Mechanisms of Mobile IP in delivering packets and its trends for changing from IPv4 to IPv6

Nguyen Ngoc Chan (**P**osts & **T**elecommunications **I**nstitute of **T**echnology, Viet Nam)
E-mail: ngoc_chan@ptithcm.edu.vn
Tran Cong Hung Ph.D. (**P**osts & **T**elecommunications **I**nstitute of **T**echnology, Viet Nam)
E-mail: conghung@ptithcm.edu.vn

Abstract - **Mobile IP was produced by the IP Routing for Wireless/Mobile Hosts working group of the IETF, approved by the Internet Engineering Steering Group (IESG) in June 1996 and published as a Proposed Standard in November 1996 [12]. It gave solutions to solve problems that a mobility device obtains when moving from one link to another. The movement makes the network-prefix routing fail in delivering packets because the mobile node's new network-prefix is no longer equal the network-prefix assigned to its current link. This paper describes mechanisms used to deliver IP packets to mobile nodes which allow them to maintain all ongoing communications while changing links. Then, mobile IPv6's mechanisms on MPLS network are briefly presented as solutions for mobility devices in the future. Finally, the conclusion gives the approach to do research on mobile IP in the trends of making it scalable, secure and adaptive with the future network, especially in the period of changing from IPv4 to IPv6 [1].**

Keyword – **Mobile Ipv4, Mobile Ipv6, Agents, MPLS network, Correspondent Node, Router**

I. Introduction

From recent 20 years, when the Internet appeared and broke out, the needs of using public resources and communicating between people became more and more important. Many people work, do research, exchange data or manage the company through network and they need to keep on the connections every time and every where. The appearance of mobility devices such as laptops, notebooks, PDA or even routers makes their work much easier and more smoothly. However, difficulty occurs when they changes from one place to another place. They need to interrupt current connections and re-setup them after moving to a new location. Mobile IP mechanisms have been researched to solve this problem that means mobility devices still communicate while roaming without interruption by applying some procedures. Two solutions at IP layer are given to hold the connections. First, each mobile node (MN) uses only one IP address at every location. In this solution, routers use a specific routing protocol and they must update their routing table frequently and add an entry when a MN moves from network to network. Then, the routing table becomes bigger and bigger and routing is difficult because of the limits of memory, computing ability and routing algorithms. Thus, this is not scalable solution. Second, each MN use two addresses [9]: home address (HA) and care-of-address (CoA). HA is used when MN is at home network (HN) and CoA is used in foreign network (FN). MN is allocated a new CoA when it moves to a new network and its current CoA will be deleted by routers in previous network. Routers in MN's HN must recognize the MN's movement and forward every packet with the destination MN's HA to MN's CoA. Thus, a correspondent node (CN) just needs to know MN's HA and communicates with MN through MN's HN. This method is flexible and acceptable. So, it is researched and simulated to deploy in reality.

II. Delivering data in mobile IPv4:

Mobile IP or Mobile IPv4 is an Internet protocol designed to support mobile devices keep communications when moving without physical interruption and reconnection (Fig.1).

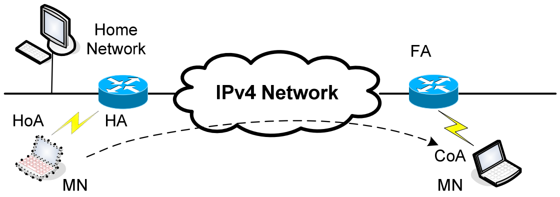


Fig. 1: Implementation of Mobile IPv4.

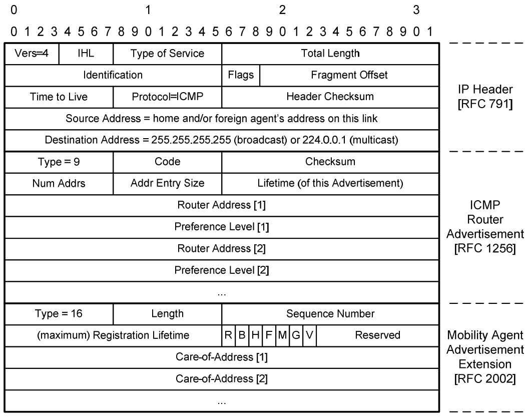
Operations of Mobile IPv4 include 3 main steps [12]:

Agent Discovery: In this step, MN recognizes where it is. If it is in a foreign network, its will require a new CoA.

