Mobile IPv6 support in MPLS Network

<draft-choi-mobileip-ipv6-mpls-01.txt>

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026 except that the right to produce derivative works is not granted.

This document is an Internet-Draft and is NOT offered in accordance with Section 10 of RFC2026, and the author does not provide the IETF with any rights other than to publish as an Internet-Draft

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/1id-abstracts.txt
The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

Abstract

This document discusses how to build the large-scale mobile IPv6 network along with the MPLS network. It proposes that CR-LDP/RSVP-TE can be applied to set up the QoS guaranteed Label switched path (LSP) tunnels between an LER of mobile node and an LER of correspondent node. It means that the IPv6-in-IPv6 tunnels can be replaced by one or multiple LSPs on the MPLS network. This follows design principles such as idle mobile node consideration and QoS guarantee, smooth handoff, no change of Mobile IPv6 etc.

Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP26.
"SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119.

Table of Contents

1. Introduction ................................................ 2
2. Benefits from MPLS .............................................. 3
   2.1. Independency from lower layer technologies ............... 3
   2.2. IPv6 transition benefit .................................. 3
   2.3. Connection-Oriented Switching Paradigm .................. 4
   2.4. Well defined QoS support with DiffServ .................. 4
   2.5. Secure VPN .............................................. 4
3. Features of Mobile IPv6 with MPLS .............................. 5
4. Description of Operation ...................................... 6
   4.1. When MN initiates data transmission .................... 6
   4.2. When CN initiates data transmission .................... 7
   4.3. Smooth Handoff ......................................... 8
   4.4. QoS supported LSP ...................................... 8
5. Required Messages and TLVs .................................... 10
6. Conclusion .................................................. 10
7. Security considerations ....................................... 11
8. References ................................................... 11
9. Author’s Addresses ........................................... 11

1. Introduction

Mobile IPv6 [1] allows a mobile node to be always addressable by its home address, whether it is currently attached to its home link or is away from home. While a mobile node is attached to some foreign link away from home, it is also addressable by one or more care-of addresses, in addition to its home address. A care-of address is an IP address associated with a mobile node while visiting a particular foreign link. The subnet prefix of a mobile node’s care-of address is the subnet prefix (or one of the subnet prefixes) on the foreign link being visited by the mobile node; if the mobile node is connected to this foreign link while using that care-of address, packets addressed to this care-of-address will be routed to the mobile node in its location away from home.

The MPLS network provides the backbone solution for high-speed IP forwarding and large scalability. And also the MPLS network support appropriate quality-of-service paths for differentiated mobile IP services. The initial MPLS effort will be focused on IPv4. However, the core technology will be extendible to new network layer protocols (e.g., IPv6).

If IPv6 employs MPLS technology, variable benefit will be expected. Because MPLS is not confined to certain specific link layer technology, it can work with any media over which Network Layer packets can be passed between network layer entities. This aspect will be applicable to guarantee user’s required QoS and Traffic Engineering because MPLS is well suited for DiffServ and sort of ATM Traffic Engineering. In addition, secure VPN and IPv6 transition benefit will be expected.
This document proposes the MPLS network architecture and tunneling procedures to support the mobile IPv6 network. Similar concerns on the integration of MPLS network and Mobile IP network are also investigated in [2][3]. However those documents are lack of Mobile IPv6 consideration.

In terms of control plane concern, both CR-LDP and RSVP-TE are applicable to set up the QoS guaranteed Label Switched Path (LSP) tunnel between a router of the mobile hosts and a router of the correspondent node.

When the integration of wired and wireless network is designed, there are things to consider. For example, idle mobile node, smooth handoff, QoS guarantee, etc. Next part describes those design principles.

2. Benefits from MPLS

2.1. Independency from lower layer technologies

The MPLS control component centers around IP functionality, which is similar to proprietary multilayer switching solutions. However, MPLS defines new standard-based IP signaling and label distribution protocols, as well as extensions to existing protocols, to support multivendor interoperability. In this way, MPLS brings significant benefits to a packet-oriented Internet.

The MPLS forwarding component is based on the label-swapping algorithm. If the Layer 2 technology supports a label field (such as the ATM VPI/VCI or the Frame Relay DLCI fields), the native label field encapsulates the MPLS label. However, if the Layer 2 technology does not support a label field, the MPLS label is encapsulated in a standardized MPLS header that is inserted between the Layer 2 and IP headers. The MPLS header permits any link layer technology to carry an MPLS label so it can benefit from label-swapping across an LSP.

