier: As defined in Section 6.4.
- o Connection Id: This field shall be mandatorily be included if the reason is 'Handover'.
- o Delivery Node Identity (ECGI in case of LTE and WiFi AP Id or MAC address in case of WiFi). This field shall be mandatorily be included if the reason is 'Handover'.

6.4. Discovery & Capability Exchange

Figure 4 shows the MAMS discovery and capability exchange procedure consisting of the following key steps:

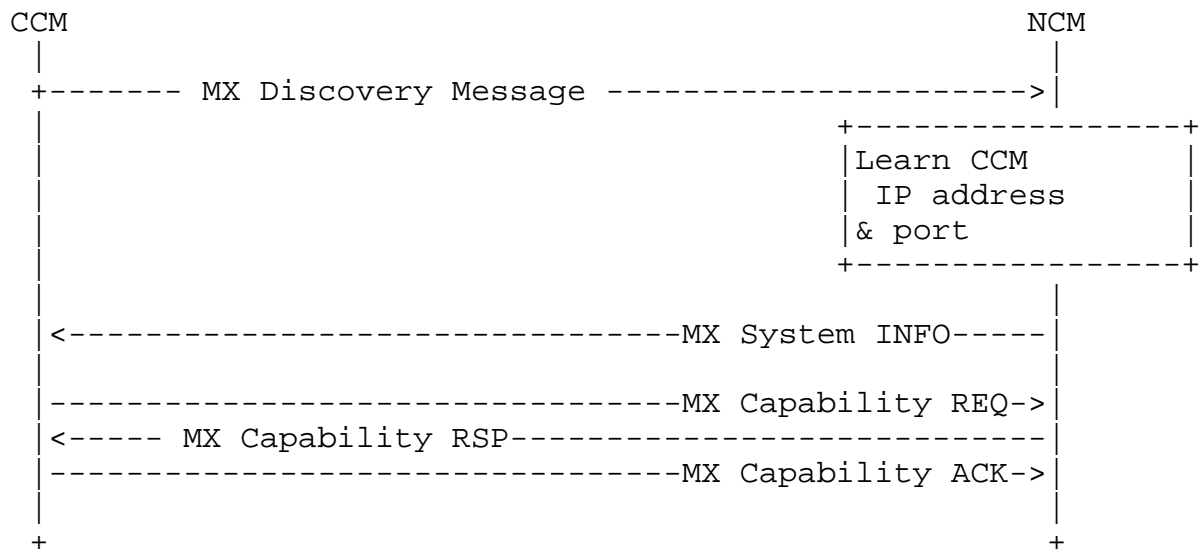


Figure 4: MAMS Control Procedure for Discovery & Capability Exchange

Step 1 (Discovery): CCM periodically sends out the MX Discovery Message to a pre-defined (NCM) IP Address/port until MX System INFO message is received in acknowledgement.

MX Discovery Message includes the following information:

- o MAMS Version

MX System INFO includes the following information:

- o Number of Anchor Connections

For each Anchor Connection, it includes the following parameters:

- * Connection ID: Unique identifier for the Anchor Connection
- * Connection Type (e.g., 0: Wi-Fi; 1: 5G NR; 2: MulteFire; 3: LTE)
- * NCM Endpoint Address (For Control Plane Messages over this connection)
 - + IP Address or FQDN (Fully Qualified Domain Name)
 - + Port Number

Step 2 (Capability Exchange): On receiving MX System Info message CCM learns the IP Address and port to start the step 2 of the control plane connection, and sends out the MX Capability REQ message, including the following Parameters:

- o MX Feature Activation List: Indicates if the corresponding feature is supported or not, e.g. lossless switching, fragmentation, concatenation, Uplink aggregation, Downlink aggregation, Measurement, probing, etc.
- o Number of Anchor Connections (Core Networks)

For each Anchor Connection, it includes the following parameters:

- * Connection ID
- * Connection Type (e.g., 0: Wi-Fi; 1: 5G NR; 2: MulteFire; 3: LTE)
- o Number of Delivery Connections (Access Links)

For each Delivery Connection, it includes the following parameters:

- * Connection ID
- * Connection Type (e.g., 0: Wi-Fi; 1: 5G NR; 2: MulteFire; 3: LTE)
- o MX Convergence Method Support List
 - * Trailer-based MX Convergence
 - * MPTCP Proxy
 - * GRE Aggregation Proxy
- o MX Adaptation Method Support List
 - * UDP Tunnel without DTLS
 - * UDP Tunnel with DTLS
 - * IPsec Tunnel [RFC3948]
 - * Client NAT

In response, NCM creates a unique identity for the CCM session, and sends out the MX Capability RSP message, including the following information:

- o MX Feature Activation List: Indicates if the corresponding feature is enabled or not, e.g. lossless switching, fragmentation, concatenation, Uplink aggregation, Downlink aggregation, Measurement, probing, etc.
- o Number of Anchor Connections (Core Networks)

For each Anchor Connection, it includes the following parameters:

- * Connection ID
- * Connection Type (e.g., 0: Wi-Fi; 1: 5G NR; 2: MulteFire; 3: LTE)
- o Number of Delivery Connections (Access Links)

For each Delivery Connection, it includes the following parameters:

- * Connection ID
- * Connection Type (e.g., 0: Wi-Fi; 1: 5G NR; 2: Multi-Fire; 3: LTE)
- o MX Convergence Method Support List
 - * Trailer-based MX Convergence
 - * MPTCP Proxy
 - * GRE Aggregation Proxy
- o MX Adaptation Method Support List
 - * UDP Tunnel without DTLS
 - * UDP Tunnel with DTLS
 - * IPsec Tunnel [RFC3948]
 - * Client NAT

Unique Session Identifier: Unique session identifier for the CCM which has setup the connection. In case the session for the UE already exists then the existing unique session identifier is sent back.

- o NCM Id: Unique Identity of the NCM in the operator network.
- o Session Id: Unique identity assigned to the CCM instance by this NCM instance.

In response to MX Capability RSP message, the CCM sends confirmation (or reject) in the MX Capability ACK message. MX Capability ACK includes the following parameters

- o Unique Session Identifier: Same identifier as provided in MX Capability RSP.
- o Acknowledgement: An indication if the client has accepted or rejected the capability phase.
 - * MX ACCEPT: CCM Accepts the Capability set proposed by the NCM.
 - * MX REJECT: CCM Rejects the Capability set proposed by the NCM.

If MX_REJECT is received by the NCM, the current MAMS session will be terminated.

If CCM can no longer continue with the current capabilities, it should send an MX SESSION TERMINATE message to terminate the MAMS session. In response, the NCM should send a MX SESSION TERMINATE ACK to confirm the termination.

