INTERNATIONAL TELECOMMUNICATION UNION

ITU-T Y.1281

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(09/2003)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT GENERATION NETWORKS

Internet protocol aspects – Architecture, access, network capabilities and resource management

Mobile IP services over MPLS

ITU-T Recommendation Y.1281

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT GENERATION NETWORKS

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	**Y.1200–Y.1299**
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Numbering, naming and addressing	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899

For further details, please refer to the list of ITU-T Recommendations.

ITU-T Recommendation Y.1281

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 architecture and application procedures to provide the mobility service over the MPLS network.

Source

ITU-T Recommendation Y.1281 was approved by ITU-T Study Group 13 (2001-2004) under the ITU-T Recommendation A.8 procedure on 13 September 2003.

Keywords

CR-LDP, Home Agent (HA), Foreign Agent (FA), IP-in-IP Tunnel, Label Edge Router (LER), Label Switched Path (LSP), Label Switched Router (LSR), LDP, mobile IPv4, mobile IPv6, MPLS, Quality of Service (QoS), route optimization, RSVP-TE, Smooth Handover, Virtual Private Network (VPN).

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

Introduction

This Recommendation defines service definition and requirements to support mobile IP services through the MPLS network. It also describes the service architecture and application procedures to provide the mobility 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. This makes mobile IP 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 in order to receive packets from other nodes. In fact, a mobile node is given a long-term IP address on a home network, the "home" address. This home address is administered in the same way that 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 tunnelling to hide a mobile node's home address to 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 extracted from the tunnel and is delivered to the mobile node.

In the basic mobile IPv4 protocol, there is no direct routing from any correspondent node to any mobile node. Packets need to pass through the mobile node's home network and be forwarded by its home agent, which is called the problem of "triangle routing". To solve this problem, the route optimization capability allows direct routing from any correspondent node to any mobile node [19]. In IPv6 network, IPv6 node caches the binding of a mobile node's home address with its care-of address, and then sends any packets destined to the mobile node directly to this care-of address. To support this operation, mobile IPv6 defines an IPv6 protocol and a destination option [29]. All IPv6 nodes, whether mobile or stationary, support communications with mobile nodes.

From the network provider's point of view, future networks are designed to support network operation and maintenance by guaranteeing acceptable quality of service (QoS) levels and satisfying various service level agreements (SLAs) negotiated with customers. To support future business models, the IP network has to be upgraded to meet the demands placed by real-time and multimedia applications. It then provides various features such as fault tolerance, traffic prioritization, and QoS classes. To meet these requirements over future mobile services, first, the end-to-end performance would be manageable and predictable regardless of whether end users are moving or not. Second, for the mobile IP service, the functions of home agent and foreign agent are positioned after consideration of architectural consequences. Third, the existing and future transport technologies, including an optical one, would be able to support a future mobile world.

In the MPLS network, once a packet is classified 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. There is no need to analyze the IP 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 supporting MPLS traffic engineering. In MPLS, a label can be used to represent this explicit route, which is called a traffic engineered tunnel.

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

By combining tunnelling functions of a home agent and a foreign agent into the MPLS forwarding paradigm, the MPLS node is capable of handling the mobile IP 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 a MPLS node, the tunnelling between the home agent and the foreign agent being provided at the MPLS layer. To avoid the problem of triangle routing, the MPLS nodes can allow a direct binding, which is the same with routing optimization of IP layer, from any correspondent node to any mobile IP node by assigning a label.

As far as the support of the MPLS network is concerned, the MPLS network can provide the QoS-enabled and reliable tunnels for mobile IP service for the various sets of service requirements. The MPLS tunnelling capabilities can be implemented at the layer 2 level rather than the layer 3 mobile IP protocol level, then achieving higher service rate and lower overhead during tunnelling operation. Specifically, the MPLS network supporting the mobile IP services has the following features:

– The flow concept of MPLS network provides the connection-oriented virtual channel capability with acceptable quality of service (QoS) levels for transfer delay and loss.
– A direct cut-through tunnel between the mobile node and the correspondent node may be established while the mobile IPv4 protocol does not support it. This can save overall resource consumption and reduce the processing overhead of home agent.
– The binding cache information of the mobile IPv6 protocol can be mapped one-to-one to the MPLS label information table in each MPLS node, without requiring any complex interworking feature.
– If the home agents and/or the foreign agents can be located at the MPLS node, the L3 tunnels between the home agents and the foreign agents can be mapped into the L2 tunnels of the MPLS layer.
– The mobile agents and mobile nodes do not need any knowledge of the MPLS backbone network. This means that the mobile IPv4 and mobile IPv6 nodes do not need to modify their tunnelling procedures through the MPLS backbone network.
– The MPLS network can provide seamless end-to-end connectivity without any performance degradation during handover operations (smooth handover).

ITU-T Recommendation Y.1281

Mobile IP services over MPLS

1 Scope

The scope of this Recommendation covers:

- Service requirements and definitions for mobile IPv4 and mobile IPv6 services over MPLS;
- Service architecture to support mobile IP service over MPLS;
- LSP tunnelling scenarios to support the mobile IP services over MPLS;
- Application procedures to support the mobile IP services over MPLS.

However, this Recommendation does not cover:

- The detailed signalling protocol and packet formats for tunnel establishment;
- 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 algorithms of MPLS network with mobility support.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

2.1 Normative References

ITU-T

[1] ITU-T Recommendation Y.1310 (2000), *Transport of IP over ATM in public networks*.

[2] ITU-T Recommendation Y.1311 (2002), *Network-based VPNs – Generic architecture and service requirements*.

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

[4] ITU-T Recommendation Y.1241 (2001), *Support of IP-based services using IP transfer capabilities*.

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

[6] ITU-T Recommendation Y.1540 (2002), *Internet protocol data communication service – IP packet transfer and availability performance parameters*.

[7] ITU-T 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*, RFC 3344, August 2002.

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

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

[12] E. Rosen, et. al., *Multiprotocol Label Switching Architecture*, RFC 3031, January 2001.

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

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

[15] S. Kent and R. Atkinson, *Security Architecture for the Internet Protocol*, RFC 2401, November 1998.

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

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

[18] P. Ashwood-Smith, et. al., *Generalized MPLS Signaling – CR-LDP Extensions*, RFC 3472, January 2003.

[19] L. Berger, et. al., *Generalized MPLS Signaling – RSVP-TE Extensions*, RFC 3473, January 2003.

2.2 Informative References

[20] W. Simpson, *IP in IP Tunnelling*, RFC 1853, October 1995.

[21] S. Hanks, et. al., *Generic Routing Encapsulation (GRE)*, RFC 1701, October 1994.

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

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

[24] S. Blake, et. al., *An Architecture for Differentiated Service*, RFC 2475, December 1998.

[25] C. de Laat, et. al., *Generic AAA Architecture*, RFC 2903, August 2000.

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

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

[28] C. Perkins and Pat R. Calhoun, *AAA Registration Keys for Mobile IP*, <draft-ietf-mobileip-aaa-key-13.txt>, June 2003.

[29] David B. Johnson, et. al., *Mobility Support in IPv6*, <draft-ietf-mobileip-ipv6-22.txt>, June 2003.

[30] Thomas D. Nadeau, et. al., *Multiprotocol Label Switching (MPLS) Management Overview*, <draft-ietf-mpls-mgmt-overview-06.txt> June 2003.

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

[32] E. Gustafsson, et. al., *Mobile IPv4 Regional Registration*, <draft-ietf-mobileip-reg-tunnel-07.txt> October 2002.

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

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

3 Terms and Definitions

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

3.1 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].

3.2 anchor node: An MPLS node capable of changing the routing path when a better next hop becomes available at some LSR along the LSP during handover time of the mobile node. The anchor node provides the cross-over location from old LSP to new LSP between the correspondent node and the new mobile node's location.

3.3 binding acknowledgement: A binding acknowledgement message is used to acknowledge receipt of a binding update [29].

3.4 binding cache: A cache of mobility bindings of mobile nodes, maintained by a node for use in tunnelling packets to those mobile nodes [29].

3.5 binding update: A message indicating a mobile node's current mobility binding, and in particular its care-of address [22].

3.6 Correspondent Node (CN): A peer with which a mobile node is communicating. A correspondent node may be either mobile or stationary [9].

3.7 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 "colocated 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 [29].

3.8 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 tunnelled by the mobile node's home agent [9].

3.9 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) [12].

3.10 Gateway Foreign Agent (GFA): Foreign Agent which has a publicly routable IP address [32].

3.11 gateway LER/HA: One or more LER/HAs responsible for a specific administrative domain (defined by network operator), in which the mobile nodes register the current care-of address.

3.12 gateway LER/FA: One or more LER/FAs responsible for a specific administrative domain (defined by network operator).

3.13 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 [29].

3.14 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 [29].

3.15 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], [11].

3.16 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 [12].

3.17 Layer 3 (L3): The protocol layer at which IP and its associated routing protocols operate link layer synonymous with layer 2 [12].

3.18 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 [12].

3.19 Label Edge Router/Foreign Agent (LER/FA): An MPLS edge node with functions of foreign agent. It notes that there is no need of foreign agent in IPv6 [LER in IPv6].

3.20 Label Edge Router/Home Agent (LER/HA): An MPLS edge node with functions of home agent.

3.21 Label Switched Path (LSP): The path through one or more LERs/LSRs at one level of the hierarchy followed by packets in a particular FEC [12].

3.22 Label Switching Router (LSR): An MPLS node which is capable of forwarding native L3 packets [12].

3.23 Mobility Agent: Either a home agent or a foreign agent [9].

3.24 mobility binding: The association of a home address with a care-of address, along with the remaining lifetime of that association [9].

3.25 MPLS domain: A contiguous set of nodes which operate MPLS routing and forwarding and which are also in one Routing or Administrative Domain [12].

3.26 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 [29].

3.27 MPLS egress node or egress LER: An MPLS edge node in its role of handling traffic as it leaves an MPLS domain [12].

3.28 MPLS ingress node or ingress LER: An MPLS edge node in its role of handling traffic as it enters an MPLS domain [12].

3.29 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 [12].

3.30 path extension: When a mobile node moves and registers with a new foreign agent, IP datagrams for old foreign agent are tunnelled to the mobile node's new care-of-address [29].

3.31 Regional Foreign Agent (RFA): A Foreign Agent which may be the target of a request for regional registration [32].

3.32 route optimization: Route optimization provides a means for any node to maintain direct path connectivity to the destination mobile node. When sending an IP datagram to a mobile node, if the sender has a binding cache entry for the mobile node, it may tunnel the datagram directly to the care-of address [29].

3.33 regional registration: A mobile node performs registration locally at the visited domain, by sending a Regional Registration Request to RFA/GFA, and receiving a Regional Registration Reply in return [32].

3.34 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 [29].

3.35 smooth handover: When a mobile node moves from one old care-of address to a new care-of address and registers with a 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 during mobile node moving are usually 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 capability provides a means for the mobile node's old foreign agent to be reliably notified of the mobile node's new mobility binding, allowing datagrams in flight to the mobile node's old care-of address to be forwarded to its new care-of address [29].

3.36 triangle routing: A situation in which a correspondent node packets to a mobile node follow a path which is longer than the optimal path because the packets must be forwarded to the mobile node via a home agent [29].

