INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2001-2004

COM 13 – C 28 – E

May 2003

English only

Original: English

Question(s): 11/13

STUDY GROUP 13 – CONTRIBUTION 28

Source: Editor

Title: Draft new Recommendation Y.MIPoMPLS (Mobile IP Services over MPLS) (05/2003)

The draft new Recommendation Y.MIPoMPLS is planned for consent at the next ITU-T SG 13 meeting (21 July – 1 August 2003).

Contact: Jun Kyun Choi

Tel: +82 42 866 6122
Fax: +82 42 866 6110
Email jkchoi@icu.ac.kr

Draft Recommendation Y.MIPoMPLS

Mobile IP Services over MPLS

Summary

This Recommendation defines service definition and requirements to support mobile IP services through the MPLS network. It also describes the service architectures and application procedures to provide the mobility service support over the MPLS network.

Source

To be added.

Keywords

MPLS, Label Switched Path (LSP), mobile IPv4, mobile IPv6, route optimization, Home Agent (HA), Foreign Agent (FA), Label Edge Router (LER), Label Switched Router (LSR), Quality-of-Service (QoS), Virtual Private Network (VPN)

DRAFT RECOMMENDATION Y.MIPoMPLS

Mobile IP Services over MPLS

(Sophia Antipolis, 2003)

1. Introduction

The purpose of this Recommendation describes the service architecture and application procedure to support mobile IP service over the MPLS network.

In the mobile IP network, a node's IP address uniquely identifies the node's point of attachment. Therefore, a mobile node must be located on the network indicated by its IP address in order to receive packets destined to it. Otherwise, packets destined to the mobile node would be undeliverable. In order not to lose its ability to communicate whenever it changes its point of attachment, the mobile node must change its IP address. The IP address of mobile node must be advertised through the entire Internet to receive packets whenever it moves. The link by which a mobile node is directly attached to the Internet may often be a wireless link [7].

Mobile IP is intended to enable nodes to move from one IP subnet to another. It is just as suitable for mobility across heterogeneous media. If the mobile node moves from one LAN segment to another (e.g., a wireless LAN), the mobile node's IP address remains the same after such a movement. A mobile node is given a long-term IP address on a home network. This home address is administered in the same way as a "permanent" IP address is provided to a fixed host. When away from its home network, a "care-of address" is associated with the mobile node and reflects the mobile node's current point of attachment.

When away from home, Mobile IP uses protocol tunneling to hide a mobile node's home address from intervening routers between its home network and its current location. The tunnel terminates at the mobile node's care-of address [8]. The care-of address must be an address to which packets can be delivered via conventional IP routing. At the point of care-of address, the original packet is escaped from the tunnel and delivered to the mobile node.

In the basic mobile IPv4 protocol, there is no direct routing from any correspondent node to any mobile node. It needs to pass through the mobile node's home network and be forwarded by its home agent, which is called by the problem of “triangle routing.” To solve this problem, the Route Optimization allows direct routing from any correspondent node to any mobile node [24]. In IPv6 network, IPv6 nodes cache the binding of a mobile node's home address with its care-of address, and to then send any packets destined for the mobile node directly to it at this care-of address. To support this operation, mobile IPv6 defines a new IPv6 protocol and a new destination option [25]. All IPv6 nodes, whether mobile or stationary, support communications with mobile nodes.

In the network provider’s point of views, future network should be designed to create greater functionality, generality, adaptability, and/or robustness in order to support network operation and maintenance by guaranteeing acceptable quality-of-service (QoS) levels and satisfying various service level agreements (SLAs). To support the on-going or future business models over wireline and wireless network environments, original Internet would be upgraded to meet the demands placed on it by real-time and multimedia applications. It thus delivers variable features such as fault tolerance, prioritization, QoS classes. These distinct features give network managers the ability to tailor network service to the specific needs of diverse applications with varying classes of service.

To meet these requirements for future mobile service, first, the end-to-end performance should be manageable regardless of whether end applications are moving or not. Second, for the mobile IP service, the cost of layer model including functions of home agent and foreign agent should be proved after exploration of the architectural consequences. Third, the existing and future transport technologies including optical network should be applicable to support future mobile world.

In the MPLS network, once a packet is assigned to relevant classification according to quality of service, no further header analysis is done by subsequent routers; all forwarding is driven by the labels. This has a number of advantages over conventional IP layer forwarding. The MPLS forwarding can be done by switches which are capable of doing label lookup and replacement at adequate speed and QoS. It does not need to analyze the network layer headers. Sometimes it is desirable to force a packet to follow a particular route which is explicitly chosen at or before the time the packet enters the network, rather than being chosen by the normal dynamic routing algorithm as the packet travels through the network. This may be done as a matter of policy, or to support traffic engineering. In conventional forwarding of the original Internet, this requires the packet to carry an encoding of its route along with it ("source routing"). In MPLS, a label can be used to represent the explicit route, which is, called by a tunnel.

For mobile service, the home agent intercepts packets on the home link destined to the mobile node's home address, encapsulates them, and tunnels them to the mobile node's registered care-of address via foreign agent. The foreign agent de-tunnels and delivers packets to the mobile node.

By combining tunneling functions of a home agent and a foreign agent into the MPLS forwarding paradigm, the MPLS node can be capable of handling the mobile node by assigning labels for a tunnel between a home agent and a foreign agent. In this case, the home agent and the foreign agent can be located or attached at the MPLS node. It results that the tunneling between the home agent and the foreign agent are merged into the MPLS layer. To avoid the problem of triangle routing, the MPLS nodes can allow a direct binding, which is routing optimization, from any correspondent node to any mobile node by assigning a label.

2. Scope

The scope of this recommendation covers:

- Service requirements and definitions for mobile IPv4 and mobile IPv6 services over MPLS
- Service architecture including all functions to support mobile IP service over MPLS
  - the edge MPLS node directly attached to mobile IPv4 and mobile IPv6 hosts or emulation of hosts
- LSP tunneling scenarios to support the mobile IP services over MPLS
- Application procedures to support the mobile IP services operation and provisioning

However, it is out of scope in this recommendation.

- the detailed interworking procedures between the external mobile IP network and the MPLS network including traffic and QoS parameters
- The mapping and conversion procedures between the IP-in-IP tunnels inside the mobile IP network and the LSP tunnels of the MPLS network.
- Coverage of more than one MPLS administrative domain
- QoS negotiation procedures between mobile IP nodes and the MPLS network

- Routing algorithm of MPLS network with mobility support
- How to use datagram traffic (e.g., UDP) and stream-like traffic (e.g., TCP) for specific network applications
- The detailed protocol and packet formats for RSVP-TE and CR-LDP tunnel establishment

3. References

3.1 Normative Reference

ITU-T

[1] Recommendation Y.1310 (2000) - Transport of IP over ATM in Public Networks

[2] Recommendation Y.1311 (2001) - IP VPNs - Generic architecture and service requirements

[3] Recommendation Y.1311.1 (2001) - Network-based IP VPN over MPLS architecture

[4] Recommendation Y.1241 (2000) - IP Transfer Capability for Support of IP based Services

[5] Recommendation Y.1401 (2000) - General requirements for interworking with Internet protocol (IP)-based networks

[6] Recommendation Y.1540 (2000) - Internet Protocol Data Communication Service – IP Packet Transfer and Availability Performance Parameters

[7] Recommendation Y.1541 (2001) - Network Performance Objectives for IP-Based Services

IETF

[8] L. Andersson, et. al, "LDP Specification," RFC 3036, January 2001.

[9] C. Perkins, "IP Mobility Support for IPv4," RFC3220, January 2002.

[10] C. Perkins, "IP Encapsulation within IP," RFC 2003, October 1996.

[11] C. Perkins, "Minimal Encapsulation within IP," RFC 2004, October 1996.

[12] S. Deering, et al, "ICMP Router Discovery Messages," RFC 1256, September 1991.

[13] E. Crawley, et. al. “A Framework for QoS-based Routing in the Internet,” RFC 2386, August 1998.

[14] E. Rosen, et. al, “Multiprotocol Label Switching Architecture,” RFC 3031, January 2001

[15] D. Awduche, et. al, “RSVP-TE: Extensions to RSVP for LSP Tunnels.” RFC 3209, December 2001

[16] B. Jamoussie, et al.” Constraint-Based LSP Setup using LDP,” RFC 3212, January 2002.

[17] S. Blake, et. al, “An Architecture for Differentiated Service,” RFC 2475, December 1998.

[18] R. Braden et. al, “Integrated Services in the Internet Architecture: an Overview,” RFC 1633, June 1994.

[19] S. Kent and R. Atkinson. “Security Architecture for the Internet Protocol,” RFC 2401, November 1998.

[20] C. de Laat, et. Al, “Generic AAA Architecture,” RFC2903, August 2000

[21] S. Glass, et. al, "Mobile IP Authentication, Authorization, and Accounting Requirements," RFC 2977, October 2000

[22] D. Cong , et. al, "The Definitions of Managed Objects for IP Mobility Support using SMIv2," RFC 2006, October 1996

[23] Thomas Narten, Erik Nordmark, "Neighbor Discovery for IP Version 6 (IPv6)," RFC 2461, December, 1998.

[24] S. Thomson and T. Narten, "IPv6 Stateless Address Auto-configuration," RFC 2462, 1998.

[25] F. Le Faucheur, et. al, "Multi-Protocol Label Switching (MPLS) Support of Differentiated Services," RFC 3270, May 2002

[26] P. Ferguson and D. Senie. "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing," RFC 2267, January 1998.

[27] L. Berger, et. al., "Generalized MPLS Signaling - RSVP-TE Extensions," RFC3473, January 2003

[28] P. Ashwood-Smith, et. al., "Generalized MPLS Signaling – CR-LDP Extensions," RFC3472, January 2003

3.2 Informative Reference

[29] C. Perkins and Pat R. Calhoun AAA Registration Keys for Mobile IP, <draft-ietf-mobileip-aaa-key-11.txt>, March 2003

[30] David B. Johnson, et al, "mobility support in IPv6," <draft-ietf-mobileip-ipv6-21.txt>, February 2003

[31] Thomas D. Nadeau, et.al, "Multiprotocol Label Switching (MPLS) Management Overview," <draft-ietf-mpls-mgmt-overview-03.txt> February 2003

[32] G. Tsirtsis, "Fast Handovers for Mobile IPv6," <draft-ietf-mobileip-fast-mipv6-06.txt>, March 2003

[33] E. Gustafsson, "Mobile IPv4 Regional Registration,"<draft-ietf-mobileip-reg-tunnel-07.txt>, October 2002

[34] Pat R. Calhoun, et. al, " Diameter Base Protocol," <draft-ietf-aaa-diameter-17.txt>, 2002

[35] Pat R. Calhoun, et. al, " Diameter Mobile IPv4 Application," <draft-ietf-aaa-diameter-mobileip-14.txt>, 2002

4. Terms and Definitions

In relation with mobile IPv4, mobile IPv6 and MPLS, this Recommendation defines the following terms.

- **Mobile Node (MN)**

  A node that can change its point of attachment from one link to another, while still being reachable via its home address. [30]

- **Correspondent Node (CN)**

  A peer with which a mobile node is communicating. A correspondent node may be either mobile or stationary. [9]

- **Home Agent (HA)**

  A router on a mobile node's home link with which the mobile node has registered its current care-of address. While the mobile node is away from home, the home agent intercepts packets on the home link destined to the mobile node's home address, encapsulates them, and tunnels them to the mobile node's registered care-of address. [30]

- **Foreign Agent (FA)**

  A router on a mobile node's visited network which provides routing services to the mobile node while registered. The foreign agent detunnels and delivers packets to the mobile node that were tunneled by the mobile node's home agent [9]

- **Mobility Agent**

  Either a home agent or a foreign agent [9]

- **Agent Discovery**

  Home agents and foreign agents may advertise their availability on each link for which they provide service (that is, Agent Advertisement). A newly arrived mobile node can send a solicitation on the link to learn if any prospective agents are present (that is, Agent solicitation). [9]

- **Home Address**

  An IP address assigned to a mobile node, used as the permanent address of the mobile node. This address is within the mobile node's home link. Standard IP routing mechanisms will deliver packets destined for a mobile node's home address to its home link. [30]

- **Care-of Address (CoA)**

  The termination point of a tunnel toward a mobile node, for packets forwarded to the mobile node while it is away from home. The protocol can use two different types of care-of address: a "foreign agent care-of address" is an address of a foreign agent with which the mobile node is registered, and a "co-located care-of address" is an externally obtained local address which the mobile node has associated with one of its own network interfaces.[9] In IPv6, among the multiple care-of addresses that a mobile node may have at any given time (e.g., with different subnet prefixes), the one registered with the mobile node's home agent is called its "primary" care-of address.[30]

- **Mobility Binding**

  The association of a home address with a care-of address, along with the remaining lifetime of that association [9]

- **Binding Update**

  A message indicating a mobile node's current mobility binding, and in particular its care-of address. [12]

- **Binding Acknowledgement**

  A Binding Acknowledgement message is used to acknowledge receipt of a Binding Update. [30]

- **Binding Cache**

  A cache of mobility bindings of mobile nodes, maintained by a node for use in tunneling packets to those mobile nodes. [30]

- **Triangle Routing**

  A situation in which a Correspondent Host's packets to a Mobile Host follow a path which is longer than the optimal path because the packets must be forwarded to the Mobile Host via a Home Agent.[30]

- **Quality-of-Service (QoS)**

  A set of service requirements to be met by the network while transporting a flow [13]

- **IP-in-IP Encapsulation**

  To encapsulate an IP datagram using IP in IP encapsulation, an outer IP header is inserted before the datagram's existing IP header. [10]

- **Label Edge Router (LER)**

  An MPLS node that connects an MPLS domain with a node which is outside of the domain, either because it does not run MPLS, and/or because it is in a different domain. [14]

- **Label Switching Router (LSR)**

  An MPLS node which is capable of forwarding native L3 packets [14]

- **Layer 3 (L3)**

  The protocol layer at which IP and its associated routing protocols operate link layer synonymous with layer 2 [14]

- **Layer 2 (L2)**

  The protocol layer under layer 3 (which therefore offers the services used by layer 3). Forwarding, when done by the swapping of short fixed length labels, occurs at layer 2 regardless of whether the label being examined is an ATM VPI/VCI, a frame relay DLCI, or an MPLS label.[14]

- **Label Switched Path (LSP)**

  The path through one or more LSRs at one level of the hierarchy followed by packets in a particular FEC [14].