6.5. User Plane Configuration

Figure 5 shows the user plane configuration procedure consisting of the following key steps:

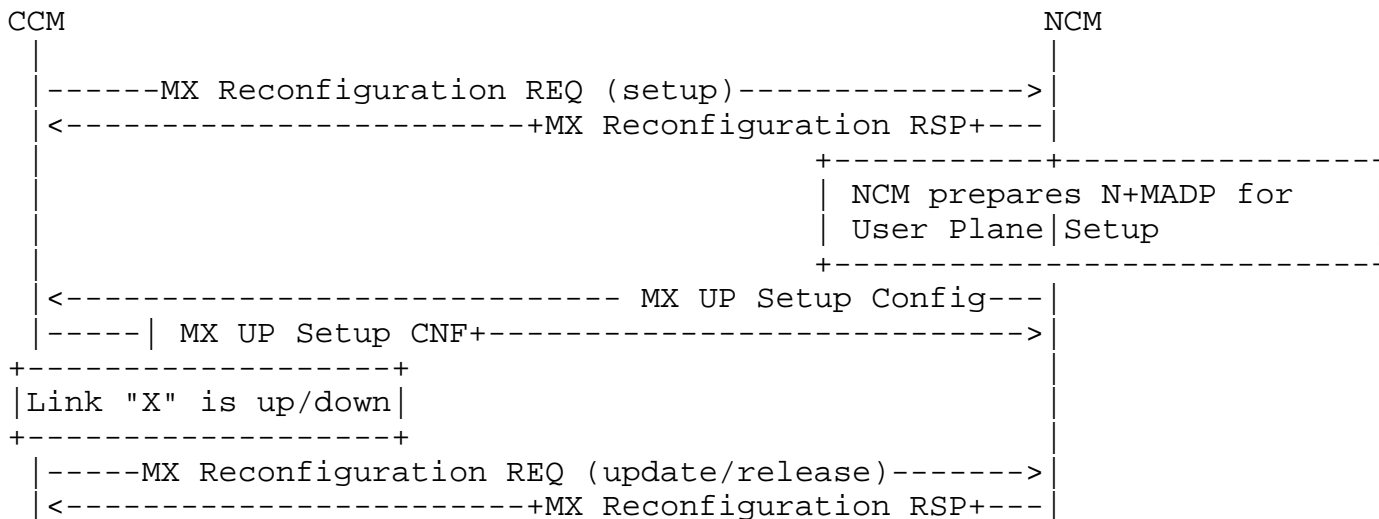


Figure 5: MAMS Control Procedure for User Plane Configuration

Reconfiguration: when the client detects that the link is up/down or the IP address changes (e.g. via APIs provided by the client OS), CCM sends out a MX Reconfiguration REQ Message to setup / release / update the connection, and the message SHOULD include the following information

- o Unique Session Identifier: Identity of the CCM identity at NCM, created by NCM during the capability exchange phase.
- o Reconfiguration Action: indicate the reconfiguration action (0:release; 1: setup; 2: update).
- o Connection ID: identify the connection for reconfiguration

If (Reconfiguration Action is setup or update), then include the following parameters

- o IP address of the connection
- o SSID (if Connection Type = WiFi)
- o MTU of the connection: MTU of the delivery path that is calculated at the UE for use by NCM to configure fragmentation and concatenation procedures[I-D.zhu-intarea-mams-user-protocol] at N-MADP.

- o Delivery Node Identity: Identity of the node to which the client is attached. ECGI in case of LTE and WiFi AP Id or MAC address in case of WiFi.

At the beginning of a connection setup, CCM informs the NCM of the connection status using the MX Reconfiguration REQ message with Reconfiguration Action type set to "setup". NCM acknowledges the connection setup status and exchanges parameters with the CCM for user plane setup, described as follows.

User Plane Protocols Setup: Based on the negotiated capabilities, NCM sets up the user plane (Adaptation Layer and Convergence Layer) protocols at the N-MADP, and informs the CCM of the user plane protocols to setup at the client (C-MADP) and the parameters for C-MADP to connect to N-MADP.

Each MADP instance is responsible for one anchor connection. The MX UP Setup Config consists of the following parameters:

- o Number of Anchor Connections (Core Networks)

For Each Anchor Connection, it includes the following parameters

- * Anchor Connection ID
- * Connection Type (e.g., 0: Wi-Fi; 1: 5G NR; 2: MulteFire; 3: LTE)
- * MX Convergence Method
 - + Trailer-based MX Convergence
 - + MPTCP Proxy
 - + GRE Aggregation Proxy
- * MX Convergence Method Parameters
 - + Convergence Proxy IP Address
 - + Convergence Proxy Port
- * Number of Delivery Connections

For each Delivery Connection, include the following:

- + Delivery Connection ID
- + Connection Type (e.g., 0: Wi-Fi; 1: 5G NR; 2: MulteFire; 3: LTE)
- + MX Adaptation Method
 - UDP Tunnel without DTLS
 - UDP Tunnel with DTLS
 - IPsec Tunnel
 - Client NAT

- + MX Adaptation Method Parameters
 - Tunnel Endpoint IP Address
 - Tunnel Endpoint Port
 - Shared Secret

e.g. When LTE and Wi-Fi are the two user plane accesses, NCM conveys to CCM that IPsec needs to be setup as the MX Adaptation Layer over the Wi-Fi Access, using the following parameters - IPsec end-point IP address, Pre-Shared Key., No Adaptation Layer is needed or Client NAT may be used over the LTE Access as it is considered secure with no NAT. The MX Convergence Method is configured as MPTCP Proxy along with parameters for connection to the MPTCP Proxy, namely IP Address and Port of the MPTCP Proxy for TCP Applications.

Once the user plane protocols are configured, CCM informs the NCM of the status via the MX UP Setup CNF message. The MX UP Setup CNF consists of the following parameters:

- o Unique Session Identifier: Session identifier provided to the client in MX Capability RSP.
- o MX Probe Parameters (included if probing is supported):
 - * UDP Port Number for receiving Probes
- o Client Adaptation Layer Parameters:
 - * Number of Delivery Connections
 - * For each Delivery Connection, include the following:
 - + Delivery Connection ID
 - + UDP port number: If UDP based adaptation is in use, the UDP port at C-MADP side

6.6. MAMS Path Quality Estimation

Path quality estimations can be done either passively or actively. Traffic measurements in the network could be performed passively by comparing the real-time data throughput of the device with the capacity available in the network. The utilization of a cell/eNB attached to a device could be used as an indicator for path quality estimations without creating an extra traffic overhead. Active measurements by the device are alternatives to measure path quality estimations.