4 Abbreviations

This Recommendation uses the following abbreviations:

AP	Access Point
ARP	Address Resolution Protocol
BA	Behavior Aggregate
CN	Correspondent Node
CoA	Care-of Address
CR-LDP	Constraint-based Label Distribution Protocol
DHCP	Dynamic Host Configuration Protocol
DiffServ	Differential Service
DLCI	Data Link Connection Identifier
DNS	Domain Name Service
DSCP	DiffServ Code Point
FA	Foreign Agent
FEC	Forwarding Equivalence Class
FIB	Forwarding Information Base
GFA	Gateway Foreign Agent

HA	Home Agent
ICMP	Internet Control Message Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
L2	Layer 2
L3	Layer 3
LAN	Local Area Network
LDP	Label Distribution Protocol
LER	Label Edge Router
LER/FA	Label Edge Router/Foreign Agent
LER/HA	Label Edge Router/Home Agent
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
NNI	Network Node Interface
PHB	Per Hop Behavior
QoS	Quality Of Service
Resv	Reserved
RFA	Regional Foreign Agent
RSVP-TE	Resource Reservation Protocol – Traffic Engineering
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
TLV	Type, Length, and Value
UDP	User Datagram Protocol
UNI	User Network Interface
VPI/VCI	Virtual Path Identifier/Virtual Channel Identifier
VPN	Virtual Private Network

5 Service definitions and requirements

5.1 Service definitions

5.1.1 MIPv4 over MPLS (MIPv4oMPLS) service

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

A mobile IPv4 over MPLS service is intended to enable nodes to move from one MPLS domain to another. It is then suitable for mobility across various MPLS domains. Concerning handover management amongst MPLS domains, as long as node movement does not occur between points of attachment on different MPLS domains, layer 2 mechanisms for mobility (i.e. link-layer handoff) may offer faster convergence and less overheads than those preceded by mobile IP. MobileIPv4 over MPLS service can provide the LSPs between different mobile IP subnets.

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

5.1.2 MIPv6 over MPLS (MIPv6oMPLS) service

In mobile IPv6, the route optimization is built in as a fundamental part of the protocol. The route optimization capability 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 mobile IPv4 protocol. The registration function and the route optimization function are performed by a single protocol rather than by two separate protocols in mobile IPv4. These functions can safely and efficiently deliver though the MPLS network. Two LSPs from the mobile node may be set up respectively to the home agent (for registration) and to the correspondent node (for route optimization).

While a mobile node is away from home, its home agent intercepts any packets that arrive at the home network of the mobile node, using IPv6 neighbor discovery like that used in mobile IPv4. The use of neighbor discovery improves the robustness of the mobile IP protocol and decouples mobile IP from any particular link layer, unlike to IPv4 protocol (ARP is used).

While away from home, a mobile node registers its care-of addresses on its home agent. The association between 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 of 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. The LSP between the correspondent node and care-of address of the mobile node, along with its cache binding, may be set up with relevant bandwidth reservation.

5.2 Service requirements

5.2.1 General requirements

In order to support mobile IPv4 and mobile IPv6 services, the MPLS network satisfies 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 decapsulation of packets is taken with label header information.

– For security, a filtering function can be added at the ingress LER [27].

– A label switched path with the requested QoS level, if any, is provided between the ingress LER and egress LER.

– Minimized service interruption at handover time is required. The negotiated QoS level should be maintained during handover.

5.2.2 MIPv4oMPLS requirements

- *Requirements for connectivity*

  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 home IP address. During handover, the seamless connectivity is provided by obtaining the care-of address of the mobile node at the visited location.

- *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.

- *Requirements for location management and registration*

  When a mobile node detects that it is located on a foreign location, it obtains a care-of address and operates with mobility services by registering with its home agent. When returning to its home location, the mobile node deregisters with its home agent. The MPLS node updates the correspondent label cache table accordingly.

- *Requirements for routing*

  No additional routing requirements are imposed on the MPLS network. When the mobile node is away from home location, route optimization, by using direct short-cut LSP between the mobile node and the correspondent node, can be used to avoid the triangle routing.

- *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 wireless 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.

5.2.3 MIPv6oMPLS requirements

- *Mobile IPv6 protocol requirements*

  While away from its home, a mobile IPv6 node is associated with a colocated 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 colocated 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 then to send any packet destined to the mobile node directly to it at this care-of address. The LSPs are directly set up between the mobile node and the correspondent node with the cache binding information.

6 Service architecture

6.1 Overview

6.1.1 Introduction

The MPLS backbone network can build the large-scale mobile IP network. A mobile node can communicate to any other fixed or mobile nodes via the Label Edge Router (LER). The LER is capable of forwarding IP packets by encapsulating them. The packet with label encoding travels a particular route through the MPLS network since a label is used to represent the explicit route and is encoded by relevant classification according to quality of service (QoS). It defines the standard-based MPLS signalling (e.g., label distribution protocol) to support multi-vendor interoperability. In this way, the MPLS network brings significant benefits to a connection-oriented IP network.

The MPLS forwarding logic is based on the label swapping algorithm. 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 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, a precedence and/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 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 a particular network.

To support mobile service, the MPLS network has to accommodate the foreign agent and the home agent. By combining or merging functions of the home agent and the foreign agent into the MPLS node, the MPLS network is capable of handling the mobile node. The home agent and/or the foreign agent can be located in MPLS nodes which are called LER/HA and LER/FA. The packets intercepted by LER/HA are encapsulated, in this case, using a label and tunnelled to the current location of the mobile node via LER/FA. The LSP, between the home agent and the foreign agent, is used to tunnel with quality of service. Both MPLS signalling protocols, CR-LDP and RSVP-TE, may be used to set up the LSP tunnel between the mobile agents (that is, foreign agent and home agent) through the MPLS network. The IP-in-IP tunnels between the home agent and the foreign agent are merged into one or multiple LSPs through the MPLS network [10], [11]. To avoid the problem of triangle routing of the native mobile IPv4 protocol addictively, 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 interruption because smooth handover can be applied. The path rerouting procedures may be also used to avoid the triangle routing and provide the short-cut path.

To set up the LSPs between the correspondent node and the mobile node, four types of LSP tunnelling scenarios may take place as follows:

– Scenario 1 (MPLS-based mobile IPv4 tunnelling scenario) applies basic mobile IPv4 services over the MPLS network setting up the LSP between the correspondent node and

the mobile node. It is a natural extension of the existing mobile IPv4 protocol via home agent. The ingress LER intercepts the incoming packets to be forwarded to the mobile node via both LER/HA and egress LER/FA. In this scenario, two LSPs are required between ingress LER and LER/HA, and between LER/HA and egress LER/FA, respectively.

– Scenario 2 (MPLS-based mobile IPv4 route optimization scenario) applies route optimization over the MPLS network to avoid the problem of triangle routing of mobile IPv4 protocol. A direct short-cut LSP between ingress LER and egress LER/FA is used without routing through the home agent.

– Scenario 3 (MPLS-based mobile IPv6 binding update scenario) applies the binding update procedure of mobile IPv6 protocol to cache the binding information of a mobile node's home address with its care-of address. There is no need of foreign agents as in mobile IPv4. The LSPs between ingress LER and egress LER transparently deliver packets to the mobile node.

– Scenario 4 (MPLS-based hierarchical mobile IP tunnelling scenario) applies hierarchical mobile IPv4 or IPv6 protocol over MPLS network. The relevant mobile agents are located at the hierarchical MPLS nodes. This scenario performs regional registration locally such as regional FA and gateway FA. In case of handover, these FAs assume the role of an anchor node for LSP rerouting at a visited area.

Further details are provided in 6.3

6.1.2 Assumptions

– A single MPLS administrative domain is concerned. The inter-domain MPLS networks between different network operators are beyond the scope of this Recommendation.

– There are no additional requirements on the MPLS network for support of the mobile IPv4 and mobile IPv6 protocol features such as agent discovery and location management.

– All the mobile nodes are directly connected to LER/FAs. If one or more mobile IP networks are attached to the LER/FA, in which a number of HAs and FAs consists of a single mobile IP network, the links to LER/FA are emulated as direct interface from a mobile node. In this case, the LER/FA may be an external gateway router of the attached mobile IP network to communicate with the external world.

– The LERs have the role of foreign agent to identify the visiting mobile nodes. In mobile IPv6 over MPLS, the LER can have also a function of ingress filtering. The home agent can be located at LER or LSR nodes depending on coverage of a mobile IP's home address.

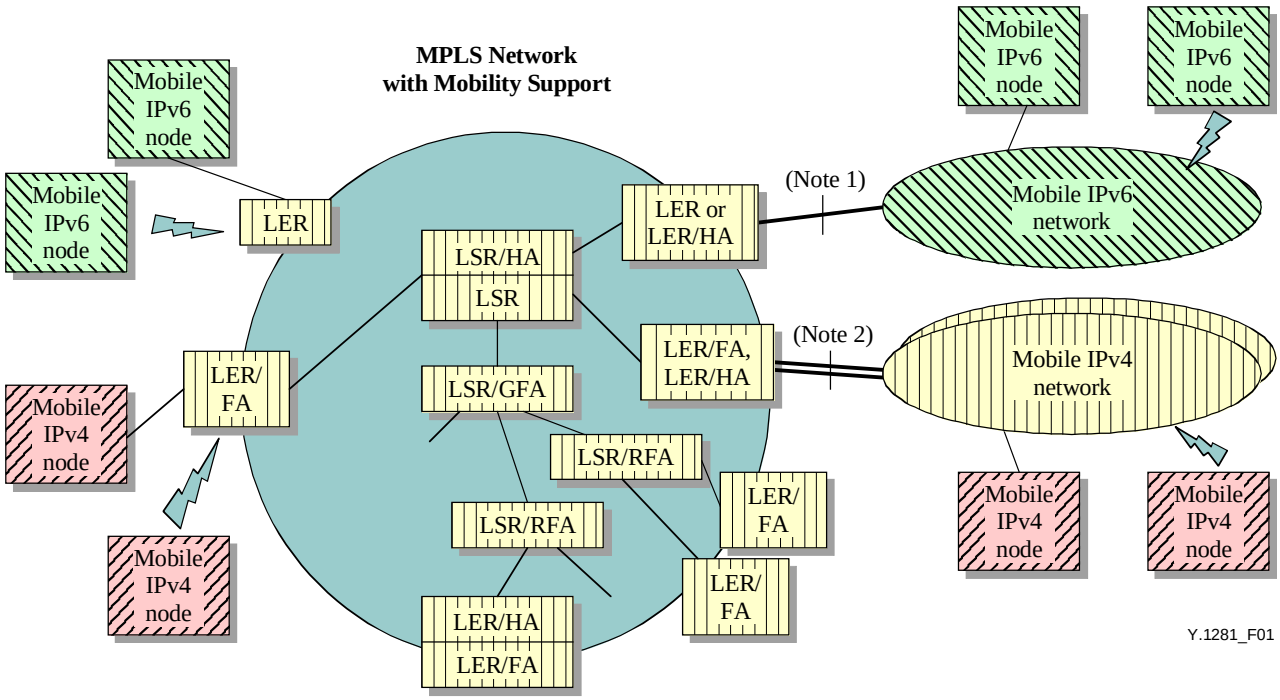
– The forwarding process on the MPLS network is taken on the datagram IP traffic (the UDP traffic) as well as the stream-like IP traffic (the TCP traffic).

– The LER/HA and LER/FA must support security associations.