2.2. IPv4 to IPv6 transition benefit

The ability of the underlying Internet infrastructure to accommodate architectural improvements has proven to be a significant factor in its overall success. Though IPv6 Transition still has lots of scenarios and burdens simultaneously. MPLS, a forwarding and control plane architecture, is a notable example of this.

Therefore given the wide-scale backbone adoption of MPLS, it is key that IPv6 integrate with this technology. We believes that both are highly complementary since integrating IPv6 transport services over an MPLS topology requires much less backbone infrastructure upgrades or reconfiguration while also supporting dynamic connectivity between peripheral IPv6 networks. This results from the fact that with MPLS networks, forwarding is based upon labels rather than the IP header itself. As such, the data plane dependency on being able to support native IPv6 packet forwarding is removed, hence eliminating the need for network core hardware and software upgrades, a likely reality for native end-to-end IPv6 forwarding.

2.3. Connection-Oriented Switching Paradigm
As a packet of a connectionless network layer protocol travels from one router to the next, each router makes an independent forwarding decision for that packet. That is, each router analyzes the packet’s header, and each router runs a network layer routing algorithm. Each router independently chooses a next hop for the packet, based on its analysis of the packet’s header and the results of running the routing algorithm.

Unlike normal routers MPLS LSRs deliver connection-oriented network service. Rather than determining the path of each packet independently, the LSRs establish a path between the endpoints of a connection in a network and send the packets across that path. That LSP is still a virtual connection, sharing the bandwidth of the physical circuit. In contrast to connectionless routing, the LSRs can define the parameters of the virtual connection, including allowable speed and priority. This is crucial to the LSR’s ability to manage bandwidth and QoS.

These distinct features give network managers the ability to tailor network service to the specific needs of diverse applications with varying classes of service. Demanded LSPs make use of LSR thus deliver the variable features such as Fault tolerance, Prioritization, QoS Classes.

2.4. Well defined QoS support with DiffServ

Though IPv6 has QoS consideration, it still has things to be solved such as Flow ID issue. In addition, the MPLS shim header achieves the original goals of the Flow ID field.

MPLS allows the precedence or class of service to be fully or partially inferred from the label. In this case, one may say that the label represents the combination of a FEC and a precedence or class of service.

In a DiffServ domain all the IP packets crossing a link and requiring the same DiffServ behavior are said to constitute a Behavior Aggregate (BA). At the ingress node of the DiffServ domain the packets are classified and marked with a DiffServ Code Point (DSCP), which corresponds to their Behavior Aggregate. At each transit node, the DSCP is used to select the Per Hop Behavior (PHB) that determines the scheduling treatment and, in some cases, drop probability for each packet.

Recent work [4] allows the MPLS network administrator to select how Diff-Serv Behavior Aggregates (BAs) are mapped onto Label Switched Paths (LSPs) so that he/she can best match the Diff-Serv, Traffic Engineering and protection objectives within his/her particular network.

2.5. Secure VPN

The secure VPN, one of major applications of MPLS, is also applicable to IPv6 network. The inherent VPN and Traffic Engineering services available within an MPLS environment could enable IPv6 networks going
forward to be combined into virtual private networks or extranets over an infrastructure also supporting IPv4 VPNs and MPLS-TE. Additionally MPLS VPNs offer the same level of security as connection-oriented VPNs. Packets from one VPN do not inadvertently go to another VPN.

VPN traffic is kept separate. Malicious spoofing is nearly impossible because the packets received from customers are IP packets. These IP packets must be received on a particular interface or subinterface to be uniquely identified with a VPN label.

3. Features of Mobile IPv6 with MPLS

3.1. QoS guaranteed LSP setup
It is required to program appropriate QoS support for the MN’s packets in the intermediate network domains, so that the performance of QoS-sensitive applications running on the MN is maintained at desired level. To achieve this, our model adopts QoS Object [5] to interoperate with CR-LDP/RSVP-TE.

3.2. Idle mobile node consideration
We imagine that wireless IP communicators will be turned around the clock, ready to receive or initiate services. In fact, the vast majority of subscribers will not be actively communicating most of the time. Rather, wireless IP communicators will be switched on, ready for service, constantly reachable by the wireless Internet. In essence, MN will be in an idle state but passively connected to the network infrastructure. Thus design principle is that only active data are supposed to traverse over QoS guaranteed LSP. This will prevent LSP abusing that can be caused by lots of control packets. Thus an LSP is established only between MN’s router and CN’s router other than LSP via HA. This would be efficient scheme to save bandwidth on network and to reduce end-to-end delay.