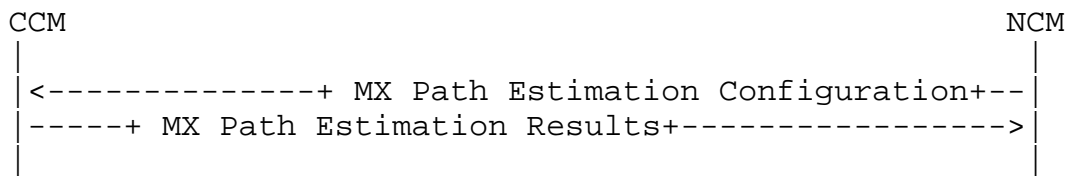


Figure 6: MAMS Control Plane Procedure for Path Quality Estimation

NCM sends following the configuration parameters in the MX Path Estimation Configuration message to the CCM

- o Connection ID (of Delivery Connection whose path quality needs to be estimated)
- o Init Probe Test Duration (ms)
- o Init Probe Test Rate (Mbps)
- o Init Probe Size (Bytes)
- o Init Probe Ack Required (0 -> No/1 -> Yes)
- o Active Probe Frequency (ms)
- o Active Probe Size (Bytes)
- o Active Probe Test Duration (ms)
- o Active Probe Ack Required (0 -> No/1 -> Yes)

CCM configures the C-MADP for probe reception based on these parameters and for collection of the statistics according to the following configuration.

- o Unique Session Identifier: Session identifier provided to the client in MX Capability RSP.
- o Init Probe Results Configuration
 - * Lost Probes (%)
 - * Probe Receiving Rate (packets per second)
- o Active Probe Results Configuration
 - * Average Throughput in the last Probe Duration

The user plane probing is divided into two phases - Initialization phase and Active phase.

- o Initialization phase: A network path that is not included by N-MADP for transmission of user data is deemed to be in the Initialization phase. The user data may be transmitted over other available network paths.

- o Active phase: A network path that is included by N-MADP for transmission of user data is deemed to be in Active phase.

In Initialization phase, NCM configures N-MADP to send an MX Idle Probe REQ message. CCM collects the Idle probe statistics from C-MADP and sends the MX Path Estimation Results Message to NCM per the Initialization Probe Results configuration.

In Active phase, NCM configures N-MADP to send an MX Active Probe REQ message.. C-MADP calculates the metrics as specified by the Active Probe Results Configuration. CCM collects the Active probe statistics from C-MADP and sends the MX Path Estimation Results Message to NCM per the Active Probe Results configuration.

6.7. MAMS Traffic Steering

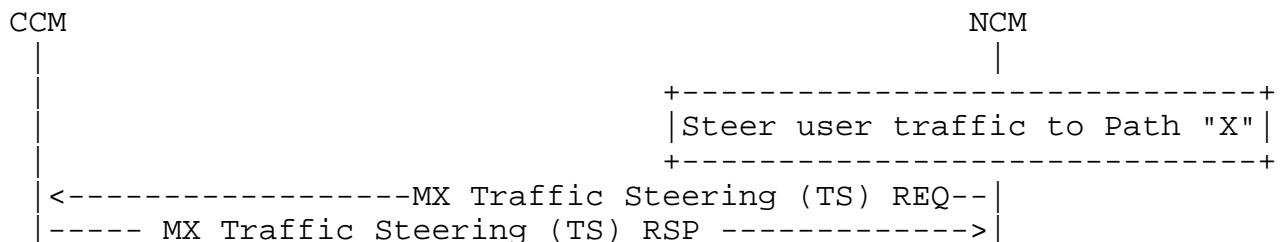


Figure 7: MAMS Traffic Steering Procedure

NCM sends out a MX Traffic Steering (TS) REQ message to steer data traffic. It is also possible to send data traffic over multiple connections simultaneously, i.e. aggregation. The message includes the following information:

- o Connection ID of the Anchor Connection
- o Connection ID List of Delivery Connections for DL traffic
- o For the number of Specific UL traffic Templates, include the following
 - * Traffic Template for identifying the UL traffic
 - * Connection ID List of Delivery connections for UL traffic identified by the traffic template
- o MX Feature Activation List: each parameter indicates if the corresponding feature is enabled or not: lossless switching, fragmentation, concatenation, Uplink aggregation, Downlink aggregation, Measurement, probing

In response, CCM sends out a MX Traffic Steering (TS) RSP message, including the following information:

- o Unique Session Identifier: Session identifier provided to the client in MX Capability RSP.
- o MX Feature Activation List: each parameter indicates if the corresponding feature is enabled or not: lossless switching, fragmentation, concatenation, Uplink aggregation, Downlink aggregation, probing

6.8. MAMS Network ID Indication

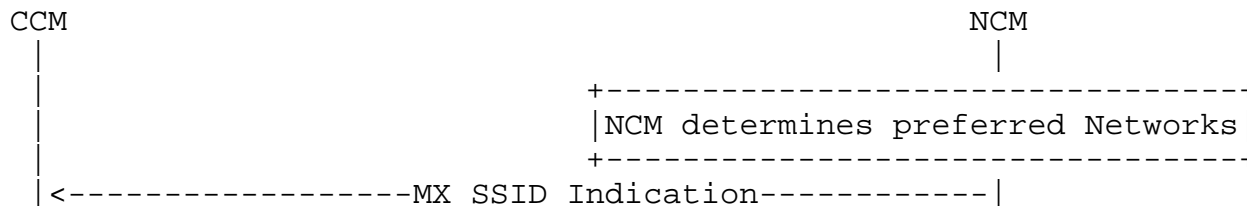


Figure 8: MAMS Network ID Indication Procedure

NCM indicates the preferred network list to the CCM to guide client on networks that it should connect to. To indicate preferred Wi-Fi Networks, the NCM sends the list of WLAN networks, represented by SSID/BSSID/HESSID, available in the MX SSID Indication.

6.9. MAMS Client Measurement Configuration and Reporting

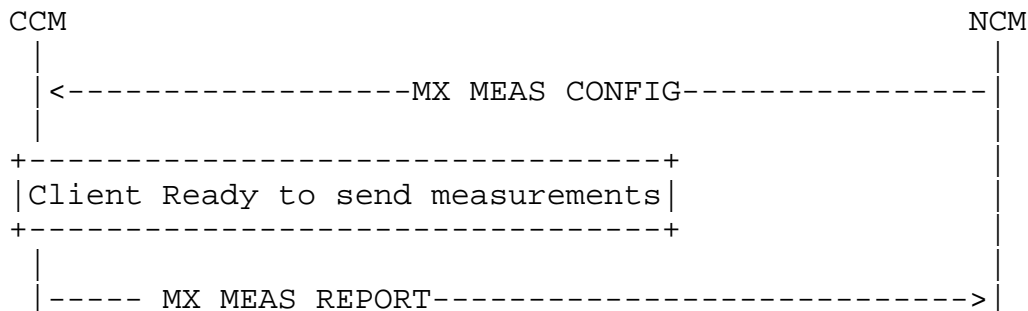


Figure 9: MAMS Client Measurement Configuration and Reporting Procedure

NCM configures the CCM with the different parameters (e.g. radio link information), with the associated thresholds to be reported by the client. The MX MEAS CONFIG message contains the following parameters. For each Delivery Connection, include the following:

- o Delivery Connection ID
- o Connection Type (e.g., 0: Wi-Fi; 1: 5G NR; 2: MulteFire; 3: LTE)
- o If Connection Type is Wi-Fi
 - * WLAN_RSSI_THRESH: High and Low Thresholds for sending Average RSSI of the Wi-Fi Link.
 - * WLAN_RSSI_PERIOD: Periodicity in ms for sending Average RSSI of the Wi-Fi Link.
 - * WLAN_LOAD_THRESH: High and Low Thresholds for sending Loading of the WLAN system.
 - * WLAN_LOAD_PERIOD: Periodicity in ms for sending Loading of the WLAN system.
 - * UL_TPUT_THRESH: High and Low Thresholds for sending Reverse Link Throughput on the Wi-Fi link.
 - * UL_TPUT_PERIOD: Periodicity in ms for sending Reverse Link Throughput on the Wi-Fi link.
 - * DL_TPUT_THRESH: High and Low Thresholds for sending Forward Link Throughput on the Wi-Fi link.
 - * DL_TPUT_PERIOD: Periodicity in ms for sending Forward Link Throughput on the Wi-Fi link.
 - * EST_UL_TPUT_THRESH: High and Low Thresholds for sending Reverse Link Throughput (EstimatedThroughputOutbound as defined in [IEEE]) on the Wi-Fi link.
 - * EST_UL_TPUT_PERIOD: Periodicity in ms for sending Reverse Link Throughput (EstimatedThroughputOutbound as defined in [IEEE]) on the Wi-Fi link.
 - * EST_DL_TPUT_THRESH: High and Low Thresholds for sending Forward Link Throughput (EstimatedThroughputInbound as defined in [IEEE]) on the Wi-Fi link.
 - * EST_DL_TPUT_PERIOD: Periodicity in ms for sending Forward Link Throughput (EstimatedThroughputInbound as defined in [IEEE]) on the Wi-Fi link.
- o If Connection Type is LTE
 - * LTE_RSRP_THRESH: High and Low Thresholds for sending RSRP of Serving LTE link.
 - * LTE_RSRP_PERIOD: Periodicity in ms for sending RSRP of Serving LTE link.
 - * LTE_RSRQ_THRESH: High and Low Thresholds for sending RSRQ of the serving LTE link.
 - * LTE_RSRQ_PERIOD: Periodicity in ms for sending RSRP of Serving LTE link.
 - * UL_TPUT_THRESH: High and Low Thresholds for sending Reverse Link Throughput on the serving LTE link.
 - * UL_TPUT_PERIOD: Periodicity in ms for sending Reverse Link Throughput on the serving LTE link.
 - * DL_TPUT_THRESH: High and Low Thresholds for sending Forward Link Throughput on the serving LTE link.

- * DL_TPUT_PERIOD: Periodicity in ms for sending Forward Link Throughput on the serving LTE link.

The MX MEAS REPORT message contains the following parameters

- o Unique Session Identifier: Session identifier provided to the client in MX Capability RSP.
- o For each Delivery Connection, include the following:
 - * Delivery Connection ID
 - * Connection Type (e.g., 0: Wi-Fi; 1: 5G NR; 2: MulteFire; 3: LTE)
 - * Delivery Node Identity (ECGI in case of LTE and WiFi AP Id or MAC address in case of WiFi)
 - * If Connection Type is Wi-Fi
 - + WLAN_RSSI: Average RSSI of the Wi-Fi Link.
 - + WLAN_LOAD: Loading of the WLAN system.
 - + UL_TPUT: Reverse Link Throughput on the Wi-Fi link.
 - + DL_TPUT: Forward Link Throughput on the Wi-Fi link.
 - + EST_UL_TPUT: Estimated Reverse Link Throughput on the Wi-Fi link (EstimatedThroughputOutbound as defined in [IEEE]).
 - + EST_DL_TPUT: Estimated Forward Link Throughput on the Wi-Fi link (EstimatedThroughputInbound as defined in [IEEE]).
 - * If Connection Type is LTE
 - + LTE_RSRP: RSRP of Serving LTE link.
 - + LTE_RSRQ: RSRQ of the serving LTE link.
 - + UL_TPUT: Reverse Link Throughput on the serving LTE link.
 - + DL_TPUT: Forward Link Throughput on the serving LTE link.

6.10. MAMS Session Termination Procedure

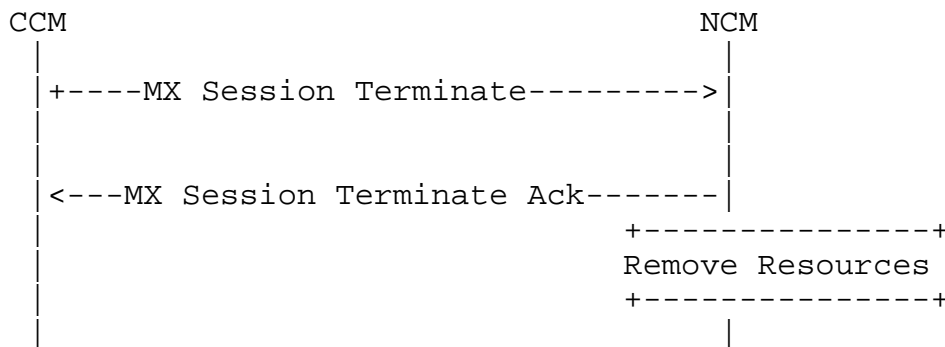


Figure 10: MAMS Session Termination Procedure - Client Initiated

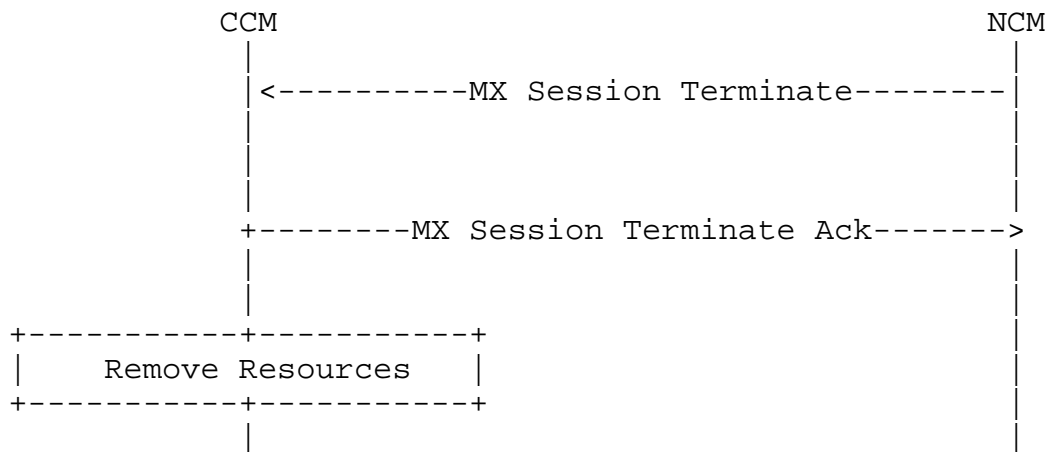


Figure 11: MAMS Session Termination Procedure - Network Initiated

At any point in MAMS functioning if CCM or NCM is unable to support the MAMS functions anymore, then either of them can initiate a termination procedure by sending MX Session Terminate to the peer, the peer shall acknowledge the termination by sending MX Session Terminate ACK message. After the session is disconnected the CCM shall start a new procedure with MX Discover Message. MX Session Terminate message shall contain Unique Session Identifier and reason for termination in Request. Possible reasons for termination can be:

- o Normal Release
- o No Response from Peer
- o Internal Error

7. Applying MAMS Control Procedures with MPTCP Proxy as User Plane

If NCM determines that N-MADP is to be instantiated with MPTCP as the MX Convergence Protocol, it exchanges the MPTCP capability support in discovery and capability exchange procedures. NCM then exchanges the credentials of the N-MADP instance, setup as MPTCP Proxy, along with related parameters to the CCM. CCM configures C-MADP with these parameters to connect with the N-MADP, MPTCP proxy (e.g. [I-D.wei-mptcp-proxy-mechanism], [I-D.boucadair-mptcp-plain-mode]) instance, on the available network path (Access).

Figure 8 shows the call flow describing MAMS control procedures applied to configure user plane and dynamic optimal path selection in a scenario with MPTCP Proxy as the convergence protocol in the user plane.

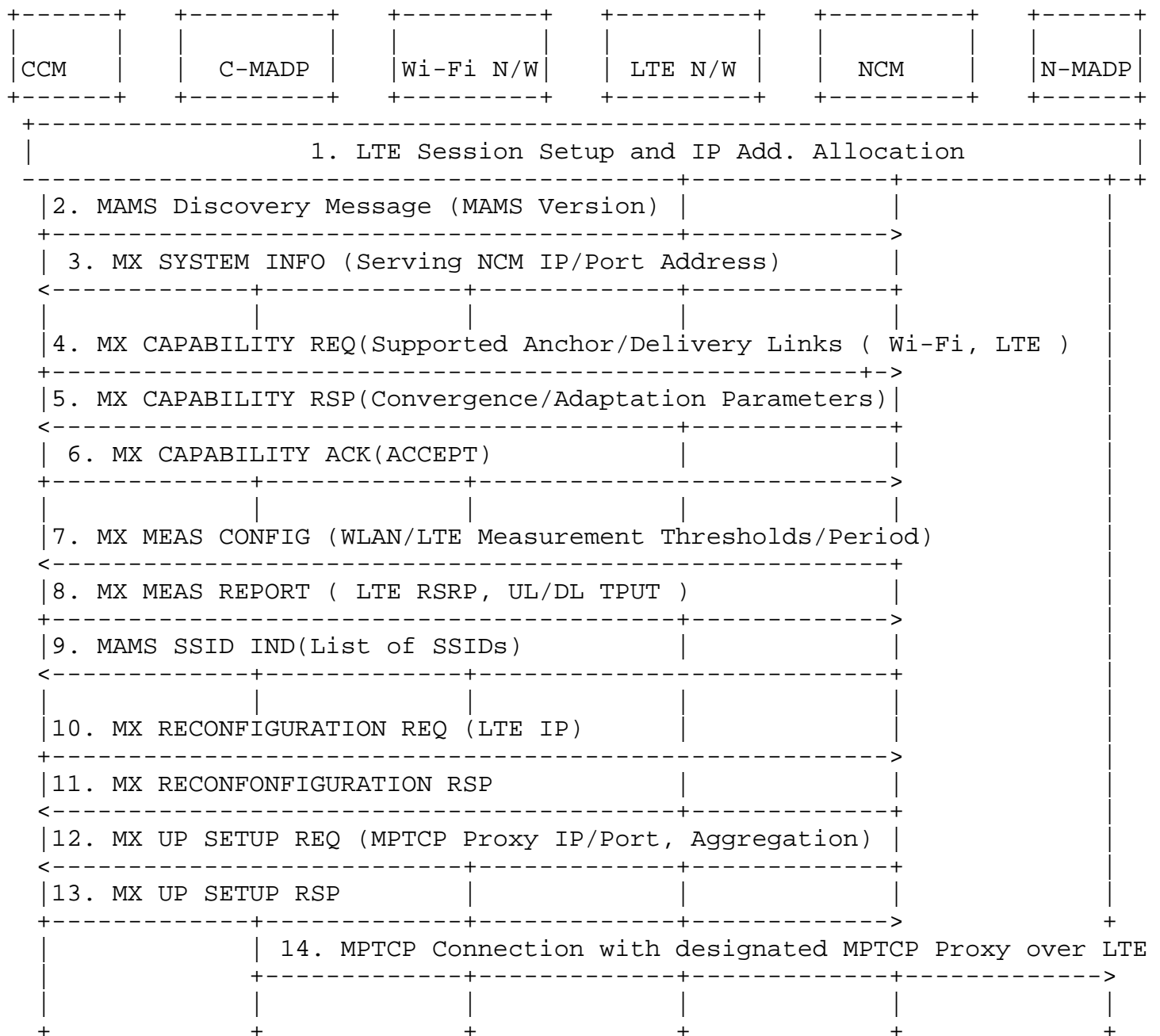


Figure 12: MAMS-assisted MPTCP Proxy as User Plane - Initial Setup with LTE leg

Following are the salient steps described in the call flow. The client connects to the LTE network and obtains an IP address (assume LTE is the first connection), and initiates the NCM discovery procedures and exchange capabilities, including the support for MPTCP as the convergence protocol at both the network and the client.

The CCM informs the LTE connection parameters to the NCM. NCM provides the parameters like MPTCP Proxy IP address/Port for configuring the convergence layer. This is useful if N-MADP is reachable via different IP address or/and port, from different access networks. The current MPTCP signaling can't identify or differentiate the MPTCP proxy IP address and port among multiple access networks. Since LTE is the only connection, the user plane traffic flows over the single TCP subflow over the LTE connection. Optionally, NCM can provide assistance to the device on the neighboring/preferred Wi-Fi networks that it can associate with.