- **Forwarding Equivalence Class (FEC)**

  A group of IP packets which are forwarded in the same manner (e.g., over the same path, with the same forwarding treatment) [14]

- **MPLS Domain**

  A contiguous set of nodes which operate MPLS routing and forwarding and which are also in one Routing or Administrative Domain [14]

- **MPLS Node**

  A node which is running MPLS (e.g., LER and LSR). An MPLS node will be aware of MPLS control protocols, will operate one or more L3 routing protocols, and will be capable of forwarding packets based on labels. An MPLS node may optionally be also capable of forwarding native L3 packets [14]

- **MPLS Egress Node or Egress LER**

  An MPLS edge node in its role in handling traffic as it leaves an MPLS domain [14]

- **MPLS Ingress Node or Ingress LER**

  An MPLS edge node in its role in handling traffic as it enters an MPLS domain [14]

- **Label Edge Router/Home Agent (LER/HA)**

  An MPLS edge node with functions of Home Agent. While the mobile node is away from home location, the LER/HA intercepts packets on the home link destined to the mobile node's home address, encapsulates them, and tunnels them to the mobile node's registered care-of address.

- **Label Edge Router/Foreign Agent (LER/FA)**

  An MPLS edge node with functions of Foreign Agent. The LER/FA detunnels and delivers packets to the mobile node that were tunneled by the mobile node's home agent. It notes that there is no need of foreign agent in IPv6. It means that the LER/FA is equivalent to the LER in IPv6.

- **Gateway LER/HA**

  One or more LER/HA’s responsible for a specific administrative domain (defined by network operator), in which all the mobile nodes have registered its current care-of address.

- **Gateway LER/FA**

  One or more LER/FA’s responsible for a specific administrative domain (defined by network operator), which provides routing and encapsulation/de-capsulation services to all the visited mobile nodes while registered.

- **Path Extension**

  When a mobile node moves and registers with a new foreign agent, IP datagrams of old foreign agent are tunneled to the mobile node's new care-of-address[30].

- **Route Optimization**

  Route optimization provides a means for any node to maintain direct path information to the destination mobile node. When sending an IP datagram to a mobile node, if the sender has a binding cache entry for the destination mobile node, it may tunnel the datagram directly to the care-of address indicated to the mobile nodes [30].

- **Gateway Foreign Agent (GFA)**

  Foreign Agent which has a publicly routable IP address. A GFA may, for instance, be placed in or near a firewall [33].

- **Regional Foreign Agent (RFA)**

  A Foreign Agent which may be the target of a request for regional registration [33].

- **Regional Registration**

  A mobile node performs registration locally at the visited domain, by sending a Regional Registration Request to a GFA, and receiving a Regional Registration Reply in return [33].

- **Smooth Handover**

  When a mobile node moves and registers with a new foreign agent, IP datagrams intercepted by the home agent after the new registration are tunnelled to the mobile node's new care-of address, but datagrams in flight that had already been intercepted by the home agent and tunnelled to the old care-of address when the mobile node moved are likely to be lost and are assumed to be retransmitted by higher-level protocols if needed. The old foreign agent eventually deletes its visitor list entry for the mobile node after the expiration of the registration lifetime. Smooth handover provides a means for the mobile node's previous foreign agent to be reliably notified of the mobile node's new mobility binding, allowing datagrams in flight to the mobile node's previous foreign agent to be forwarded to its new care-of address [30].

- **Virtual Private Network (VPN)**

  A virtual private network (VPN) is a network which provides connectivity amongst a limited and specific subset of the total set of users. A VPN has the appearance of a network that is dedicated specifically to the users within the subset. This dedication is achieved through logical rather than physical means, hence the use of the word virtual. Users within a VPN cannot communicate, via the VPN provider, with users not included in the specific VPN subset and vice versa [2].

- **Security Association**

  A security association is a simplex "connection" that affords security services to the traffic carried by it. Security services are afforded to a security association by the use of the authentication protocols [30].

5. Abbreviations

ARP	Address Resolution Protocol
CN	Correspondent Node
CR-LDP	Constraint-based Label Distribution Protocol
FA	Foreign Agent
FEC	Forwarding Equivalence Class
FIB	Forwarding Information Base
GFA	Gateway Foreign Agent
HA	Home Agent
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
LDP	Label Distribution Protocol
LER	Label Edge Router
LIB	Label Information Base
LSP	Label Switched Path
LSR	Label Switching Router
MIPv4oMPLS	Mobile IPv4 over MPLS
MIPv6oMPLS	Mobile Ipv6 over MPLS
MN	Mobile Node
MPLS	Multiprotocol Label Switching
QoS	Quality-Of-Service
RFA	Regional Foreign Agent
Resv	Reserved
RSVP-TE	Resource Reservation Protocol - Traffic Engineering
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

6. Service Definitions and Service Requirements

6.1 Service Definitions

- MIPv4 over MPLS (MIPv4oMPLS) service definition

  A mobile node with running IPv4 protocol must be able to communicate with other nodes after changing its link-layer point of attachment within the MPLS network, yet without changing its IP address. Whenever it changes its point of attachment, a mobile node does not lose its ability to communicate.

A mobile IPv4 over MPLS service is intended to enable nodes to move from one MPLS domain to another. It is just as suitable for mobility across various MPLS domains. That is, mobile IP facilitates node movement from one MPLS domain to another as long as the mobile node's IP address remains the same after such a movement.

One can think of handover management amongst MPLS domains, each of which covers a small geographic area. As long as node movement does not occur between points of attachment on different IP subnets, layer 2 mechanisms for mobility (i.e., link-layer handoff) may offer faster convergence and far less overhead than Mobile IP. MobileIPv4 over MPLS service can provide the LSPs between different mobile IP subnets both for layer 2 and layer 3.

In applications of MPLS related to traffic engineering, it is desirable to set up an explicitly routed path, from ingress to egress. It is also desirable to apply resource reservations along that LSP.

- MIPv6 over MPLS (MIPv6oMPLS) service definition

  In mobile IPv6, route optimization is now built in as a fundamental part of the protocol The route optimization functionality allows direct routing from any correspondent node to any mobile node, without needing to pass through the mobile node's home network and be forwarded by its home agent, and thus eliminates the problem of "triangle routing" present in the base Mobile IPv4 protocol. The registration function and the route optimization function are performed by a single protocol rather than two separate protocols in mobile IPv4. While a mobile node is away from home, its home agent intercepts any packets for the mobile node that arrive at the home network, using IPv6 neighbor discovery as is used in mobile IPv4. The use of neighbor discovery improves the robustness of the protocol and decouples Mobile IP from any particular link layer, unlike in ARP in IPv4 protocol.

  While away from home, a mobile node registers its care-of-addresses on its home agent for the mobile node. The association between a mobile node's home address and care-of address is known as a "binding" for the mobile node. The mobile node performs this binding registration by sending a "Binding Update" message to the home agent The Binding Update procedure provides a way to verify that a mobile node is reachable at its home address and at its care-of address. When sending a packet to any IPv6 destination, a node checks its cached bindings for an entry for the packet's destination address. If a cached binding for this destination address is found, the node uses a new type of IPv6 Routing header. By applying the MPLS protocol, the LSP between the corresponding node and care-of address of the mobile node along with its cache binding may be set up with bandwidth reservation.

6.2 General Requirements

In order to support mobile IPv4 and mobile IPv6 services, the MPLS network satisfy the following general requirements.

- The location of mobile nodes is registered at the gateway LER/HA.
- The LER or LER/FA keeps the information of mobile nodes as LSP tunnel end point, in which encapsulation or de-capsulation of packets is taken with label header information.
- It provides the label switched path with the requested QoS levels, if any, between the ingress LER and egress LER.
- It requires minimizing service interruption at a time of handover. The acceptable QoS level should be maintained during handover.

6.3 MIPv4oMPLS Functional Requirements

- A mobile node must be able to communicate with other nodes after changing its link-layer point of attachment to the MPLS network, yet without changing its IP address.

- Requirements for agent discovery
  Mobility agents (i.e., foreign agents and home agents) advertise their presence via agent advertisement messages. A mobile node may optionally solicit an agent advertisement from any locally attached mobility agents through an agent solicitation.

- Requirements for registration
  When the mobile node detects that it is located on its foreign location, it operates with mobility services by registering with its home agent. If returning to its home location from being registered, the mobile node deregisters with its home agent, through exchange of a registration request and registration reply message with it.

- Requirements for location management
  When a mobile node detects that it has moved to a foreign location, it obtains a care-of address on the foreign MPLS domain.

- Requirements for routing including handover
  Transparent routing of IP packets to mobile nodes in the MPLS network has to be supported. Handover has to be supported.

- Requirements for security
  The mobile network environment is potentially very different from the fixed network environment. In many cases, mobile nodes will be connected to the network via wireless links. The LSPs using such links are particularly vulnerable to passive eavesdropping, active replay attacks, and other active attacks. Home agents and mobile nodes must be able to perform authentication.

6.4 MIPv6oMPLS Functional Requirements

- Mobile IPv6 protocol requirements
  While situated away from its home, a mobile IPv6 node is associated with a co-located care-of address, which provides information about the mobile node's current location. IPv6 packets addressed to a mobile node's home address are transparently routed to its care-of address.

- Route optimization (or binding update) requirements
  The mobile IPv6 protocol enables IPv6 nodes to cache the binding of a mobile node's home address with its care-of address, and to then send any packets destined for the mobile node directly to it at this care-of address.

7. Service Architecture

7.1 Introduction

The MPLS backbone network can build the large-scale Mobile IP network. A mobile node is connected to any other fixed or mobile nodes via the Label Edge Router (LER). The LER is capable

of forwarding Mobile IP packets by encapsulating with shim label header. The packet with label encoding travels a particular route through the network since a label is used to represent the explicit route and is encoded by relevant classification according to quality of service (QoS). The MPLS defines the standard-based IP signaling (e.g., label distribution protocol) to support multi-vendor interoperability. In this way, MPLS brings significant benefits to a connection-oriented Internet.
The MPLS forwarding logic 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.
Unlike normal routers MPLS 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. The MPLS shim header achieves the original goals of the flow identification. 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. It allows the MPLS network administrator to select how DiffServ Behavior Aggregates (BAs) are mapped onto Label Switched Paths (LSPs) so that it can match the DiffServ, traffic engineering and protection objectives within particular network.

For mobile service, the MPLS network has to accommodate the foreign agent and the home agent. By combining of functions of the home agent and the foreign agent into the MPLS node, the MPLS network can be capable to handle the mobile node by assigning labels. In this case, the home agent and the foreign agent can be located at the MPLS node which are called by LER/HA and LER/FA, respectively. The packets intercepted by LER/HA are encapsulated with label header and tunnels to the current location of mobile node via LER/FA. The label switched path (LSP) between the home agent and the foreign agent are used to tunnel with relevant quality-of-service. The label distribution protocol such as CR-LDP and RSVP-TE may be used to set up the LSP tunnel between the mobile agents (that is, foreign agents and home agents) through the MPLS network. The IP-in-IP tunnels between the home agent and the foreign agent are merged into one or multiple LSP's through the MPLS network. To avoid the problem of triangle routing, a direct LSP can be established from any correspondent node to any mobile node.

