

Internet Engineering Task Force
Shen
Internet Draft
CWC

Qi

[draft-shen-ipv6-flow-trans-00.txt](#)

Winston

Seah

Date: February 2001

CWC

Expires: July 2001

Anthony

Lo

Ericsson

Flow Transparent Mobility and QoS Support for IPv6-based
Wireless Real-time Services

STATUS OF THIS MEMO

This document is an Internet-Draft and is in full conformance with 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/ietf/lid-abstracts.txt>

To view the list Internet-Draft Shadow Directories, see <http://www.ietf.org/shadow.html>.

1 Abstract

This draft proposes a Mobile IPv6 and RSVP interworking scheme. In this scheme, the underlying mobility support mechanism is required to

provide a unique flow identity regardless of node mobility, making 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. We also discuss solutions to achieve this scheme which utilizes the new IPv6 flow label. Finally, issues related to security and scalability will also be considered.

2 Introduction

Interworking of Mobile IP [[1](#),[2](#)] and RSVP [[3](#)] may provide simultaneous mobility and QoS support for wireless mobile Internet real-time services. The crucial aspect for such a scheme is the resultant

handoff QoS performance. Specifically, the handoff QoS signaling

delays are required to be small enough to minimize the handoff data packet delays and losses, thus also minimize possible service degradation during handoff. In this draft we propose a Flow Transparent Mobile IP and RSVP integration scheme to achieve this goal. By taking advantage of the new IPv6 flow label, we can greatly facilitate the implementation of this scheme. Thus the scheme fits more naturally for the integration of Mobile IPv6 and RSVP with flow label support, although the Flow Transparency concept applies also to IPv4.

The organization of this draft is as follows, we begin with the Flow Transparency concept, followed by the handoff operation of the flow transparent scheme as well as its main features; then we provide solutions to accomplish the scheme; finally we discuss security and scalability aspects of this scheme.

3 Flow Transparency Concept

According to IPv6 specification [4], a flow is a sequence of packets sent from a particular source to 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 running Mobile IPv6, however, the flow source or flow destination may change in the middle of an application session. This is because existing work on Mobile IPv6 and RSVP integration [5,6] usually identifies the flow source or flow destination with the Mobile Node (MN) 's care-of address. According to Mobile IPv6's built-in route optimization, the Correspondent Nodes (CNs) usually send packets directly to MN's care-of address when MN acts as receiver; Mobile IPv6 also substitutes the MN's home address in the source address field of outgoing packets with MN's care-of address when MN acts as sender.

The result of this is that at the network layer, the flow identity changes each time the MN performs a handoff and obtains a new care-of address. Thus a single application session corresponds to multiple network layer flows, each requires a new RSVP renegotiation. This could cause situations where the new reservation is denied because the old reservation is still active and blocks resources. More importantly, change of network layer flow identity means all intermediate routers along the path have to re-build related flow information. So all handoff RSVP renegotiations have to be performed end-to-end, no matter how significant the handoff affects the flow path. This introduces long handoff QoS signaling delay and increases the delays and losses of data packets, which could lead to notable

handoff service degradation.

To address these issues, we introduced a Flow Transparency concept [7] 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 MN's address thus enables the network layer flow handling mechanism to function normally regardless of node mobility. A flow transparent approach naturally avoids the above two problems.

First, since the network layer flow identity remains the same after a handoff, old reservation can be reused by the same flow whenever possible. This prevents deny of reservation for that flow caused by resources blocked by old reservation. Second, with a constant flow identity after handoff, the routers residing in the common portion of the new and old flow path could be exempted from performing handoff QoS update; only those routers that are in the newly added portion of the flow path may be needed for the update process. This avoids the 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.

4 Handoff Operation of Flow Transparent Mobile IPv6 and RSVP Integration

In this section we describe the handoff operation of the flow transparent Mobile IPv6 (with route optimization) and RSVP interworking and summaries its major features. We assume a constant flow source and flow destination are kept for a specific application session, so that the network layer flow identity is constant for the router flow handling mechanism (e.g., the packet classifier) regardless of node mobility. Detailed solutions will be presented in the later sections. In order to achieve an efficient integration, we also exploit existing RSVP features in our scheme, namely, Merge and Local Repair. Figure 1 shows the architecture where both scenarios, MN as sender and MN as receiver, will be considered.