6.2 Reference architecture

Figure 1 provides the reference model of MPLS network to support mobile IPv4 services and mobile IPv6 services.

In this figure, the HA is located at LER or LSR. The FA is only located at LER. The GFA and RFA in the hierarchical MPLS network are located at LSR. But, there is no FA for the IPv6 network.



NOTE 1 – This interface emulates the mobile IPv6 nodes. The LER is responsible for the attached mobile IPv6 network as a border gateway router.
NOTE 2 – This interface emulates the mobile IPv4 nodes. The LER is responsible for the attached mobile IPv4 network as a border gateway router.

Figure 1/Y.1281 – Reference architecture of MPLS network with mobility support

NOTE – The interworking between mobile IP networks and the MPLS network is beyond the scope of this Recommendation. The reference architectures for mobile IPv4 and mobile IPv6 are provided in Appendix I.

6.3 LSP tunnelling scenarios

6.3.1 MPLS-based mobile IPv4 tunnelling scenario

This scenario describes the MPLS tunnelling mechanisms to support the mobile IPv4 service. While the mobile node is moving to a foreign area, the LER/HA intercepts packets having the home IP address of the mobile node and forwards them to the LER/FA of the temporarily visiting area of the mobile node. The LSP provides layer 2 tunnels without IP-in-IP encapsulation [10], [11]. It notes that the IP-in-IP tunnel utilizes the layer 3 forwarding capability. The ingress LER forwards IP packets all the way to the home agent to the egress LER/FA of the foreign mobile node. The whole forwarding process is done at the MPLS layer.

Since a label header is much smaller than an IP encapsulation header, the tunnelling 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 shows the MPLS-based mobile IPv4 tunnelling scenario. In this scenario, a LER/HA intercepts packets and forwards them to the mobile node.

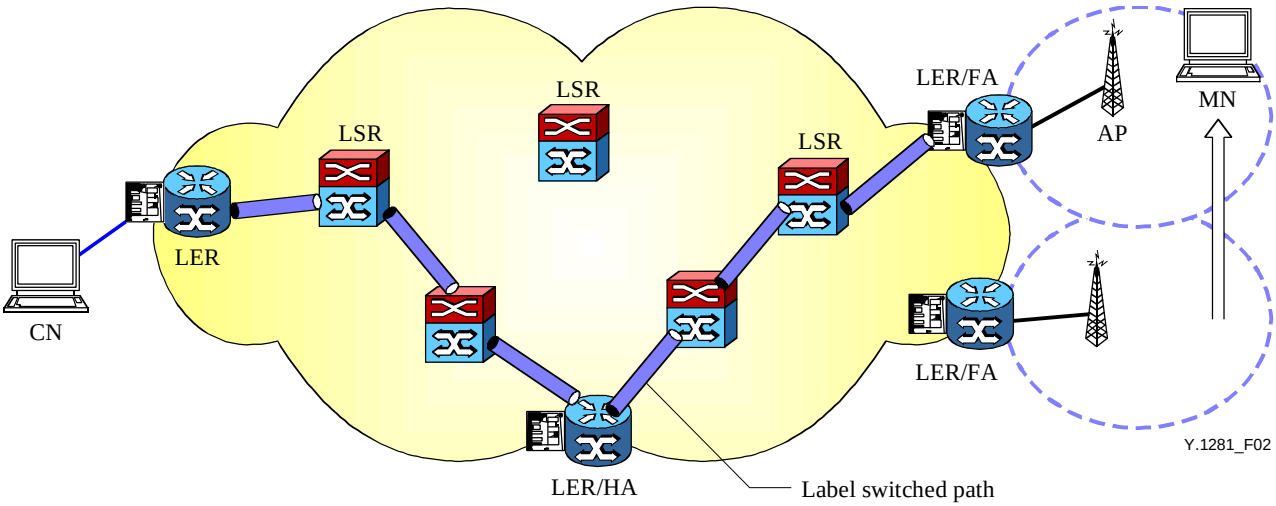


Figure 2/Y.1281 – MPLS-based mobile IPv4 tunnelling scenario

In this scenario, all the home agents and the foreign agents can be located at the LERs. The LSPs can be set up the same way that "tunnels" are set up between the home agent and the foreign agent. In mobile IPv4, in addition, they can be the IP/QoS-enabled paths by using the constrained-based routing and signalling.

6.3.2 MPLS-based mobile IPv4 route optimization scenario

In this scenario, the data forwarding paths from the ingress LER to egress LER are recalculated after the discovery procedure. If the routing path is significantly longer than the optimal path after handover, the routing optimization procedure takes place. The route optimization is applied only inside the MPLS network, in which the tunnelling end points are the ingress LER and the egress LER/FA. The label forwarding entries 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 paths from ingress LER are cut through to the egress LER/FA, which can solve the problem of the triangle routing. The ingress LER finds the forwarding path in query process to find the destination tunnel endpoints, that is, the destination LER/FA. The incoming packets at ingress LER look for the outgoing LSP in the LER's label information table: when the appropriate label forwarding entry is found, packets are sent to the egress LER by using the explicit routed path. If no entry is found, packets are sent to the home agent by using hop-by-hop routed path.

Figure 3 shows the MPLS-based mobile IPv4 route optimization scenario.

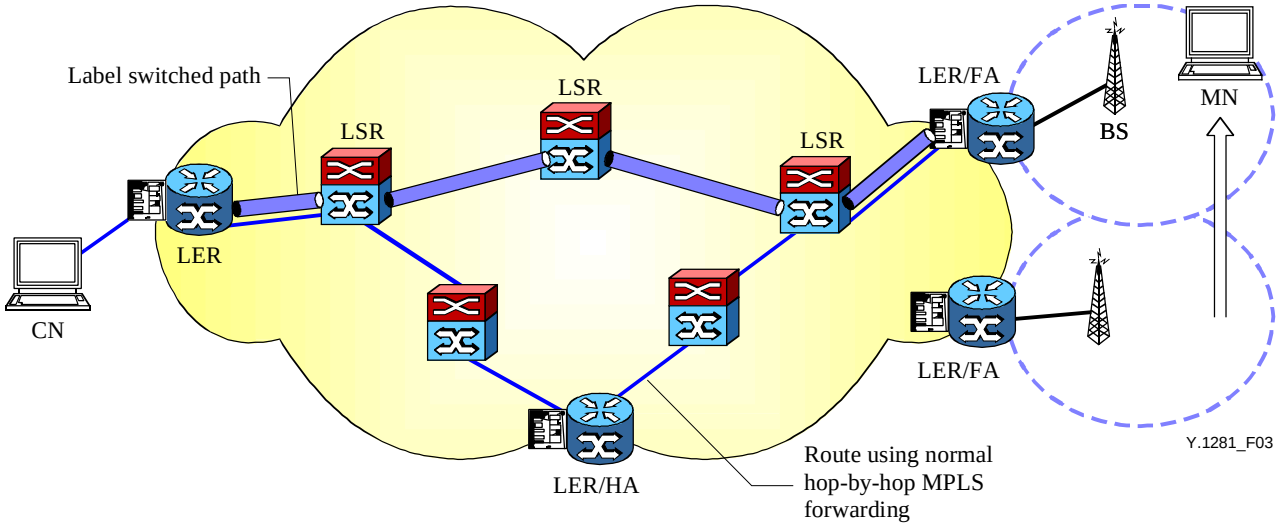


Figure 3/Y.1281 – MPLS-based mobile IPv4 route optimization scenario

6.3.3 MPLS-based mobile IPv6 binding update scenario

In this scenario, the direct forwarding path from the ingress LER to egress LER are built after the IPv6 binding update procedure, which is similar to the mobile IPv4 routing optimization scenario. 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 IPv4. 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 colocated care-of address. Instead, the LER performs ingress filtering [27]. 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 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 shows the MPLS-based mobile IPv6 binding update scenario.

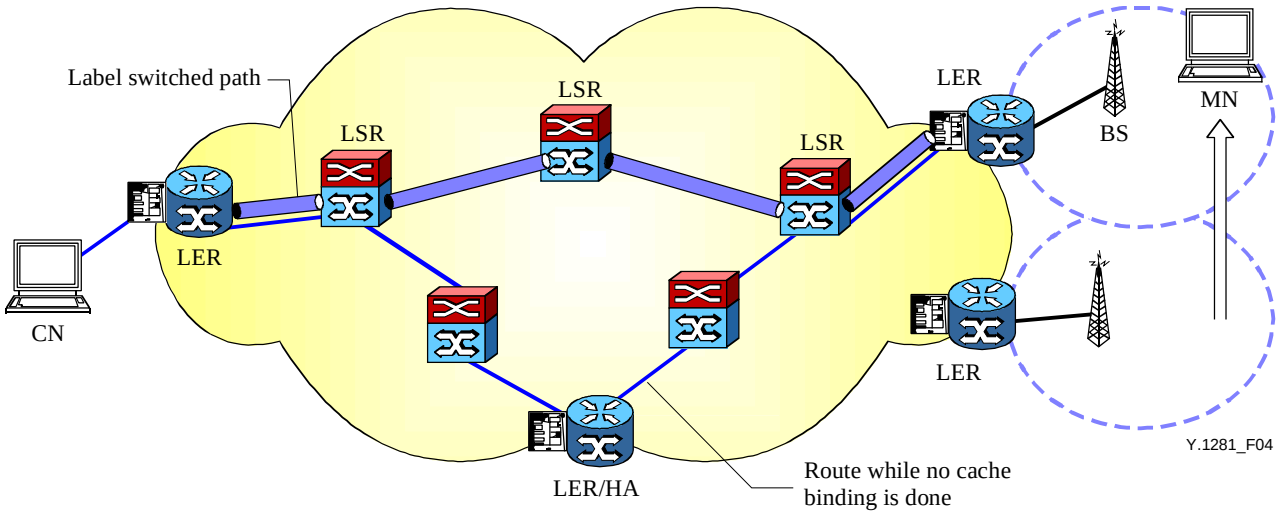


Figure 4/Y.1281 – MPLS-based mobile IPv6 binding update scenario

6.3.4 MPLS-based hierarchical mobile IP tunnelling scenario

In this scenario, mobile IPv4 or mobile IPv6 services over the hierarchical MPLS network are considered. It is assumed 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 LERs or LSRs. 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 a new foreign agent.

As the network scale increases, handover latency may be significant. The hierarchical mobile tunnelling scenario allows a mobile node to perform registration locally in order to reduce a number of registration messages to the home agent. This reduces signalling delay when a mobile node moves to the new foreign agent and, therefore, improves performance during handover time.

In this network architecture, the hierarchical mobility agents allow seamless location management operations while maintaining ongoing sessions and maximizing data throughout. The foreign agents handle local movements of mobile nodes within the domain.

The hierarchical mobile IP tunnelling scenario over MPLS is shown in Figure 5.