When a mobile node is moving to a neighbor region, the existing LSPs are extended without service interrupt. The path re-routing may be needed to avoid the triangle routing and provide the short-cut path.

To support mobile IPv4 and mobile IPv6, the MPLS protocol can set up the LSP's between the corresponding node and mobile node with the help of the home agent and the foreign agent. There may be four types of LSP tunneling scenarios as follows.

- Scenario 1 (MPLS-based Mobile IPv4 Tunneling Scenario) applies basic mobile IPv4 services over the MPLS network while it sets up the LSP between the corresponding node and mobile node. It is a natural extension of the existing mobile IPv4 protocol via home agent. The Ingress LER intercepts the incoming packets to forward the mobile node via both

LER/HA and Egress LER/FA. In this scenario, two LSP's are required between Ingress LER and LER/HA, and between LER/HA and Egress LER/FA.

- Scenario 2 (MPLS-based Mobile IPv4 Route Optimization Scenario) applies route optimization over the MPLS network to avoid the problem of triangle routing of existing mobile IP protocol. The direct short cut LSP's between Ingress LER and Egress LER is used without access to the home agent.
- Scenario 3 (MPLS-based Mobile IPv6 Binding Update Scenario) applied the Binding Update procedure of the IPv6 nodes to cache the binding of a mobile node's home address with its care-of address. There is no longer any need of "foreign agents" as in mobile IPv4. In Mobile IPv6 a mobile node makes use of IPv6 features, such as neighbor discovery and address auto-configuration. The LER has the equivalent capabilities with ingress filtering of mobile IPv6 and build LSP's between Ingress LER and Egress LER to transparently deliver packets to the mobile node.
- Scenario 4 (MPLS-based Hierarchical Mobile IP Tunneling Scenario) applies hierarchical Mobile IP protocol over MPLS network. The relevant mobile agents are located at the hierarchical MPLS node to build large scale network. This scenario performs regional registration locally such as regional FA and gateway FA. In case of handover, these FA take a role of anchor node for LSP re-routing at a visited area.

7.2 Service Reference Architecture

7.2.1 Assumptions of Environment

In order to provide the backbone solution for Mobile IP network, it considers the following assumptions on the MPLS network.

- It assumes the intra-domain in coverage of a single MPLS administrative domain. It does not consider the inter-MPLS domain between different network operators.
- There are no additional requirements on MPLS for support of the existing Mobile IPv4 and Mobile IPv6 protocol such as agent discovery and location management including registration.
- All the mobile nodes should be directly connected at the LER/FA. If one or more mobile networks are attached to the LER/FA, in which a number of HA and FA's consists of a single mobile IP network, the connections to LER/FA should be emulated as direct interface from a mobile node. In this case, the LER/FA may be an external gateway router of the attached mobile network to communicate the external world.
- In the MPLS network, all the LERs have a role of foreign agent to identify the visiting mobile nodes. In mobile IPv6 over MPLS, the LER has a function ingress filtering. The functions of the home agent may be located at LER or LSR depending on coverage of a mobile IP's home address.
- The forwarding process on the MPLS network should be taken on the datagram IP traffic (the UDP traffic) as well as the stream-like IP traffic (the TCP traffic).
- The LER/HA and LER/FA support security associations.

7.2.2 Reference Architecture

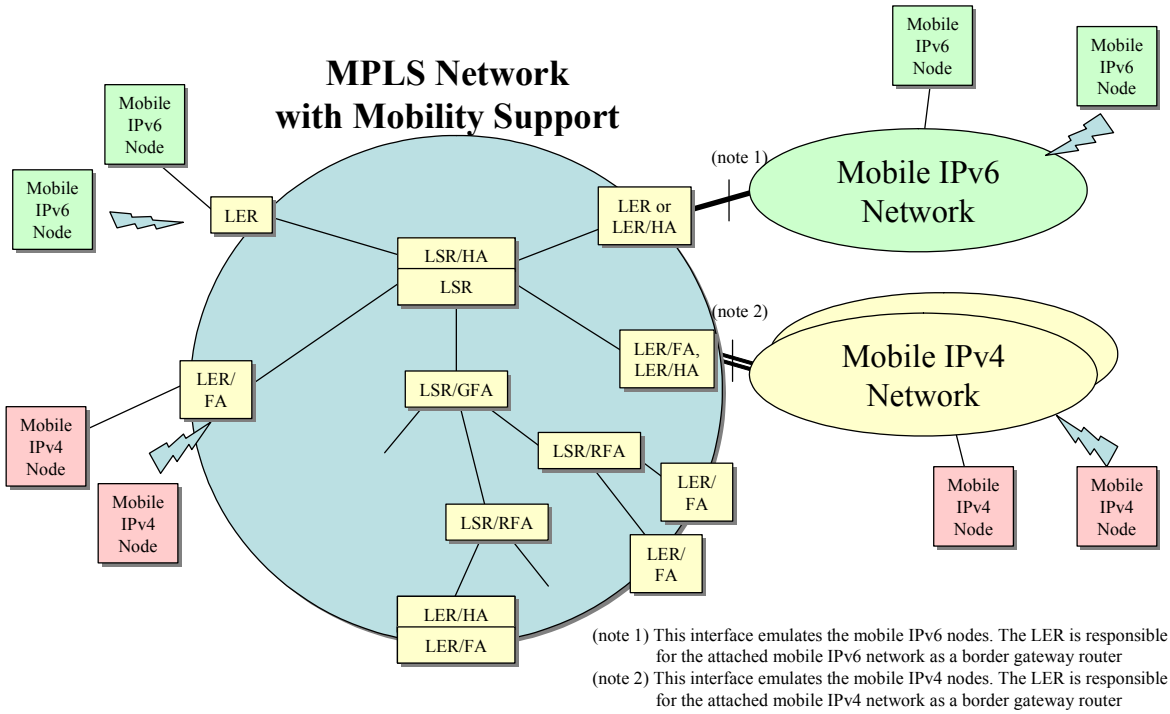


FIGURE 1/Y.MIPoMPLS

Reference architecture of MPLS network with mobility support

(Note) The interworking between mobile IP network and the MPLS network is out-of-scope in this Recommendation. The reference architecture for mobile IPv4, mobile IPv6, and MPLS network with fixed IP and mobile IP nodes is provided in Appendix A.

7.3 LSP Tunnelling Scenarios

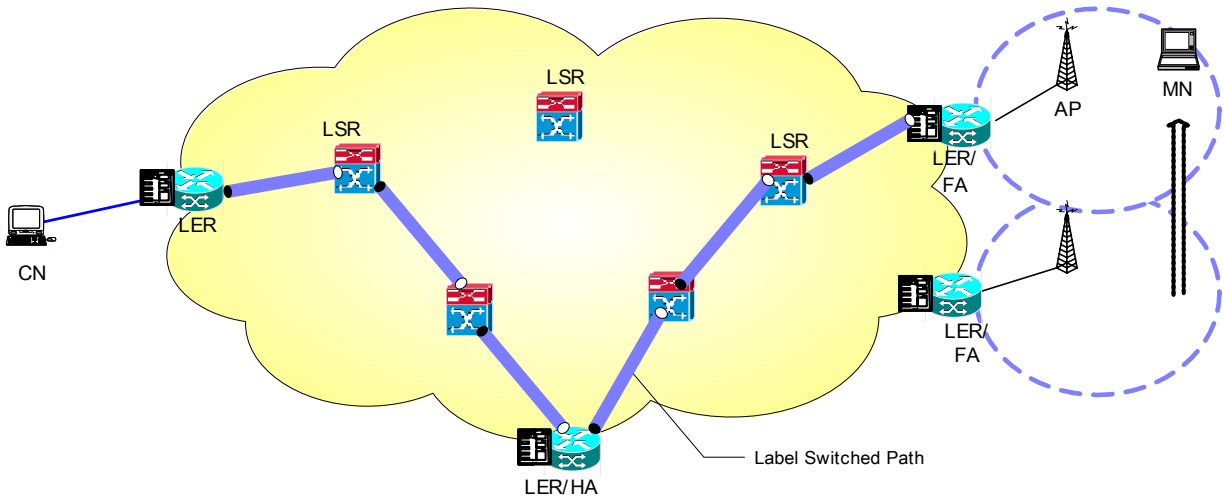
There are four LSP tunnelling scenarios both for mobile IPv4 and mobile IPv6 services.

7.3.1 MPLS-based Mobile IPv4 Tunneling Scenario

In this scenario, the MPLS tunneling mechanism to support mobile IPv4 service are described. While the mobile node is moving to a foreign area, the LER/HA intercepts packets with home IP address of mobile node and forwards them to the LER/FA on temporarily visiting area of the mobile node. The label switched path (LSP) tunnel provides tunnels without IP-in-IP encapsulation. It notes that the IP-in-IP tunneling utilizes the layer 3 forwarding capability in IP routing. The Ingress LER forwards IP packets all the way to the home agent to the Egress LER to the foreign mobile node. The whole forwarding process is done at the MPLS layer.

Since label header is much smaller than IP encapsulation header, the header overhead from the home agent to the foreign agent is also reduced. Moreover, an LSP satisfying the quality-of-service (QoS) requirements and traffic engineering could be set up with CR-LDP or RSVP-TE.

Figure 2/Y.MIPoMPLS shows the MPLS network architecture using Scenario 1 (MPLS-based Mobile IPv4 Tunneling Scenario). In this scenario, a LER/HA intercepts packets and forwards them to a mobile node. The relevant LSP will be set up with associations of the Forwarding Equivalence Class (FEC).



LER: Label Edge Router

LSR: Label Switching Router

HA: Home Agent

FA: Foreign Agent

MN: Mobile Node

AP: Access Point

CN: Correspondent Node

FIGURE 2/Y.MIPoMPLS

MPLS-based Mobile IPv4 Tunneling Scenario

In this scenario, all the home agents and all the foreign agents can be located in the LERs. The LSPs can be setup the same way as "tunnels" are setup between the home agent and the foreign agent. In addition, it applies the QoS-enabled path by using the constrained based routing.

7.3.2 MPLS-based Mobile IPv4 Route Optimization Scenario

In this scenario, the data forwarding paths from the Ingress LER to Egress LER should be re-calculated after the discovery procedure. If the routing path is significantly longer than the optimal path during the time of handover, the routing optimization procedure takes place. The route optimization is applied only inside the MPLS network, in which the tunneling end points are the Ingress LER and the Egress LER/FA. The label forwarding entries including label information base (LIB) will be updated both at the Ingress LER and the Egress LER after executing route optimization. There is no need to update the binding cache of correspondent node. The forwarding path from Ingress LER should be cut through the Egress LER/FA, which can solve the problem of the triangle routing. The Ingress LER should find the forwarding path with relevant query process to find the destination tunnel endpoints, that is, the destination LER/FA. The incoming packets at Ingress LER try to find their label table. When the label forwarding entries are matched, packets are sent to the Egress LER by using the explicated routed path. If no entry is found, packets are sent to the home agent by using hop-by-hop routed path.

Figure 3/Y.MIPoMPLS shows the MPLS-based Mobile IPv4 Route Optimization Scenario.

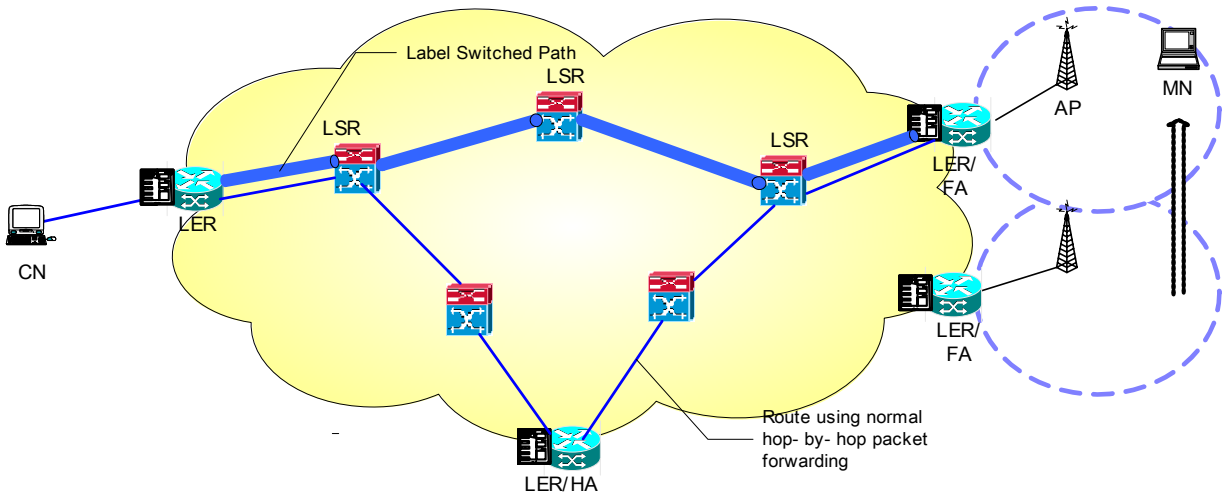


FIGURE 3/Y.MIPoMPLS

MPLS-based Mobile IPv4 Route Optimization Scenario

7.3.3 MPLS-based Mobile IPv6 Binding Update Scenario

In this scenario, the direct forwarding paths from the Ingress LER to Egress LER should be built after binding an update procedure of IPv6, which is similar to routing optimization scenario of mobile IPv4. The difference with mobile IPv4 is, first, that the binding update procedure of mobile IPv6 is a fundamental part of the protocol operation where the route optimization in mobile IPv4 is an optional set of extensions. In mobile IPv6, the registration procedure and the route optimization procedure are performed by a single protocol entity. Second, there is no LER/FA in IPv6 since the mobile IPv6 nodes only use the co-located care-of address. Instead, the LER perform ingress filtering [26]. A mobile IPv6 node uses its care-of address as the source address in the IP header of packets it sends, allowing the packets to pass normally through ingress filtering routers. The use of the care-of address as the source address in each IPv6 header simplifies routing in order to establish label switched paths to a mobile node.

