

INTAREA
Internet-Draft
Intended status: Standards Track
Expires: January 18, 2017

S. Kanugovi
S. Vasudevan
Nokia
F. Baboescu
Broadcom
July 17, 2016

Multiple Access Management Protocol
draft-kanugovi-intarea-mams-protocol-00

Abstract

A communication network includes an access network element that delivers data to/from the user and an associated core network element that typically is the IP gateway having connectivity with the application servers. Multiconnectivity scenarios are common where a device can be simultaneously connected to multiple communication networks based on different technology implementations and network architectures like WiFi, LTE, DSL. A smart combination and selection of access and core network paths can improve quality of experience that a user in a multiconnectivity scenario. This document presents the problem statement and proposes solution principles. It specifies the requirements and reference architecture for a multi access management services framework that can be used to flexibly select the best combination of uplink and downlink access and core network paths, ensuring better network efficiency and enhanced application performance.

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 18, 2017.

Copyright Notice

Copyright (c) 2016 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	2
2. Terminology	3
3. Problem Statement	3
4. Solution Principles	4
5. Requirements	4
5.1. Access technology agnostic interworking	4
5.2. Support common transport deployments	5
5.3. Independent Access path selection for Uplink and Downlink	5
5.4. IP anchor selection independent of uplink and downlink access	5
5.5. Adaptive network path selection	5
5.6. Multipath support and Aggregation of access link capacities	5
5.7. Scalable mechanism based on IP interworking	5
5.8. Separate Control and Data plane functions	6
6. MAMS Reference Architecture	6
7. MAMS call flow	8
8. Security Considerations	9
8.1. Data and Control plane security	9
9. Contributors	9
10. References	10
10.1. Normative References	10
10.2. Informative References	10
Authors' Addresses	10

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. Terminology

"Client": The end-user device supporting connections with multiple access nodes, possibly over different access technologies.

"Multiconnectivity Client": A client with multiple network connections.

"Access network element": The functional element in the network that delivers user data packets to the client via a point-to-point access link like WiFi airlink, LTE airlink, DSL.

"Core": The functional element that anchors the client's IP address used for communication with applications via the network.

"User Plane Gateway": The functional element that can intercept and route user data packets.

"Network Connection manager"(NCM): A functional entity in the network that oversees distribution of data packets over the multiple available access and core network paths.

"Client Connection Manager" (CCM): A functional entity in the client that exchanges MAMS Signaling with the Network Connection Manager and configures the multiple network paths for transport of user data.

"Anchor network element": The functional element in the network with connectivity via multiple access paths to the client.

"Multi Access Data Proxy" (MADP): This entity handles the user data traffic forwarding across multiple network paths.

3. Problem Statement

Typically, a device has access to multiple communication networks based on different technologies, say LTE, WiFi, DSL, MuLTEfire, for accessing application services. Different technologies exhibit benefits and limitations in different scenarios. For example, WiFi leverages the large spectrum available in unlicensed spectrum to deliver high capacities at low cost in uncongested scenarios with small user population, but can show significant degradation in application performance in congested scenarios with large user population. Another example is LTE network, the capacity of which is often constrained by high cost and limited availability of the licensed spectrum, but offers predictable service even in multi-user scenarios due to controlled scheduling and licensed spectrum usage.

Additionally, the use of a particular access network path is often coupled with the use of the associated core network. For example, in an enterprise that has deployed WiFi and LTE communications network, enterprise applications, like printers, Corporate Audio and Video conferencing, are accessible only via WiFi access connected to the enterprise hosted WiFi core, whereas the LTE access can be used to get LTE operator core anchored services including access to public internet.

Application performance in different scenarios, therefore becomes dependent on the choice of the communication networks due to the tight coupling of the access and the core network paths. Therefore to leverage the best possible application performance in the widest possible scenarios, a framework is needed that allows flexible selection of the combination of access and core network paths for application data delivery.

For example, in uncongested scenarios, it would be beneficial to use WiFi access in the uplink and downlink for connecting to enterprise applications. Whereas in congested scenarios, where use of WiFi in uplink by multiple users can lead to degraded capacity and increased delays due to contention, it would be beneficial to use scheduled LTE uplink access combined with WiFi downlink.