4.1 Scenario 1: Mobile Node as Sender

After a handoff, the MN sends a Binding Update to CN according to Mobile IPv6, and it immediately triggers a Path message to CN - with

the same source flow identity as the one before handoff. According to RSVP, this Path message can be merged at a router where there is

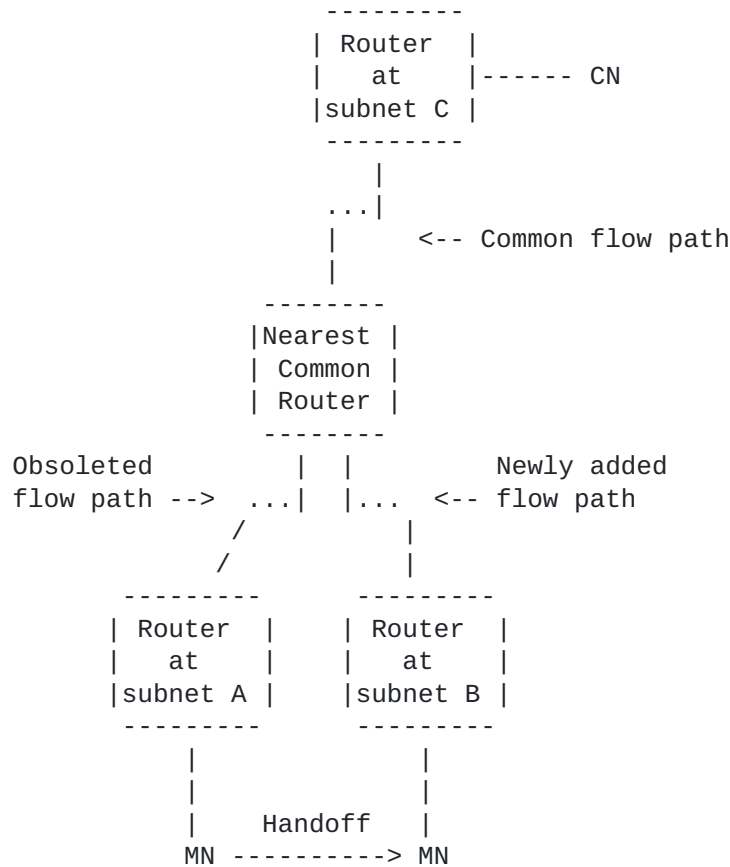


Figure 1: Flow Transparent Mobile IPv6 and RSVP Integration

already a path state for that flow which is created during previous RSVP message exchanges. In this case, the router where merge occurs is also the nearest router common to both the old and new path (Nearest Common Router) for the flow from MN to CN. It sees the same Path message arriving with a previous hop address that differs from the one stored in the original path state. This will cause RSVP to trigger a Local Repair for sender route change, which is actually due to sender mobility. So it will immediately send a Resv message associated with that flow to reserve resources along the newly added path to the MN. Thus resources for the flow will be reserved in the newly added flow path, while in the common flow path the previously

reserved resources will be reused.

4.2 Scenario 2: Mobile Node as Receiver

The situation becomes 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 Nearest Common Router of its mobility information to trigger a handoff Path message from the Nearest Common Router. This avoids waiting for a handoff Path message

from the CN, which usually has to be issued after the CN gets the Binding Update.

As an extension to RSVP, the mobility information, containing the flow destination and the MN's current location, will either be carried alone in a new RSVP message if MN acts solely as a receiver, or be piggybacked in the Path message sent by MN itself for sender mobility if the MN acts as both sender and receiver. This message will have CN as destination address and will be examined by each intermediate routers. Upon receiving this message, the router decides whether it is the Nearest Common Router by looking up its existing RSVP states. If it decides itself as the Nearest Common Router, a Local Repair for 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 location. Then the

original RSVP message will be discarded. After receiving this handoff

Path message, the MN replies with a Resv message to reserve resources

along the newly added flow path. Again because of RSVP merge functionality, this Resv message will not be forwarded farther than the Nearest Common Router since there is already a reservation for this flow made from that router onwards during the previous RSVP message exchanges.