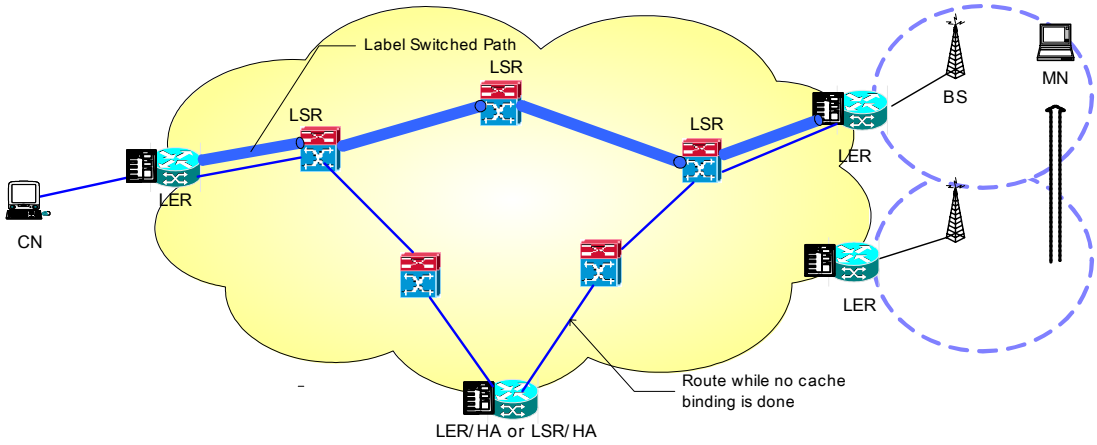


FIGURE 4/Y.MIPoMPLS

MPLS-based Mobile IPv6 Binding Update Scenario

7.3.4 MPLS-based Hierarchical Mobile IP Tunneling Scenario

In this scenario, it considers mobile IPv4 or mobile IPv6 services over the hierarchical MPLS network. It assumes that there are a number of foreign agents such as Gateway foreign Agent (GFA) and the regional foreign agent (RFA) in a hierarchical manner, which can be located at the LER or LSR. Such foreign agents support regional registration with security associations. It notes that whenever the mobile node migrates to an adjacent subnet, location of the mobile node should be updated at the home agent. The label switched paths from the home agent are set up or extended to new foreign agent.
Depending on network topology and dimension, handover latency including registration may be significant. The hierarchical mobile IPv4 tunneling scenario allows a mobile node to perform registration locally in order to reduce a number of registration messages to the home agent. This reduces signaling delay when a mobile node moves to the new foreign agent, and therefore, improves performance during a time of handover.
The hierarchical mobile IP tunneling scenario over MPLS is shown in Figure 5/Y.MIPoMPLS.

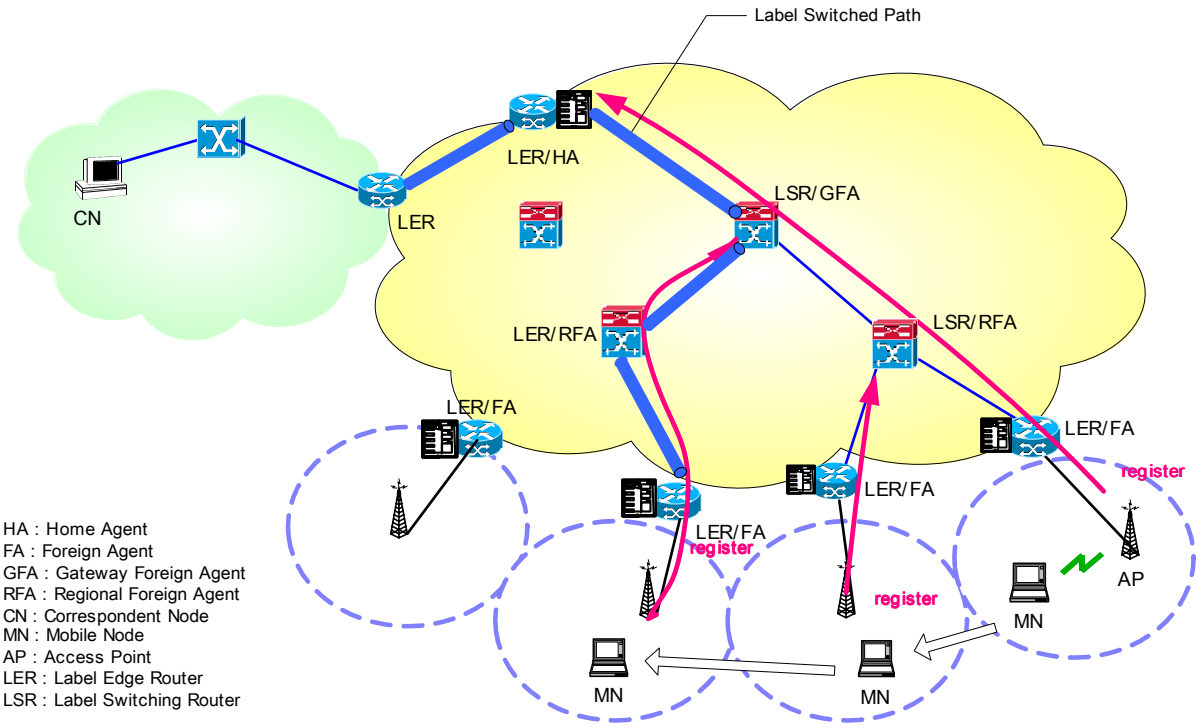


FIGURE 5/Y.MIPoMPLS

MPLS-based Hierarchical Mobile IP Tunneling Scenario

In this network architecture, the MPLS based mobility agents are distributed to allow frequent and seamless location management operations while maintaining ongoing sessions and maximizing data throughout. In this architecture, the foreign agents handle local movements of mobile nodes within the domain.

8. Application Procedures for Mobility Support

8.1 General Assumptions

The main issues of MPLS network architecture with mobility support are focused on the control procedures such as registration, LSP establishment and LSP Extension for handover, etc. It requires

LSP tunnels to send a stream of mobile IP packets over the MPLS network. The existing LDP specification is well described to establish LSP tunnels for mobility. The address of a home agent and a foreign agent for LSP tunnels will be given by the registration and agent discovery Procedure within the mobile IP protocol.

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 a desired level. The label switched paths between Ingress LER and Egress LERs are set up with signaling of CR-LDP or RSVP-TE. There is no additional message or TLV/Object on existing CR-LDP or RSVP-TE to setup QoS guaranteed LSP.

It requires LSP tunnels to send a stream of mobile IP packets through the MPLS network. The existing LDP specification is well described to establish LSP tunnels for mobility. The address of home agent and foreign agent for LSP tunnels will be given by the registration and agent discovery Procedure within the Mobile IP protocol.

While traditional traffic engineered MPLS are unidirectional, generalized MPLS supports the establishment of bi-directional LSP. Depending on applications, bi-directional LSP have the benefit of lower setup latency and lower number of messages required during setup. It takes only one initiator-eliminator round trip time. It is possible to be expended to the optical network.

8.2 LSP Tunneling Procedures

This tunneling procedure applies to the tunneling scenario described above.

8.2.1 MPLS-based Mobile IPv4 Tunneling Procedures

Figure 6/Y.MIPoMPLS shows LSP tunneling procedures for mobile IPv4 service over MPLS. There can be LSP tunnels in this scenario;

- LSP tunnels between the Ingress LER and home agent
- LSP tunnels between home agent and the Egress LER/FA

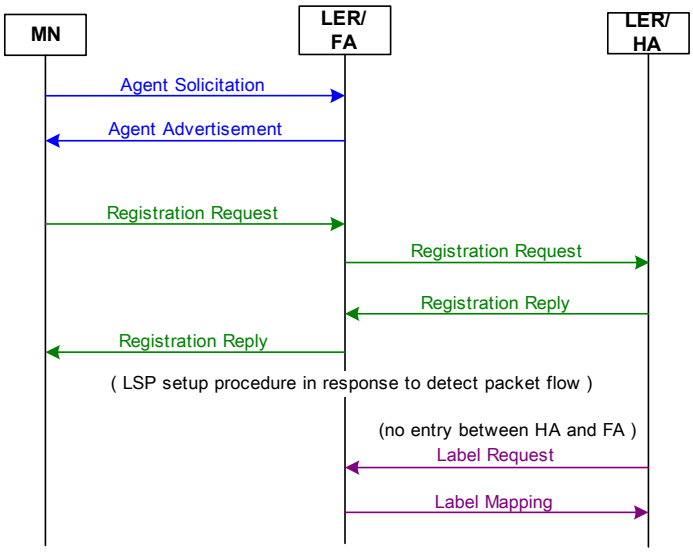


FIGURE 6/Y.MIPoMPLS

LSP tunneling procedures for mobile IPv4 service over MPLS.

In this scenario, mobile node determines whether it is at home or in a foreign location when it receives an agent advertisement broadcasted by mobility agents. If the mobile node determines that it is in a foreign location, the mobile node acquires a temporary care-of address from the foreign agent. Since the foreign agent is in an edge LER, it will analyze the incoming Registration Request Message and updates its routing table with the value of the mobile node home address. Based on the routing table, foreign agent forwards the Registration Request Message toward the home agent.

The registration request is forwarded to the home agent using hop-by-hop routing. When the home agent gets the registration request and learns of the care-of address of the mobile node, it sends a registration reply to the mobile node via foreign agent. In the home agent, if there are long lived message streams between the correspondent node and the mobile node, then the home agent will send a Label Request/Path Message to the foreign agent with the care-of address of the mobile node. A foreign agent replies with Label Mapping/Resv Message to the home agent. When the Label Mapping/Resv Message arrives at the home agent, the LSP would have been established. In this way, the home agent can relay the packets destined to mobile node home address to its current location in the foreign network.

When a foreign agent receives packets on the LSP, it records the incoming port number, label value and IP address of the correspondent node of the packet. Therefore, the foreign agent should send user packets through the established bi-directional LSP from the mobile node to the correspondent node because it should know that for which mobile node the LSP is established.

Packets from a correspondent node to the mobile node are addressed to the mobile node home address. If the mobile node is located in a foreign network, packets are intercepted by the home agent. The home agent uses the incoming label value as an index to look up its label table. It inserts the label value in the label table into the packet and sends it out through the port indicated in the table. If a mobile node is still in the home network, then the outgoing port entries are empty. The packet will be sent to the IP layer and sent out from the port indicated in the corresponding routing table entry. If a mobile node is in foreign network and a LSP is established from the home agent to the foreign agent, then the home agent must send user packets to the foreign agent by using label swapping method.

8.2.2 MPLS-based Mobile IPv4 Route Optimization Tunneling Procedures

This scenario is used to solve the problem of the triangle routing of all the routing paths via the home agent in the mobile IPv4 protocol. The forwarding path from Ingress LER should be cut through the Egress LER/FA without a visit of the home agent. In this scenario, data forwarding paths from the Ingress LER to Egress LER should be re-calculated after the router discovery procedure. The route optimization is applied only inside the MPLS network, in which the tunneling end points are the Ingress LER and the Egress LER/FA. When a correspondent node sends packets to a mobile node located in the foreign area, the Ingress LER has to decide the relevant forwarding path depending on routing information.

There can be LSP tunnels in this scenario;

- Direct LSP tunnels between the Ingress LER and the Egress LER/FA
- LSP tunnel between old foreign agents and new foreign agents (only for LSP extension)

Figure 7/Y.MIPoMPLS shows Route optimized LSP tunneling procedure for mobile IPv4 service over MPLS.