Agent Registration: MN registers its CoA to HA. HA updates its routing table and prepares for forwarding packets addressed with MN's home address (HoA) to MN.

Data Delivering: CN communicate with MN via HA.

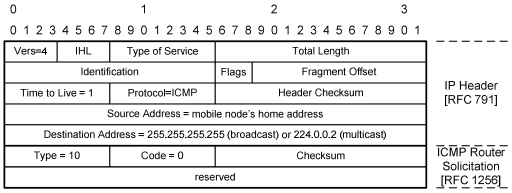
Agent Discovery:



0 0 1 2 3 4 5 6 7	1 8 9 0 1 2 3 4 5	2 6 7 8 9 0 1 2 3	3 4 5 6 7 8 9 0 1	
Vers=4 | IHL	Type of Service	Total Length		IP Header [RFC 791]
Identification		Flags	Fragment Offset	
Time to Live	Protocol=ICMP	Header Checksum		
Source Address = home and/or foreign agent's address on this link				
Destination Address = 255.255.255.255 (broadcast) or 224.0.0.1 (multicast)				
Type = 9	Code	Checksum		ICMP Router Advertisement [RFC 1256]
Num Addrs	Addr Entry Size	Lifetime (of this Advertisement)		
Router Address [1]				
Preference Level [1]				
Router Address [2]				
Preference Level [2]				
...				
Type = 16	Length	Sequence Number		Mobility Agent Advertisement Extension [RFC 2002]
(maximum) Registration Lifetime		R B H F M G V	Reserved	
Care-of-Address [1]				
Care-of-Address [2]				
...				

Fig. 2. Agent Advertisement Message

HA and FA broadcast or multicast Agent Advertisement Message constantly (Fig. 2) to monitor MN. When MN moves far from HN, it tries to catch the Agent Advertisement message, compares the IP inside message with its HoA to recognize where its is now, then it sends an Agent Solicitation Message (Fig. 3) to announce to the local router about its appearance and requires a CoA. If MN doesn't receive any Advertisement Message, it will broadcast Solicitation Message continuously to find out a Mobility Agent (HA or FA) and request the Agent to allocate to it's the Advertisement message immediately [9][12].



0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Vers=4	IHL	Type of Service	Total Length		IP Header [RFC 791]
Identification			Flags	Fragment Offset	
Time to Live = 1		Protocol=ICMP	Header Checksum		
Source Address = mobile node's home address					
Destination Address = 255.255.255.255 (broadcast) or 224.0.0.2 (multicast)					
Type = 10		Code = 0	Checksum		ICMP Router Solicitation [RFC 1256]
reserved					

Fig. 3. Agent Solicitation Message

Agent Registration:

When receives a CoA, MN must register this address to HA in order to HA can forward packets destined to MN exactly to MN. This process can be described as follow (Fig. 4):

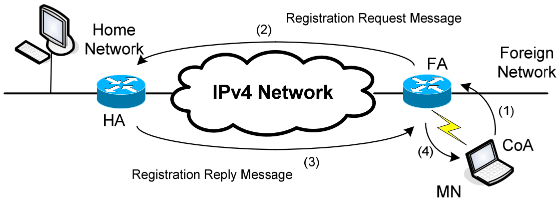
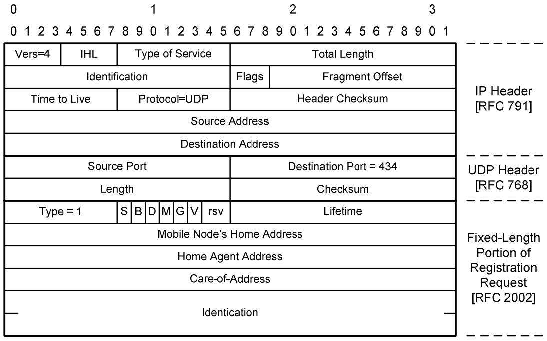


Fig. 4. CoA registration

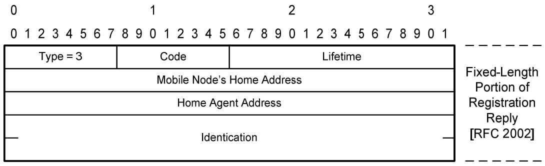
MN sends a Registration Request Message (Fig. 5) to HA via FA (1). If FA has not enough resource or this message is not suitable with the rights set up at FA, FA can discard the message. If the message is accepted by FA, it will be forwarded to HA (2). When HA receives the message, it updates the binding cache and sends a Registration Reply Message (Fig. 6) back to MN bypass HA (3). HA then forwards this message to MN (4) and the CoA registration process is completed and data transferring between MN and CN can be implemented.