4.3 Seamless Handoff QoS Provision

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 [[8](#), [9](#), [10](#), [11](#)]. 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 interworking 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 handoff delay may incur 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.

5 Proposed Solutions

A flow transparent mobility support is fundamental in the above scheme. 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 MN's home address instead of its care-of address to identify a flow. By using MN's home address as flow identifier,

we

separate routing and QoS function in a router. The former is based on

care-of address, reflecting the node mobility; the latter based on home address, without the impact of node mobility.

5.1 Requirements for Mobile IPv6

A potential problem of using MN's home address as flow identifier with current Mobile IPv6 specification [2] is packet classification.

When MN acts as sender, for packets sent by a MN, Mobile IPv6 will move the MN's home address in IPv6 packet header to a Home Address option carried in an IPv6 Destination Options Header. Since this header will not be examined until reaching the packet destination, intervening routers will not be able to correctly classify packets belong to the flow. Therefore, when flow transparency is required,

we

suggest that Mobile IPv6 SHOULD ignore this special processing for MN's home address and leave it in the IP source address field to enable router QoS processing. Note that this only requires modifications at end nodes.

When MN acts as receiver, for packets sent to a MN, Mobile IPv6 also hides the MN's home address from all intermediate routers. In this case, however, no modification is required for Mobile IPv6 to support

Flow Transparency due to IPv6 flow label support. In IPv6, a flow can be uniquely identified by the flow source and flow label, therefore allows the router to perform packet classification without examining

the flow destination. This is why the flow transparent scheme fits naturally in IPv6.

5.2 Requirements for RSVP

On the RSVP side, it is more natural and convenient to use MN's home address instead of its care-of address, specifically,

When MN acts as sender, the MN's home address is used as flow source and put in the SENDER_TEMPLATE field of RSVP Path messages, and subsequent Resv messages sent by the receiver will also use MN's home address in the FILTER_SPEC field;

When MN acts as receiver, the MN's home address is used as flow destination and put in the SESSION object of RSVP messages.

As described in the operation of the flow transparent scheme, when MN acts as sender, no additional RSVP signaling is needed; when MN acts as a receiver, however, extension to RSVP is required. MN should notify the Nearest Common Router of its flow identity and new location to enable the issuing of handoff Path message. This information can be encoded in a new RSVP MOBILITY object and then either be piggybacked in a Path message or sent alone in a newly defined RSVP PathReq message.

The PathReq message has a common header followed by the objects like any other RSVP messages defined in [Section 3.1 of RFC2005](#), except that Meg Type is given 18. Figure 2 shows the MOBILITY object.

The length field indicates total object length in bytes. The Class Num for the MOBILITY object is 28. The C-Type is 2 since it is intended for IPv6. Following this common object header are two 128-bit fields, each containing an IPv6 address.

The first address is MN's home address which serves as the flow destination and indicates the whole RSVP session. According to RSVP specification, when doing adaptation to receiver route change, which is actually receiver mobility in our case, a Local Repair should be triggered for all flows with a particular destination, regardless of other parameters such as flow label. So only the MN's home address is required for the Nearest Common Router to decide which Path message to send out. The second address in the mobility object is MN's current care-of address denoting the updated location of the MN.

This address will be put in the destination address field of the subsequent handoff Path message sent by Nearest Common Router to ensure correct routing of the message to the MN. These two addresses are the minimum information required for the flow transparent scheme