4. Solution Principles

This document proposes a Multiple Access Management Services(MAMS) framework for dynamic selection of uplink and downlink access and core network paths for a device connected to multiple communication networks. The selection of paths is based on negotiation of capabilities and network link quality between the device and a functional element in the network, namely the network connection manager. NCM has the intelligence to setup and offer the best network path based on device and network capabilities, application needs and knowledge of the network state.

5. Requirements

The requirements set out in this section are for the behavior of the MAMS mechanism and the related functional elements.

5.1. Access technology agnostic interworking

The access nodes can be of different technology types like LTE, WiFi etc. Since MAMS routes user plane data packets at the IP layer, which makes it agnostic to the type of underlying technology used at the access node for delivery of data to the client.

5.2. Support common transport deployments

The network path selection and user plane distribution should work transparently across transport deployments that include e2e IPsec, VPNs, and middleboxes like NATs and proxies.

5.3. Independent Access path selection for Uplink and Downlink

IP layer routing enables the client to transmit on uplink using one access and receive data on downlink using another access, allowing client and network connection manager to select the access paths for uplink and downlink independent of each other.

5.4. IP anchor selection independent of uplink and downlink access

A client is able to flexibly negotiate the IP anchor, core network, independent of the access paths used to reach the IP anchor depending on the application needs.

5.5. Adaptive network path selection

The network connection manager node has the ability to determine the quality of each of the network paths, e.g. access link delay and capacity. The network path quality information is fed into the logic for selection of combination of network paths to be used for transporting user data. The path selection algorithm can use network path quality information, in addition to other considerations like network policies, for optimizing network usage and enhancing QoE delivered to the user.

5.6. Multipath support and Aggregation of access link capacities

MAMS supports distribution and aggregation of user data across multiple network paths. MAMS allows the client to leverage the combined capacity of the multiple network connections by enabling simultaneous transport of user data over multiple network paths. If required, packet re-ordering is done at the receiver, client and/or the Anchor network element, when user data packets are received out of order. MAMS allows flexibility to choose the flow steering and aggregation protocol based on capabilities supported by the client and the Anchor network element.

5.7. Scalable mechanism based on IP interworking

The mechanism is based on IP interworking, requiring only the IP connectivity between the access nodes and the interworking functionality is based on generically available IP routing and

encapsulation capabilities. This makes solution easy to deploy and scale easily when different networks are added and removed.

5.8. Separate Control and Data plane functions

The client negotiates with a network connection manager the choice of access for both uplink and downlink accesses and the IP anchor(core). The network connection manager configures the actual user data distribution function residing in the Anchor element, thus maintaining a clear separation between the control and data plane functions. This makes the MAMS framework amenable to SDN based architecture and implementations.

