Internet Engineering Task Force Charles Qi Shen
Internet Draft
CWC
draft-shen-rsvp-mobileipv6-interop-00.txt Winston Seah
Date: July 2001
CWC
Anthony Lo

Ericsson
Haihong Zheng

Nokia
Marc Greis

Nokia

An Interoperation Framework for Using RSVP in Mobile IPv6 Networks
<draft-shen-rsvp-mobileipv6-interop-00.txt>

STATUS OF THIS MEMO

1 Abstract

This draft proposes a Mobile IPv6 and RSVP interoperation scheme. In this scheme, the underlying mobility support mechanism is required to provide a unique flow identity regardless of node mobility, making the node mobility transparent to flow QoS handling mechanisms. Thus QoS signaling delay as well as data packet delays and losses during handoff can be reduced.

2 Introduction

With the growing demand for the development of commercially viable wireless and cellular services over Mobile IP [1] and especially

Mobile IPv6 [2], it is highly important to consider the interaction between mobility and QoS [3,4]. In particular, it is necessary to evaluate the applicability of existing QoS mechanisms for IP mobility and to enhance them, where necessary.

This draft focuses on issues of the operation of RSVP [5] over Mobile IPv6, more precisely on the resulting handoff QoS performance. More specifically, the handoff QoS signaling delays are required to be small enough to minimize the handoff data packet delays and losses, thus also avoiding possible service degradation during handoff. In this draft we first identify the problems of running RSVP over MIPv6, and then propose a Flow Transparent Mobile IP and RSVP interoperation scheme to achieve this goal.

The organization of this draft is as follows: We begin with the problem analysis and then discuss the Flow Transparency concept. Then we propose the solutions in detail, followed by the handoff operation of the flow transparent scheme as well as its main features. Finally, we discuss the security and scalability aspects of this scheme.

3 Problem Statement

A flow [6] is a sequence of packets sent from a particular source to a particular destination for which the source desires special handling by the intervening routers. This special handling can be non best effort QoS treatment set up through RSVP. In a fixed network, the flow source and flow destination are fixed after the RSVP resource reservation is established for that flow. In a mobile environment using Mobile IPv6, however, the flow source or flow destination may change during an application session.

The existing work on Mobile IPv6 and RSVP integration [7,8] usually identifies the flow source or flow destination based on the Mobile Node's care-of address. According to Mobile IPv6's built-in route optimization, the Correspondent Nodes (CNs) usually send packets directly to the Mobile Node's care-of address when the Mobile Node (MN) is the receiver; Mobile IPv6 also substitutes the MN's home address in the source address field of outgoing packets with the MN's care-of address when the MN is the sender, while placing the home address in the Home Address Option in the destination option header.

The result is that at the network layer, the flow identity changes each time when the MN performs a handoff and obtains a new care-of

address. Thus, a single application session corresponds to multiple network layer flows, each of which requires a new RSVP renegotiation.

This could cause situations where a new reservation is denied because the old reservation is still active and blocks resources, or the new reservation exists simultaneously along with the old reservation.

More importantly, a change in the network layer flow identity means that all the intermediate routers along the path have to re-build related flow information. Thus, all handoff RSVP renegotiations have to be performed end-to-end, no matter how small the impact of the handoff on the flow path may be. This introduces long handoff QoS signaling delay and increases the delays and losses of data packets, which could lead to notable service degradation during handoffs.

In summary, using RSVP over Mobile IPv6 poses several problems. These problems are caused by address inconsistencies as well as a lack of efficiency in the RSVP operation when the MN performs handoff and changes its care-of address. The problems can be separated in three different categories as described in the following sections.

3.1 Packet Classification Mismatch

When a mobile acts as a sender, the PATH message from the MN contains the MN's home address in the SENDER_TEMPLATE object, as it can be assumed that the RSVP daemon in the MN is unaware of Mobile IPv6. This implies that the FILTER_SPEC in resulting RESV messages contains the mobile node's home address, i.e. the classification of packets in intermediate routers for the relevant session is based on the home address of the MN. However, the source address for packets sent from the MN is not the nodes home address, but its current careof address, as the mobile IP stack in the MN replaces the home address with the care-of address in any outgoing packets to avoid problems related to ingress filtering. This means that RSVP routers on the path of the relevant traffic flows are not able to classify these packets correctly, i.e. the traffic flow would not receive the requested QoS.

The same applies for the case where the MN acts as a receiver. A PATH message arriving at a MN contains the mobile node's home address in the SESSION object. However, the destination address for packets sent to the MN is the node's care-of address, while the home address of the MN is carried in the routing header. This again prevents the packets for the flow from receiving the correct QoS, as they can not be assigned to the correct RSVP session in intermediate routers. Obviously, the packet classification mismatch issue when the MN acts as a receiver is not just for the Mobile IPv6 case, but is also a generic issue for RSVP when source routing is used. When source routing is used, the address of the real destination is not placed in the destination address field in the IP header, but in the last entry

of the routing header instead, unless all the intermediate routers on
the source routing path have processed the packet.

3.2 Handoff Inefficiency

Another problem arises when the MN moves to a new point of attachment

and changes its care-of address. In the uplink direction (i.e. the direction from the MN towards the CN), it could simply reissue a PATH message, which causes a RESV message to be sent from the nearest common router (i.e. the nearest router common to both the old and new path for the flows from the MN to the CN). In the case that the old path and the new path does not share any common path, the nearest common router is the CN.