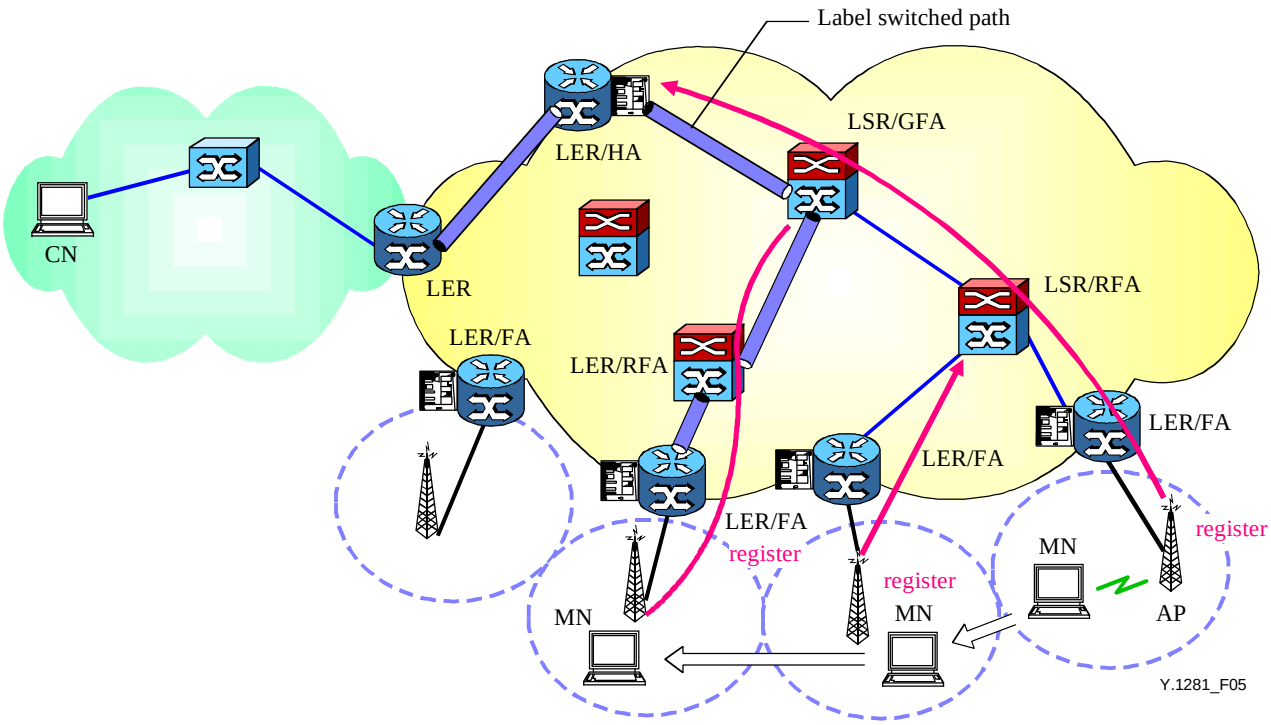


Figure 5/Y.1281 – MPLS-based hierarchical mobile IP tunnelling scenario

7 Application procedures for mobility support

7.1 General assumptions

In the MPLS network, mobility support is focused on the control procedures such as registration, LSP establishment and LSP extension for handover, etc.

LSP tunnels are required to send mobile IP packets over the MPLS network. CR-LDP or RSVP-TE MPLS signalling protocols are used to establish LSP tunnels with appropriate QoS levels. The locations of home agents and foreign agents are found with the registration and agent discovery procedures of the mobile IP protocol.

The label switched paths between ingress LER and egress LERs are set up with CR-LDP or RSVP-TE signalling.

Depending on applications, bidirectional LSPs have some benefits of lower setup latency and lower number of messages required during setup.

7.2 LSP tunnelling procedures

7.2.1 MPLS-based mobile IPv4 procedures

In this scenario, there can be LSP tunnels:

– between the ingress LER and the home agent;

– between the home agent and the egress LER/FA.

Figure 6 shows the procedures for the mobile IPv4 service over the MPLS tunnelling scenario.

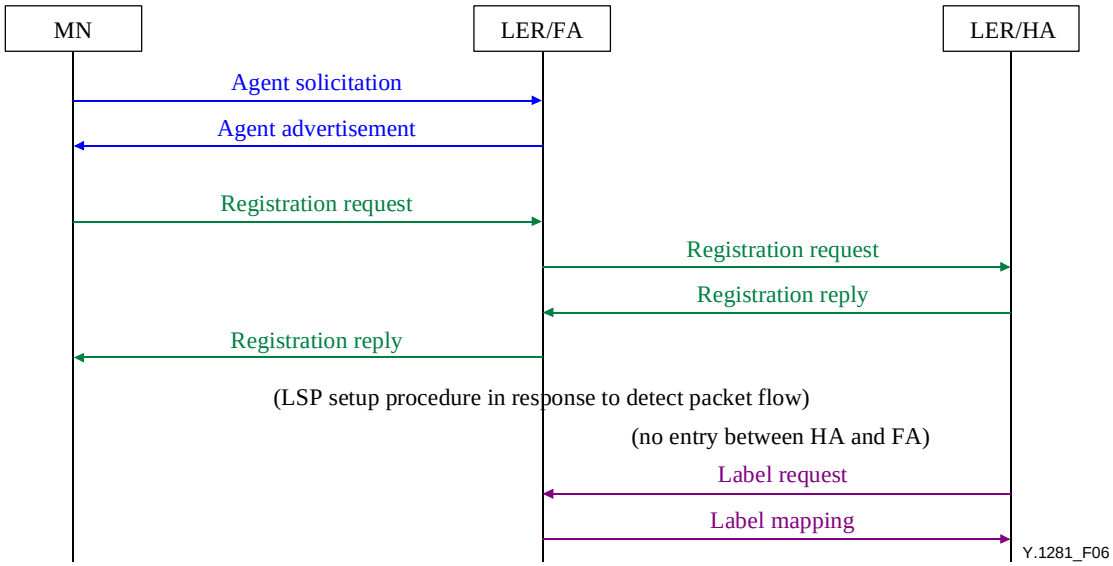


Figure 6/Y.1281 – Procedures for the mobile IPv4 service over MPLS tunnelling scenario

In this scenario, the mobile node determines whether it is at home or in a foreign location when it receives an agent advertisement message broadcast 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 update its label information table with the value of the mobile node home address. Based on this table, the foreign agent forwards the registration request message towards the home agent.

The registration request message is forwarded to the home agent using hop-by-hop routing. When the home agent gets the registration request message and learns of the care-of address of the mobile node, it sends a registration reply message to the mobile node via the foreign agent. Then the home agent sends a label request/path message to the foreign agent if there is no LSP between the home agent and the foreign agent (no action is required if a LSP already exists). The 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 will be established. In this way, the home agent can relay the packets destined to mobile node's 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 sends user packets through the LSP from the mobile node to the correspondent node.

Packets from a correspondent node to the mobile node are addressed to the mobile node's 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 information

table. It inserts the label value in the label information 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 no entries are available in the table.

7.2.2 MPLS-based mobile IPv4 route optimization procedures

This scenario is used to solve the mobile IPv4 problem of the triangle routing of all the routing paths via the home agent. The forwarding path from ingress LER is cut through the egress LER/FA without visiting the home agent. In this scenario, data forwarding paths from the ingress LER to egress LER are recalculated via the router discovery procedure. The route optimization is applied only inside the MPLS network, the tunnelling end points being 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.

In this scenario, there can be LSP tunnels:

– between the ingress LER and the egress LER/FA;

– between the old foreign agent and the new foreign agent (only for the LSP extension case).

Figure 7 shows the route optimization procedures for the mobile IPv4 service over MPLS tunnelling scenario.

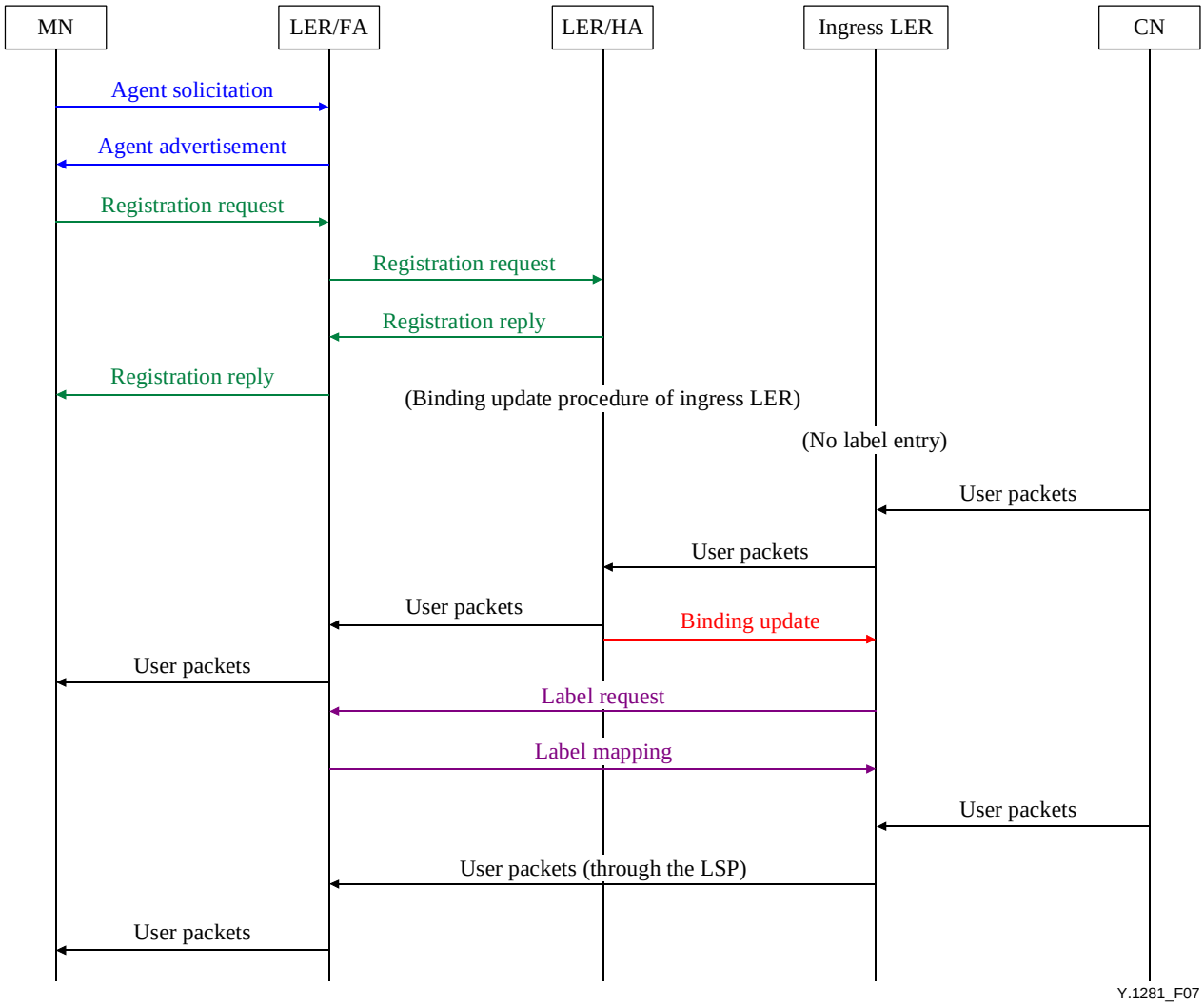


Figure 7/Y.1281 – Route optimization procedures for the mobile IPv4 service over MPLS tunnelling scenario

When a mobile node's home agent intercepts a packet from the home network and tunnels it to the mobile node, the home agent sends 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 for mobile IPv4 can be defined similarly to mobile IPv6 in [29]. As in the case of a binding update message sent by the mobile node's home agent, ingress LER maintains a binding cache to optimize mobile node's communication with correspondent 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. Each binding in the cache entry 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 the foreign agent receives a packet, if it has a binding cache entry for the destination mobile node and has no visitor list entry for this mobile node, then the foreign agent deduces that the binding cache entry for this mobile node has expired. In this case, the foreign agent sends a binding warning message to the mobile node's home agent, advising it to send a binding update message to the ingress LER that tunnelled this packet.

