

INTERNET-DRAFT
File: [draft-paskalis-rsvmp-00.txt](#)

Sarantis Paskalis
Alexandros Kaloxylas
Lazaros Merakos
University of Athens
Evangelos Zervas
TEI of Athens
15 December 2001

RSVP Mobility Proxy
<[draft-paskalis-rsvmp-00.txt](#)>

Status of this Memo

This document is an Internet-Draft and is subject to all provisions of [Section 10 of RFC2026](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/1id-abstracts.html>

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>

Abstract

Mobility management and QoS provision have been research topics in the past years. Mobile IP is the dominant protocol for mobility management, whereas RSVP is a well established protocol for QoS provision. These protocols when deployed separately can work quite efficiently. However, their interworking has been widely recognized to be problematic. We propose a new approach that limits mobility and QoS related network modifications inside the domain in which a user moves.

1. Introduction

The wireless communication devices industry sector is experiencing an enormous growth in terms of units as well as capabilities for the embedded systems. People are getting accustomed to be productive while on the move, utilizing the capabilities those devices offer. The connectivity support, one of the most essential requirements, is likely to rely on the Internet Protocol architecture. It provides a simple, scalable and robust framework for building data communication applications. However, IP still lacks some of the necessary qualities for the full deployment of applications suitable for those small, yet so powerful devices. Two major factors were not taken into account when designing this model some decades ago: mobility and guaranteed QoS.

Efforts have been underway worldwide to provide support for the missing links of mobility and QoS guarantee. Mobile IP [1] is the dominant protocol for mobility management support developed for IP. Mobile hosts (MHs) are uniquely identified by their Home Address, which corresponds to the address used when located in their home networks. When roaming in foreign networks, MHs request and acquire a new address, the Care-of Address (CoA). This new address is registered with their Home Agent (their mobility enhanced home router) and the MHs become accessible to other hosts through their home network. When route optimization [2] is used, or IPv6 and Mobile IPv6 [3] is deployed, then any host wishing to communicate with the MH uses the CoA for direct communication instead of going through the Home Agent.

Concerning QoS provision, two schools of thought have gained ground in the Internet community: the Integrated Services architecture [4] and the Differentiated Services architecture [5]. RSVP [6] is the signaling protocol for Integrated Services architecture support. It provides a well defined means to specify data flows and to reserve resources in the communication path of the flow. It is designed to deal with end-to-end unidirectional flows, facilitating QoS requests throughout the communication route. In this paper we assume the use of the Fixed Filter reservation style (defined in [6]), suitable for unicast applications.

It is argued that the Integrated Services architecture is best applied to access networks due to its fine-grained classification, whereas core networks can scale better when the Differentiated Services architecture is applied. In our study, we assume that QoS reservations are performed with RSVP in the access network. The core network can support either kind of QoS architecture. If it only supports Differentiated Services, then some interworking scheme can be employed [7].

The aforementioned efforts to provide mobility support and QoS guarantees in the Internet began--and mostly continued--independently, leading to inefficiencies and/or incompatibilities between the approaches. Only recently, was the need for their integration identified. Our proposal builds on the already established schemes for mobility and QoS guarantees and provides the necessary functionality for their seamless integration.

The rest of this draft is organized as follows: [Section 2](#) presents an overview of the problematic interaction of RSVP and Mobile IP. [Section 3](#) introduces the concept of RSVP-MP, i.e. the modifications that are needed to RSVP, and the modified message flows after the functionality change. [Section 4](#) concludes this draft and points to possible further study. [Section 5](#) deals with security considerations of the proposed approach.

2. Problem Formulation

A MH changing points of attachment to the network during an active call is performing a handoff. Two different types of handoffs can be identified: Handoffs between access points that are linked to the same access router and handoffs between access points that are linked to different routers. In the former case, the handoff is handled exclusively at the link layer and no modification in the IP address of the MH is performed. In the latter case, however, a new IP address (CoA) is assigned to the mobile. For our study, we assume an access network large enough to accommodate network layer handoffs, where special Mobile IP-RSVP interworking is required. The topology of such a network is illustrated in Fig. 1. The existence of Mobile IPv4 with route optimization [2] or Mobile IPv6 [3] is also assumed.

