Chapter 13

Quality of Service Support for MPLS-based Wired-Wireless Domains

13.1. Abstract

Wireless technologies have experienced an explosive growth in recent years. This trend is clear from the emergence of various wireless devices such as Personal Digital Assistants (PDAs), wireless computer, and cellular phones. Wireless networks have also been proliferating at a rapid pace in our society and are increasingly being used as extensions to the wired Internet infrastructure to allow ubiquitous service access, anywhere, anytime. These networking developments have also been paving the way for a plethora of applications (such as those involving audio and video) many of which have stringent Quality of Service (QoS) requirements (bandwidth, delay, loss) that must be satisfied. However, there still remains a significant challenge to provide QoS solutions that operate seamlessly over wired-wireless domains and maintain end-to-end QoS with user mobility. The advent of MPLS technology promises to address some of these QoS challenges. We present and discuss various MPLS-based approaches that have recently been proposed for the support of QoS over wired networks connected to wireless networks (as the last hop). We highlight and discuss the effectiveness and benefits of each of the approaches in minimizing end-to-end QoS degradations (for example, due to large handover delays) when deployed over wired-wireless domains for mobile users. Additionally, we present the limitations associated with each of the MPLS-based approaches proposed.

Chapter written by Scott FOWLER, Sherali ZEADALLY and Abdelhamid MELLOUK.

13.2. Introduction

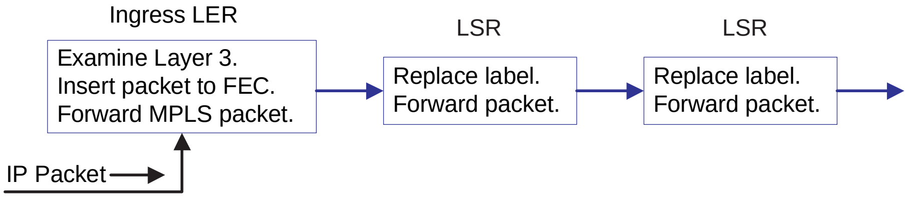
Wireless technology is a fast growing industry. This trend is clear from the emergence of various wireless, portable devices such as Personal Digital Assistants (PDAs), laptops and cellular phones. With the development of wireless technology, wireless networks have become an integral part of wired networks. To meet the increasing demand for mobile services, wireless providers are currently implementing third generation (3G) and fourth generation (4G) [VAS 03, CHI 02a] networking technologies that are heavily based on the Internet Protocol (IP). To support mobile applications, Mobile IP (MIP) [PER 02] was developed. MIP provides seamless mobility when a Mobile Node (MN) moves across IP subnets. However, MIP was not designed to support fast handovers and seamless mobility in a handover-intensive environment. With the rapid proliferation of wireless networks, the cell radius continues to decrease [VAS 03, CHI 02a]. Smaller cells result in more handovers from one cell to another cell, because of frequent registration updates. To reduce the signaling load that results from frequent MIP registration messages when the MN is far away from the Home Agent (HA), a hierarchical registration (otherwise called IP Micro-Mobility Protocols) [CAM 01] has been proposed to enhance the basic MIP.

Multimedia support over networks has been extensively studied over the last decade. Several QoS approaches and protocols have been proposed and implemented. However, very few of these proposed approaches have been incorporated into commercial products. Consequently, these techniques have not been widely deployed. However, one of the latest traffic engineering technologies capable of providing QoS that has gained wide acceptance over the last few years is Multi-Protocol Label Switching (MPLS), which is supported by many commercial switches and routers on the market. In high speed wired networking environments, MPLS is deployed in the Internet backbone to support service differentiation and traffic engineering [XIA 00, FAU 02, NOR 01]. In MPLS, the packet forwarding process is accomplished by means of label swapping. Since labels are short and have fixed length, MPLS can achieve high efficiency compared to conventional IP routing where longest prefix matching is used.