However, the reservation on the old path between the nearest common router and the MN's former point of attachment would remain in place until the reservation state for this path times out. This is not acceptable, especially when considering that a MN could change its care-of address very frequently, potentially leaving behind a large number of "stale" reservations at old access routers. It also needs to be considered that the refresh delay and resulting from this also the reservation timeout delay may be set to relatively high values in MNs (and their respective) access networks to reduce the number of PATH and RESV refresh messages, as it is necessary to preserve expensive air interface resources in wireless and cellular networks, which are likely to constitute a major use case for Mobile IPv6.

For the downlink direction, when the MN changes its care-of address, the CN or the crossover router do not automatically issue new PATH messages for any sessions involving the MN. This implies that on the new path between the nearest common router and the MN, the data flow would only receive best-effort QoS. A problem related to this is that even if the corresponding node could be forced to immediately issue a new PATH message for the session towards the new care-of address when a binding update message is received from the MN, the intermediate routers would not recognize that this PATH message is not a refresh message (as the RSVP objects contained in the message would not change, since RSVP is unaware of the MN's movement), which means that the PATH "update" would only reach the first RSVP-capable router, but would not be sent on from there, as this router assumes that it is only a refresh message.

3.3 Refresh and Forwarding of RSVP Messages

RSVP processes on RSVP-capable routers do not receive any information about the source and destination address from the IP header of the PATH message which created a PATH state. Thus, when a PATH state is refreshed, the source and destination address of the PATH refresh message have to be constructed from the SESSION object and the

SENDER_TEMPLATE object contained in the PATH message. However, when mobile nodes are involved in the session, these objects again contain only home addresses but not care-of addresses. Hence, the PATH messages are sent with the wrong addresses and may even be routed incorrectly, i.e. the correct path is no longer refreshed and

eventually the reservation times out.

Note that this problem does not apply for RESV messages, as they are routed hop-by-hop based on the PATH state information. However, the hop-by-hop forwarding mechanism used for RESV messages causes yet another problem for the interoperation between RSVP and Mobile IPv6. Before forwarding a PATH message, each RSVP-capable router writes the address of the interface over which the PATH message is sent into the RSVP_HOP object in the PATH message so that the corresponding RESV messages can later be sent towards this interface from the next RSVP router. The interface address is determined by the RSVP process by querying the routing tables in the router based on the address information given in the SESSION and SENDER_TEMPLATE objects. As these objects contain the MN's home address, the RSVP_HOP object would contain the address of the interface which would be used to send the RSVP message towards the home address, when it is actually forwarded towards the care-of address. This causes the RESV messages to be routed incorrectly.

3.4 Using the Care-of Address to Identify Flows

One could argue that the simplest solution for at least some of the problems described above would be to make the RSVP processes in the end nodes (i.e. MN and CN) aware of Mobile IPv6. This would imply that in any RSVP objects contained e.g. in PATH or RESV messages sent by the MN and the CN, the mobile node's current care-of address could be used, instead of its home address. As a result, the packets belonging to the relevant traffic flows would be classified correctly. This is a very simple approach with the advantage that only changes in end nodes are required. However, this approach has several disadvantages, which are listed below:

- As the intermediate routers only see the care-of address, the PATH and RESV messages which are sent with the new care-of address would trigger a totally new reservation in the intermediate routers instead of re-using the old reservation, even though the new and old reservation may share mostly the same path. In addition, the delay caused by the RSVP signal processing would be one round trip for the uplink and one and a half round trips for the downlink if we assume the binding update sent from the MN to the CN triggers the PATH message sent from the CN. During this period, the packets sent to and from the MN can only be handled using best effort, which could lead to a notable service degradation during handoff.

- It is not clear how a MN would remove an old session after receiving a new care-of address if sessions are identified based on

the care-of address. The reservation with the old care-of address would remain in place until the RSVP soft state for this reservation

times out. This would imply that the user may have to pay for two potentially expensive reservations for a certain amount of time. This is not acceptable, especially when considering that a MN could change its point of attachment and its care-of address very frequently, thus leaving behind a lot of old unused reservations.

- The old care-of address of a MN may be reused after it changes its point of attachment to the Internet, which may imply that if reservations are identified based on the care-of address, another node could benefit from a reservation which has not been removed and which has also not timed out yet.

- If sessions are identified based on the care-of address, it is necessary to set up fully new RSVP sessions after a MN receives a new care-of address instead of just updating the existing sessions. In the worst case this could mean that a session which still exists for a node's old care-of address (i.e. a session which has not timed out yet) could block the establishment of the session for the new care-of address, even though both sessions are meant to handle the same traffic flow.

- In order for an RSVP process in a CN to obtain the care-of address of the MN, Mobile IP needs to provide an interface to reveal the care-of address of the MN, which could also be used by any other applications. This may violate location privacy requirements.

- If all RSVP sessions for a MN have to be re-established whenever this node changes its point of attachment and obtains a new care- of address, this also implies that all procedures related to admission control and policy control have to be performed again, e.g. bandwidth brokers and policy servers may have to be contacted by RSVP-capable routers on the path. This potentially implies a latency which is not acceptable e.g. for handoffs in cellular environments.

- In this approach, it is also necessary to always "negotiate" the new RSVP sessions all the way between the MN and the correspondent node. This precludes optimized solutions where it would be possible to only set up the path between the MN and the nearest common router.

4 Proposed Solutions

To address the issues described above, we propose an interoperation scheme between RSVP and MIPv6. This framework is based on the flow transparency concept, which is discusssed in section 4.1. Based on the flow transparency concept, multiple new features are proposed to

either implement the concept, or to supplement it for achieving a seamless "QoS handoff".