6. MAMS Reference Architecture

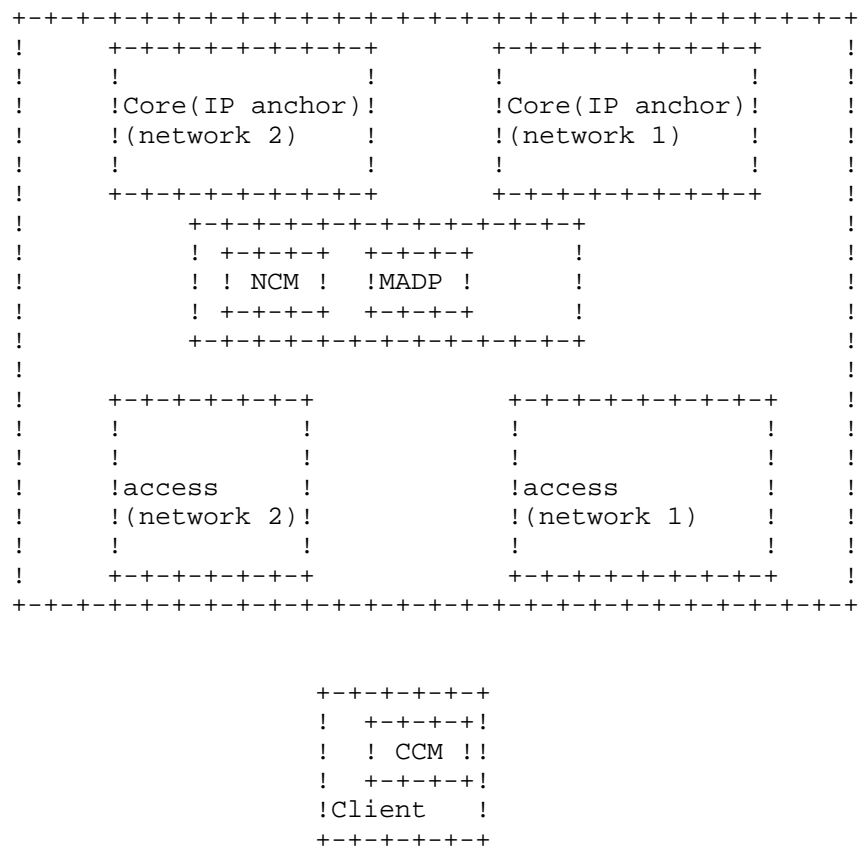


Figure 1: MAMS Reference Architecture

Figure 1 illustrates MAMS architecture for the scenario of a client served by 2 networks. The NCM and MADP, functional elements, are introduced for supporting MAMS mechanisms. The architecture is extendable to combine more than 2 networks, as well as any choice of participating network types (e.g. LTE, WLAN, MuLTEfire, DSL) and deployment architectures (e.g. with user plane gateway function at the access edge).

The MADP entity handles the user data traffic forwarding across multiple network paths. MADP is the distribution node for uplink and downlink data with visibility of packets at the IP layer. Identification and distribution rules for different user data traffic type at the MADP are configured by the NCM. The NCM configures the routing in the MADP based on signaling exchanged with the CCM in the client. In the UL, NCM specifies the core network path to be used by MADP to route uplink user data. In the DL, NCM specifies the access links to be used for delivery of data to the client.

The distribution algorithm at the MADP is configured by the NCM, based on static and/or dynamic network policies like assigning access and core paths for specific user data traffic type, data volume based percentage distribution, and link availability and feedback information from exchange of MAMS signaling with the CCM at the Client.

At the client, the Client Connection Manager (CCM) manages the multiple network connections. CCM is responsible for exchange of MAMS signaling messages with the NCM for supporting functions like configuring UL and DL user network path configuration for transporting user data packets, link sounding and reporting to support adaptive network path selection by NCM. In the downlink, for the user data received by the client, it configures IP layer forwarding for application data packet received over any of the accesses to reach the appropriate application module on the client. In the uplink, for the data transmitted by the client, it configures the routing table to determine the best access to be used for uplink data based on a combination of local policy and network policy delivered by the NCM.

A user plane tunnel, e.g. IPsec, may be needed for transporting user data packets between the MADP and the client. The user plane tunnel is needed to ensure security and routability of the user plane packets between the MADP and the client. The most common implementation of the user plane tunnel is the IPsec. In deployments where the access node belonging to the two networks are connected via a secure and direct IP path, user plane tunnel may not be needed.