3.3. Smooth handoff support
There are two goals in term of handoff; the first, to reduce the latency or interruption due to handoffs; and second, to reduce the signaling load. Mobile IPv6 is considered as optimal solution for those needs. Use of more than one care-of-address by a MN may be useful to improve smooth handoff when the MN moves from one wireless link to another. Our suggested model supports the smooth handoff scheme of Mobile IPv6 and gives solution to QoS consideration with providing QoS guaranteed multiple LSP for the number of MN’s care-of-address.

3.4. Bi-directional LSP extensible
While traditional traffic engineered MPLS are unidirectional, generalized MPLS [6] supports the establishment of bi-directional LSP. Bi-directional LSP has the benefit of lower setup latency and lower number of messages required during setup. It takes only one initiator-eliminator round trip time. The suggested model is possible to be expended to generalized MPLS.

3.5. No obligation of MPLS signaling on MN
Mobile IPv6 embedded MN and CN doesn’t need to install CR-LDP/RSVP-TE
at all. CR-LDP/RSVP runs on a router or switch of MNs and CNs. This will reduce memory cost and complexity of a MN device.

3.6. No additional messages on legacy MPLS signaling
There is no additional Message or TLV/Object on existing CR-LDP/RSVP-TE to setup QoS guaranteed LSP between CN’s LER and MN’s LER. The suggested model adopts data-driven LSP setup.

4. Description of Operation

4.1. When MN initiates data transmission
We assume a MN has already done new default router finding [7], Address auto-configuration [8], Registration, and Biding Acknowledgement reception as Mobile IPv6 procedures.

Figure 1. The MPLS Network with Mobile IPv6 Support

When the MN sends packets to any other correspondent node, it sends packets directly to the destination. The MN sets the source address of this packet to the care-of-address and includes a ‘Home Address’ destination option. Then the correspondent node must process the option in a manner consistent with exchanging the Home Address field from the Home Address option into the IPv6 header. Since the home address is static (in contrast to the care-of-address), this allows every correspondent node the transparent use of the care-of-address for layers above the Mobile IPv6 support. Higher layers including applications do not recognize the care-of-address. They only notice
the home address. Then the packets from the correspondent node are routed to the HA and tunneled to MN by IPv6-in-IPv6. This routing is called Triangle Routing.

To avoid triangle routing a MN sends Binding Update that may be together with QoS Object to correspondent node. The MN’s LER receiving the Binding Update message should determine whether to initiate REQUEST/PATH message or not. If the Binding Update message has zero H bit, the LER initiates REQUEST/PATH for a destination address (FEC). Now the correspondent IPv6 node receiving the Binding Update message is able to send packets to MN directly. Newly established QoS guaranteed LSP provides tunnel for packets to traverse.

![Figure 2. MN initiates data transmission](draft-choi-mobileip-ipv6-mpls-01.txt)

4.2. When CN initiates data transmission

We assume a MN has already done new default router finding, Address auto-configuration, Registration, and Binding Acknowledgement reception as Mobile IPv6 procedures.

Before a CN sends any packet to the MN, the CN should examine its Binding Cache for an entry for the destination address (Home address) to which the packet is being sent. If the CN has a Binding Cache entry for this address, the CN should use a Routing header to route the packet to the MN by way of the care-of-address in the binding recorded in that Binding Cache entry. We assume that a CN has no Binding Cache entry for the MN in this part. The packet sent by the CN will be intercepted by the MN’s HA and tunneled (using IPv6-in-IPv6 encapsulation) to the MN’s current primary care-of-address.

To avoid triangle routing a MN sends Binding Update that may be together with QoS Object to correspondent node. The MN’s LER receiving the Binding Update message should determine whether to
initiate REQUEST/PATH or not. If the Binding Update message has zero H bit, the LER initiates REQUEST/PATH for a destination address (FEC). Now the correspondent IPv6 node receiving the Binding Update message is able to send packets to MN directly. Newly established QoS guaranteed LSP provides tunnel for packets to traverse.

[Diagram]

<table>
<thead>
<tr>
<th>MN</th>
<th>MN’s LER2</th>
<th>HA</th>
<th>CN’s LER3</th>
<th>CN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IPv6-in-IPv6 tunneling</td>
<td></td>
<td>packet</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Binding update with QoS Object</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>REQUEST/PATH</td>
<td></td>
<td>MAPPING/RESV</td>
<td></td>
</tr>
<tr>
<td></td>
<td>QoS guaranteed LSP</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 3. CN initiates data transmission

4.3. Smooth Handoff

Use of more than on care-of-address by a MN may be useful to improve smooth handoff when the MN moves from one wireless link to another. If each of these wireless links is connected to the Internet through a separate base station, such that the wireless transmission range from the two base stations overlap, the mobile node may be able to remain connected to both links while in the area of overlap. In this case, the MN could acquire a new care-of-address on the new link before moving out of transmission range and disconnecting from the old link. The MN may thus still accept packets at its old care-of-address while it works to update its HA and CNs, notifying them of its new CoA on the new link.