4.1 Flow Transparency Concept

To address the issues described in section 3, we introduced a Flow Transparency concept [9,10] i.e., the underlying mobility support scheme is required to keep node mobility completely transparent to network layer flow handling mechanism. Essentially, flow transparency calls for a unique flow identity irrespective of the change of the mobile node's address, thus enabling the network layer flow handling mechanism to function normally regardless of node mobility. A flow transparent approach naturally avoids the following two problems:

First, since the network layer flow identity remains the same after a handoff, the old reservation can be reused by the same flow whenever possible. Second, with a constant flow identity after handoff, the routers residing in the common portion of the new and old flow path do not have to perform a QoS update during handoff; only those routers that are on the new path section may be needed for the update process. This avoids the need for end-to-end renegotiation.

It is worth noting that with node mobility, the number and identity of routers involved in the same flow are dynamic and usually unpredictable. It is the routers common to both new and old path of the flow that constitute the scope of flow transparency. This implies that automatic flow handling adaptation for those routers in the newly added path is required in order to exploit the flow transparency concept.

The flow transparent mobility support is fundamental in the interoperation framework of using RSVP over MIPv6. With Mobile IPv6 and RSVP, the natural solution to provide flow transparency, i.e., a unique flow identity regardless of node mobility, is to use the mobile node's home address instead of its care-of address to identify the source or the destination of a flow. By using the mobile node's home address to identify the source or destination of a flow, we separate the routing and the QoS functionality in a router. The former is based on the care-of address, reflecting the node's mobility; the latter is based on the home address, without the impact of node mobility.

In order to identify a flow using the home address, the home address needs to be carried in every packet, no matter if the MN is acting as a sender or a receiver. The two scenarios are discussed in the following sections.

4.1.1 Mobile Node as Sender

Two approaches can be used to carry the home address of an MN when it acts as a sender.

- Approach 1: According to the Mobile IPv6 specification, for packets sent by a mobile node, Mobile IPv6 will move the MN's home address to the IPv6 packet header to the Home Address option carried in an IPv6 Destination Options Header. Since this header will not be examined until reaching the packet destination, intermediate routers will not be able to correctly classify packets belonging to the flow. Therefore, when flow transparency is required, we suggest that Mobile IPv6 ignores this special processing for MN's home address and leaves it in the IP source address field to enable router QoS processing. Note that this only requires modifications at end nodes. The ingress filting problem resulting from this approach will be discussed in the Security Considerations section.

- Approach 2: MN uses its care-of address as source address as specified in the Mobile IPv6 specification, and certain modifications to the intermediate RSVP nodes will be required. Three alternatives are proposed below.

* Alternative 1: The Home Address Option is carried in the destination option as defined in Mobile IPv6. Upon receiving an IPv6 packet, an IPv6 RSVP node classifies the source of the packet using the home address in the Home Address destination option if present, instead of the care-of address in the source address field in the IPv6 header. In order to do so, the IPv6 RSVP node checks the presence of the Home Address option in the destination option header when it receives an IPv6 packet. If it is present, the RSVP node classifies the packet using the home address; otherwise, it still uses the address carried in the source address field in the IP header.

* Alternative 2: The Home Address Option is still carried in the Destination Option Header, but a newly defined Flow Transparency Router Alert Option carried in a Hop-by-hop Options Header may be inserted into the outgoing packets sent by the MN to notify each intermediate router of the need to classify the source address of the sender using the Home Address Option carried in the Destionation option header.

* Alternative 3: A Mobile IPv6 node may simply move the Home Address Option into a Hop-by-hop Options Header when flow transparency is required, so that all intermediate routers will have access to the MN's home address.

The three alternatives above all require modifying intermediate routers to look for the MN's home address at an appropriate place to

perform packet classification correctly.

4.1.2 Mobile Node as Receiver

When MN acts as a receiver, no modification is required to the current MIPv6, where MN's care-of address is carried in the destination address field in the IP header and the home address is carried in the routing header. However, certain modifications of the packet classification procedure are needed in the intermediate RSVP nodes, as described in section 4.2. Note that in this draft, only the case that no additional source routing other than the MN's care-of address is considered. The other case where other explict routing is included requires more complicated system design and will be discussed in a future version of this draft.

4.2 Proper Packet Classification

Based on the flow transparency concept, the home address instead of the care-of address is used to classify the packet. In order to classify a packet properly, special handling may be needed depending on the approach used to carry the home address.

4.2.1 Scenario 1: Mobile Node as Sender

When approach 1 described in section 4.1.1 is used to carry the home address, no modification is required for the packet classification procedure defined in the current RSVP specification. Slight modifications are needed for the Ingress Filtering mechanism, as detailed in the Security Considerations section of this draft. However, since Ingress Filtering is normally deployed only in the periphery of the networks [11], the number of affected routers is expected to be small.

If approach 2 is used, slight modifications are needed in the packet classifier in the intermediate RSVP routers. Upon receiving an IPv6 packet, an RSVP node classifies the source of the packet using the home address in the destination option. Depending on the schemes for carrying the home address proposed for approach 2, such a checking procedure can be triggered by observing either the presence of the home address option in the destination option, or the presence of the flow transparency alert in the hop-by-hop option, or the presence of the home address carried in the hop-by-hop option.