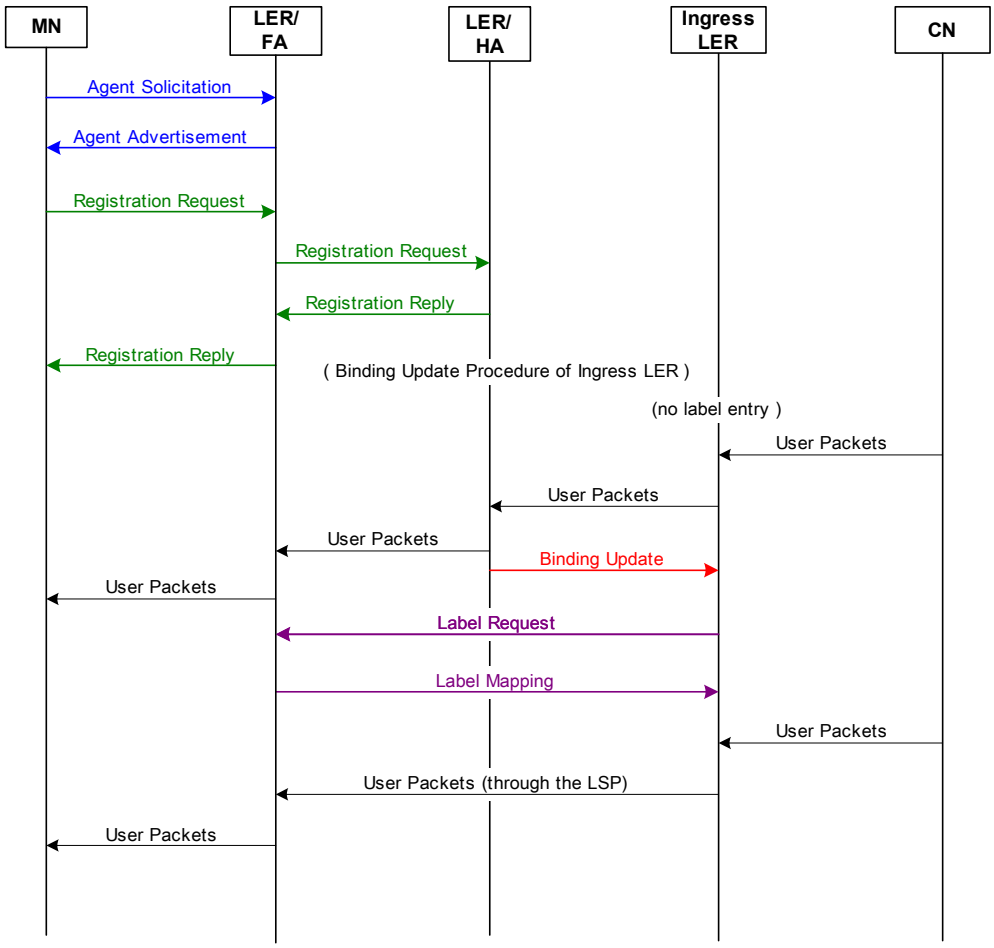


FIGURE 7/Y.MIPoMPLS

Route optimized LSP tunneling procedure for mobile IPv4 service over MPLS

When a mobile node's home agent intercepts a datagram from the home network and tunnels it to the mobile node, the home agent should then send a Binding Update Message to the Ingress LER of correspondent node, informing it of the mobile node's current mobility binding. The binding update procedure is defined in [30]. As in the case of a Binding Update sent by the mobile node's home agent, Ingress LER may maintain a binding cache to optimize mobile node's communication with mobile nodes. An Ingress LER may create or update a binding cache entry for a mobile node only when it has received and authenticated the mobile node's mobility binding. As before, each binding in the cache entry also has an associated lifetime, specified in the Binding Update Message. After the expiration of this time period, the binding is deleted from the cache.

When any foreign agent receives a tunneled datagram, if it has a binding cache entry for the destination mobile node and thus has no visitor list entry for this mobile node, the node receiving this tunneled datagram may deduce that the tunneling node has an out-of-date binding cache entry for this mobile node. In this case, the receiving node should send a Binding Warning Message to the mobile node's home agent, advising it to send a Binding Update message to the Ingress LER that tunneled this datagram.

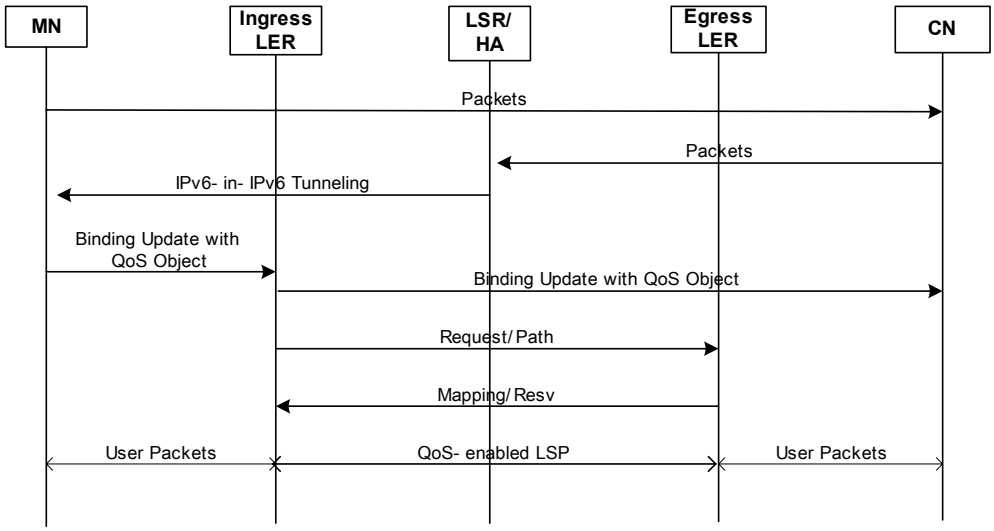
8.2.3 MPLS-based Mobile IPv6 Binding Update Tunneling Procedures

This scenario is nearly same with routing optimization procedure in IPv4 mentioned above. The only difference is that mobile IPv6 does not use "foreign agents" since the IPv6 features, like neighbor discovery and address auto-configuration, are used to identify the mobile node at the visiting location. The Binding Update procedure is applied to the IPv6 nodes to cache the binding of a mobile node's home address with its care-of address. The Ingress LER has the equivalent capabilities with ingress filtering of mobile IPv6 and build LSP’s between Ingress LER and Egress LER to transparently deliver packets to a mobile node [26].
When the mobile node sends packets to any other correspondent node, it sends packets directly to the destination. The mobile node 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.
To avoid triangle routing, a mobile node sends a Binding Update that may be together with QoS Object to a correspondent node. The LER receiving the Binding Update message should determine whether to initiate REQUEST/PATH message. Newly established QoS guaranteed LSP provides tunnel for packets to traverse. The correspondent IPv6 node receiving the Binding Update message is able to send packets to the mobile node directly.

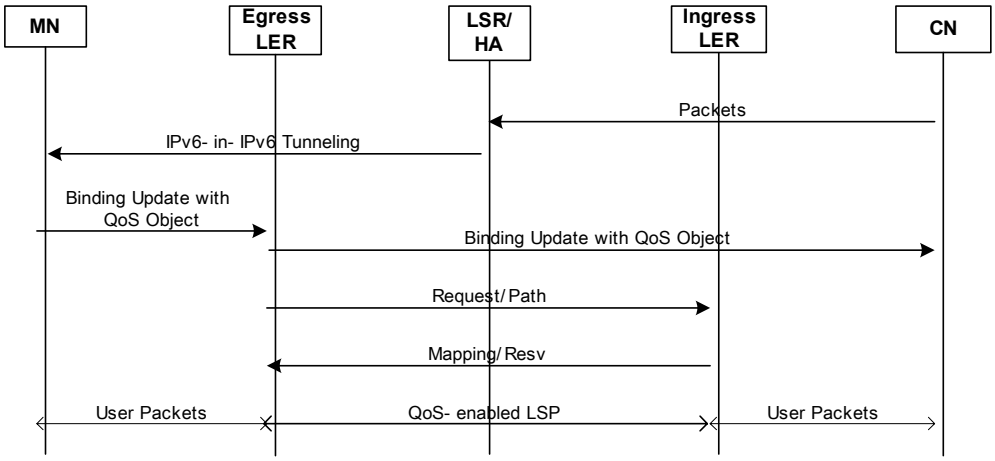
There can be LSP tunnels in this scenario;

- Direct LSP tunnels between the Ingress LER and the Egress LER

Figure 8/Y.MIPoMPLS shows LSP tunneling procedures for mobile IPv6 service over MPLS.



(a) The mobile node initiates data transmission



(b) CN initiates data transmission

FIGURE 8/Y.MIPoMPLS

LSP tunneling procedures for mobile IPv6 service over MPLS

In this scenario, it assumes that a MN has already accomplished new default router finding, address auto-configuration, and registration as Mobile IPv6 procedures. Before a corresponding node sends any packet to the mobile node, the corresponding node should examine its binding cache for an entry table on the destination address (that is the home address of mobile node) to which the packet is being sent. If the corresponding node has a binding cache entry for this address, it should use a routing header to route the packet to the mobile node by way of the care-of address in the binding recorded in that binding cache entry. If a corresponding node has no binding cache entry for the mobile node, the packet sent by the corresponding node will be intercepted by the mobile node's HA and tunneled (using IPv6-in-IPv6 encapsulation) to the mobile node's current care-of address.

8.2.4 MPLS-based Hierarchical Mobile IP Tunneling Procedures

This scenario considers LSP tunneling procedures of mobile IPv4 or mobile IPv6 services over hierarchical MPLS, in which there are a number of foreign agents such as Gateway foreign Agent (GFA) and the regional foreign agent (RFA) in a hierarchical manner. The address of GFA and RFA for LSP tunnels will be given by the registration procedure to home agent.

In this scenario, there can be LSP tunnels;

- LSP tunnels between the Ingress LER and home agent
- LSP tunnels between home agent and GFA
- LSP tunnels between GFA and RFA
- LSP tunnels between RFA and the Egress LER/FA

The address of GFA, RFA and the Egress LER/FA for LSP tunnels will be given by the Registration Procedure within the Mobile IP Regional Registration.

A foreign agent advertises addresses of a hierarchical foreign agent in order, between its own address (first) and the GFA address (last) in the Agent Advertisement. If the mobile node determines that it is in a foreign location, the mobile node sends a Registration Request. When the LER/FA closest to the mobile node receives the Registration, it will analyze the incoming Registration Request message and then relays the Registration Request to the next LSR/RFA or LER/RFA in the hierarchy toward the LSR/GFA. If the next LSR/RFA receives the Registration Request, it maintains a visitor list entry and inserts its own address to the registration packet. This procedure is repeated to the LSR/GFA. When the LSR/GFA receives the Registration Request, it cashes information about the next lower-level LSR/RFA in the hierarchy. It then relays the Registration Request to the home agent. For each pending or current registration, the LSR/GFA maintains a visitor list entry. The request message is forwarded to the home agent hop-by-hop using normal IP routing.

When a home agent gets the Registration Request message and learns the care-of address of GFA within the packet, the home agent sends a Registration Reply to the GFA. When GFA receives the Registration Reply message, GFA can recognize that the Registration Reply is coming from the specific mobile node that is registered. GFA can know the lower-level RFA of a registered mobile node by reading the information of the mobile node entry corresponding to a received Registration Reply packet. And then GFA sends a Registration Reply to the RFA. This procedure is repeated in every FA in the hierarchy, until the Registration Reply message reaches the FA closest to the mobile node. When the lowest-level FA receives Registration Reply, it checks its cached information and relays the Registration Reply to the mobile node.
Figure 9/Y.MIPoMPLS shows LSP tunneling procedures of mobile IP service over hierarchical MPLS.