When a MN acquires new CoA while communicating with CN over legacy LSP, The MN sends Binding Update along with QoS Object to the CN for Route Optimization. The MN’s LER receiving the Binding Update message will initiates REQUEST/PATH. Now the correspondent IPv6 node receiving the Binding Update message is able to send packets to MN directly while previous flow have been traversed over the legacy LSP. Which supports smooth handoff scheme over both legacy LSP and newly established QoS guaranteed LSP. The old LSP will be released automatically as time goes by because no more data transmitted over the LSP.

[Diagram]
There are still lots of discussion to adopt appropriate handoff scheme\[9\][10]. Our document keeps an eye on those emerging handoff algorithm and will adopt some of them to establish LSP between CN’s LSR and MN’s one. Thus above handoff support LSP scheme may change. For example, If a Handoff scheme use tunnel method between Old Access Router (AR) and New AR, Our scheme may evolve to setup extended LSP between Old AR and New AR. In this case MN can receive data through old LSP and extended LSP as well as newly established LSP associated new CoA.

4.4. QoS supported LSP

The composition of a QoS OBJECT is shown in Figure 5. A QoS OBJECT is an extension of RSVP QoS and FILTER_SPEC objects. This is originally from [5].
MN’s packet stream in terms of traffic class. An example is specification in terms of DiffServ PHB classes such as EF or AF. IntServ classes such as guaranteed service or controlled load service and UMTS QoS class [11] such as delay sensitivity, interactive-delay sensitive, non-interactive delay sensitive or delay insensitive are also supported.

Some examples are,

00000xxx: DiffServ EF PHB
00001xxx: DiffServ AF PHB

After some sort of authentication, which is beyond the scope of this document, MN’s LSR can send Label REQUEST/PATH message with DiffServ TLV/DiffServ Object to establish E-LSP or L-LSP.

5. Required messages and TLVs

There are no additional messages and TLVs to existing Mobile IPv6 [1], CR-LDP/RSVP-TE, and Generalized MPLS [6] to operate the suggested model. In order to support QoS guaranteed communication in Mobile IPv6, QoS object described in [5] is required.

6. Conclusion

We have proposed a scheme to integrate Mobile IPv6 and MPLS. This scheme eliminates usages of IP-in-IP tunneling in the data forwarding.

Switching is much faster than hop-by-hop IP forwarding, so the transmission delay and packet processing overhead is reduced. We have designed principles such as No change to Mobile IPv6, Idle node consideration, smooth handoff, bi-directional LSP, and QoS guaranteed service. This document will be divided by RSVP-TE centered memo and CR-LDP centered one.

7. Security Considerations

The Mobile IPv6 and MPLS scheme described in this document is subject to the same security considerations that apply to draft-ietf-mobileip-ipv6-13.txt[1], RFC3036[11], RFC3031[12].

8. References


8. Author’s Addresses

Jun Kyun Choi
Information and Communications University (ICU)
58-4 Hwa Ahm Dong, Yusong, Taejon
Korea 305-732
Phone: +82-42-866-6122
Email: jkchoi@icu.ac.kr

Myoung Hun Kim
Information and Communications University (ICU)
58-4 Hwa Ahm Dong, Yusong, Taejon
Korea 305-732
Phone: +82-42-866-6198

Email: fiaa@icu.ac.kr

Yoon Ju Lee
Electronics and Telecommunication Research Institute (ETRI)
161 Kajung Dong Yusong, Taejon
Korea 305-305
Phone: +82-42-860-1130
Email: yjlee@etri.re.kr

Full Copyright Statement

"Copyright (C) The Internet Society (date). All Rights Reserved. This
document and translations of it may be copied and furnished to others,
and derivative works that comment on or otherwise explain it or
assist in its implementation may be prepared, copied, published and
distributed, in whole or in part, without restriction of any kind,
provided that the above copyright notice and this paragraph are
included on all such copies and derivative works. However, this
document itself may not be modified in any way, such as by removing
the copyright notice or references to the Internet Society or other
Internet organizations, except as needed for the purpose of
developing Internet standards in which case the procedures for
copyrights defined in the Internet Standards process must be followed,
or as required to translate it into languages other than English. The
limited permissions granted above are perpetual and will not be
revoked by the Internet Society or its successors or assigns."