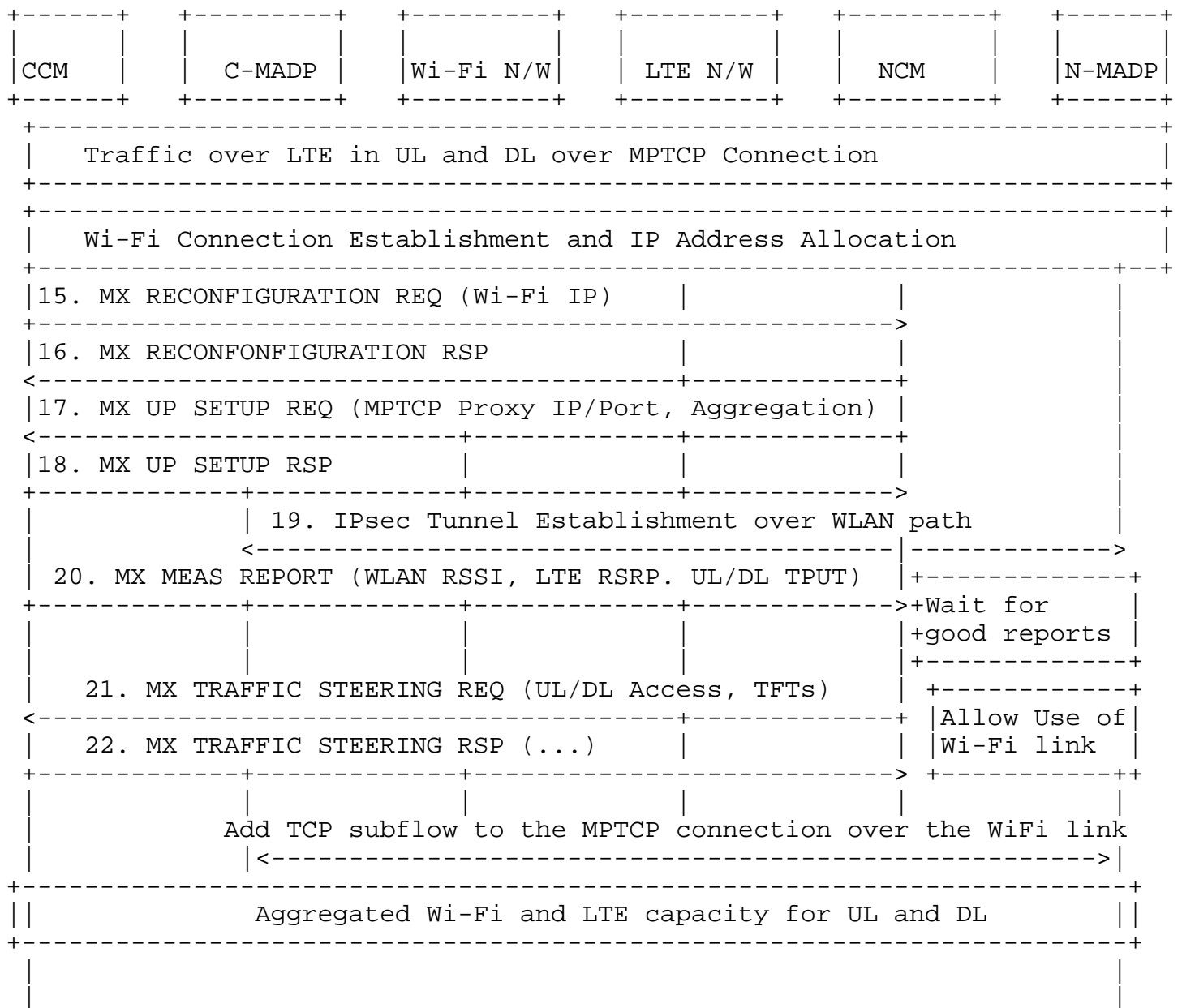


Figure 13: MAMS-assisted MPTCP Proxy as User Plane - Add Wi-Fi leg

Figure 9 describes the steps, when the client establishes a Wi-Fi connection. CCM informs the NCM of the Wi-Fi connection along with parameters like the Wi-Fi IP address, SSID. NCM determines that the Wi-Fi connection needs to be secured configures the Adaptation Layer to be IPsec and provides the required parameters to the CCM. In addition, NCM provides the information to configure the convergence layer, (e.g. MPTCP Proxy IP Address), and provides the Traffic Steering Request to indicate that client should use only the LTE

access. NCM may do this, for example, on determination from the measurements that the Wi-Fi link is not consistently good enough. As the Wi-Fi link conditions improve, NCM sends a Traffic Steering Request to use Wi-Fi access as well. This triggers the client to establish the TCP subflow over the Wi-Fi link with the MPTCP proxy