0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Vers=4	IHL	Type of Service	Total Length		IP Header [RFC 791]
Identification			Flags	Fragment Offset	
Time to Live		Protocol=UDP	Header Checksum		
Source Address					
Destination Address					
Source Port			Destination Port = 434		UDP Header [RFC 768]
Length			Checksum		
Type = 1		S B D M G V rsv	Lifetime		Fixed-Length Portion of Registration Request [RFC 2002]
Mobile Node's Home Address					
Home Agent Address					
Care-of-Address					
Identication					

Fig. 5. Registration Request Message



0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Type = 3	Code	Lifetime	Fixed-Length Portion of Registration Reply [RFC 2002]
Mobile Node's Home Address			
Home Agent Address			
Identication			

Fig. 6. Registration Reply Message

Data Delivering:

In transferring data to MN, CN just needs to know MN's HoA and communicates with MN by this address. In the case that MN is at its HN, CN sends packets to MN's HoA and HA forwards these packets to MN directly. In other case, when MN is at FN, CN still sends data destined to MN to HA. Then HA encapsulates each of packets with MN's CoA and forwards them to MN's current address via FA (Fig. 7). When MN receives packets, it decapsulates them and gets the original data sent from CN. In this process, data transfer from CN to MN can be divided in 2 stages and HA is intermediate. A tunnel between HA and FA can be established to enhance the security and safety of data.

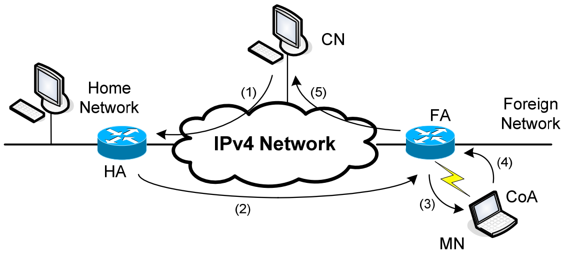


Fig. 7. Data delivering between CN and MN

III. Improvement in IPv6

Mobility support in IPv6 [11] is detailed in RFC 3775 [5]. This report gathers information from documents and briefly presents about Mobile IPv6 and its characteristics different from Mobile IPv4.

Differences between Mobile IPv6 and Mobile IPv4 [5]:

+ There is no need to deploy special routers as "Foreign Agents", as in Mobile IPv4. Mobile IPv6 operates in any location without any special support required from the local router.
+ Support for route optimization is a fundamental part of the protocol, rather than a nonstandard set of extensions.
+ Mobile IPv6 route optimization can operate securely even without pre-arranged security associations. It is expected that route optimization can be deployed on a global scale between all mobile nodes and correspondent nodes.
+ Support is also integrated into Mobile IPv6 for allowing route optimization to coexist efficiently with routers that perform "ingress filtering".
+ The IPv6 Neighbor Unreachability Detection assures symmetric reachability between the mobile node and its default router in the current location.
+ Most packets sent to a mobile node while away from home in Mobile IPv6 are sent using an IPv6 routing header rather than IP encapsulation, reducing the amount of resulting overhead compared to Mobile IPv4.
+ Mobile IPv6 is decoupled from any particular link layer, as it uses IPv6 Neighbor Discovery instead of ARP. This also improves the robustness of the protocol.

- The use of IPv6 encapsulation (and the routing header) removes the need in Mobile IPv6 to manage "tunnel soft state".
- The dynamic home agent address discovery mechanism in Mobile IPv6 returns a single reply to the mobile node. The directed broadcast approach used in IPv4 returns separate replies from each home agent.

Mobile IPv6 components are quite similar to Mobile IPv4. However, network devices' requirements in Mobile IPv6 differ from Mobile IPv4 and there isn't any FA in Mobile IPv6 network. All IPv6 routers and hosts contain Home Address option, manage a binding cache and can send Binding Acknowledgement to devices when required [7].

HA stores a binding for each MN in its Binding Cache, receives packets destined to MN in home link, encapsulates packets with MN's CoA and returns a Binding Ack Message when it gets a Binding Update message. HA also accepts anycast messages sent to it to support "Dynamic home agent address discovery".