If a MH, with established RSVP data flows, performs a network layer handoff, its IP address changes, and a new round of RSVP signaling exchanges must be triggered. RSVP creates soft session states in every intermediate router of the traffic flow. Each session is uniquely identified by the Session object, which is constructed by the triplet <DestAddress, DestPort, [ProtocolId]>. Thus, the downlink reservation (the packet flow toward the mobile) becomes invalid, since the DestAddress parameter has been changed. The new uplink re-establishment is also affected, since the Path messages sent from the MH contain its new IP address. These messages are considered to correspond to a new session and generate a new Path state, according to [8].

With the existing RSVP functionality, independent RSVP sessions are established between the correspondent host and the MH, after the execution of a network layer handoff. The RSVP message exchange is

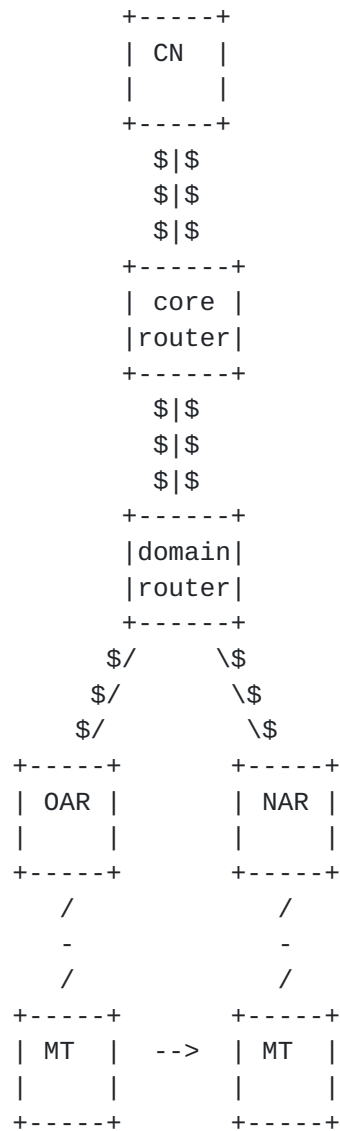


Figure 1: Network Topology

illustrated in Fig. 2. In this signaling exchange, it is assumed that the MH is handed off to the "new" access router, whereas the "old" access router has no way to be informed about the MH's migration. The MH has already acquired a new CoA and has informed its correspondent host (and its Home Agent) about its new location. The MH and the correspondent host begin independently a re-establishment of the resources necessary for a QoS supported session by exchanging Path and Resv messages. These messages contain the new CoA of the mobile and act as new reservation requests.

This scheme is obviously slow, inefficient, and bandwidth consuming. Some of the major problems identified with this approach are the following:

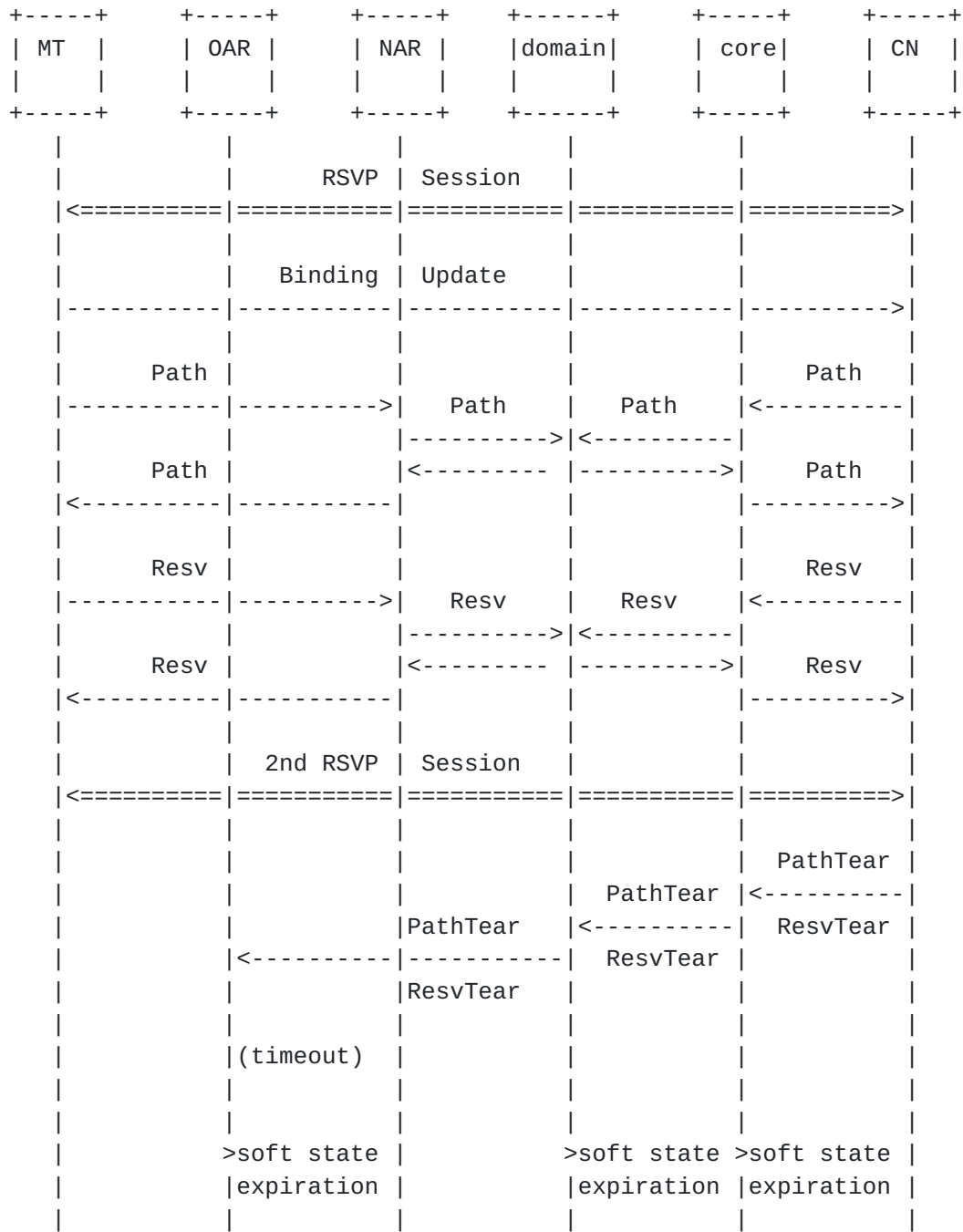


Figure 2: RSVP signaling after a handoff

- o Long delay for reservation re-establishment: RSVP messages must traverse twice the network end-to-end to re-establish a session, resulting in a major deterioration in the quality of active flows.
- o Duplicate reservation of resources for a non-negligible time period: After the execution of a handoff, network resources are

allocated twice for the same session, toward the old and the new location of the MH. This duplication exists until resources on the old path are explicitly released or timed out.

- o Increased blocking probability of new session requests: The duplication of resource requirements in high mobility environments or in networks that support a large number of MHs, can affect the overall efficiency of the network. In such environments a new reservation request will experience a higher probability of getting rejected.
- o Increased cost for providing QoS enabled services: It is safe to assume that the service provider of the access network will have a prearranged Service Level Agreement (SLA) with an upstream Internet Service Provider (ISP, core network provider). Duplication of reserved resources on the access-core link would lead to lower average resource utilization levels for the same cost.

2.1 Previous Work

The interworking problems of Mobile IP and RSVP have been widely recognized and several methods have been proposed to deal with this inconsistency.

Much work has been done both in the IETF and in the research literature to address the RSVP-Mobile IP problematic interaction. An analysis of the current situation is presented in [9] along with guidelines for future refinements. The obvious modification would be to change the RSVP semantics to include a different unique identifier in the Session object (possibly a unique integer) instead of the IP Destination Address [10]. Other proposed approaches include multicast trees, path extension, movement prediction, etc.