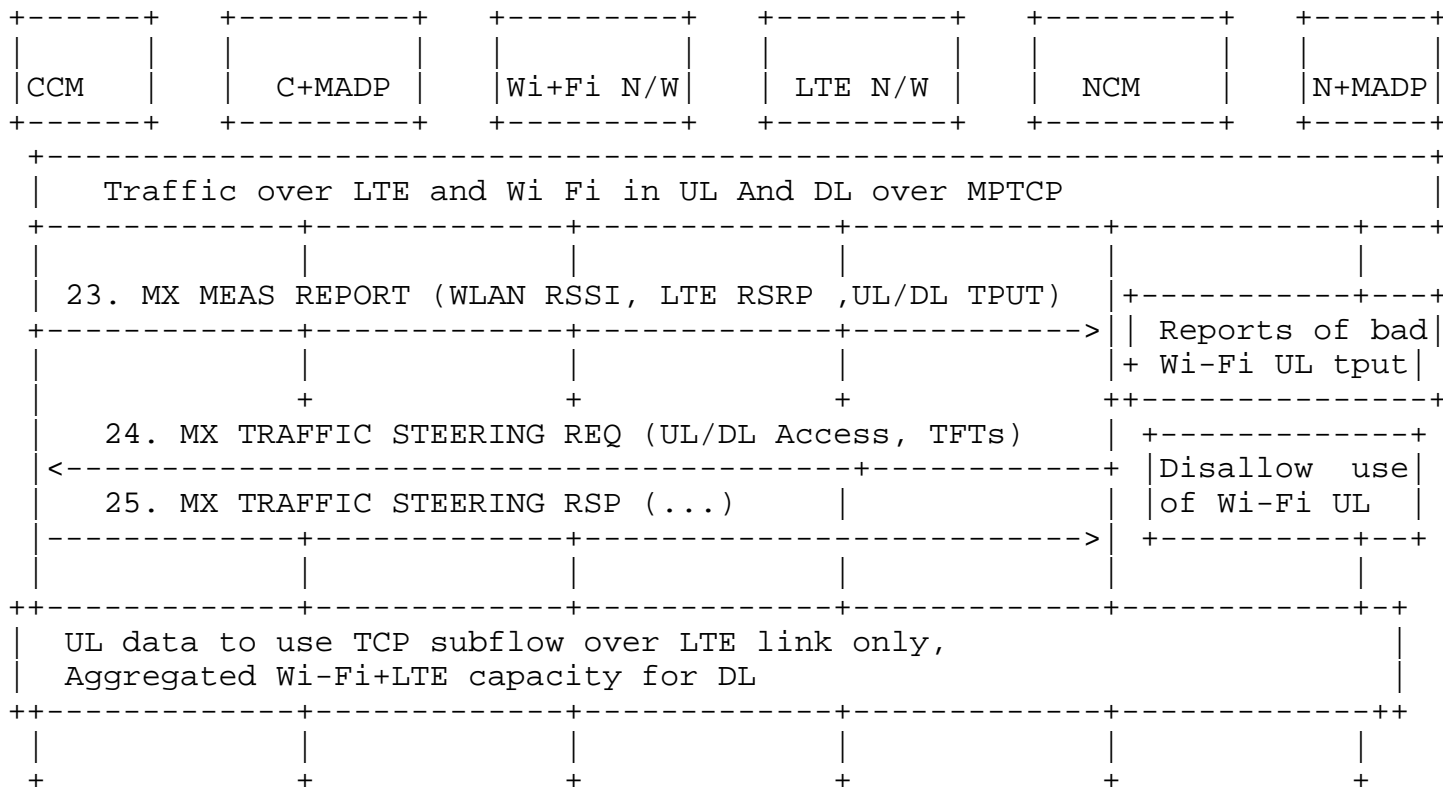


Figure 14: MAMS-assisted MPTCP Proxy as User Plane - Wi-Fi UL degrades

Figure 10 describes the steps, when the client reports that Wi-Fi link conditions degrade in UL. MAMS control plane is used to continuously monitor the access link conditions on Wi-Fi and LTE connections. The NCM may at some point determine increase in UL traffic on Wi-Fi, and trigger the client to only LTE in the UL via Traffic Steering Request to improve UL performance.

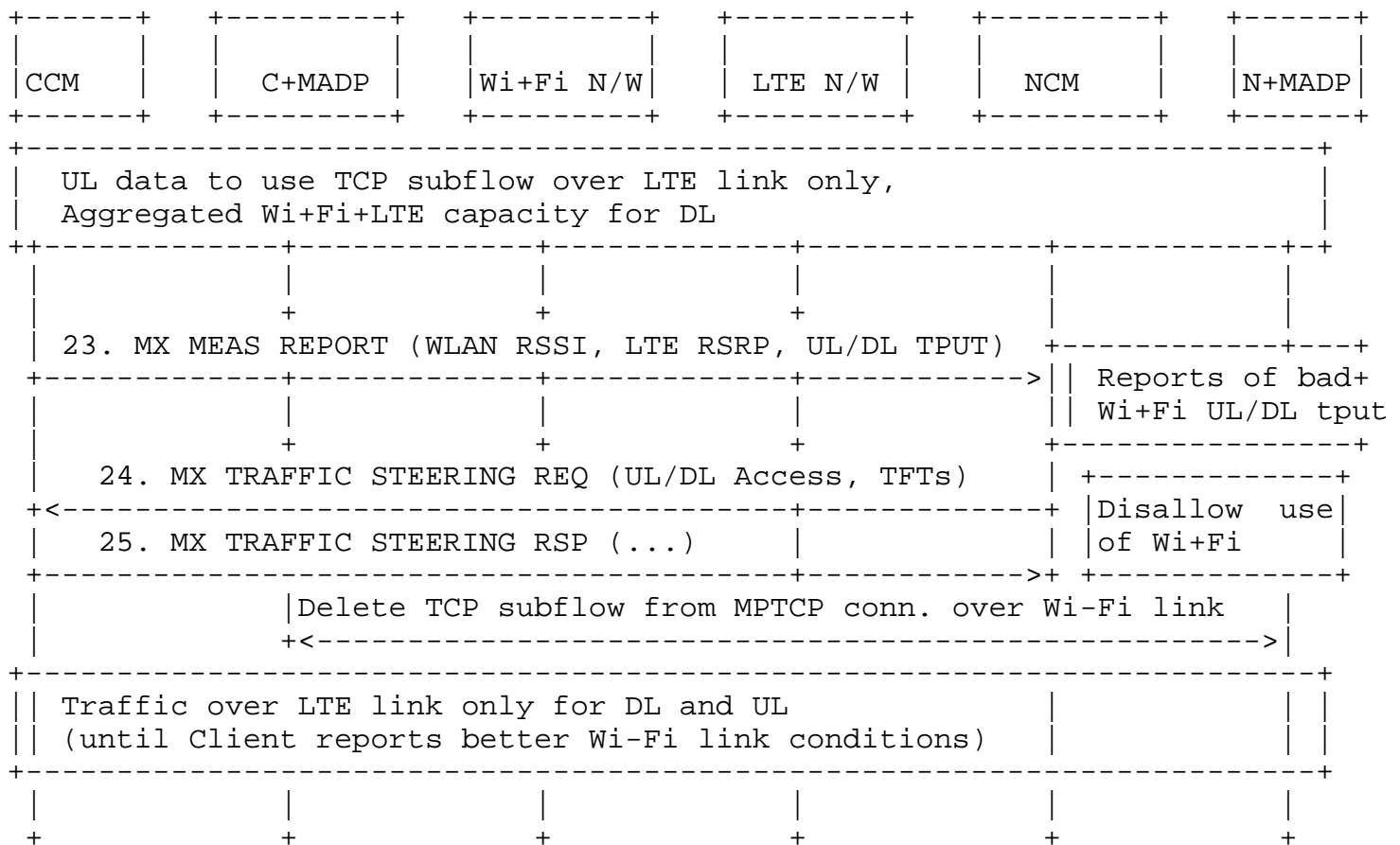


Figure 15: MAMS-assisted MPTCP Proxy as User Plane - Part 4

Figure 11 describes the steps, when the client reports that Wi-Fi link conditions degrade in both UL and DL. As the Wi-Fi link conditions deteriorate further, the NCM may determine to send Traffic Steering Request guiding the client to stop using Wi-Fi, and to use only LTE access in both UL and DL. This condition may be maintained until NCM determines, based on reported measurements that Wi-Fi link has become usable.

8. Applying MAMS Control Procedures for Network Assisted Traffic Steering when there is no convergence layer

Figure Y shows the call flow describing MAMS control procedures applied for dynamic optimal path selection in a scenario convergence and Adaptation layer protocols are not omitted. This scenario indicates the applicability of a MAMS Control Plane only solution.

In the capability exchange messages, NCM and CCM negotiate that Convergence and Adaptation layer protocols are not needed (or

supported). CCM informs the NCM of the availability of the LTE and Wi-Fi links. NCM determines the access links, Wi-Fi or LTE to be used dynamically based on the reported link quality measurements.