MN in Mobile IPv6 must have ability of encapsulation and decapsulation packet received. MN manages a Binding Update List and sends Binding Update Message to HA and CN periodically or when it receives a Binding Update Request Message from HA or CN. It also has "Dynamic home agent address discovery" ability.

Mobility ability of Mobile IPv6 node is defined in extension headers of IPv6 packet (Fig. 8). Parameters of extension headers, especial in Message Data portion depend on type of message (defined in Type field).

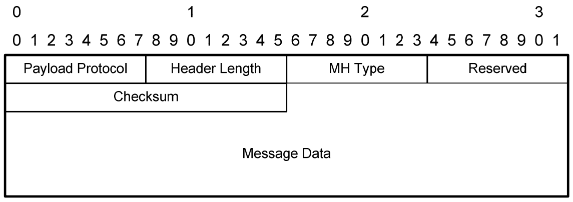


Fig. 8. Extension header of Mobile IPv6 packet

Mobile IPv6 Operations

Mobile IPv6 operations are quite similar to Mobile IPv4 and divided in 4 stages: *movement detection, CoA creation, CoA registration and data delivering*[2][3].

In CoA creation step, MN can configure its CoA automatically by using one of two methods: stateless or stateful. By default, MN uses stateless way. That means MN combines IPv6-prefix it received with its MAC address to create a new IPv6 address, different from other addresses. By using stateful method, MN sends a CoA Request Message to the local router and then this router allocates a new IPv6 address to MN by using DHCPv6.

MN's CoA used in IPv6 network is called Colocated CoA because there is no FA and MN can encapsulate, decapsulate packets or connect to HA and other nodes directly without intermediate router as FA in Mobile IPv4.

There are two ways to send data from CN to MN (Fig. 9). First, CN sends data to MN indirectly via HA. In this method, a bidirectional tunnel between HA and MN may be established to enhance security level. This method increases delay and gains bandwidth of HA-MN connection. Second, route optimization mechanism is used and data are sent directly between CN and MN. This mechanism is defined in IPv6 packet header as a portion of protocol and is an advanced characteristic of Mobile IPv6 in comparison with Mobile IPv4.

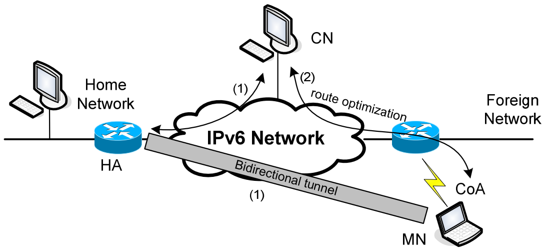


Fig. 9. Data delivering between CN and MN in Mobile IPv6

CN and HA send Binding Refresh Request Message to MN periodically to require updates for their Binding Cache. MN also sends Binding Update Messages to CN and HA constantly. If an error occurs, a Binding Error Message will be sent.

In case MN's new network is HN (MN return home), it will send a Binding Update Message to HA with lifetime=0 and CoA=MN's HoA. When receiving this message, HA updates its Binding Cache and stops the proxy role in HN. Then, HA sends a Binding Ack Message to MN and announce to nodes in HN to send data directly to MN without passing HA.

IV. Deployment in MPLS network

MPLS routers classify data packets base on QoS requirement and send those packets to destination via Label Switching Path (LSP) established. By using label switching mechanism and routing independent on IP layer of MPLS, Mobile IPv6 can be implemented on MPLS core network [8][10]. Traffic management and flow control in MPLS can enhance communication performance among mobile nodes and guarantee the best QoS for end users.

After being classified by QoS requirements, packets are arranged in queues and routed to destination on available LSPs. Routers in core network forward packets in flows after determining resources reserved for them. Edge routers which support Mobile IP have a Label Information Base (LIB) table and an IP Routing table.

In MPLS network supporting Mobile IPV6, there isn't any Label Edge Router with the role of FA (LER/FA) because Mobile IPv6 nodes used CCoA instead of FA's CoA.