The common point in most proposal is that they modify heavily the RSVP functionality and semantics in order to solve the interaction problems between RSVP and Mobile IP. Some other propose the introduction of entirely different protocols which also increase the network resource usage. In the following section we describe a new approach that requires modifications only in the RSVP router at the edge of the access network. Our proposal also minimizes the delay in re-establishing data flows, does not waste network resources, and is compatible with other QoS related protocols

3. RSVP Mobility Proxy

3.1 Reasoning and necessary infrastructure

As [9] and [10] proposed, using a unique and permanent identifier for every RSVP flow should be the basic concept to achieve efficient interworking between RSVP and Mobile IP. Our goal however is to affect as less as possible the existing infrastructure and protocols. The key idea of our proposal is to minimize any modifications (i.e., RSVP flows re-establishments) inside the access network where a MH moves. To achieve this, we propose that a MH may acquire different CoAs (Local Care-of Addresses, LCoAs) while moving inside an access domain, but it would always be reachable by a ``global'' CoA (Regional Care-of Address, RCoA) through tunneling, address translation, host routing or any other routing variety, as suggested in various hierarchical mobility management schemes [17] [18].

In the rest of the paper the existence of such a mobility management functionality is assumed, i.e. the use of a unique RCoA. Note that it is only mandatory to keep the same RCoA for as long as there are on-going connections to/from the MH. The MH may change RCoA when no active connections are in place as proposed in [13]. This could be a useful flexibility when designing the routing functionality.

Furthermore, we assume a mobility management authority component such as the Mobility Anchor Point (MAP) [11] or the Gateway Foreign Agent (GFA) [12], which can supply authoritative answers about the MH's Home Address, location or current CoA.

3.2 Basic Functionality

Based on the aforementioned assumptions, we propose the introduction of the RSVP-MP (RSVP Mobility Proxy). RSVP-MP is actually the router responsible for the RSVP message handling at the edge of the access network and in addition is capable of:

- o keeping track of the correspondence between the RCoAs and the LCoAs and recording any modification of it, by communicating with the mobility controlling authority of the access network (e.g. MAP or GFA).
- o performing dynamic address translation of DCOA to LCOA and vice versa, for packets entering/leaving the access network.

RSVP reservations are made based on the (unique for each MH) RCoA. This means that the IP address of the MH is always represented in the RSVP internal State Blocks (Path State Block PSB, Resv State Block

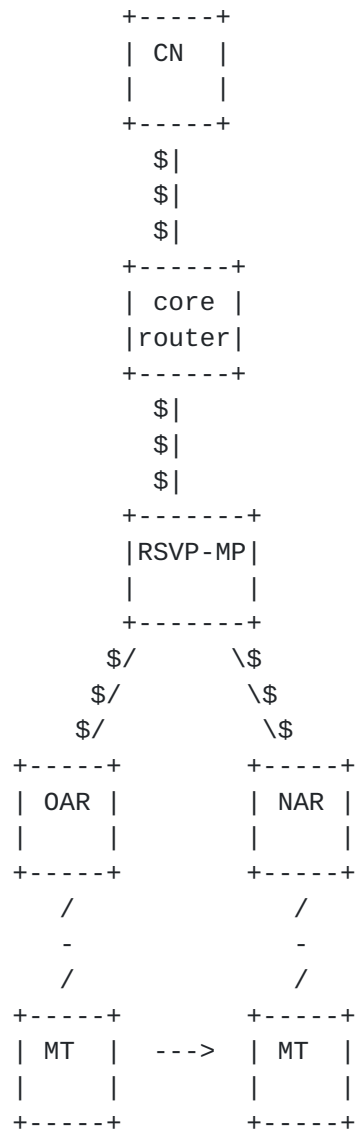


Figure 3: RSVP Mobility Proxy Introduction

RSB, etc.) in its RCoA format. The address translation is performed only at the packet header level at the edge of the network, usually by means of en- or de-capsulation. RSVP messages contain the communicating addresses in their bodies, which must also be replaced by the respective LCoAs or RCoAs (depending whether the packet is forwarded inward or outward of the mobile access network).