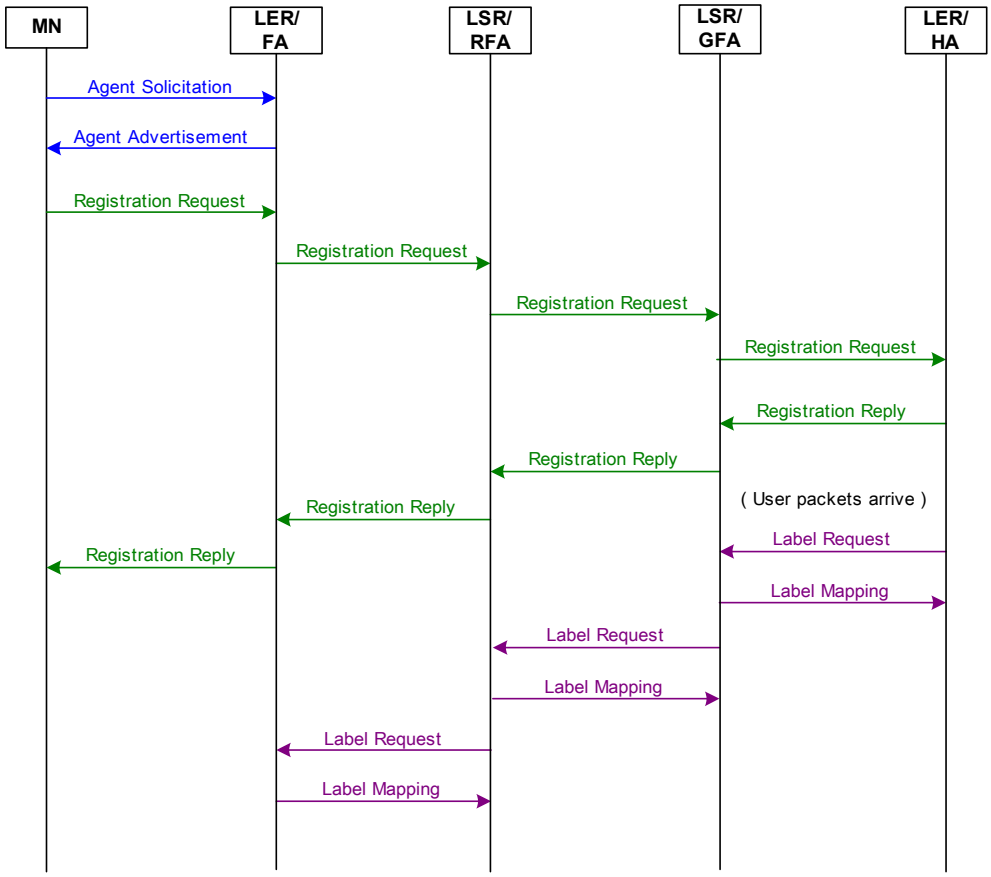


FIGURE 9/Y.MIPoMPLS

LSP tunneling procedures of mobile IP service over hierarchical MPLS.

When a home agent gets user packets to the mobile node, it will send a Label Request/Path Message to GFA with the care-of address of the mobile node. GFA replies with a label mapping/Resv message to the home agent. GFA should assign labels and keep the home address of a mobile node and binding table of a specific label about being registered mobile nodes. When this Label Mapping/Resv Message arrives at the home agent, the LSP would have been established. Figure 9/Y.MIPoMPLS shows the registration and LSP establishment procedure. After that, a home agent changes its label information table that contains the home address and the care-of address of the mobile node. It sets the empty out label and outgoing port entries to the values of out label and outgoing port. In this way, a home agent can relay the packets destined to mobile node home address to its GFA in the foreign network. Finally, a home agent sends user packets to GFA along the LSP from a home agent to GFA.

When GFA receives the labelled user packets, GFA can recognize what the Registration Reply is coming from the specific mobile node that is registered after the operation of a label pop. GFA writes the label value attached to user packets on an incoming value of corresponding mobile node. GFA can know the lower-level RFA of a registered mobile node by reading the information of the mobile node entry corresponding to a received user packets. LSR/GFA will send a label request/Path message to next LSR/RFA with the care-of address of the mobile node. LSR/RFA replies with a Label Mapping/Resv Message to the home agent. LSR/RFA should keep the information of a binding table and the Home address by assigning a Label about the registered whole mobile nodes. When this Label Mapping/Resv Message arrives at LSR/GFA, the LSP would have been established.

After that, LSR/GFA changes its label information table which contains the home address and the care-of address of a mobile node. It sets the empty out label and outgoing port entries to the values of out label and outgoing port. In this way, LSR/GFA can relay the packets destined to a mobile node home address from the home agent to LSR/RFA. Finally, LSR/GFA sends user packets to LSR/RFA through the LSP. This procedure is repeated in every LER/FA in the hierarchy, until the user packets reach the LER/FA closest to the mobile node. When the lowest-level LER/FA receives user packets, it should remove its labels and check its cached information and relay the user packets to the mobile node.

8.3 Agent Discovery

The agent discovery procedure includes both agent discovery and agent solicitation. The same agent advertisement and solicitation procedures with mobile IP are used at the MPLS network since mobile agents are located at the MPLS node. Mobile agents (i.e., foreign agents and home agents) advertise their presence via Agent Advertisement messages. A mobile node may optionally solicit an Agent Advertisement message from any locally attached mobility agents through an Agent Solicitation message. A mobile node receives these Agent Advertisements and determines whether it is on its home or a foreign location.

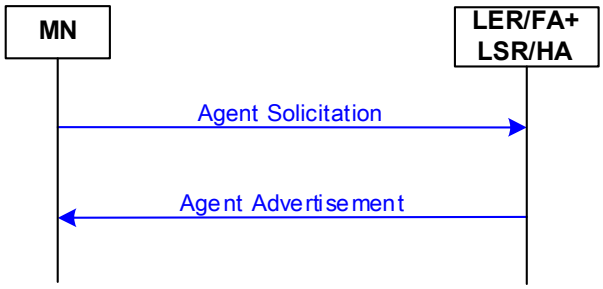


FIGURE 10/Y.MIPoMPLS

Agent discovery of mobile node over the MPLS Network

If sent periodically, the nominal interval at which Agent Advertisements are sent should be 1/3 of the advertisement Lifetime given in the MPLS shim header. This allows a mobile node to miss three successive advertisements before deleting the agent from its list of valid agents.

8.4 LSP Re-Routing Procedures during Handover

When the mobile node moves from one foreign location to another, the registration procedure is repeated once between a home agent and a new foreign agent. The existing LSP should be changed to the new foreign agent. The following issues can be considered on the MPLS network.

- LSP extension
- LSP optimization

There are two goals in terms of handover; the first, to reduce the latency or interruption due to handover; and second, to reduce signalling overhead. In case of IPv6, use of more than one care-of address by a mobile node may be useful to improve smooth handover when the mobile node moves

from one wireless link to another. The LSP in the MPLS protocol can support smooth handover capability and gives solution to QoS-enabled path for the MN's care-of-address.

However, it can 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 the LSP setup procedure is that only active channels are supposed to traverse over QoS guaranteed LSP. This will prevent LSP abusing that which 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 an efficient scheme to save bandwidth on network and to reduce end-to-end delay.

8.4.1 LSP Extension

When the mobile node is moving to other foreign location, IP packets intercepted by the home agent are tunneled to the mobile node's new foreign agent (that is the new Egress LER), but packets in flight that had already been intercepted by the home agent and tunneled to the old foreign agent (that is the old Egress LER) are likely to be lost. Route optimization provides a means for the mobile node's previous foreign agent to be reliably notified with the mobile node's new binding update information, allowing packets in flight to the mobile node's previous foreign agent to be forwarded to its new foreign agent.

When an old foreign agent receives a Binding Update Message from the new foreign agent to notify the mobile node's new location, it looks up its forwarding information base (FIB) to find a label of the mobile node. If the forwarding information base has a label of that mobile node, then the old foreign agent set up label switches path to the new foreign agent. Therefore, the existing label switches path from an Ingress LER to an old foreign agent to be extended to the new the foreign agent.

After signaling is exchanged between an old foreign agent and a new foreign agent, the current LSP can be extended by establishing a LSP between current foreign agent and a new foreign agent. During that time, the old foreign agent can buffer all the packets from and to the mobile node. Once the LSP is established, packets are sent along the new path to the mobile node. Any packets for the mobile node that arrive at its previous foreign agent can then be re-tunneled to the mobile node's new foreign agent through the extended LSP. If there isn't any label to the destination mobile node at the old foreign agent, packets received from the correspondent node should be sent to the new foreign agent by using hop-by-hop routing.

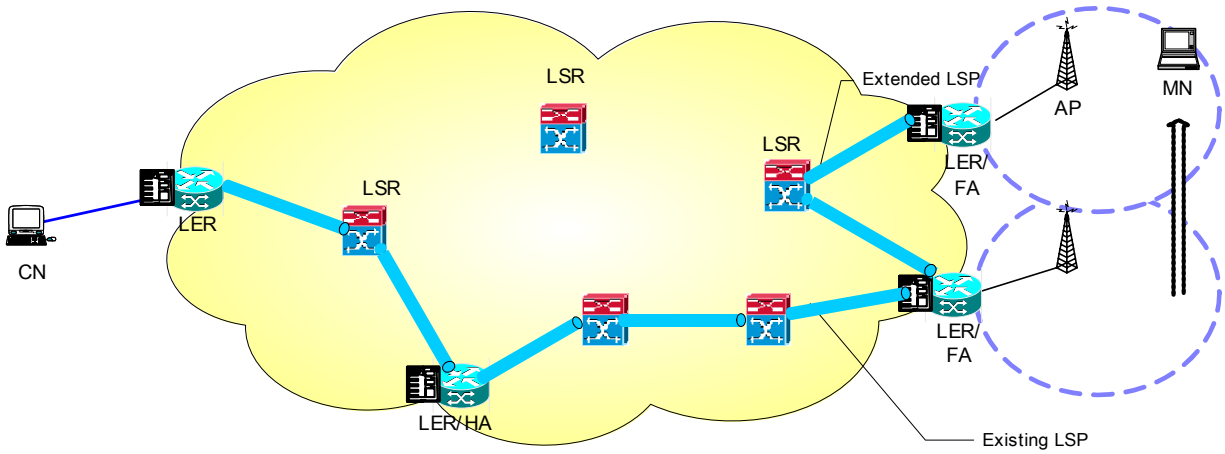


FIGURE 11/Y.MIPoMPLS

LSP Extension for mobile IP service for a time of handover

Whenever a mobile node migrates to an adjacent subnet, existing LSP from the Ingress LER to the old foreign agent is extended to the new foreign agent. When the Ingress LER receives a Binding Update Message in response to a Binding Warning Message or Binding Request Message, the Ingress LER should recognize that a destination mobile node migrates the new foreign agent. However, whenever a destination mobile node migrates, the Ingress LER shouldn't set up a new LSP to the new foreign agent.

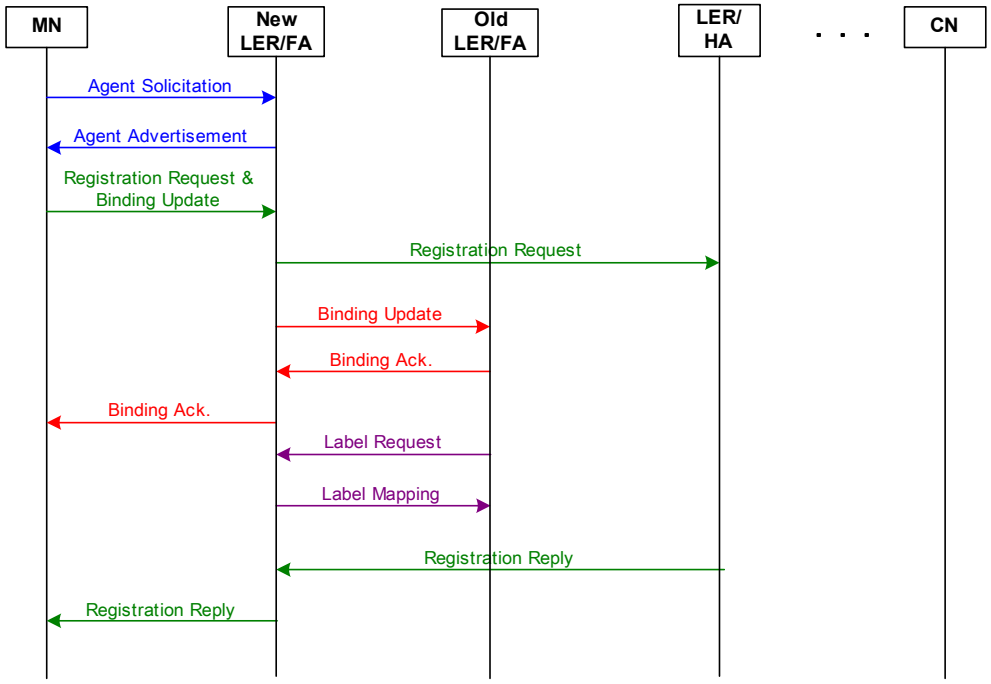


FIGURE 12/Y.MIPoMPLS

Message sequence chart for LSP extension

The LSP extension procedures in Figure 12/Y.MIPoMPLS are as follows.