4.2.2 Scenario 2: Mobile Node as Receiver

To send a packet to a Mobile IPv6 node which is not in its home network, the home address of the MN is placed in the last entry in the address list of the routing header. The ability to correctly process a routing header in a received packet is required in all IPv6 nodes, whether mobile or stationary, whether host or router. Based on this fact, we propose to identify the MN as a receiver using the address in the last entry of the routing header, instead of the

address carried in the destination address field in the IP header. With this approach, slight modifications are needed in the packet classifier in the intermediate RSVP routers.

An alternative approach is enabled by the IPv6 flow label. An IPv6 flow can be uniquely identified by the combination of a source address and a non-zero flow label. In order to maintain a unique flow identity to facilitate packet classification in a mobile environment, we suggest that the flow label be constant during the whole lifetime of the session regardless of node mobility. With this usage of flow label, as well as the use of existing flow-label related objects defined in RSVP protocol, routers may perform packet classification without examining the flow destination. Thus, this approach does not require modification to packet classification in intermediate RSVP routers. Another benefit of this approach is that it facilitates the use of RSVP in the presence of IPSec.

4.3 Refresh and Forwarding of RSVP Messages

To solve the problem of sending PATH refresh messages in the uplink direction from a MN towards a CN, we propose to carry MN's mobility information in every PATH message sent from the MN and record the mobility information in the path state maintained by each RSVP node. The mobility information, containing the mapping between the home address and the current care-of address of the MN, is carried in a new RSVP object called "mobility object". The mobility information maintained in the PATH state is established upon receiving the first mobility object for a specific home address, and updated by subsequent mobility objects. Theoretically the mobility object only needs to be sent at the beginning of a session and whenever the CoA of MN has been changed, however, due to the unreliable transmission nature of RSVP messages, it needs to be carried in every PATH message originating from a MN to reduce the chance of non-updated PATH state due to packet loss.

When the mobility object is used, not only the SESSION and SENDER_TEMPLATE objects, but also the care-of address maintained in the path state are used to determine the source address of a PATH refresh message. More specifically, the source address field in the PATH refresh message should carry the up-to-date care-of address of the MN, while the home address is carried in the destination option header.

To solve the problem of sending PATH refresh message in the downlink direction from a CN towards a MN, we propose that the source routing information (i.e., the destination address plus the address list in the routing header) in the latest PATH message sent from the CN to the MN is added to the PATH state. In this draft, since we only

consider the case that no extra source routing is used except what MIPv6 requires, the source routing only consists of the home address and the current CoA of the MN. The source routing information in the PATH state is established upon recieving the first PATH message towards the MN, and is updated by the consecutive PATH message sent towards the MN with the same home address.

Whenever a PATH refresh message needs to be sent, not only the SESSION and SENDER_TEMPLATE object, but also the source routing information is used to construct the PATH message. More specifically, a PATH refresh message contains the current care-of address of the MN in the destination address field, and the home address in the routing header.

Including the source routing information into the PATH state also solves the problem of correctly routing RESV messages. As described in section 3.3, before forwarding a PATH message, each RSVP router writes the address of the interface over which the PATH message is sent into the RSVP_HOP object in the PATH message. Instead of using the SESSION and SENDER_TEMPLATE objects for querying the routing tables, we propose to use the care-of address maintained in the PATH state. Thus, the RSVP_HOP object would contain the address of the interface that is used to send the RSVP message towards the care-of address instead of the home address, which enables the RESV messages to be routed correctly.

4.4 Handoff Efficiency

Improving the handoff efficiency is the major focus of this scheme. Based on the Flow Transparancy concept, we propose following scheme to improve the handoff efficiency.

4.4.1 Scenario 1: Mobile Node as Sender

If the Home Address is used to classify the sender, the resource reservation efficiency problem on the uplink direction for the MN after its handoff is solved without any further changes to Mobile IPv6 or RSVP. After changing the care-of address, the MN immediately sends a PATH message towards the CN. This PATH message will trigger the establishment of PATH state in the RSVP routers on the path until it reaches the Uplink Nearest Common Router (UNCR - the first common router on the old path and new path for the flows from the MN towards the CN). The UNCR observes the PATH message arriving with a previous hop address different from the one stored in the path state, upon which it will immediately reply with a RESV message towards the MN using the new path. The reserved resources between the UNCR and the CN can be reused. In the case that there is no common path shared by

the new path and the old path on the uplink, the UNCR is the CN.

After processing the PATH message, the UNCR needs to forward the PATH message to the next hop in any case. The purpose of this is to update the mobility information in all the RSVP routers on the path between in order to issue a proper refresh message. The details have been discussed in section 4.3.

However, as mentioned in section 3.2, although the new path between the mobile nodes current point of attachment and the nearest common router is established, the old path between the MNs former point of attachment and the nearest common router still remains in place. Therefore, we propose that upon receiving the PATH message, the UNCR not only replies with a RESV message using the new path, but also sends a RESVTEAR message towards the previous hop stored in the old path state. The RESVTEAR message will trigger the removal of the reserved resources on the old path which are no longer needed.

4.4.2 Scenario 2: Mobile Node as Receiver

The situation is more complicated when the MN is acting as a receiver. After a handoff, the receiver sends a Binding Update to the CN. At the same time, it should inform the Downlink Nearest Common Router (DNCR - the closest router to the MN, which is on both the old and the new path for the flows from CN to MN) of its mobility information in order to trigger a handoff PATH message from the DNCR on the downlink. This avoids waiting for a handoff PATH message from the CN, which usually has to be issued after the CN receives the Binding Update.