7.2.3 MPLS-based mobile IPv6 binding update procedures

This scenario is nearly the same as that of the mobile IPv4 routing optimization one mentioned previously. The only difference is that mobile IPv6 does not use "foreign agents" since some IPv6 features, such as 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 mobile IPv6 ingress filtering capability and builds the LSP between ingress LER and egress LER to transparently deliver packets to the mobile node [27].

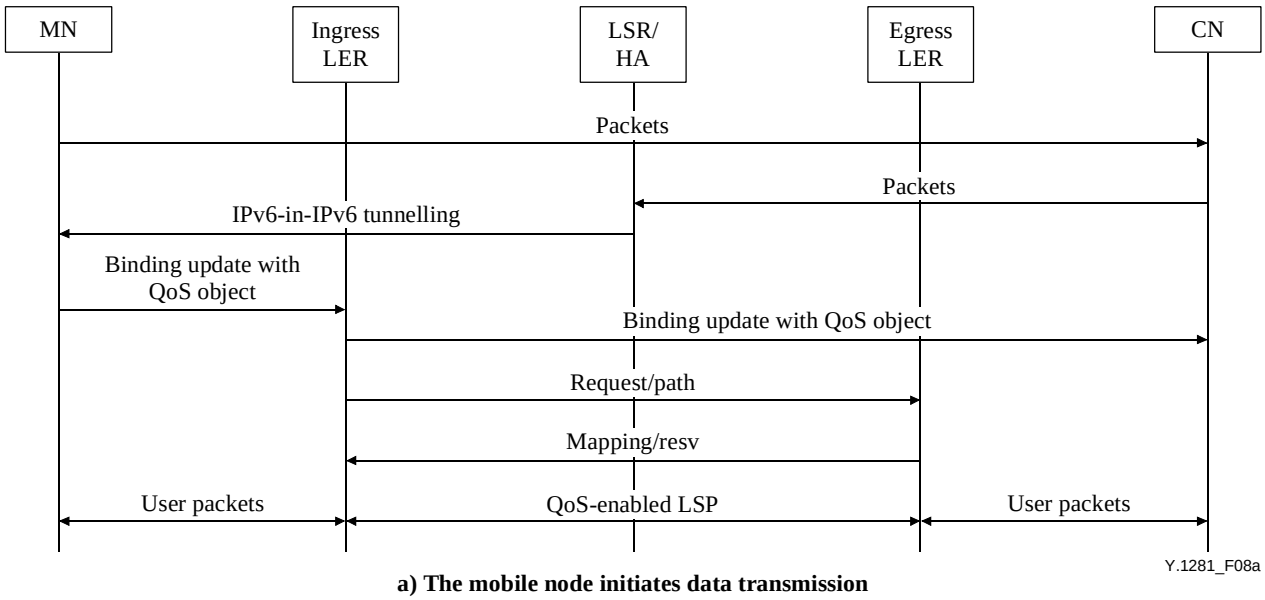
When the mobile node sends packets to any other correspondent node, it sends packets directly to the destination. The mobile node sets the source address of this packet to the care-of address and includes a 'Home Address' destination option. Then, the correspondent node must process the home address option when sending packets using the same home address value contained in the home address option of received packets.

To avoid triangle routing, a mobile node sends a binding update with QoS object to a correspondent node. The LER receiving the binding update message determines whether to initiate request/path message. The new established LSP provides a tunnel for packets to traverse. The correspondent IPv6 node receiving the binding update message is then able to send packets to the mobile node directly.

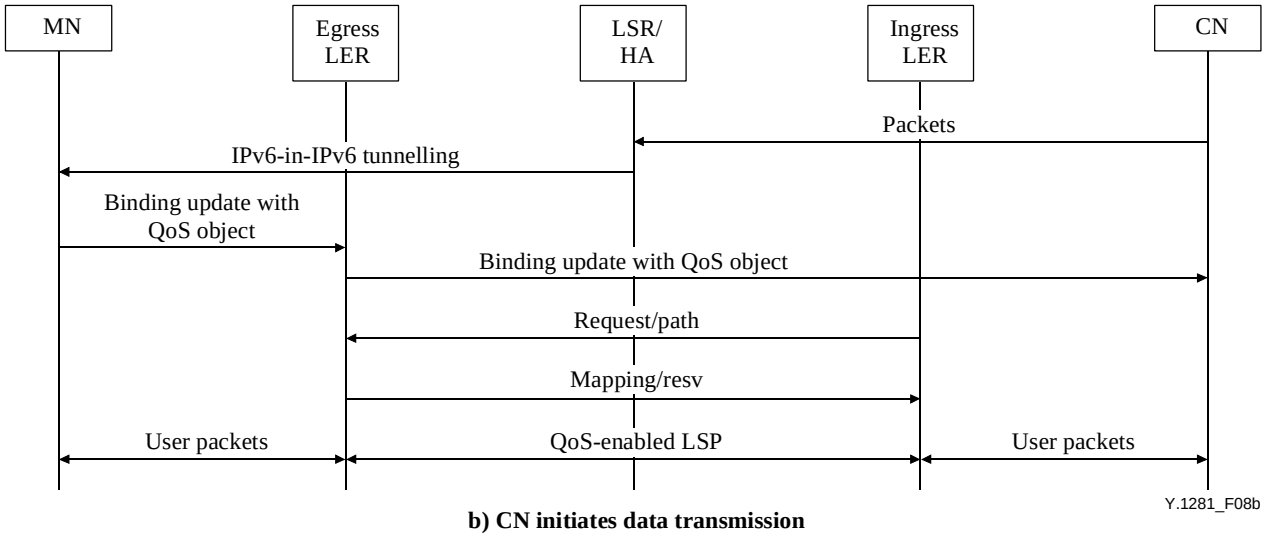
In this scenario, there can be LSP tunnels:

– between the ingress LER and the egress LER.

Figure 8 shows procedures for the mobile IPv6 service over MPLS tunnelling scenario.



a) The mobile node initiates data transmission



b) CN initiates data transmission

Figure 8/Y.1281 – Procedures for the mobile IPv6 service over MPLS tunnelling scenario

In this scenario, it is assumed that a mobile node has already accomplished default router discovery, address auto-configuration, and registration as defined in mobile IPv6 procedures. Before a correspondent node sends any packet to the mobile node, the correspondent node should examine its binding cache for an entry table on the destination address (that is, the home address of the mobile node) of the packet. If the correspondent node has a binding cache entry for this address, it uses a routing header to route the packet to the mobile node via the care-of address of that binding cache entry. If a correspondent node has no binding cache entry, the packet will be intercepted by the mobile node's home agent and tunnelled (using IPv6-in-IPv6 encapsulation) to the mobile node's current care-of address. When the mobile node gets the packets with IPv6-in-IPv6 encapsulation, it sends the bind update message. In the case that it is the egress LER that receives the bind update message from the mobile node, it initiates the signalling procedure to set up the LSP between ingress LER and egress LER.

7.2.4 MPLS-based hierarchical mobile IP procedures

This scenario considers procedures of the mobile IPv4 or mobile IPv6 services over the hierarchical MPLS tunnelling scenario in which a number of foreign agents, such as Gateway Foreign Agent (GFA) and the Regional Foreign Agent (RFA), are distributed in the MPLS network in a

hierarchical manner. The locations of GFA and RFA are identified via the registration procedure to the home agent.

In this scenario, there can be LSP tunnels:

– between the ingress LER and the home agent;

– between the home agent and GFA;

– between GFA and RFA;

– between RFA and the egress LER/FA.

The egress LER/FA advertises, in the agent advertisement message, the locations of hierarchical foreign agents in hierarchical order, between its own address (first) and the GFA address (last). If the mobile node determines that it is in a foreign location, the mobile node sends a registration request message. When the LER/FA closest to the mobile node receives the registration, it analyzes the incoming registration request message and then relays the registration request message to the next LSR/RFA in the hierarchy towards the LSR/GFA. When the next LSR/RFA receives the registration request message, it inserts a visitor list entry with the mobile node's home address and care-of address contained in the registration request message. This procedure is repeated up to the LSR/GFA. When the LSR/GFA receives the registration request message, it caches information about the next lower-level LSR/RFA in the hierarchy. Then the LSR/GFA relays the registration request message to the home agent. For each pending or current registration, the LSR/GFA maintains a visitor list entry. The registration request message is forwarded to the home agent hop-by-hop using normal IP routing.

When the home agent gets the registration request message and learns the GFA care-of address within the packet, the home agent sends a registration reply to the GFA. When the GFA receives the registration reply message, it can recognize that the registration reply message is coming from the specific registered mobile node. The GFA can know the egress LER/FA of the mobile node by reading the information of the mobile node entry correspondent to the received registration reply message. The GFA then sends a registration reply message to the RFA. This procedure is repeated in every FA in the hierarchy until the registration reply message reaches the egress LER/FA. When the egress LER/FA receives the registration reply message, it checks its cached information and relays the registration reply message to the mobile node.

Figure 9 shows procedures of the mobile IPv4 or IPv6 service over the hierarchical MPLS tunnelling scenario.