Registration procedure in single domain (Fig. 10):

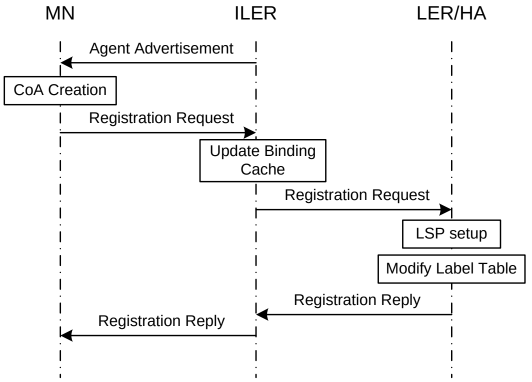


Fig. 10. Registration procedure in single MPLS domain

Label Edge Routers (LER) broadcast Router Advertisements Message continuously to monitor the movement of MNs. When MN moves from network to network and receives this advertisement message, it analyses IP-prefix included in the message received and recognizes where it is. If it is far from home network, it creates a CCoA by using stateless or stateful mechanism and then registers this address to LER/HA via Ingress LER (ILER).

ILER updates its Binding Cache, adds a new entry with MN's HoA, set out port's value equal to in port's value and out label's value be null. Then, it forwards Registration Request Message to HA by using IP routing mechanism.

If LER/HA receives Registration Request message, it updates CoA to Binding Cache, checks Label Forward Information Base (LFIB) table to find MN's HoA and considers packets sent to MN's CoA as a Forward Equivalence Class (FEC). Then, value of out label and out port to MN is set to be null.

LER/HA sends a Label Request Message to ILER using Label Distribution Protocol (LDP). ILER replies a LDP label mapping message to LER/HA. If LER/HA receives this message, a LSP will be established and out label and out port to MN is set by out label and out port to ILER by LER/HA.

Finally, LER/HA sends a Registration Reply Message to MN via ILER.

Delivering datagram in a single domain (Fig. 11)

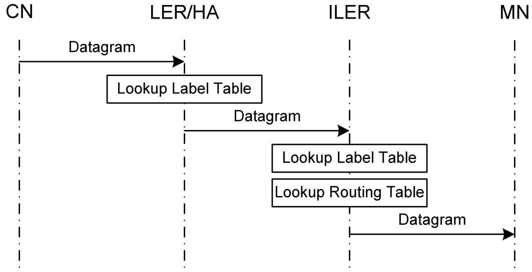


Fig. 11. Deliver datagram in a single domain.

Destination address of packets sent from CN to MN is set by MN's HoA and these packets are caught by LER/HA. LER/HA finds packets' in-label and in-port in is LFIB, maps new labels and forward them to MN. If MN is still at its HN, these packets' out-labels are set null and striped out before sending to IP layer and routing to MN.

In case MN is at HN, packets from LER/HA are routed to ILER on an established LSP by label exchange mechanism.

ILER receives packets, looks in its LFIB and recognizes that out-labels of packets received are null because they are sent from LER/HA. ILER strips labels and forwards them to IP layer. Packets then are sent directly to MN.

MN returns home in single domain:

When receiving a Router Advertisement Message of LER/HA, MN realizes that it is at home network. Then it sends a Registration Request Message to LER/HA with the field lifetime=0 and CoA=MN's HoA.

After receiving MN's Registration Request Message, LER/HA removes out-label and out-port entry of MN maintained in its LFIB.

Packets destined to MN's HoA are sent to LER/HA, stripped labels, forwarded to IP layer and routed directly to MN by using IP routing mechanism.

Implementation in case of many MPLS domains (Fig. 12):

Single domains in MPLS are connected by Label Edge Routers which support both MPLS and Mobile IP and routing between two single domains is implemented by routing protocols used on these routers, such as LDP Border Gateway Protocol (BGP). This means a router in a single MPLS domain can communicate with another one in another single MPLS domain by using label switching mechanism. So, registration procedure, LSP establishment between ILER and LER/HA and datagram delivering process in many MPLS domains can be done as the case of implementation in a single domain.

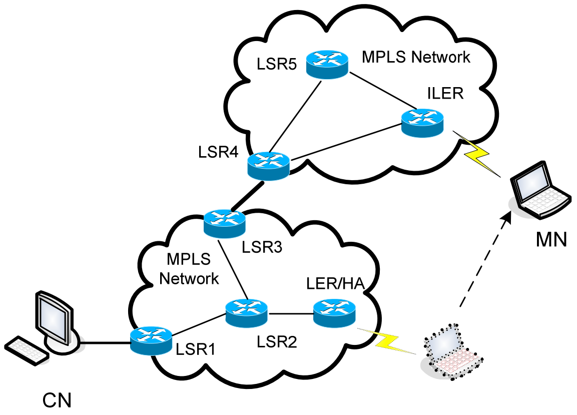


Fig. 12. Implementation in many MPLS domains

By the implementation of Mobile IP on MPLS network, there is no need of IP-in-IP tunneling mechanisms. Label switching technique is used and label switching process performs at MPLS layer, independent on IP layer. This mechanism enhances many services developed on IP layer. In addition, label size in bits is much smaller than IP header, thus, header's traffic from LER/HA to ILER is low. LDP or RSVP in MPLS makes it easier to satisfy QoS and flow control.