The RSVP messages are translated into their ``DCOA'' format before PSB, RSB updating takes place. Some functions in the RSVP message processing though require knowledge of the RCoA-LCoA binding to operate correctly. These functions are identified in the following analysis. The states for the other State Blocks must be updated accordingly. We examine the processing of the four basic message

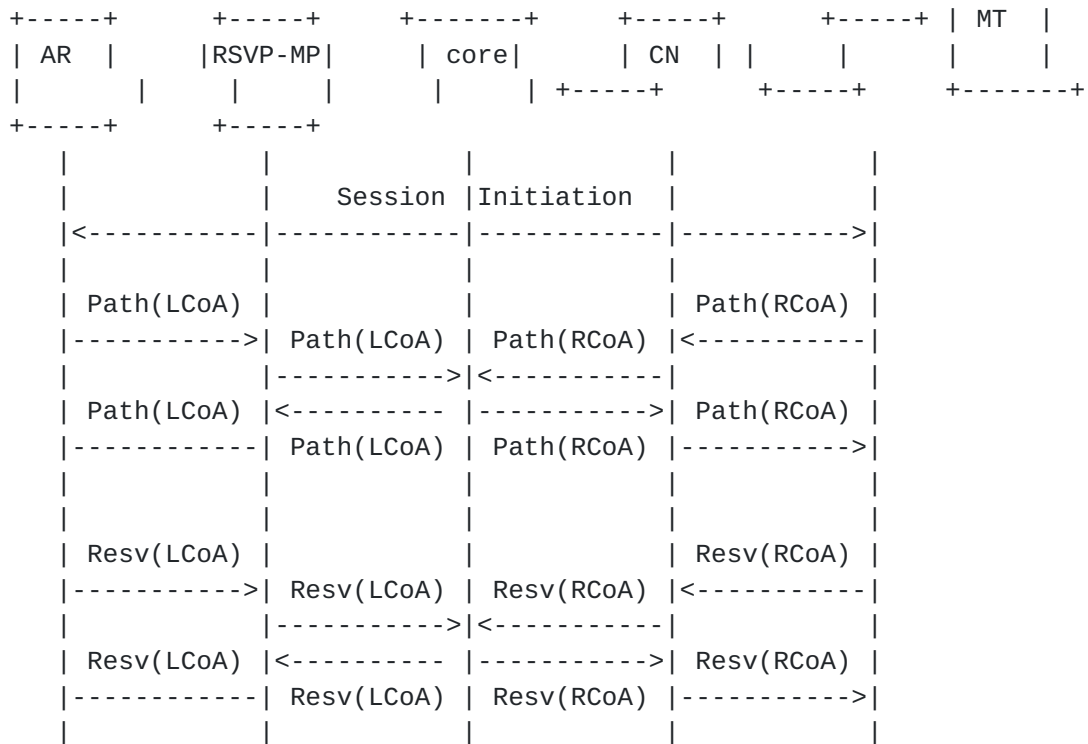


Figure 4: Initial RSVP Session Establishment with RSVP-MP

cases in RSVP-MP and point out the implementation differences in comparison to [8]. The important factors are the type of the message and the incoming interface.

1. Path message from an internal interface (LCoA)
 - o Swap LCoA in the source header of the packet with RCoA.
 - o Swap LCoA in the Sender_Template object with RCoA.
 - o Update PSB.
 - o Forward Path to the respective external interface.
2. Resv message from an external interface (RCoA)
 - o Swap RCoA in the Sender_Template object with LCoA. This object resides in the Resv message's Filter_Spec object, which is contained in the flow descriptor in the RSVP message.
 - o Check if reservation is possible (resources, policy).
 - o Update RSB.