The mobility object can be carried alone in a newly defined RSVP PATHREQ message if the MN acts solely as a receiver or it can be piggybacked in a PATH message sent by the MN itself if the MN acts as both sender and receiver. Besides the common header, the PATHREQ message carries the mobility object. The PATHREQ message and the PATH message with a mobility object will have the CN as destination address and will be examined by each intermediate RSVP node. The format of the PATHREQ message and the mobility object is specified in section 5.1.

Upon receiving a PATHREQ message or a PATH message carrying a mobility object sent from the MN, the RSVP router decides whether it is the DNCR by comparing the home address and the care-of address in the mobility object sent from the MN against the same information in the PATH state for the flow destined to the MN. The rules of DNCR decision are described in section 5.2.

If the router decides that it is the DNCR and it observes that there is a PATH state that matches the mobility object on the downlink direction, a Local Repair for the receiver route change will be

triggered, that is, the router sends a handoff PATH message for the flow indicated by the flow destination, to the MN's new care-of address. Inside the handoff PATH message, the destination address contains the new CoA carried in the mobility object, and the routing header carries the home address of the MN. Furthermore, if the mobility object is carried in a PATHREQ message, the NCR doesn't need to forward the the PATHREQ to the next RSVP router. If it is carried in a PATH message, then the NCR needs to forward the PATH message to the next hop until it reaches the CN. The purpose of forwarding the PATH message is to update the mobility information in all the RSVP routers on the path between in order to issue a proper refresh message. The details are discussed in section 4.3. The format of the PATHREQ message and the mobility object is described in section 5.1. The processing rules of the PATHREQ message as well as the PATH message with the mobility object are described in section 5.2.

In addition, although the new path between DNCR and MN has been established, the old path between DNCR and MN's old point of attachment still remains in place. Therefore, we propose that after sending a handoff PATH message towards the MN's new CoA, NCR also sends a PATHTEAR message towards the MN's old CoA. The PATHTEAR message will trigger the removal of the resources on the old path which are no longer needed.

With this approach, the RSVP process does not need to get the care-of address of the MN from the IP header of the RSVP messages, but just uses the information provided by the mobility object. The clear interface between the IP layer and the RSVP process does not need to be modified. Furthermore, the classification rules (i.e., whether to use the source address of the packet or home address in the home address option) can be based on the question if a home address/care-of address mapping state has been established for the flow. This makes the classification more efficient.

5 Message Format, Algorithms and Processing Rules

Some details of the message format, algorithms and message processing rules are discussed in the following sections.

5.1 Format of Mobility Object and PATHREQ Message

The mobility object contains the home address and the current care-of address of the MN. Figure 1 shows the format of the mobility object. The length field indicates the total object length in bytes. The Class Num and the C-Type for the mobility object would have to be assigned by IANA.

The PATHREQ message has a common header followed by the mobility

object defined above. Again, the message type would have to be assigned by IANA.

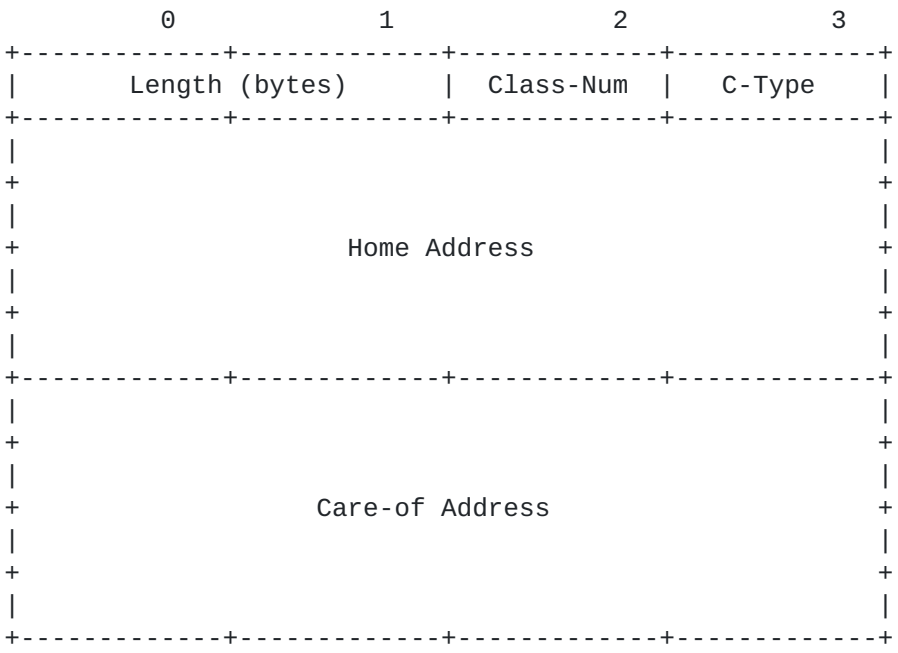

Figure 1: MOBILITY Object

5.2 Nearest Common Router Decision

When a RSVP router receives a PATHREQ message, it needs to decide if it is the DNCR. When it receives a PATH message, it needs to decide if it is the DNCR and/or UNCR. DNCR and UNCR may be physically collocated in the same router, or could be two different network entities.

On the uplink direction, a RSVP router decides if it is the UNCR just by comparing the home address, the CoA and the previous RSVP hop carried in the PATH message against the same information stored in the Path State in the uplink direction.

- If there is no PATH state matching the home address, the router could be one of the new routers on the new path between the MN and the UNCR, or one of the routers on the path between the UNCR and the

CN if the path is changed due to the failure of a RSVP router, load balancing or other reasons.