- A mobile node moves to a new foreign agent and sends a Registration Request and Binding Update message to new foreign agent.
- New foreign agent sends a Registration Request message to the home agent and sends a Binding Update Message to the old foreign agent.
- When the old foreign agent receives the Binding Update Message, it responds with a Binding Acknowledgement Message to the mobile node via the new foreign agent. The old foreign agent may send a Label Request Message to the new foreign agent
- A LSP is established between the old foreign agent and the new foreign agent when the old foreign agent receives a Label Mapping/Resv message.
- Then, a home agent sends a Registration Reply message in response to the Registration Request.

8.4.2 LSP Optimization

When the QoS of LSP tunnel is temporarily degraded, LSP re-establishment is triggered by the Ingress or Egress LERs. After LSP re-establishment, the route between the Ingress LER and new foreign agent can be optimized. Old LSP is torn down and a new path is set up. If performance degradations are detected, the LSP re-establishment message is initiated by the Ingress or Egress LERs. The detail measurement and judgment scheme of performance degradation are for further study.
Use of more than one care-of address by a mobile node may be useful to improve smooth handover when the mobile node moves from on wireless link to another. If each mobile node is connected to the Internet through a separate wireless link, the mobile node may be able to remain connected to both links while in the area of overlap. In this case, the mobile node could acquire a new care-of address on the new link before moving out of transmission range and disconnecting from the old link. The mobile node may thus accept packets at its old care-of address while it works to update its home agent and cache of the CN's LER, notifying them of its new CoA on the new link.

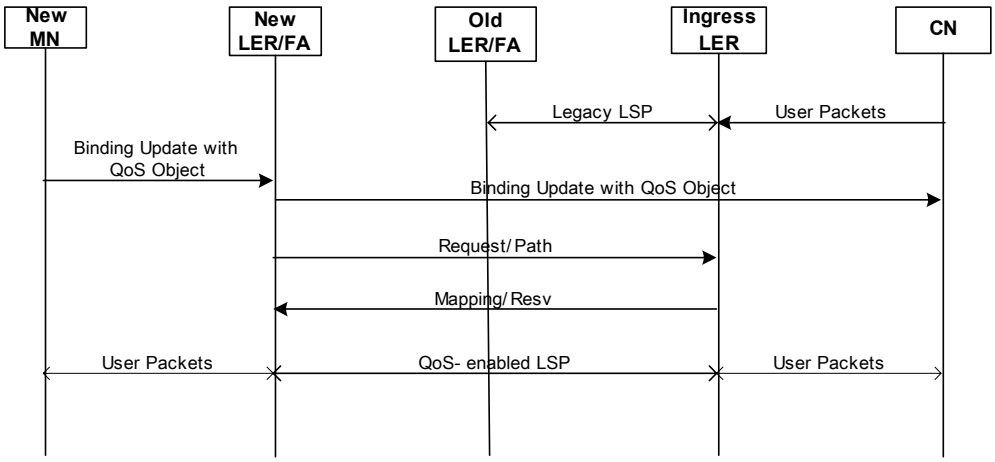


FIGURE 13/Y.MIPoMPLS
LSP optimization procedure

When a mobile node acquires a new CoA while communicating with the corresponding node over legacy LSP, the mobile node sends a Binding Update message along with QoS object to the

corresponding node for route optimization. The mobile node's LER receiving the Binding Update message will initiate Request and Path Messages. Now the correspondent IPv6 node receiving the Binding Update message is able to send packets to mobile node directly while previous flows have been traversed over the legacy LSP, which supports smooth handover 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 is transmitted over the LSP.

8.4.3 LSP Optimization for Hierarchical MPLS

In a Mobile IPv4 Regional Registration, when a handover occurs, mobile node compares the new vector of care-of address with the old one. It chooses the lowest-level foreign agent that appears in both vectors, and sends a Regional Registration Request to the anchor foreign agent which may be LSR/RFA or LSR/GFA. Any higher-level agent need not be informed of this movement since the other end of its forwarding LSP tunnel still points to the current location of the mobile node.

A Registration Request is forwarded to the LSR/GFA by way of one or more intermediate LSR/RFA. When the Registration Request message arrives at the first LER/FA, the foreign agent checks its visitor list to see if this mobile node is already registered with it. If it is not, the foreign agent checks which next higher-level LSR/RFA to relay the Registration Request. The next LER/RFA or LSR/RFA checks its visitor list to see if the mobile node is already registered with it. If it is not, the LSR/RFA relays the message to the next higher-level LSR/RFA in the hierarchy toward the LSR/GFA. This process is repeated in each LSR/RFA in the hierarchy, until an LSR/RFA recognizes the mobile node. If the mobile node is registered with the relevant LSR/RFA, it will transmit the Registration Reply toward the lower-level LSR/RFA. If the mobile node is already registered with this LSR/RFA, it will transmit the Registration Reply toward the lower-level LSR/RFA. When the lower-level RFA receives the Registration Reply, the LSR/RFA is able to point out the received Registration Reply so that the packet is associated with which mobile node. The LSR/RFA reads the information about mobile node entry equivalent to received Registration Reply, and recognizes the mobile node as the registered lower-level one. LSR/RFA will send Registration Reply message to the lower LSR/RFA. Above sequence is repeated up to the new FA of network that mobile node is moved to.

If there is an established LSP about the mobile node to the anchor LSR/RFA, it will send a Label Request/Path Message to the next lower-level LSR/RFA in the hierarchy. The lower-level LSR/RFA replies with a Label Mapping/Resv Message to the upper-level. The foreign agents should keep the binding table information of a label and home address of a mobile node about registered whole mobile nodes by assigning label. On the whole, for mobile nodes registered to foreign agent, it is necessary to assign a label, and to maintain the binding table of home address and label of mobile node. When a Label Mapping/Resv Message from lower-level LSR/RFA arrives at upper-level LSR/RFA, the LSP would have been established. After LSR/RFA receives the label from the lower-level one, it is necessary to modify the label mapping/Resv entry on the associated mobile node in the label table. The incoming label value of label mapping/Resv entry is unchanged as the received label value form the upper-level LSR/RFA, and outgoing label value is changed into a new acquired label value from the new lower-level LSR/RFA through the Regional Registration method. And then, LSR/RFA will send a Label Request/Path Message to next LSR/RFA with the care-of address of the mobile node. When this Label Mapping/Resv Message arrives at LSR/RFA, the LSP would have been established.

Above sequence is repeated up to the new foreign agent of network that mobile node is moved to. In this way, the LSP is newly established from anchor foreign agent to new foreign agent. In this

LSP partial re-establishment method, since the LSP is maintained from home agent to anchor foreign agent and a new LSP is established from anchor foreign agent to new foreign agent, the LSP setup time can be reduced.

Packet is delivered from the home agent to a new foreign agent along the LSP by label swapping. A new foreign agent receives the packet and looks up its label table. Since it is the egress point of the LSP from the home agent to a new foreign agent, new foreign agent strips off the label shim header and sends the packet to the IP layer. Finally, a new foreign agent as a border gateway router within the corresponding local domain forwards the packet to mobile node based on the newly added routing table. A mobile node receives the packet sent by the correspondent node.

Figure 14/Y.MIPoMPLS shows an example of Regional Registration and LSP optimization process for mobile IP service over hierarchical MPLS when the mobile node moves to new LER/FA.

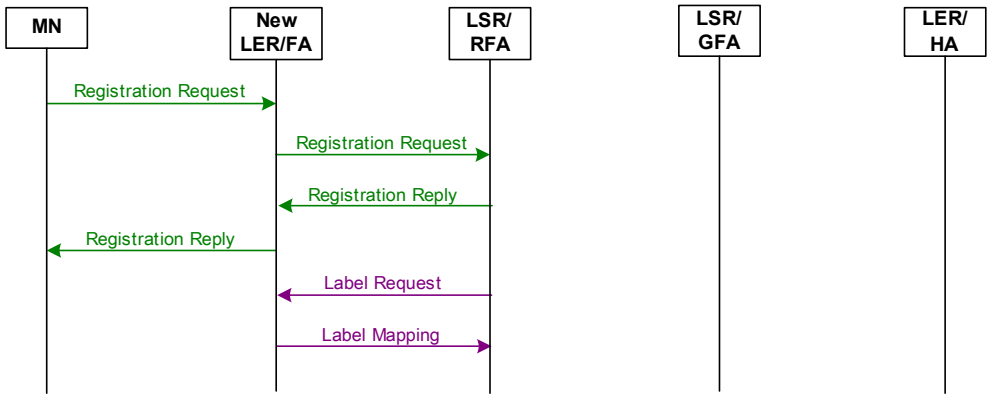


FIGURE 14/Y.MIPoMPLS

LSP optimization procedure at mobile IP over hierarchical MPLS during handover

In the MPLS-based Hierarchical Mobile IPv4 network, additionally, it is necessary to clear the registration information on the old foreign agent and the upper-level LSR/RFA, and to release the LSP. If old locations are not deregistered, it is possible that tunnels are not correctly redirected when a mobile node moves back to a previous foreign agent.

The anchor LSR/RFA should send a Binding Update with a zero lifetime and Label Release Message to the previous care-of address it had registered for the mobile node. Each foreign agent receiving the Binding Update removes the mobile node from its visitor lists. And the LSP that is assigned between upper-level foreign agents is released. The Binding Update and Label Release Message are relayed down to the new foreign agent and old foreign agent, respectively. Old foreign agents in the hierarchy receiving this notification remove the mobile node from its visitor list. A LSP that is established to an old foreign agent is released by the receiving Label Release Messages.

8.4.4 Other Considerations

- **Consideration of idle mobile nodes**

  It notes that most wireless 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. The mobile nodes will be in an idle state but passively connected to the network. Thus LSP tunnel procedure is done only by active conditions of high layer applications that are supposed to traverse over QoS guaranteed LSP. This will prevent LSP abusing that which can be caused by lots of control packets.

- **QoS service interruption**

  At the time of handover, interruption in QoS would occur if the packets sent by or destined to the mobile node arrive at the intermediate node without the information about their QoS forwarding requirement. Such QoS interruption must be minimized.

  We consider two schemes, which should minimize the interruption in QoS. One is the scheme using multicast LSP. In this method, an anchor LSP establishes a LSP to the current LER/FA and all LER/FAs in the neighborhoods of the serving LER/FA. When data arrives for that mobile node, the anchor LSR multicast the data to all the MN's multicast group. If the mobile node moves to one of the neighboring location, data is immediately available.

  The other is the method using bi-directional LSP tunnel between the FA/LER. In this scheme, LER/FA will establish bidirectional LSP to the neighbor LER/FA in advance. If the mobile node moves to the neighbor subnet, packets to the MN can be sent via bidirectional LSP tunnel between the LER/FA.

9. QoS Aspects

In an MPLS network, a Label Switched Path (LSP) can be established using relevant signaling protocols when a stream of real-time data traverses a common path. At the ingress Label Switch Router (LSR), each packet is assigned a label and is transmitted downstream. At each LSR along the LSP, the label is used to forward the packet to the next hop which can best match the differentiated service (Diff-Serv) and traffic engineering conditions in the mobile network environment.

In a Diff-Serv domain, all the packets are classified and marked with a Diff-Serv Code Point (DSCP). At each LSR, the DSCP is used to select the Per Hop Behavior. The MPLS shim header at LSPs can transport the information of the PHB [25]. For the LSP with bandwidth reservation, a LSR performs admission control of the signaled LSP over the Diff-Serv resources provisioned (e.g., via configuration, SNMP or policy protocols). It also performs adjustment to the Diff-Serv resources associated with the relevant class of services.

In Y.1540 [6] and Y.1541 [7], it defines classes of network Quality of Service (QoS), and specifies provisional objectives for Internet Protocol network performance parameters. These classes are intended to be the basis for agreements among network providers, and between end users and their network providers. The QoS and performance objective for the MPLS network are not defined yet. The detail QoS mappings between IP QoS and MPLS QoS are out of scope at this document.

10. Management Aspects

The following management aspects should be considered;

- information of registration of home address and care-of-address
- consistency and verification of registration information at LER/HA, LER/FA, and LSR/HA
- Information to add, remove or change LSPs

- Performance information and statistics of LSP including handover situation
- Information of service interrupt during handover
- Information of service class and QoS parameters
- Information of fault, configuration, accounting, and security, etc.

11. Security Aspects

The security concerns described in this section are only focused on the MPLS network ones. The network-level security is applied to access filtering, especially for authentication. Other security aspects such as application-specific or mobile IP protocol-specific are out of scope in this Recommendation.
In a mobile environment, mobile nodes may be connected to the network via wireless links. The LSPs using such links are particularly vulnerable to attacks. Home agents must be able to perform mobile node authentication. The relevant authentication procedures can be supported in mobile IPv4 and mobile IPv6 protocols [9], [30].
Mobile nodes, home agents, foreign agents and corresponding nodes can operate securely with relevant security associations between themselves. The detailed procedures for security association are out of scope in this Recommendation.
In the MPLS network, LSPs should be maintained with some security procedures especially during handover time (LSP extension/optimization). The Figure 15/Y.MIPoMPLS shows an example of security associations among mobile node, FA, HA, and corresponding node during handover with LSP extension, at which three additional security associations are required [The re-routed label switched tunnel can be securely associated both in the LSP extension and the LSP optimization scenarios]. These security associations are sometimes combined with the IPsec protocol between the corresponding node and the mobile node, and the IPv6 Binding Authorization Data option in IPv6 scenarios. The security associations would be also useful for MPLS signaling (e.g., LDP/CR-LDP or RSVP-TE).