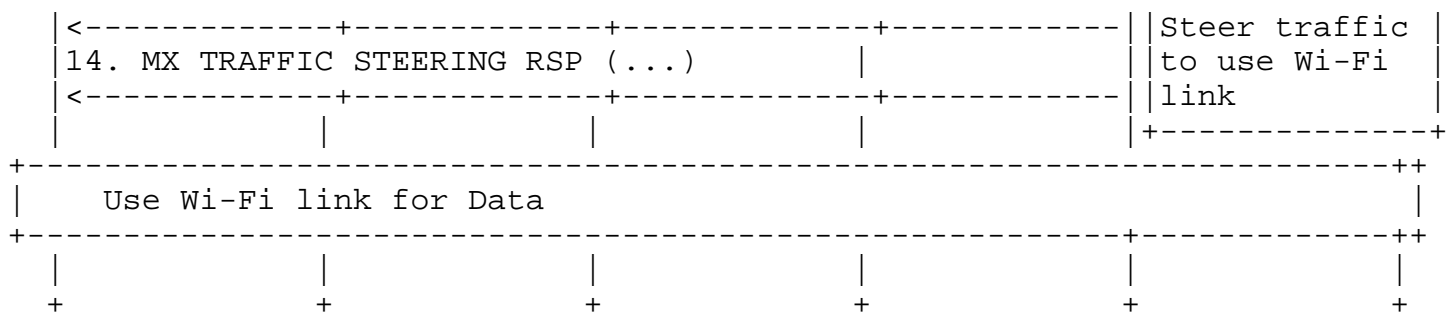


Figure 16: MAMS-assisted MPTCP Proxy as User Plane - Part 3

9. Co-existence of MX Adaptation and MX Convergence Layers

MAMS u-plane protocols support multiple combinations and instances of user plane protocols to be used in the MX Adaptation and the Convergence layer.

For example, one instance of the MX Convergence Layer can be MPTCP Proxy and another instance can be Trailer based. The MX Adaptation for each can be either UDP tunnel or IPsec. IPsec may be set up when network path needs to be secured, e.g. to protect the TCP subflow traversing the network path between the client and MPTCP proxy.

Each of the instances of MAMS user plane, i.e. combination of MX Convergence and MX Adaptation layer protocols, can coexist simultaneously and independently handle different traffic types.

10. Security Considerations

10.1. MAMS Control plane security

For deployment scenarios, where the client is configured (e.g. by the network operator) to use a specific network for exchanging control plane messages and assume the network path to be secure, MAMS control messages will rely on security provided by the underlying transport network.

For deployment scenarios where the security of the network path cannot be assumed, NCM and CCM implementations MUST support the "https" URI scheme [RFC2818] and Transport Layer Security (TLS) [RFC5246] to secure control plane message exchange between the NCM and CCM.

For deployment scenarios where client authentication is desired, HTTP Digest Authentication MUST be supported. TLS Client Authentication is the preferred mechanism if it is available.

10.2. MAMS User plane security

User data in MAMS framework relies on the security of the underlying network transport paths. When this cannot be assumed, NCM configures use of protocols, like IPsec [RFC4301] [RFC3948] in the MX Adaptation Layer, for security.

11. Contributing Authors

The editors gratefully acknowledge the following additional contributors in alphabetical order: A Krishna Pramod/Nokia, Hannu Flinck/Nokia, Hema Pentakota/Nokia, Nurit Sprecher/Nokia

12. References

12.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.
- [RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, December 2005, <<http://www.rfc-editor.org/info/rfc4301>>.

12.2. Informative References

- [ETSIRNIS] "Mobile Edge Computing (MEC) Radio Network Information API", <ETSI GS MEC 012>.
- [I-D.boucadair-mptcp-plain-mode] Boucadair, M., Jacquenet, C., Bonaventure, O., Behaghel, D., stefano.secci@lip6.fr, s., Henderickx, W., Skog, R., Vinapamula, S., Seo, S., Cloetens, W., Meyer, U., Contreras, L., and B. Peirens, "Extensions for Network-Assisted MPTCP Deployment Models", draft-boucadair-mptcp-plain-mode-10 (work in progress), March 2017.

- [I-D.kanugovi-intarea-mams-protocol]
Kanugovi, S., Vasudevan, S., Baboescu, F., Zhu, J., Peng, S., Mueller, J., and S. Seo, "Multiple Access Management Services", draft-kanugovi-intarea-mams-protocol-04 (work in progress), March 2017.
- [I-D.wei-mptcp-proxy-mechanism]
Wei, X., Xiong, C., and E. Ed, "MPTCP proxy mechanisms", draft-wei-mptcp-proxy-mechanism-02 (work in progress), June 2015.
- [I-D.zhu-intarea-mams-user-protocol]
Zhu, J., Seo, S., Kanugovi, S., and S. Peng, "User-Plane Protocols for Multiple Access Management Service", draft-zhu-intarea-mams-user-protocol-02 (work in progress), June 2017.
- [IEEE] "IEEE Standard for Information technology: Telecommunications and information exchange between systems Local and metropolitan area networks: Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.", <IEEE 802.11-2016>.
- [RFC3948] Huttunen, A., Swander, B., Volpe, V., DiBurro, L., and M. Stenberg, "UDP Encapsulation of IPsec ESP Packets", RFC 3948, DOI 10.17487/RFC3948, January 2005, <<http://www.rfc-editor.org/info/rfc3948>>.
- [RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, DOI 10.17487/RFC6347, January 2012, <<http://www.rfc-editor.org/info/rfc6347>>.
- [RFC6824] Ford, A., Raiciu, C., Handley, M., and O. Bonaventure, "TCP Extensions for Multipath Operation with Multiple Addresses", RFC 6824, DOI 10.17487/RFC6824, January 2013, <<http://www.rfc-editor.org/info/rfc6824>>.
- [RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", STD 79, RFC 7296, DOI 10.17487/RFC7296, October 2014, <<http://www.rfc-editor.org/info/rfc7296>>.

Appendix A. MAMS Control Plane Optimization over Secure Connections

If the connection between CCM and NCM over which the MAMS control plane messages are transported is assumed to be secure, UDP is used

as the transport for management & control messages between NCM and UCM (see Figure 9).

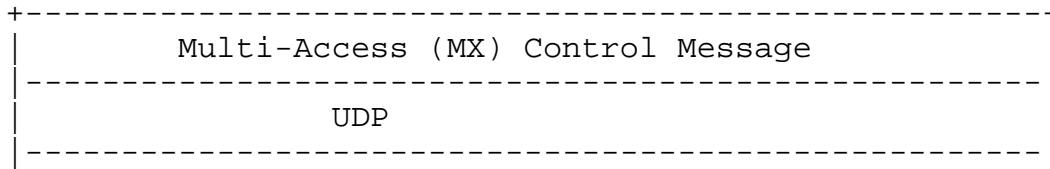


Figure 17: UDP-based MAMS Control plane Protocol Stack

Authors' Addresses

Satish Kanugovi
Nokia

Email: satish.k@nokia.com

Subramanian Vasudevan
Nokia

Email: vasu.vasudevan@nokia.com

Jing Zhu
Intel

Email: jing.z.zhu@intel.com

Florin Baboescu
Broadcom

Email: florin.baboescu@broadcom.com

Shuping Peng
Huawei

Email: pengshuping@huawei.com

SungHoon Seo
Korea Telecom

Email: sh.seo@kt.com

Julius Mueller
AT&T

Email: jml69k@att.com