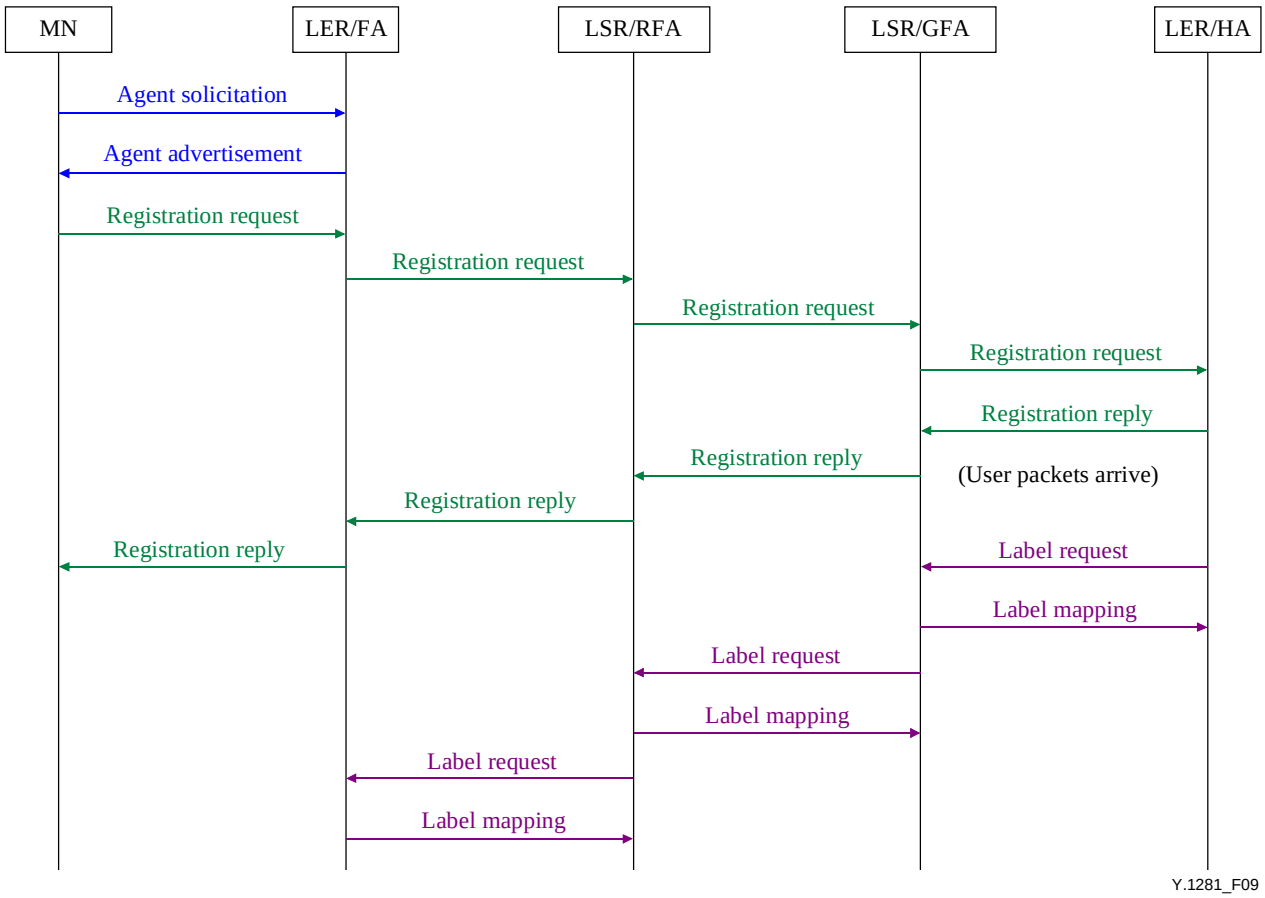


Figure 9/Y.1281 – Procedures of the mobile IPv4 or IPv6 service over the hierarchical MPLS tunnelling scenario

When a home agent sends packets to the mobile node, it sends a label request/path message to the GFA with the care-of address of the mobile node. The GFA replies with a label mapping/resv message to the home agent. It assigns labels and keeps the home address of the mobile node and the associated label binding for all registered mobile nodes. When this label mapping/resv message arrives at the home agent, the LSP is established. Figure 9 shows the registration and LSP establishment procedures. The home agent then updates its label information table that contains the home address and the care-of address of the mobile node and sets the outgoing label and outgoing port entries. In this way, the home agent can relay the packets destined to the mobile node's home address to its GFA in the foreign network. Finally, the home agent sends packets to the GFA along the LSP between the home agent and the GFA.

When the GFA receives the labelled packets, it can recognize that the registration reply is coming from the specific mobile node that is registered. The GFA can know the lower-level RFA of a registered mobile node by reading the information of the mobile node entry correspondent to received packets. LSR/GFA sends a label request/path message to the next LSR/RFA (in the hierarchy) with the care-of address of the mobile node. LSR/RFA replies with a label mapping/resv message to the home agent. LSR/RFA updates the binding information table and assigns a label for all the registered mobile nodes. When the label mapping/resv message arrives at LSR/GFA, the LSP is established.

7.3 Agent discovery

The agent discovery procedure includes both agent advertisement and agent solicitation. The same discovery procedures of mobile IP are used by the MPLS network since mobile agents are located at MPLS nodes. Mobile agents advertise their presence via agent advertisement messages. A mobile

node may optionally solicit an agent advertisement message from any locally attached mobility agent by sending an agent solicitation message. When a mobile node receives an agent advertisement, it determines whether it is on its home or a foreign location.

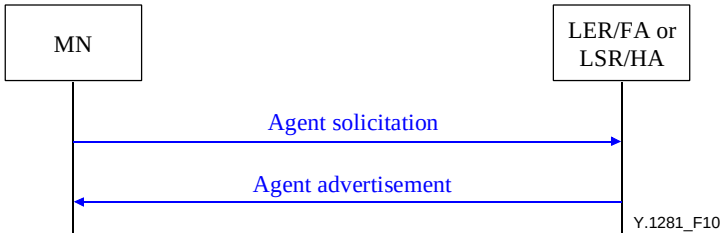


Figure 10/Y.1281 – Agent discovery of mobile node over the MPLS network

7.4 LSP rerouting procedures during handover

When a mobile node moves from one foreign location to another, the registration procedure is repeated again between the home agent and the new foreign agent. The existing LSPs are changed to the new foreign agent. The following LSP rerouting (route optimization) procedures can take place on the MPLS network:

– LSP extension;

– LSP optimization.

There are two goals to decide the rerouting procedure during handover:

a) to reduce the latency or interruption due to handover;

b) to reduce signalling overhead. The use of more than one care-of address by a mobile node may be useful to have a "smooth handover" when the mobile node moves from one foreign location to another. The LSP can support smooth handover capability and provides a solution to QoS-enabled paths for the mobile node's care-of address.

The vast majority of subscribers are not actively communicating most of the time. However, we can suppose that wireless IP is constantly switched on, ready for service, and reachable via the wireless Internet. In essence, a mobile node is in an idle state, but always connected to the network infrastructure. The LSP setup procedure activates only channels that are supposed to traverse over QoS guaranteed LSP, preventing LSP bandwidth usage. Thus, an LSP is established only between ingress LER and egress LER. This is an efficient scheme to save bandwidth in the MPLS network and to reduce end-to-end delay.

7.4.1 LSP extension

When a mobile node is moving to another foreign location, new IP packets intercepted by the home agent are tunnelled to the mobile node's new foreign agent (that is, the new egress LER), but packets in flight already intercepted by the home agent and tunnelled 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 to reach the new mobile node's location. If a FIB has a label for that mobile node, then the old foreign agent sets up an LSP to the new foreign agent. Therefore, the existing LSP from the ingress LER to the old foreign agent is extended to the new foreign agent via the extended LSP.

After signalling exchanges between the old foreign agent and the new foreign agent, the existing LSP can be extended to the 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 packet for the mobile node arriving at the old foreign agent can then be retunnelled to the mobile node's new foreign agent through the extended LSP. If no label is available to reach the new mobile node's location, packets will be sent to the new foreign agent by using hop-by-hop routing.

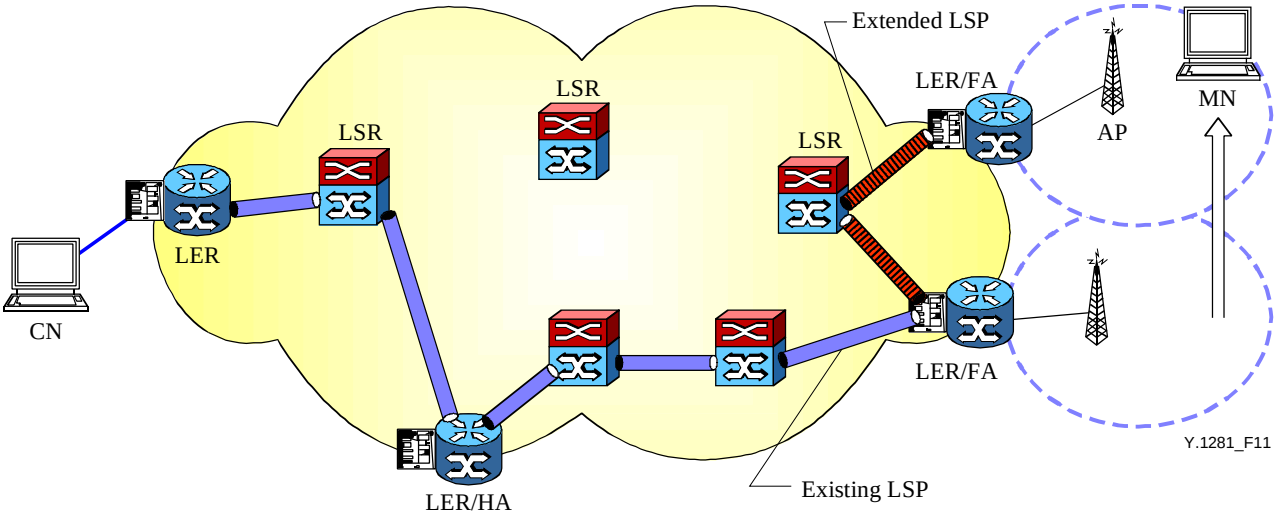


Figure 11/Y.1281 – LSP extension for mobile IP service during handover time

Whenever a mobile node migrates to an adjacent subnet, the 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 recognizes that a destination mobile node migrates to the new foreign agent. However, whenever a destination mobile node migrates, the ingress LER does not set up a new LSP to the new foreign agent. The LSP extension will take place between the old foreign agent and the new foreign agent without intervention of the ingress LER.

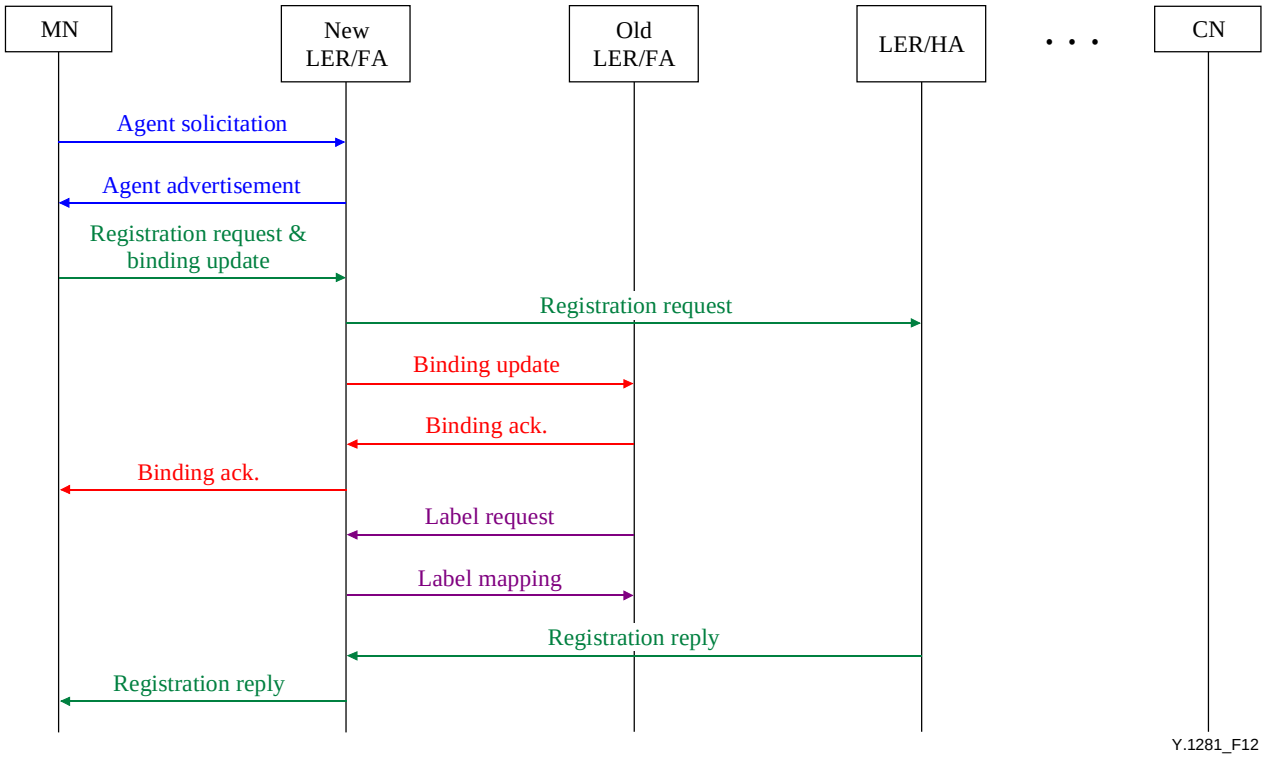


Figure 12/Y.1281 – Message sequence chart for LSP extension

The LSP extension procedures in Figure 12 are as follows:

– A mobile node moves to a new foreign agent and sends a registration request message and a binding update message to the 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

– An 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, the home agent sends a registration reply message in response to the previous registration request.