- If the home address matches but the CoA is different from what is stored in the PATH state, then

* If 1) there is a PATH state related to the home address for the flow sent from the MN, and 2) for the same home address, the previous RSVP hop remains the same, then the router is one of the routers on the existing path between the UNCR and the CN, instead of the UNCR.

* If 1) there is a PATH state related to the home address for the flow sent from the MN, and 2) for the same home address both the care-of address and the previous RSVP hop have been changed, the router is the UNCR.

On the downlink direction, a RSVP router decides if it is the DNCR by searching the home address against the PATH state on the downlink direction. If there is a match of the home address in the PATH state in the downlink direction, then the router decides it is the DNCR; otherwise it is not.

5.3 Processing Rules for PATHREQ and PATH with Mobility Object

5.3.1 Processing Rule for PATHREQ Message

The PATHREQ message is sent when a MN acts only as a receiver and it changes its care-of address. The general processing rules for the PATHREQ message are as follows

- When a RSVP node receives a PATHREQ message and it does not have any matching PATH state on the opposite direction based on the home address carried in the mobility object, it just forwards the message to the next RSVP node.

- When a RSVP node receives a PATHREQ message and it has a matching PATH state for a flow in the opposite direction based on the home address carried in the mobility object, it decides it is the DNCR and needs to send a PATH message towards MN's new CoA and performs the following procedures.

* If there is no source routing information related to the home address, which indicates that the MN was inside its home network and did not have a CoA, the RSVP router updates the source routing information by inserting the new CoA before the home address in the source routing address list. Then it constructs a PATH message based on the updated information in the PATH state and then sends it to the MN. The RSVP router also constructs a PATHTEAR message and sends it

to the MN's home address.

* If there is source routing information related to the home address,
the RSVP router just updates the source routing information by replacing the old CoA with the new CoA. Then the RSVP router constructs a PATH message based on the updated information in the PATH state and then sends it to the MN. It also constructs a PATHTEAR
message that contains the old CoA in the destination address and the home address in the destination option header, and sends it to clean up the PATH state on the old path.

5.3.2 Processing Rule for PATH Message

A PATH message is sent when a MN acts as a sender only or as both sender and receiver and it changes its CoA. The general processing rules for the PATH message with a mobility object are as follows.

- When a RSVP router receives a PATH message with a mobility object, it first checks its PATH states on the uplink direction.

* If there is no PATH state on the uplink direction matching the home address carried in the mobility object, the RSVP router establish a new PATH state, including the mobility information carried in the mobility object, then forwards the message to the next
hop.

* If there is already PATH state for the uplink direction, which matches the home address, then the RSVP router compares the CoA information maintained in the PATH state against the one in the mobility object.

- If the CoAs are the same, the PATH message is only considered as a refresh message, and whether or not to forward it to the next hop depends on the message processing rules as currently defined for RSVP.

- If the CoAs are different from each other, the PATH state should be
updated with the new mobility information carried in the mobility object and the PATH message is forwarded to the next hop. If the RSVP
router also finds out that the RSVP_HOP objects in the PATH State and
in the PATH message are different, the local repair should be invoked, and a RESV message is sent to the MN using the updated information in the PATH State. In addition, it also sends a RESVTEAR message towards the old CoA of the MN to tear down the old reservation.

- After checking the uplink PATH state, the RSVP node also checks the
PATH state on the opposite direction. The procedure is exactly the

same as described in section 5.3.1, except for the message name.

6 Seamless QoS Provision for Handoffs

Seamless handoff QoS provision is always desired in a mobile QoS scheme. Normally this requires to explicitly reserve resources in advance at the cells that the MN is about to visit [12,13,14,15]. The challenge for these schemes is, how to predict the MN's movement behavior so that pre-reservation may be done only in necessary cells.
If prediction is not available, resource pre-reservation may have to be performed in all neighboring cells, which wastes resources. Although this waste may be alleviated through definition of new RSVP reservation models (like active reservations and passive reservations), the expense would be extra protocol complexity.

The flow transparent RSVP and Mobile IPv6 interoperation provides a relatively simple alternative of making seamless handoff QoS provision possible. In the handoff mobility and QoS signaling as mentioned above, it is likely that the RSVP message will traverse shorter than the Binding Update , because the handoff RSVP message ends at a Nearest Common Router while the Binding Update has to reach the CN all the time. Thus the RSVP renegotiation holds a possibility of being finished before the CN is updated with MN's new care-of address, especially when there are congested links within the path between the Nearest Common Router and CN. This implies that before CN starts sending packets to MN's new location, resources could have already been set up along that path. As a consequence, all packets subsequently destined for MN's new location from the CN will be offered QoS as desired and no any extra delay is incurred due to handoff. In other words, the QoS provision to the flow is seamless during the handoff, which might give great improvements to handoff service quality of mobile real-time services.

7 Security Considerations

The Approach 1 in Section 4.1.1 suggests that a Mobile Node uses the home address as source address when flow transparency is required. This approach, if used, may cause problems with Ingress Filtering [11], which is a security measure used to defeat denial of service attacks that employ IP source address spoofing. Packets directly using Mobile Node's home address as source address will likely be dropped by the Ingress Filtering routers if they are sent from a foreign network. A possible solution to this problem is presented below.