- o Send Resv to next (internal) hop.
3. Path message from an external interface (RCoA)
- o Update PSB. The update_PSB function contains a route query routine, which must be enhanced to return the correct interface that points to the LCoA; RCoA is a "virtual" address.
 - o Swap RCoA in the destination header of the packet with LCoA.
 - o Swap RCoA in the Session object with LCoA.
 - o Forward Path to the respective internal interface.
4. Resv message from an internal interface (LCoA)
- o Swap LCoA in the Session object with RCoA.
 - o Determine outgoing interface; this function must be enhanced, since the correct interface should be the interface toward the LCoA.
 - o Check if reservation is possible (resources, policy).
 - o Update RSB.
 - o Send Resv to next (external) hop.

A message sequence chart for a bidirectional QoS reservation using our scheme is presented in Fig. 3. The reservation states outside the access network are configured for the stable RCoA. Only the reservations inside the access network are LCoA dependent. This establishes the necessary infrastructure to accommodate mobility events inside the access network, without the need to propagate the topology modification outside of it (Fig. 4).

3.3 Mobility Related Functionality

In case of a handoff, we assume that the mobility control authority (MAP/GFA) is either in control or immediately notified about it. An asynchronous notification about the handoff must be delivered to the RSVP-MP by e.g. MAP. The two entities may be co-located at the edge domain router. By the reception of the handoff notification, the RSVP-MP examines its internal Binding Cache, which contains the MHs' <RCoA, LCoA> binding and finds out whether a reservation for the MH that changed its point of attachment was already in place. An

analytical RSVP signaling exchange after a handoff is illustrated in Fig. 5.