7. MAMS call flow

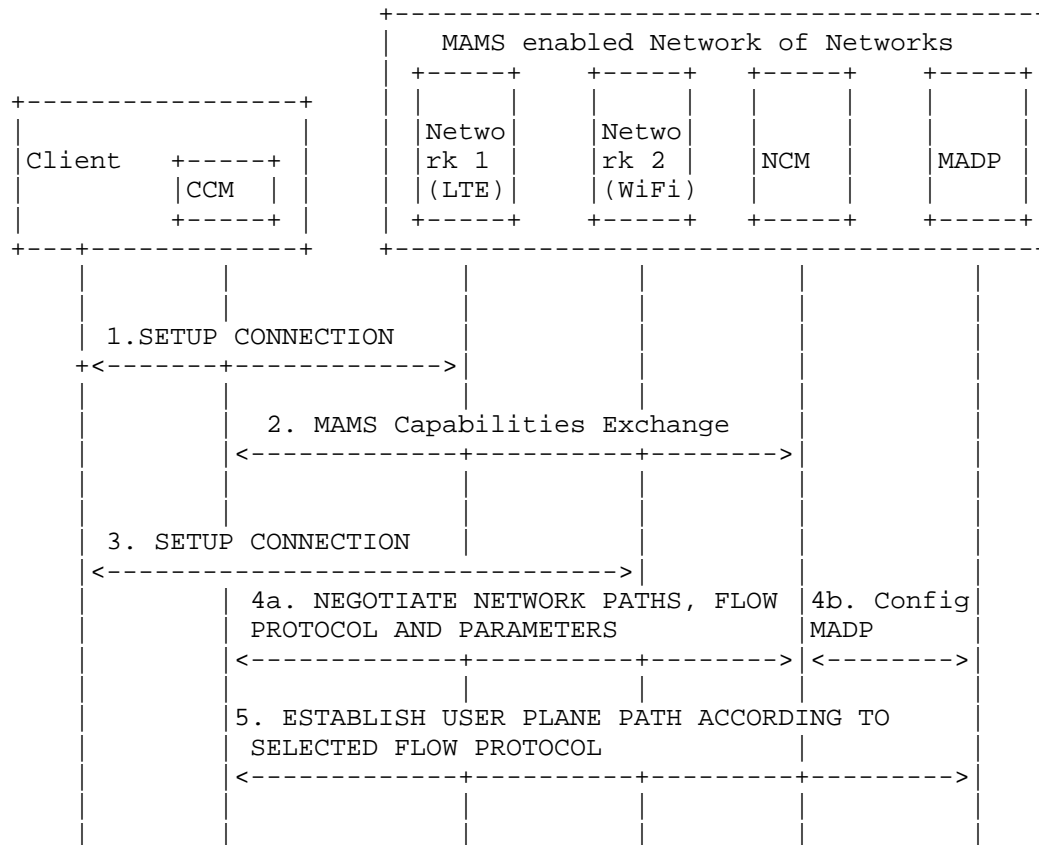


Figure 2: MAMS call flow

Figure 2 illustrates the MAMS signaling mechanism for negotiation of network paths and flow protocols between the client and the network. In this example scenario, the client is connected to two networks (say LTE and WiFi).

1. UE connects to network 1 and gets an IP address assigned by network 1.
2. CCM communicates with NCM functional element via the network 1 connection and exchanges capabilities and parameters for MAMS operation. Note: The NCM credentials can be made known to the UE by pre-provisioning.

3. Client sets up connection with network 2 and gets an IP address assigned by network 2.
4. CCM and MADP negotiate capabilities and parameters with NCM for establishment of network paths.
 - 4a. CCM and NCM negotiate network paths, flow routing and aggregation protocols, and related parameters.
 - 4b. NCM communicates with the MADP to exchange and configure flow aggregation and routing protocols, policies and parameters in alignment with those negotiation with the CCM.
5. CCM and MADP establish the user plane paths, e.g. using IKE [RFC7296] signaling, based on the negotiated flow protocol and parameters specified by NCM.

CCM and NCM can further exchange messages containing access link measurements for link maintenance by the NCM. NCM evaluates the link conditions in the UL and DL across LTE and WiFi, based on link measurements reported by CCM and/or link probing techniques and determines the UL and DL user data distribution policy. NCM configures MADP and CCM with these policies for controlling network paths over which the user data is transported. CCM may apply local policies, in addition to the network policy conveyed by the NCM.

8. Security Considerations

This section details the security considerations for the MAMS framework.

8.1. Data and Control plane security

Signaling messages and the user data in MAMS framework rely on the security of the underlying network transport paths. When this cannot be assumed, network connection manager configures use of protocols, like IPsec [RFC4301] [RFC3948], for securing user data and MAMS signaling messages.

9. Contributors

This protocol is the outcome of work by many engineers, not just the authors of this document. In alphabetical order, the contributors to the project are: Barbara Orlandi, Bongho Kim, David Lopez-Perez, Doru Calin, Jonathan Ling, Krishna Pramod A., Lohith Nayak, Michael Scharf.

10. References

10.1. 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>>.

10.2. Informative References

- [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>>.
- [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>>.

Authors' Addresses

Satish Kanugovi
Nokia

Email: satish.k@nokia.com

Subramanian Vasudevan
Nokia

Email: vasu.vasudevan@nokia.com

Florin Baboescu
Broadcom

Email: florin.baboescu@broadcom.com