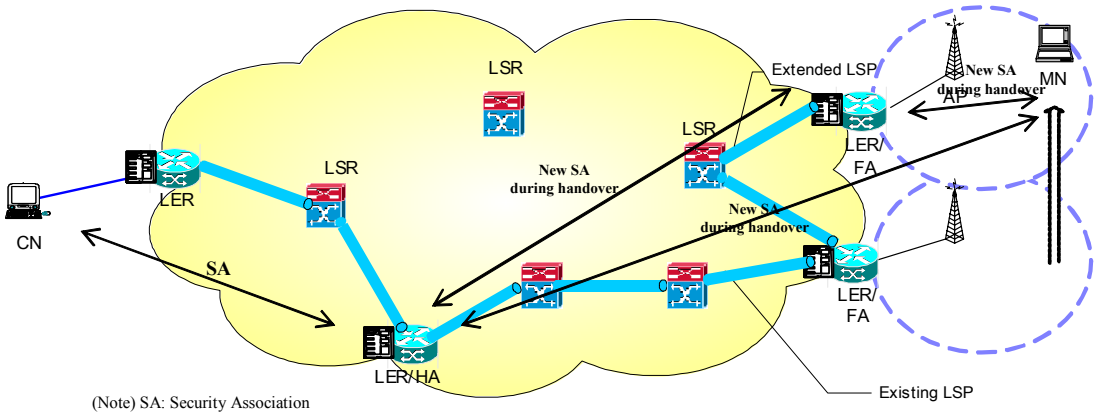


FIGURE 15/Y.MIPoMPLS
An example of security associations for mobile IP service over MPLS during handover with LSP extension

The virtual private network (VPN) constructs can be also applied to mobile IP services over MPLS. VPN and traffic engineering capabilities available within an MPLS environment could enable IPv6 and IPv4 mobile IP services over the same MPLS infrastructure [The level of security of MPLS-based VPNs is equivalent to traditional L2 circuit-based VPNs].

12. Routing Aspects

The routing on the MPLS network is depending on locations of the home agent and the foreign agent as well as the locations of LERs and LSRs.

In the MPLS network, each flow may be different in grades of service according to flow classification. The routing path on each LSP may be calculated according to Forwarding Equivalence Class. A LSP should meet certain QoS requirements of differential flows. The detail routing algorithms of the MPLS network with mobility support are further study.

Depending on routing action, the packets deliver to the destination mobile node via the hop-by-hop routed path or explicitly routed path.

13. Scalability Aspects

Generally, the level of scalability of mobile IP services over MPLS is directly dependent from the scalability of the MPLS network itself. The coverage of a single LER [with HA and/or FA] may depend on the coverage of single or multiple mobile IP areas.

14. Migration Aspects for Mobile IPv4 over MPLS to Mobile IPv6 over MPLS

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 essential that IPv6 integrate with this technology. We believe 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.

15. Interworking Aspects with Mobile IP Networks

The LER/FA or the LER/HA connected to the mobile IP network has a role of the border gateway router for the corresponding mobile IP domain and also has functions of a home agent and a foreign agent.

If there are a number of HAs and FAs in the mobile IP network, the IP-in-IP tunneling may be required between the mobile node and the corresponding LER[s]. If the LER/FA [HA] is the unique FA [HA] at the given mobile IP domain, there are no IP-in-IP tunnels with the mobile IP domain.

It is noted that the LSP tunneling scenarios are only applied inside the MPLS network. These scenarios do not require any modification on the existing Mobile IP protocols.

The relevant interworking procedure should be defined if the IP-in-IP tunneling is converted to the relevant LSP through the MPLS network. In addition, it is requested to support the QoS mapping and bandwidth provisioning of the specific mobile IP flows. The detailed interworking functions and procedures are out of scope in this recommendation.

APPENDIX A

Reference Architectures for Mobile IPv4, Mobile IPv6, and MPLS networks with fixed IP and mobile IP nodes

A.1 Reference Architecture of Mobile IPv4 network

It assumes that the reference architecture of mobile IPv4 network will be based on the viewpoints of public network. In this view, the customer premises network may be overlapped with the coverage of public network. The Figure A.1/Y.MIPoMPLS shows the reference architecture for mobile IPv4 network. There can be defined with UNIw, UNIx, UNIy, and UNIz for the user interface. The NNIx and NNIy can be defined as the network-node interface. For mobility support, the reference interface at NNI can be devided into functions of user-plane (U-plane), control-plane (C-plane), and management-plane (M-plane).

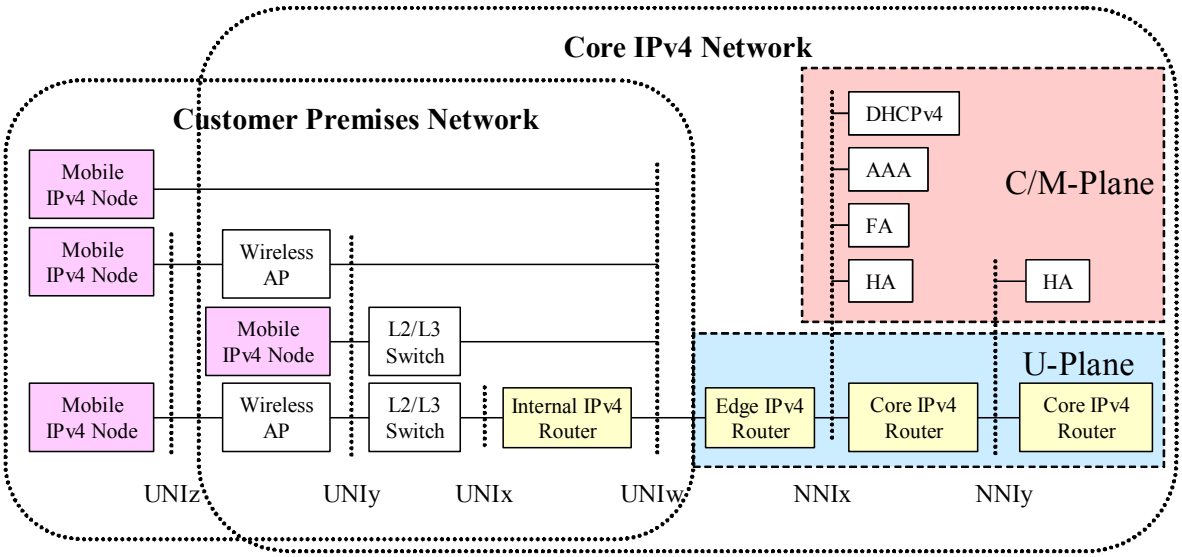


FIGURE A.1/Y.MIPoMPLS

Reference architecture of mobile IPv4 network

(Note 1) The detail interface specifications for reference points of UNIw, UNIx, UNIy, and UNIz are for further study.

(Note 2) The detail interface specifications for reference points of NNIx and NNIy are for further study.

A.2 Reference Architecture of Mobile IPv6 network

For the reference model of mobile IPv6 network, it may be compared with that of mobile IPv4 network. There is no interface for FA in the C/M-plane at the core IPv6 network. Similarly, there can be defined for the interfaces of UNI's and NNI's.

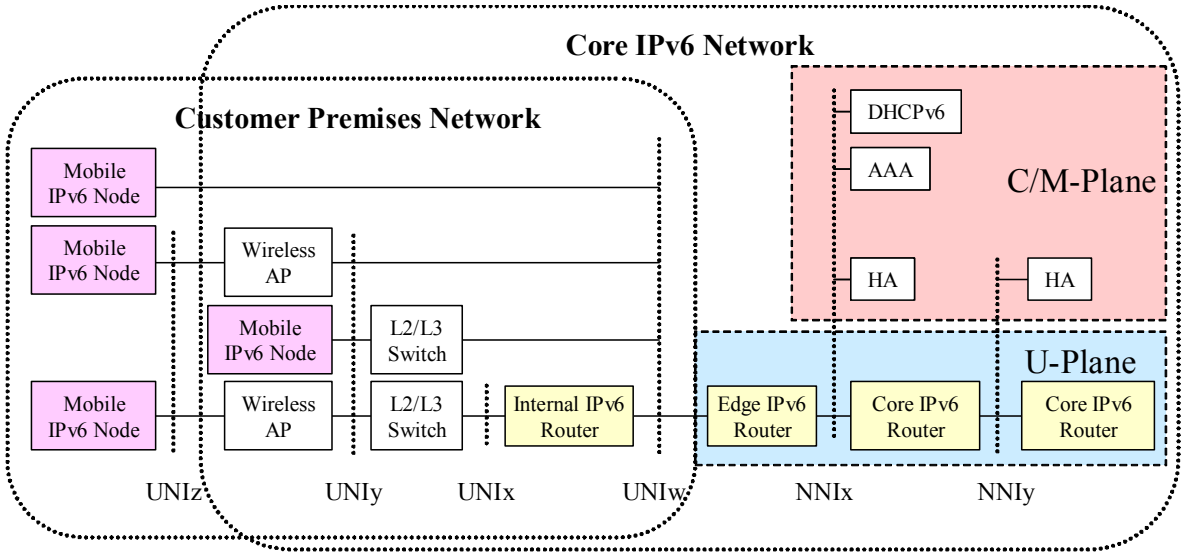


FIGURE A.2/Y.MIPoMPLS

Reference architecture of mobile IPv6 network

(Note 1) The detail interface specifications for reference points of UNIw, UNIx, UNIy, and UNIz are for further study.

(Note 2) The detail interface specifications for reference points of NNIx and NNIy are for further study.

A.3 Reference Architecture of MPLS network with fixed IP and mobile IP nodes

For mobility support, the reference model of the MPLS network can be shown with Figure A.3/Y.MIPoMPLS compared with those of mobile IPv4 and mobile IPv6 networks. Since the MPLS node has functions of layer 2 and layer 3, the MPLS network can include L2/L3 switches and routers which are overlapped with customer premises network.

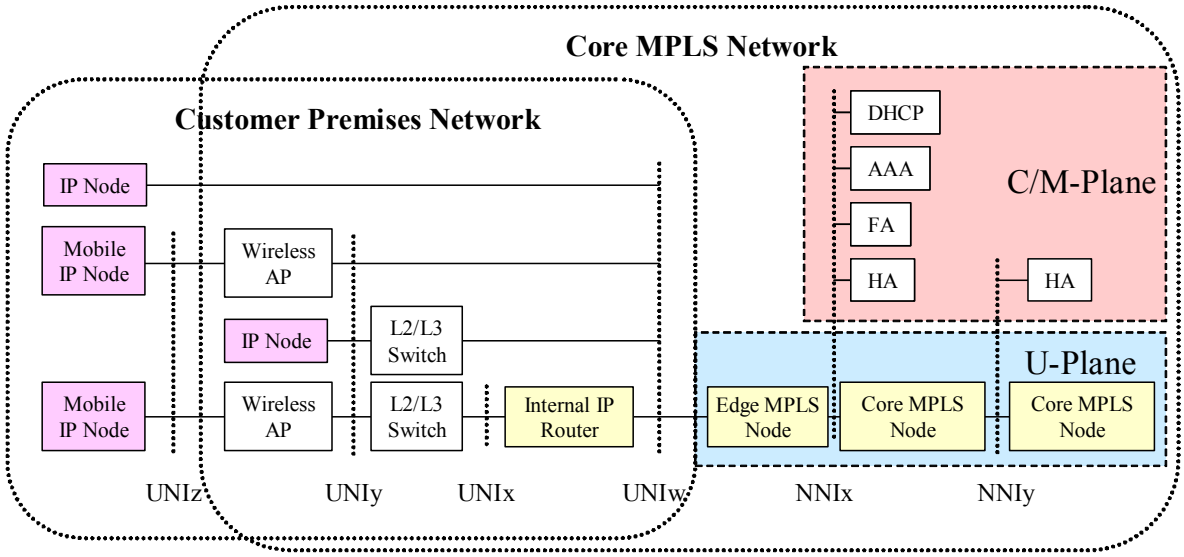


FIGURE A.3/Y.MIPoMPLS

Reference architecture of MPLS network with fixed IP and mobile IP nodes

(Note 1) The detail interface specifications for reference points of UNIw, UNIx, UNIy, and UNIz are for further study.

(Note 2) The detail interface specifications for reference points of NNIx and NNIy are for further study.

_____