7.4.2 LSP optimization

During or after handover, the LSP optimization can be requested by the mobile node or the LER/FA. The route optimization is initiated by some factors such as performance degradation or resource optimization. The decision policy for LSP optimization is beyond the scope of this Recommendation.

When the performances of an LSP tunnel are temporarily degraded after handover, the LSP reestablishment is triggered by the ingress or egress LERs. After LSP reestablishment, the route between the ingress LER and new foreign agent can be optimized. The old LSP is torn down and a new path is set up. If performance degradations are detected, the LSP reestablishment message is initiated by the ingress or egress LERs. The detailed measurement and judgment scheme of performance degradation is 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 one 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 care-of address (CoA) on the new link.

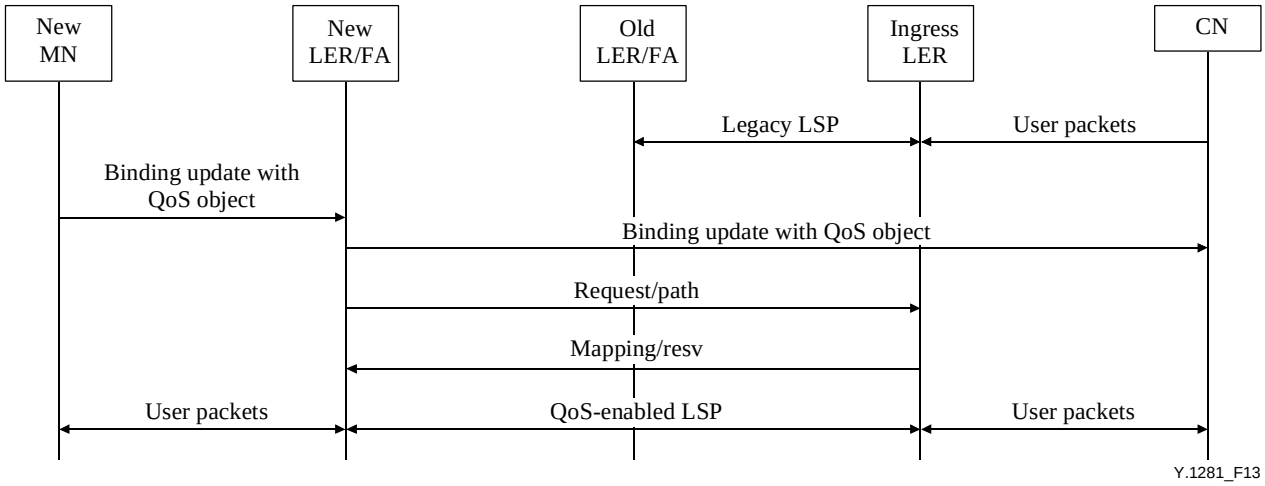


Figure 13/Y.1281 – LSP optimization procedure

When a mobile node acquires a new CoA while communicating with the correspondent node over legacy LSP, the mobile node sends a binding update message along with QoS object to the correspondent 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 directly to the mobile node while previous flows have been traversed over the legacy LSP, which supports smooth handover over both the legacy LSP and the newly established QoS guaranteed LSP. The old LSP will be released automatically, as time goes by, because no more data is transmitted over it.

7.4.3 LSP optimization for hierarchical MPLS

In a mobile IPv4 regional registration, when a handover occurs, a 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 message 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 message is forwarded to the LSR/GFA by means of one or more intermediate LSR/RFAs. When the registration request message arrives at the first LER/FA, the foreign agent checks its visitor lists to see if this mobile node is already registered with it. If it is not, the foreign agent checks which is the next higher-level LSR/RFA to which the registration request message should be relayed. The next LER/RFA or LSR/RFA checks its visitor lists 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 message toward the lower-level LSR/RFA. When the lower-level LSR/RFA receives the registration reply message, the LSR/RFA is able to point out the received registration reply message so that the packet is associated with the corresponding mobile node. The LSR/RFA reads the location

information about the mobile node entry corresponding to the received registration reply message, and recognizes the mobile node as the registered lower-level one. LSR/RFA then sends a registration reply message to the lower LSR/RFA. The above sequence is repeated up to the new LER/FA which the mobile node is moved to.

If there is an established LSP for 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. On the whole, for mobile nodes registered to a foreign agent, it is necessary to assign a label, and to maintain the binding table of the home address and the label of the mobile node. When a label mapping/resv message from lower-level LSR/RFA arrives at upper-level LSR/RFA, the LSP is established. After the LSR/RFA receives the label from the lower-level one, it is necessary to modify the label entry of the associated mobile node in the label information table. The incoming label value of the label 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 procedure. The LSR/RFA will then send a label request/path message to the next LSR/RFA with the care-of address of the mobile node. When this label mapping/resv message arrives at the LSR/RFA, the LSP is established.

The above sequence is repeated up to the new foreign agent of the network to which the mobile node has moved to. In this way, the LSP is newly established from anchor foreign agent to new foreign agent. In this LSP partial reestablishment method, since the LSP is maintained from the home agent to the anchor foreign agent, and a new LSP is established from the anchor foreign agent to the new foreign agent, the LSP setup time can be reduced.

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

Figure 14 shows an example of regional registration and LSP optimization procedure for mobile IP service over hierarchical MPLS when the mobile node moves to a new LER/FA.

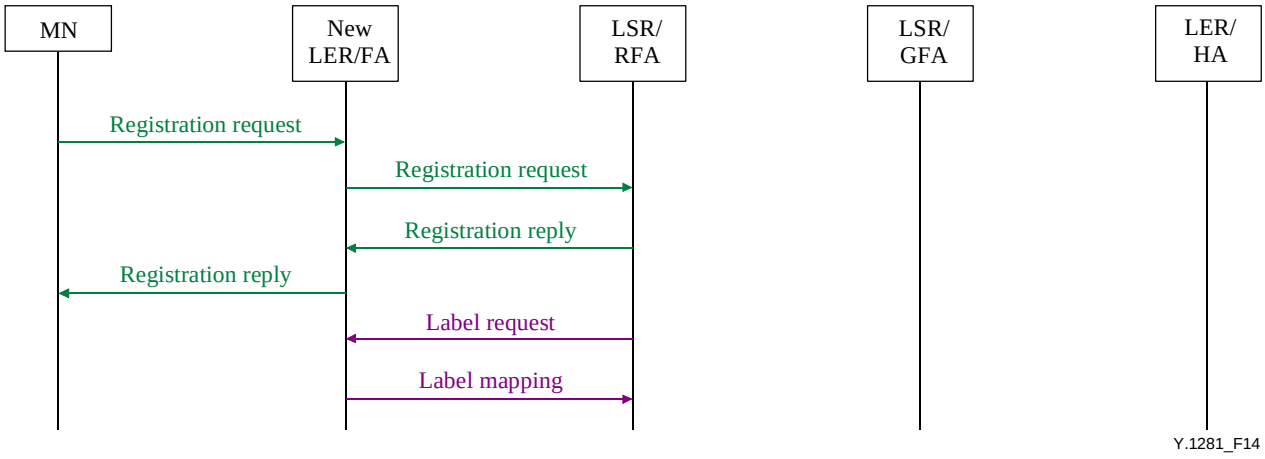


Figure 14/Y.1281 – LSP optimization procedure at mobile IP over hierarchical MPLS during handover

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. To avoid the unnecessary transient situations during clear down of the old LSP, the usage of routing preferences on the correspondent LSPs can be recommended to be applied at the anchor foreign agent.

The anchor LSR/RFA sends 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 message removes the mobile node from its visitor lists and the LSP that is assigned between upper-level foreign agents is released. The binding update message 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. An LSP that is established to an old foreign agent is released by the receiving label release messages.

8 QoS considerations

QoS service degradation

At the time of handover, QoS degradation could 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 degradation must be minimized.

Two schemes to minimize the QoS degradation are considered. One scheme uses multicast LSP: in this method, an anchor node establishes the LSPs to the current LER/FA and all LER/FAs in the neighborhoods of the serving LER/FA. When packets destined to that mobile node arrive at the anchor node, the anchor node multicasts the packets to all the MN's multicast group. If the mobile node moves to one of the neighboring locations, packets are immediately available.

The other scheme is the method using a bidirectional LSP tunnel between the new LER/FA and old LER/FA. In this scheme, LER/FA will establish bidirectional LSP to the neighbor LER/FA in advance, before handover. If the mobile node moves to the neighbor subnet, packets to the mobile node can be sent via a bidirectional LSP tunnel between the LER/FA.

QoS mapping to the MPLS network

In an MPLS network, a Label Switched Path (LSP) can be established using relevant signalling protocols. At the ingress LER, each packet is assigned a label and is transmitted downstream. At all the LERs or LSRs along the LSP, labels are used to forward the packet to the next hop which can best match the differentiated service (DiffServ) and traffic engineering requirements.

In a DiffServ domain, all the packets are classified and marked with a DiffServ Code Point (DSCP). At each LSR, the DSCP is used to select the per hop behavior. The MPLS shim header can transport the information of the PHB [17]. For an LSP set up with bandwidth reservation, LSRs perform admission control of the signalled LSP over the provisioned DiffServ resources (e.g., via configuration, SNMP or policy protocols). LSRs also perform adjustment of the DiffServ resources associated with the relevant classes of services.

In ITU-T Recs Y.1540 [6] and Y.1541 [7], classes of network QoS are defined and provisional performance objectives for IP in terms of network performance parameters are specified. The classes are intended to be the basis for service level agreements (SLAs) among network providers, and between end users and their network providers. The QoS and performance objectives for the MPLS network are not yet defined. The detailed QoS mapping between IP QoS and MPLS QoS are beyond the scope of this Recommendation.

9 Management aspects

Supports of the following management information are considered:

– Information of registration of home address and care-of address;

– consistency and verification of registration information at HA and FA including GFA and RFA;

– Information for LSP addition, removal, and change;

– Performance information and LSP statistics including handover situation;

– Information of service degradation during handover time;

– Information of service classes and QoS parameters;

– Information concerning faults, configuration, accounting, and security, etc.

10 Security aspects

The security concerns described in this clause are only focused on the MPLS network. At the ingress MPLS node, the network-level security is applied for access filtering, especially for authentication.

In a mobile environment, mobile nodes are connected to the network via wireless links. The LSPs connected to 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], [29].

Mobile nodes, home agents, foreign agents and correspondent nodes can operate securely with relevant security associations among themselves. The detailed procedures for security association are beyond the scope of this Recommendation.