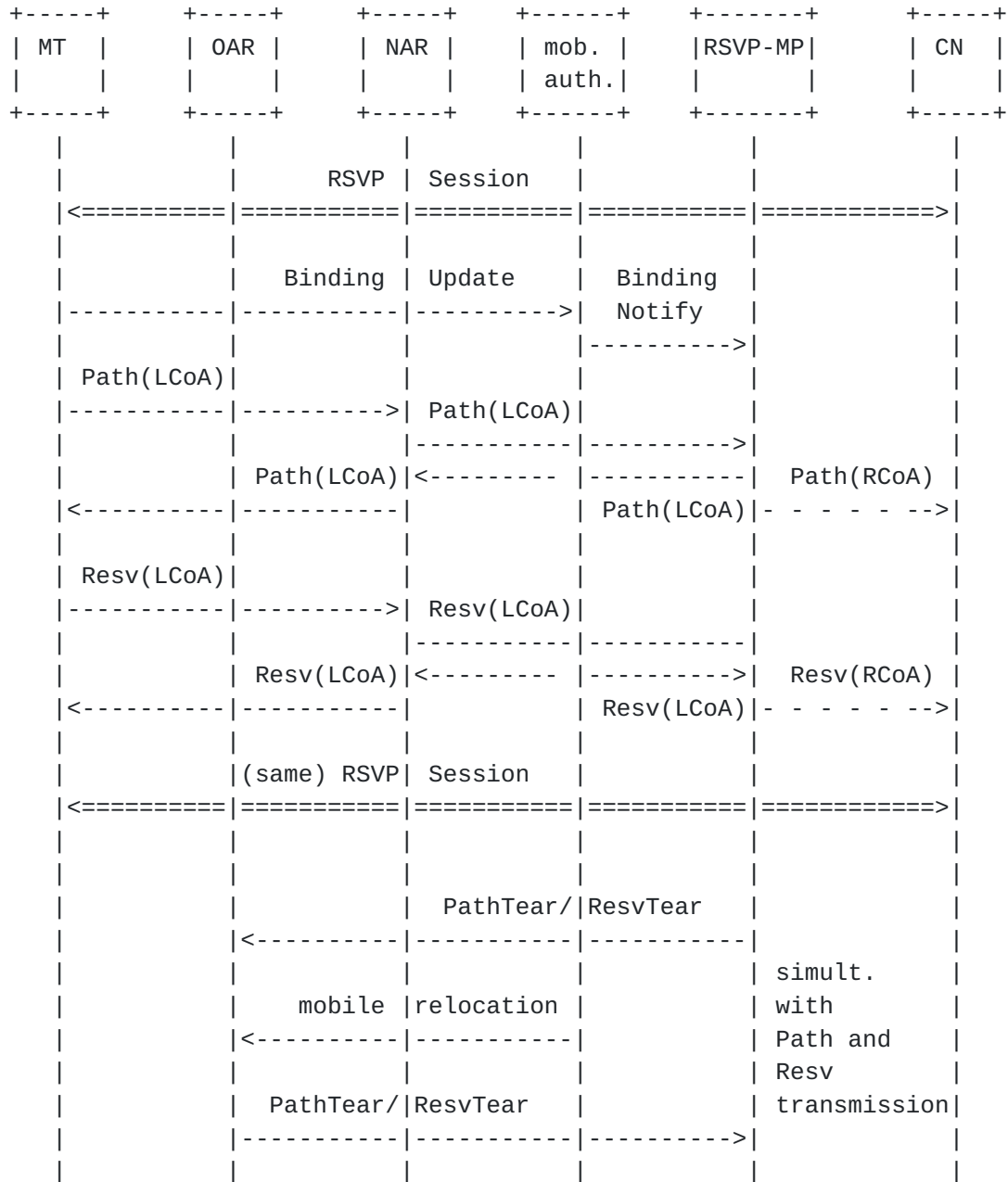


Figure 5: RSVP signaling through RSVP-MP after a handoff

In Fig. 5, it is assumed that a MH has acquired a new LCoA and wishes to re-establish the reservation for the information flow between itself and the correspondent host, and that resources must be reserved for both directions. The MH issues a Binding Update with its newly acquired LCoA, which reaches the mobility control authority

of the mobile access network. The mobility control authority then issues an asynchronous notification to RSVP-MP.

The RSVP-MP checks for reservations in the downlink direction for Session objects regarding the MH's unchanged RCoA. If such an entry exists, the RSVP-MP issues a Path message containing the correspondent host's IP address, as if it was issued by the correspondent host across the network. The MH responds with a Resv to the correspondent host. The Resv message is intercepted in the RSVP-MP and the LCoA is translated (or possibly decapsulated) into the RCoA both in the packet's headers and its contents. At the same time the MH issues in parallel a Path message to the correspondent host to re-establish the uplink QoS reservation. The RSVP-MP intercepts it, translates the LCoA into the RCoA before forwarding it to the core network and responds to it without waiting for any answer from the correspondent host.

The actual RSVP signaling is purely restricted inside the access network, whereas any Path or Resv messages transmitted to the core network merely serve as state refresh messages. No actual Path or Resv state modifications are performed in routers outside the area controlled by the RSVP-MP.

A parallel activity, of equal importance, is the release of the downlink and uplink reservations corresponding to the MH's previous LCoA. The release of the downlink Path and Resv state is triggered by the RSVP-MP that sends a PathTear/ResvTear submission toward the old LCoA, i.e. toward the old Access Router. The reservation release from the old Access Router to the RSVP Mobility Proxy and any wireless reservation controlled by that Access Router is trickier. An asynchronous notification (either by the mobility controlling authority or by the RSVP-MP) is necessary so that the uplink and the wireless reservations are released explicitly soon after the handoff completed and not after the RSVP soft states expired.

5. Security Considerations

RSVP-MP does not introduce any further security problems than the combination of Hierarchical Mobile IP (v4 or v6) and RSVP. In fact, some of the requirements are common for the deployment of Hierarchical Mobile IP and RSVP and can be convoluted. Users must be authenticated with their authentication keys with the RSVP-MP and the mobile controlling authority. The key management and distribution infrastructure deployment is a prerequisite for automatic authentication. Manual key distribution should be done otherwise.

4. Conclusions and Future Work

We have presented a new scheme that tackles efficiently the inconsistencies arising from the interworking of Mobile IP with RSVP. Our main goal is to achieve this while keeping the required modifications on existing protocols and network components to a minimum.