When a Mobile Node is sending a packet, the home address is placed in the source address field, and current Mobile IPv6 special processing

for the Mobile Node's home address is replaced with a new processing

for its care-of address. A new Care-of Address Option similar to the current Home Address Option in Mobile IPv6 is defined as shown in figure 2.

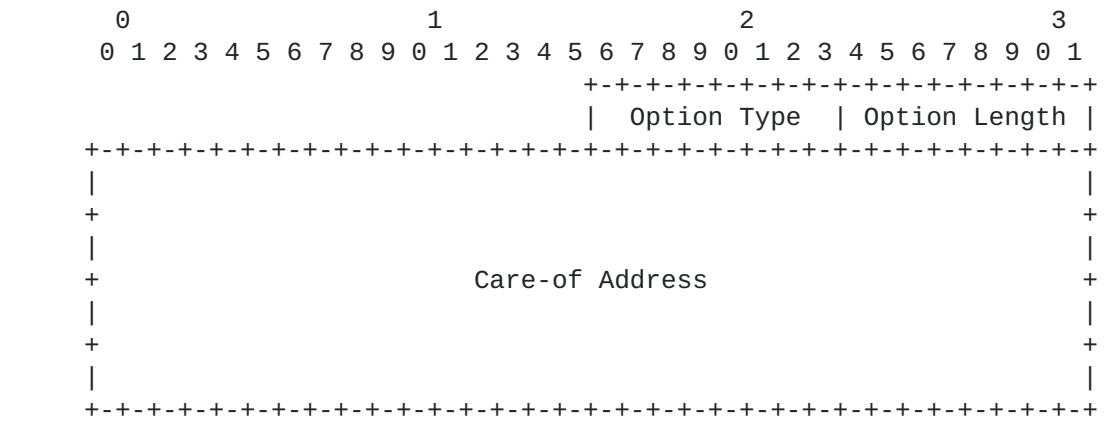

Figure 2: Care-of Address Option

This Care-of Address Option will then be carried as an IPv6 Destination Option Header in each outgoing packets sent by the MN (similar to the current Mobile IPv6 specification). The remaining part is for the Ingress Filtering mechanism to attend to this change.

So the Ingress Filtering routers will be required to not only examine the IP address in the source address field, but also to look for the Care-of Address Option before making a decision. If the care-of address matches the incoming interface of the packet, it SHOULD also forward the packet as appropriate. Note that in this case although the care-of address option is carried as a Destination Options Header, it is actually examined by an intermediate router - the router which performs Ingress Filtering. If this is seen as a confliction with the Destination Options Header definition, which says it carries optional information that needs to be examined only by a packet's destination node(s), then a new IPv6 extension header, called Intermediate Router Options Header, may be defined similarly. It will have the same format as the Destination Options Header except for the Header Type value, and it will carry optional information that needs to be examined by intermediate routers like in this case.

The above solution to Ingress Filtering maintains its original purpose, i.e., when an attack of denial of service does indeed occur,

a network administrator can be sure that the attack is actually originating from within the known prefixes that are being advertised.

The modification required for its implementation is also in line with possible additional functions that should be considered for future platform implementations as suggested in [11].

8 Scalability Considerations

There has been wide concern over the scalability of end-to-end RSVP and Integrated Service (Intserv) architecture, which has led to the development of relatively simple and coarse methods of providing differentiated classes of service for Internet traffic, such as Differentiated Service (Diffserv). However, Intserv, RSVP and Diffserv may still be viewed as complementary technologies in the pursuit of end-to-end QoS and a framework combining Intserv/RSVP and Diffserv offers great benefits [16,17]. A possible architecture of this kind could be Diffserv deployed in the backbone or core networks and Intserv/RSVP in access or edge networks. If this is the case, the flow transparent scheme may be viewed as a "Micro Mobile QoS" scheme which improves handoff QoS performance within a domain consisting of wireless and fixed access networks, because this scheme can also accommodate Flow Transparency incapable clouds. Routers that do not understand the newly defined MOBILITY object can simply ignore and forward it until a capable router is reached and decides it is the Nearest Common Router. To one extreme, if all routers along the path are flow transparency capable, each handoff will involve minimum routers possible. To the other extreme, if none of the routers in the path understand flow transparency, it goes back to the normal end-to-end scheme. If some of the routers are flow transparency enabled, the effect will be something in between, depending on the specific router deployment.

9 Concluding Remarks and Future Work

This draft proposes a Flow Transparent Mobile IPv6 and RSVP interoperation scheme. The scheme requires the node mobility to be kept transparent from QoS flow handling mechanism, thus making it possible to keep the RSVP renegotiation from being performed end-to-end each time when the MN changes its care-of address. This could minimize delays and losses of the handoff QoS signaling and data packets. Depending on the network scenario, seamless handoff QoS provision might be achieved, which would further improve handoff performance of mobile real-time services.

The future network architecture is likely to be the Internet connecting with heterogeneous wireless access networks, such as UMTS/GPRS, Wireless LAN, Bluetooth, etc. Different access technologies may overlap since they possess different

characteristics. Flow Transparency may particularly be important in the case where the MN performs a handoff at the same location, simply switching between subnets of different access technologies.

It is possible that in the wireless Internet framework, the QoS mechanism in the access part would involve mechanisms like the Packet Data Protocol (PDP) Context mechanisms in UMTS/GPRS and/or RSVP, and that of the core network would include Diffserv and/or MPLS. Further work is required to formulate details about how the flow transparent scheme operates in such a framework. A change of QoS requirements during handoff should also be considered. Multicasting support may be taken into account too. Furthermore, Flow Transparency itself might be extended from single-flow to multiple-flow transparency to accommodate mobility support with coarser QoS technologies like Diffserv.