Tunneling mechanisms:

Tunneling mechanisms used by Mobile IPv6 nodes in MPLS network support route optimization, utilize network resources effectively and guarantee quality of services.

Tunneling for route optimization (Fig. 13):

After a LSP is established between LER/HA and ILER, data delivering process between CN and MN is executed. When LER/HA receives a packet sent from CN to MN, it sends a Binding Update Message back to CN to announce about MN's recent position. Then, a new tunnel is established between CN's LER and ILER. CN now can send data directly to MN without passing LER/HA. This tunnel replaces triangle-routing, decreases delay and utilizes bandwidth better than the case of bypassing LER/HA.

Binding Update procedures:

After MN register its CoA to LER/HA, Binding Update processes are performed to keep communications between MN and other nodes. By using Binding Update Messages, a tunnel between Ingress LER and Egress LER is established to optimize LSPs.

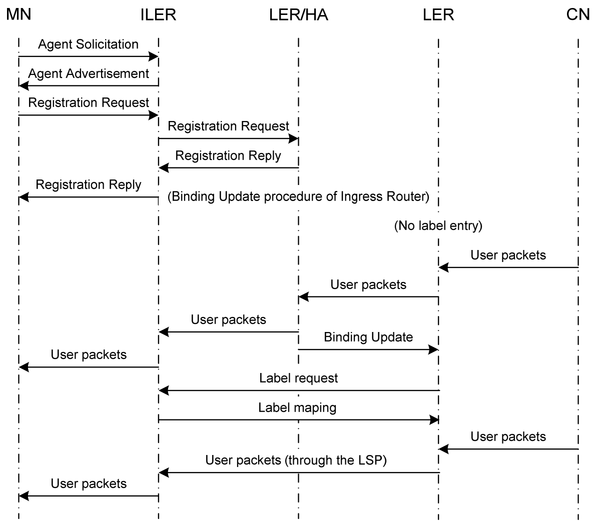


Fig. 13. LSP establishment procedures for route optimization

In case MN sets up a communication session (Fig. 14a), it sends a Binding Update Message with QoS requirement to CN. ILER receives this message, forwards it to CN, decides to initiate a request/path message and sends it to ELER. Then, a new LSP is established between ILER and ELER and data can be transferred on this tunnel.

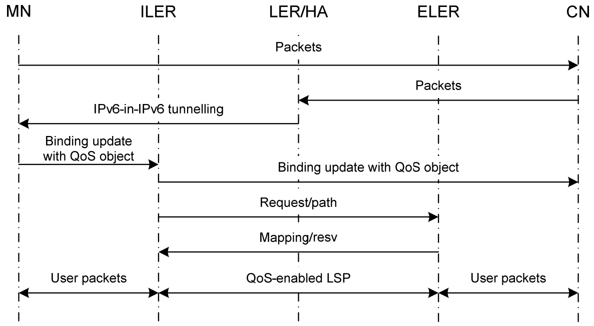


Fig. 14a. Binding Update procedures with QoS in case MN sets up a communication session.

Incase CN sets up a communication session (Fig. 14b), it sends data packets to MN via LER/HA after updating MN's HoA to its binding cache. LER/HA encapsulates IPv6-in-IPv6 and forwards packets to MN. MN decapsulates packets, gets CN's IPv6 address and sends a Binding Update Message to CN. When ELER receives this Binding Update Message, it initiates a signaling procedure to set up a LSP between ILER and ELER.

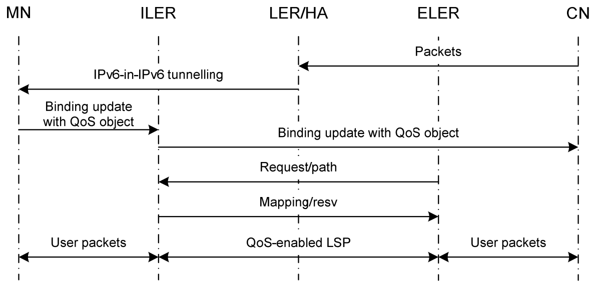


Fig. 14b. Binding Update procedures with QoS in case CN sets up a communication session.