In the MPLS network, LSPs should be maintained with security support especially during handover time (LSP extension or optimization). Figure 15 shows an example of security associations among the mobile nodes, FA, HA, and correspondent nodes during handover in case of LSP extension. (The rerouted label switched tunnel can be securely associated both in the LSP extension and the LSP optimization scenarios.) In this scenario, three security associations (SA) are required in addition to the correspondent node and LER/HA SA. These network-level SAs are sometimes combined with the IPsec protocol at the application level between the correspondent node and the mobile node, and also with the IPv6 binding authorization data option in IPv6 scenarios. The usage of security associations for MPLS signalling (e.g., LDP/CR-LDP or RSVP-TE) is for further study.

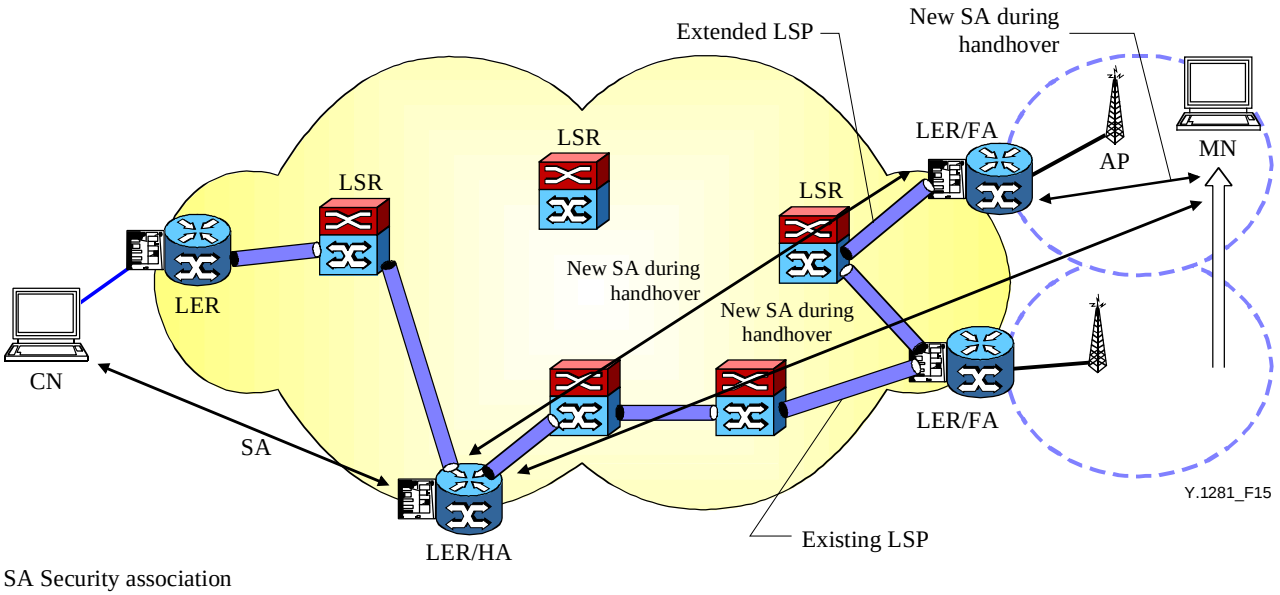


Figure 15/Y.1281 – An example of security associations for mobile IP service over MPLS during handover with LSP extension

Security constructs for Virtual Private Network (VPN) could also be applied to mobile IP services over MPLS. Other security aspects such as application-specific or mobile IP protocol-specific are beyond the scope of this Recommendation.

11 Routing aspects

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

In the MPLS network, the forwarding path of each flow may have different levels of service according to flow classification. (The routing path is calculated according to Forwarding Equivalence Class (FEC).) An LSP should meet the various QoS flow requirements.

The detailed routing algorithms of the MPLS network with mobility support are for further study.

Depending on the routing action, the packets are delivered to the destination mobile node via hop-by-hop routed paths or explicitly routed paths.

12 Scalability considerations

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) depends on the coverage of the attached single or multiple mobile IP networks.

Scalability improvement can be achieved while the labels for tunnels, among the mobile nodes and the mobile agents through the MPLS network, are distributed. Flexibility on label allocation can be obtained by usage of label swapping, stacking, merging and aggregation.

The route optimization between all mobile nodes and correspondent nodes can be deployed on a whole MPLS domain. The hierarchical MPLS network architecture can support the route optimization on a large scale by reducing the signalling overhead for mobility management.

13 Consideration of migration from mobile IPv4 over MPLS to mobile IPv6 over MPLS

In fact, the MPLS network forwards packets based on labels rather than the IP header itself. In the data transfer points of view, the MPLS network can deliver both IPv4 packets and IPv6 packets

simultaneously without replacement of network elements. Information transparency at the MPLS layer can be achieved regardless of layer 3 protocols (that is, IPv4 or IPv6).

However, from the control and management points of view, the existing MPLS signalling using IPv4 have to evolve to or simultaneously operate with the IPv6-based MPLS signalling. The routing and management functions of the MPLS network running on IPv4 protocol (e.g., ICMP, DNS, and DHCP, etc.) also have to migrate to those for IPv6 protocol.

14 Interworking with mobile IP networks

The LER/FA and the LER/HA connected to a specific mobile IP network have a role of border gateway router for the correspondent mobile IP domain since they function as a home agent and a foreign agent.

If there are a number of HAs and FAs in the mobile IP network, IP-in-IP tunnelling may be required between the mobile node and the correspondent LER(s). If the LER/FA (HA) is the unique FA (HA) for the given mobile IP domain, there is no need of IP-in-IP tunnel within the mobile IP domain.

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

Relevant interworking procedures should be defined if the IP-in-IP tunnelling is converted to the relevant LSP through the MPLS network. In addition, it is required to support the QoS mapping and bandwidth provisioning of the specific mobile IP flows.

The detailed interworking functions and procedures are beyond the scope of this Recommendation.

Appendix I

Reference architectures for mobile IPv4 and mobile IPv6 networks

NOTE – The detail interface specifications for reference points of UNIw, UNIx, UNIy, UNIz, NNIx and NNIy are for further study. They do not refer to any existing ITU-T Recommendation introduced in this appendix.

I.1 Reference architecture of a mobile IPv4 network

It is assumed that the reference architecture of mobile IPv4 networks will be based on the public network points of view. In this view, the customer premises network may be overlapped with the coverage of public network. Figure I.1 shows the reference architecture for a mobile IPv4 network. UNIw, UNIx, UNIy, and UNIz reference points can be defined as the user interfaces. The NNIx and NNIy can be defined as the network-node interfaces. For mobility support, the functions at the NNI reference interfaces can be decomposed into functions of user-plane (U-plane), control-plane (C-plane), and management-plane (M-plane).

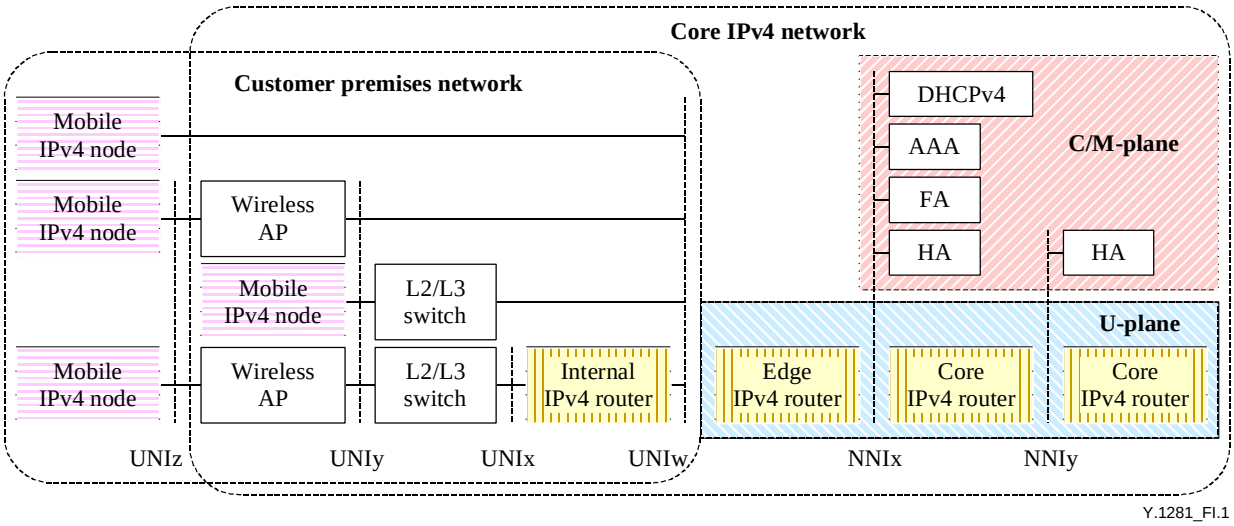


Figure I.1/Y.1281 – Reference architecture of a mobile IPv4 network

I.2 Reference architecture of a mobile IPv6 network

The reference model of a mobile IPv6 network is similar to that of a mobile IPv4 network. There is no FA function at the NNI (C/M-plane).

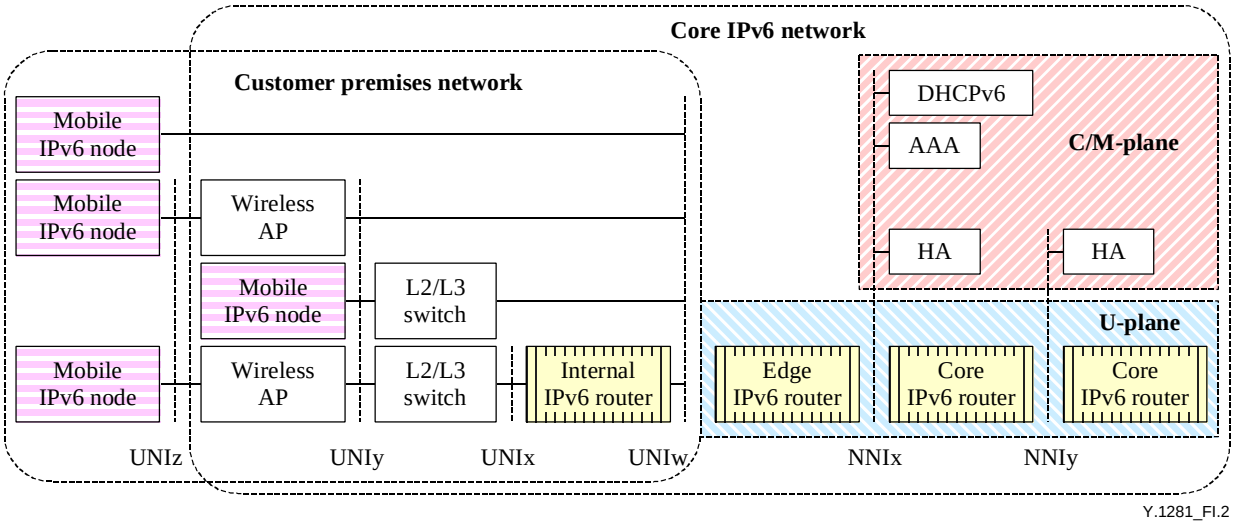


Figure I.2/Y.1281 – Reference architecture of a mobile IPv6 network

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series B	Means of expression: definitions, symbols, classification
Series C	General telecommunication statistics
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks and open system communications
Series Y	**Global information infrastructure, Internet protocol aspects and Next Generation Networks**
Series Z	Languages and general software aspects for telecommunication systems

Geneva, 2003