10 Intellectual Property Considerations

CWC may seek intellectual property protection for technologies disclosed herein. If any standards arising from this disclosure become protected by one or more patents assigned to CWC, CWC undertakes to license them on reasonable and nondiscriminatory terms based on reciprocity.

Nokia Corporation and/or its affiliates hereby declare that they are in conformity with Section 10 of RFC 2026. Nokia's contributions may contain one or more patents or patent applications. To the extent Nokia's contribution is adopted to the specification, Nokia undertakes to license patents technically necessary to implement the specification on fair, reasonable and nondiscriminatory terms based on reciprocity.

11 Bibliography

[1] C. Perkins, "IP Mobility Support," RFC 2002 , October 1996.

[2] D. Johnson and C. Perkins, "Mobility Support in IPv6," IETF Internet Draft , November 2000. work in progress.

[3] H. Chaskar, "Requirements of a QoS Solution for Mobile IP," draft-chaskar-mobileip-qos-requirements-00.txt , June 2001. work in progress.

[4] M. Thomas, "Analysis of Mobile IP and RSVP Interactions," draft-thomas-seamoby-rsvp-analysis-00.txt , February 2001. work in progress.

[5] R. Braden, L. Zhang, S. Berson, S. Herzog, and S. Jamin,

"Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification," RFC 2205 , September 1997.

[6] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," RFC 2460 , December 1998.

[7] G. Fankhauser, S. Hadjiefthymiades, N. Nikaein, and L. Stacey, "RSVP Support for Mobile IP Version 6 in Wireless Enviroments," Tech. Rep. TIK-Report Nr. 58, Computer Engineering and Networks Laboratory, Swiss Federal Institute of Technology (ETH) Zurich, 1998.

[8] G. Chiruvolu, A. Agrawal, and M. Vandenhoute, "Mobility and QoS Support for IPv6-based Real-time Wireless Internet Traffic," 1999 IEEE International Conference on Communications , vol. 1, pp. 334--8, 1999.

[9] Q. Shen, A. Lo, W. Seah, and C.C. Ko, "On Providing Flow Transparent Mobility Support for IPv6-based Wireless Real-time Services," Proceedings of the Seventh International Workshop on Mobile Multimedia Communications (MoMuC2000) , pp. 2B--4--1 -- 2B--4- --6, October 2000.

[10] Q. Shen, A. Lo, and W. Seah, "Performance Evaluation of Flow Transparent Mobile IPv6 and RSVP Integration," To appear in Proceedings of the Fifth World Multi-Conference on Systemics, Cybernetics and Informatics (SCI2001) , July 2001.

[11] P. Ferguson and D. Senie, "Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing," RFC 2827 , May 2000.

[12] A.K. Talukdar, B.R. Badrinath, and A. Acharya, "MRSVP: A Reservation Protocol for an Integrated Services Packet Network with Mobile Hosts," Tech. Rep. DCS-TR-337, Department of Computer Science, Rutgers University, U.S.A., 1997.

[13] W. Chen and L. Huang, "RSVP Mobility Support: A Signaling Protocol for Integrated Services Internet with Mobile Hosts," Proceedings of IEEE INFOCOM 2000: Conference on Computer Communications , vol. 3, pp. 1283--92, 2000.

[14] D.O. Awduche and E. Agu, "Mobile Extensions to RSVP," Proceedings of Sixth International Conference on Computer Communications and Networks , pp. 132--6, 1997.

[15] I. Mahadevan and K.M. Sivalingam, "An Experimental Architecture

for Providing QoS Guarantees in Mobile Networks Using RSVP,"
Proceedings of Ninth International Symposium on Personal, Indoor,
and

Mobile Radio Communications (PIMRC'98) , vol. 1, pp. 50--4, 1998.

[16] Y. Bernet, P. Ford, R. Yavatkar, F. Baker, and et al., "A Framework for Integrated Services Operation over Diffserv Networks," RFC 2998 , November 2000.

[17] Y. Bernet, "The Complementary Roles of RSVP and Differentiated Services in the Full-Service QoS Network," IEEE Communications , vol. 38, no. 2, pp. 154--162, 2000.

12 Authors' addresses

Charles Qi Shen
Centre for Wireless Communications
National University of Singapore
20 Science Park Road
#02-34/37, TeleTech Park
Singapore Science Park II
Singapore 117674
Singapore
Phone: +65 870-9358
Email: shenqi@cwc.nus.edu.sg

Winston Seah
Centre for Wireless Communications
National University of Singapore
20 Science Park Road
#02-34/37, TeleTech Park
Singapore Science Park II
Singapore 117674
Singapore
Phone: +65 870-9163
Email: winston@cwc.nus.edu.sg

Anthony Lo
Ericsson EuroLab Netherlands
Business & Science Park
Institutenweg 25
P O Box 645, 7500 AP Enschede
The Netherlands
Phone: +31 53-450-5480
Email: Anthony.Lo@eln.ericsson.se
(Anthony Lo's portion of the work on this draft was done when he was with CWC.)

Haihong Zheng
Nokia Research Center
6000 Connection Drive

Irving, TX 75039
USA
Phone: +1 972 894 4232
Email: haihong@zheng@nokia.com

Marc Greis
Nokia Research Center
6000 Connection Drive
Irving, TX 75039
USA
Phone: +1 972 374 0629
Email: marc.greis@nokia.com

Table of Contents