Hierarchical tunnel establishment (Fig. 15)

In hierarchical tunneling mechanism, MN is managed in levels and the path from LER/HA to MN is divided in three hops: LER/HA to Gateway LSR (G-LSR), G-LSR to Region LSR (R-LSR) and R-LSR to MN. In this method, the path from LER/HA to MN is changed a little when MN moves from network to network. So, delay in this path is reduced.

If MN migrates between two networks managed by one R-LSR, the tunnel from LER/HA to G-LSR and the tunnel from G-LSR to R-LSR will be unchanged. In another case, if MN moves between networks managed by different R-LSRs but the same G-LSR, the tunnel from R-LSR to MN will be changed but the tunnel from LER/HA to G-LSR will be unchanged. This mechanism provides calm switching when MN moves in regions.

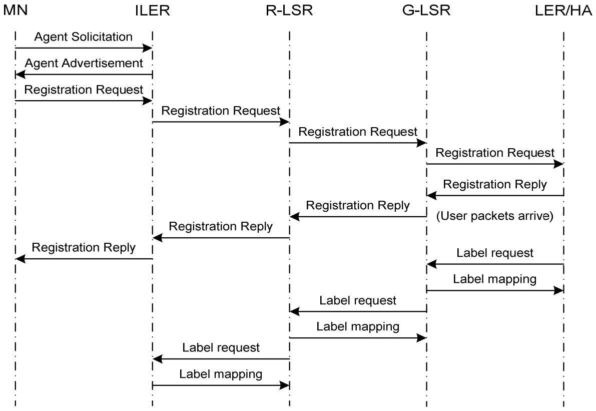


Fig. 15. Hierarchical tunnel establishment procedures

V. Trends of mobile IP's mechanisms

By researches, an IPv6 node can connect to another one through IPv4 network by using Dual-stack routers and tunneling mechanism or IP-in-IP encapsulation technique (Fig. 16). It even can make a link through MPLS core network by mapping labels and setting up LSP (Fig. 17). It can also use network address translation (NAT) mechanisms or virtual private network (VPN) to communicate with others.

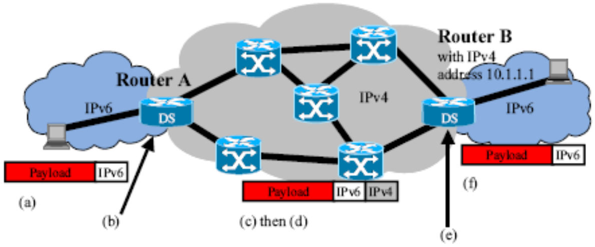


Fig. 16. IPv6 connections through IPv4 core network using Dual Stack routers and IP-in-IP encapsulation technique

The Cisco Systems has designed and developed some types of routers that support IPv4, IPv6 and MPLS such as provider edge (PE) routers or VPN provider edge (VPE) routers [1][6]. All of them create an environment on which IPv4 nodes can connect to other IPv4 nodes, IPv6 nodes can connect to other IPv6 nodes or few of IPv6 nodes can connect to IPv4 nodes. However, there is no solution for mobile IP nodes.

As concerned above, a mobile IPv6 node can keep communication with other IPv6 nodes when migrating in IPv6 network. But it hasn't connected to another mobile IPv4 node yet. There are a lot of limit and difficulty when deploy a real IPv6-and-IPv4 network. It is harder to create and keep connection between mobile IPv4 and mobile IPv6 node. Solutions are researched, discussed and simulated [4][13][14]. So, it is said that the trend of mobile IP mechanisms is solving the problem: How can a mobile IPv6 connect and keep communication with an IPv4 node while moving from network to network and vice versa?