In [14], we perform a performance analysis both with an analytical and a simulation model. The blocking probability (in the Connection Admission Control entity of the RSVP router) is minimized and the link to the upstream ISP is fully utilized. The network resource usage in the access network remains the same as in the normal RSVP operation. Our scheme also reduces the period, during which, moving users experience QoS deterioration. This is achieved by keeping the required signaling for the re-establishment of an end-to-end QoS supported session inside the access network. Finally, our scheme works without any modifications to network components other than the edge RSVP router.

In the drawbacks of our proposal we acknowledge that RSVP Mobility Proxy should be developed in cooperation with any advances in hierarchical mobility management schemes. These schemes are still at a research stage, thus, major or minor modifications are expected. The enhanced functionality of RSVP-MP imposes also a complexity burden on the access network edge router.

Our future work includes the examination of the possibility to introduce more RSVP-MP edge routers in an access network to minimize the load of a single access router. A hierarchy of RSVP-MPs and its applicability to current access networks will also be researched.

6. References

- [1] C. Perkins, "IP Mobility Support", [RFC 2002](#), October 1996.
- [2] C. Perkins and D. Johnson, "Route Optimization in Mobile IP", Internet Draft, Work in Progress, November 2000.
- [3] D. Johnson and C. Perkins, "Mobility Support in IPv6", Internet Draft, Work in Progress, November 2001.
- [4] R. Braden, D. Clark, and S. Shenker, "Integrated Services in the Internet Architecture: An Overview", [RFC 1633](#), June 1994.
- [5] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss, "An Architecture for Differentiated Services", [RFC 2475](#),

December 1998.

[6] R. Braden, ed., L. Zhang, S. Berson, S. Herzog, S. Jamin, "Resource ReSerVation Protocol (RSVP) - Version 1 Functional Specification", [RFC 2005](#), September 1997.

[7] Y. Bernet, "Format of the RSVP DCLASS Object", [RFC 2996](#), November 2000.

[8] R. Braden and L. Zhang, "Resource ReSerVation Protocol - Version 1 Message Processing Rules", [RFC 2209](#), September 1997.

[9] M. Thomas, "Analysis of Mobile IP and RSVP Interactions", Internet Draft, Work in Progress, February 2001.

[10] C. Shen, A. Lo, H. Zeng, and M. Greis, "An Interoperation Framework for Using RSVP in Mobile IPv6 Networks", Internet Draft, Work in Progress, July 2001.

[11] H. Soliman, C. Castellucia, K. El-Malki, and L. Bellier, "Hierarchical MIPv6 Mobility Management", Internet Draft, Work in Progress, February 2001.

[12] E. Gustafsson, A. Jonnson, and C. Perkins, "Mobile IP Regional Registration", Internet Draft, Work in Progress, February 20001.

[13] A. O'Neill, G. Tsirtsis, and S. Corson, "Edge Mobility Architecture", Internet Draft, Work in Progress, July 2000.

[14] S. Paskalis, A. Kaloxylos, E. Zervas, and L. Merakos, "An Efficient RSVP-Mobile IP Interworking Scheme", University of Athens, Technical Report TR01-0001, available from <http://cgi.di.uoa.gr/~paskalis/papers/tr01-0001.pdf>

7. Authors' Addresses

Questions about this memo can be directed to:

Sarantis Paskalis
Department of Informatics and Telecommunications
University of Athens
Panepistiopolis, 15784
Athens, GREECE
Phone: +30 10 7275334
Fax: +30 10 7275061
E-mail: paskalis@di.uoa.gr

Alexandros Kaloxylos
Department of Informatics and Telecommunications
University of Athens
Panepistiopolis, 15784
Athens, Greece
Phone: +30 10 7275182
Fax: +30 10 7275061
E-mail: agk@di.uoa.gr

Lazaros Merakos
Department of Informatics and Telecommunications
University of Athens
Panepistiopolis, 15784
Athens, Greece
Phone: +30 10 7275323
Fax: +30 10 7275061
E-Mail: merakos@di.uoa.gr

Evangelos Zervas
Department of Electronics
TEI of Athens
Egaleo, 12210
Athens, Greece
Phone: +30 10 5385305
Fax: +30 10 5385304
E-mail: zervas@ee.teiath.gr