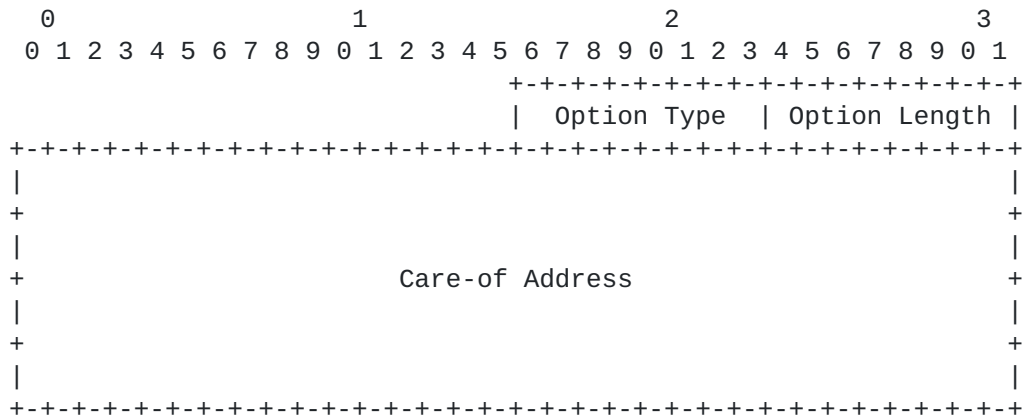


Figure 3: Care-of Address Option

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

6.2 Approach II

If the current Ingress Filtering is to remain unchanged, MN will have

to use its care-of address as source address, then modifications to

all intermediate routers will be required. Two alternatives are possible.

First: At the end nodes, the current MN Home Address Option is still carried in Destination Options Header, but a new Flow Transparency Route Alert Option carried in a Hop-by-hop Options Header may be inserted into the outgoing packets sent by MN to notify each intermediate routers the need for flow transparent handling.

Second: At the end nodes, Mobile IPv6 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.

Both of the above alternatives also require modifying intermediate routers to look for MN's home address at appropriate place to perform packet classification correctly.

6.3 Evaluation of the Two Approaches

In the above two approaches to the Ingress Filtering problem, the first one might be better in terms of implementation, because it requires changes only in end nodes and specific routers deploying Ingress Filtering mechanism. In contrast, the second approach requires changes to all nodes and routers.

7 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 [13,14]. 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 consists 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 itself as 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

Shen, Seah and Lo

[Page 10]

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.

8 Concluding Remarks and Future Work

This draft proposes a Flow Transparent Mobile IPv6 and RSVP interworking scheme. The scheme requires the node mobility to be kept

transparent from QoS flow handling mechanism, thus makes it possible to relieve 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 scheme also illustrates

a possible way of using the IPv6 flow label to facilitate the development of new protocols or mechanisms.

The future network architecture is likely to be the Internet connecting with heterogeneous wireless access networks, such as UMTS/GPRS, Wireless LAN, Bluetooth and etc. Different access technologies may overlap since they possess different characteristics. Flow Transparency might particularly makes sense 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 Packet Data Protocol (PDP)

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, 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.

9 Acknowledgments

This work received Research Grant from National University of Singapore (NUS). We would also like to thank the following people for

commenting, discussing or answering questions regarding early versions of this draft: Prof. C-C Ko, Dr. Y.M. Jiang, Dr. C.C. Foo, Ms. X. Shanguan and Ms. Y. Ge of NUS, Prof. C-K Toh of Georgia Institute of Technology, Dr. I. Curcio of Nokia, and Mr. J. Shankar of CWC.

10 Bibliography

Shen, Seah and Lo

[Page 11]

- [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] R. Braden, L. Zhang, S. Berson, S. Herzog, and S. Jamin, "Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification," [RFC 2205](#) , September 1997.
- [4] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," [RFC 2460](#) , December 1998.
- [5] 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.
- [6] G. Chiruvolu, A. Agrawal, and M. Vandenhoule, "Mobility and QoS Support for IPV6-based Real-time Wireless Internet Traffic," 1999 IEEE International Conference on Communications , vol. 1, pp. 334--8, 1999.
- [7] 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.
- [8] 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.
- [9] 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.
- [10] D.O. Awduche and E. Agu, "Mobile Extensions to RSVP," Proceedings of Sixth International Conference on Computer Communications and Networks , pp. 132--6, 1997.
- [11] 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.

[12] P. Ferguson and D. Senie, "Ingress Filtering: Defeating Denial

of Service Attacks Which Employ IP Source Address Spoofing," [RFC 2827](#), May 2000.

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

[14] 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.

11 Authors' addresses

Qi Shen
Centre for Wireless Communications
National University of Singapore
20 Science Park Road
#02-34/37, TeleTech Park
Singapore Science Park II
Singapore, Singapore 117674
Singapore
Phone: +65 870-9358
Email: shenqi@cw.c.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, Singapore 117674
Singapore
Phone: +65 870-9163
Email: winston@cw.c.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