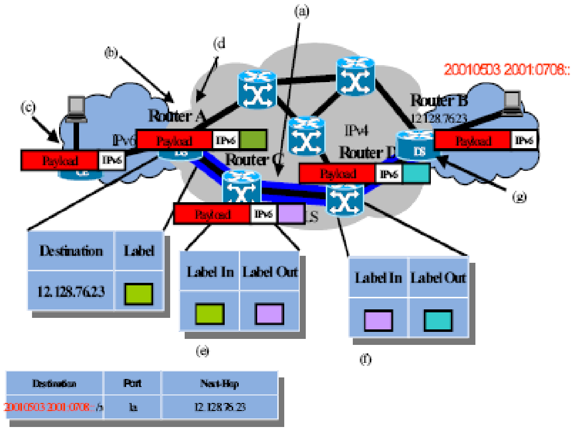


Fig. 17. IPv6 connections through MPLS core network, using label mapping technique

VI. Conclusion

Mobile IPv4 and mobile IPv6 can perform separately with high performance. However, when co-exist, they make many troubles. Mobile IPv6 can be deployed on MPLS core network with reliable data transfer procedures. Advanced mechanisms of MPLS such as traffic management and flow control guarantee QoS requirements of IPv6 end users. Because label switching routers map labels and switch datagram at layer two which is independent on IP layer, many IP-based services can be developed on MPLS network. Many researches about transferring data between IPv4 nodes and IPv6 nodes rely on these features of MPLS. Some acceptable solutions are proposed such as using dual-stacks routers, virtual private networks (VPN) and network address translation (NAT). The next step of these researches is bringing out solutions of transferring data between mobile IPv4 nodes and mobile IPv6 nodes on MPLS core network to prepare for the replacement of IPv4 devices by IPv6 devices in future.

REFERENCES

[1] J. DeClercq, D. Oooms, S. Prevost, F. Le Faucheur, "Connecting IPv6 Islands over IPv4 MPLS using IPv6 Provider Edge Routers (6PE)", IETF Internet Draft, Work in Progress.

[2] [RFC 4213] "Basic Transition Mechanisms for IPv6 Hosts and Routers", 2005.

[3] [RFC 3750] *"Unmanaged Networks IPv6 Transition Scenarios"*, 2004.

[4] Defeng Li, *"BGP-MPLS VPN extension for IPv4/IPv6 Hybrid Network"*, Internet Draft, 2004

[5] [RFC 3775] *"Mobility support in IPv6"*, 2004.

[6] Cisco Systems, Inc, *"IPv6 over MPLS : IPv6 provider edge router and IPv6 VPN provider edge router"*, 2004.

[7] Microsoft Corporation, *"Understanding mobile IPv6"*, 2004.

[8] J. K. Choi, M. H. Kim, Y. J. Lee, *"Mobile IPv6 support in MPLS Network"*, Internet Draft, 2002.

[9] [RFC 3344] *"IP Mobility support for IPv4"*, 2002.

[10] Uyless Black, *"MPLS and Label Switching Networks"*, PTR Prentice Hall, 2002.

[11] [RFC 2460] *"Internet Protocol, Version 6 (IPv6) Specification"*, 1998.

[12] James D. Solomon, *"Mobile IP – the Internet Unplugged"*, PTR Prentice Hall, Upper Saddle River, New Jersey, 1998.

[13] Thierry Ernst, "MobiWan: NS-2 extensions to study mobility in Wide-Area IPv6 Networks", Motorola Lab (http://www.inrialpes.fr/planete/mobiwan/), 2001.

[14] The Network Simulator – ns – 2 – http://www.isi.edu/nsnam/ns/

NGUYEN NGOC CHAN, born in Vietnam in 1982

He received B.E of Information Technology from Post and Telecommunication Institute of Technology (PTIT), campus in Hochiminh City, Vietnam, 2005.

He got the second prized in Scientific Research Movement of PTIT in 2003 and graduated with the thesis "Solving multi-variable problems by using a parallel processing system"

His main fields are: parallel processing, distributed computing, MPLS

He is a senior lecturer of Faculty of Information Technology of PTIT, campus in Hochminh City, Vietnam

TRAN CONG HUNG was born in VietNam in 1961

He received the B.E in electronic and Telecommunication engineering with first class honors from HOCHIMINH university of technology in VietNam, 1987.

He received the B.E in informatics and computer engineering from HOCHIMINH university of technology in VietNam, 1995.

He received the master of engineering degree in telecommunications engineering course from postgraduate department HaNoi university of technology in VietNam, 1998.

He received Ph.D at HaNoi university of technology in VietNam, 2004.

His main research areas are B – ISDN performance parameters and measuring methods, QoS in high speed networks, MPLS.

Currently, he is a lecturer, deputy head of Faculty of Information Technology II and head of section Network & Data Transmission in Posts and Telecoms Institute of Technology (PTIT), in HOCHIMINH City, VietNam.