13.3. MPLS technology

MPLS introduces a new forwarding approach (similar to ATM) to IP networks. MPLS is not a routing protocol, but is a fast forwarding mechanism designed to work with Internet routing protocols such as Open Shortest Path First (OSPF) or the Border Gateway Protocol (BGP). In traditional network layer routing, when a router receives a packet it makes an independent forwarding decision for that packet. Each router analyzes the packet's header and performs a routing table lookup to determine the next packet hop by parsing the IP address. In MPLS, packets are assigned a

Forwarding Equivalence Class (FEC) at the ingress[1] router (known as Label Edge Router (LER)) located at the edge of the MPLS domain. The FEC is assigned an IP packet depending on a number of attributes, including the address prefix in the packet's header, the destination address or the port the packet arrived at. However, a packet is only assigned to a FEC only once, as the packet enters the MPLS domain. The FEC to which the packet belongs is assured by a label which is sent with the packet to the next hop. The intermediate routers receiving this packet are called label switching routers (LSRs). The LSRs which receive this packet do not examine the network layer header. The label is used as an index in a table specifying the next hop and a new label replaces the old incoming label (Figure 13.1). Fundamentally, MPLS [MET 01, XIA 00, ROS 01b] can be thought of as an advanced forwarding scheme. In MPLS, each packet is assigned a short, fixed-length label. MPLS takes advantage of the intelligence in routers and switch speed to improve the mapping of IP packets onto a connection-oriented mechanism. MPLS also supports a QoS definition within the MPLS header and uses layer-3 routing information to establish routing tables. Layer-2 header information is used to forward packets over a path. Using these features, MPLS supports the delivery of QoS to end-users. As mentioned earlier, MPLS was designed to take advantage of the high efficiency of ATM switching in IP routers. The MPLS forwarding algorithm analyzes the IP packet header once, at the ingress of the MPLS domain, by an label edge router (LER). Once a packet has been assigned to a FEC, packet forwarding can be performed solely on the labels used by the underlying label switched path (LSP) established.



FEC: Forwarding Equivalence Class
IP: Internet Protocol
LER: Label Edge Router
LSR: Label Switching Routers
MPLS: Multi-Protocol Label Switching

Figure 13.1. *MPLS forwarding*

---

[1] Ingress: the entry point of the MPLS domain.

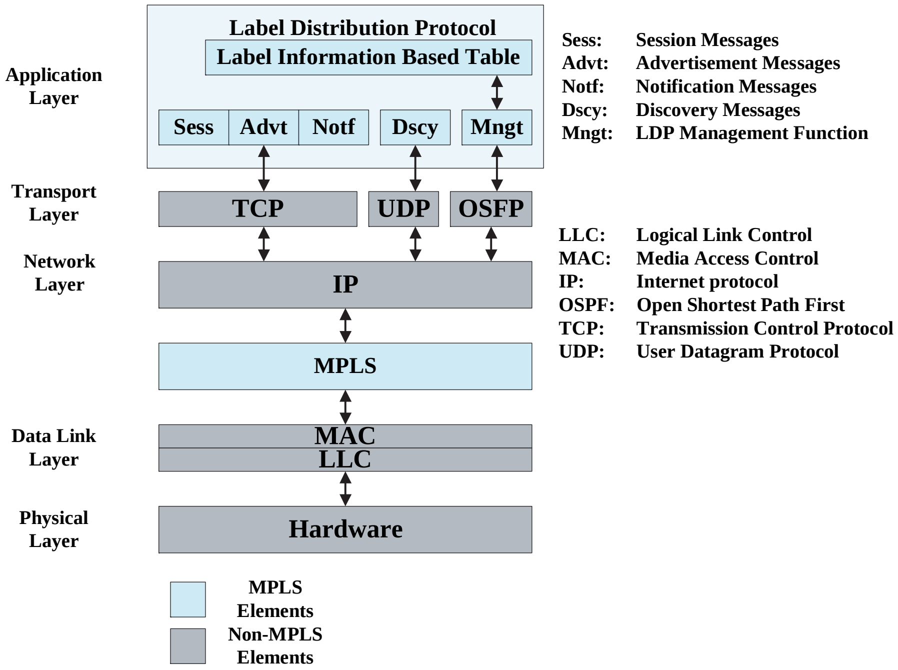


Figure 13.2. *MPLS protocol components in relation to IP*

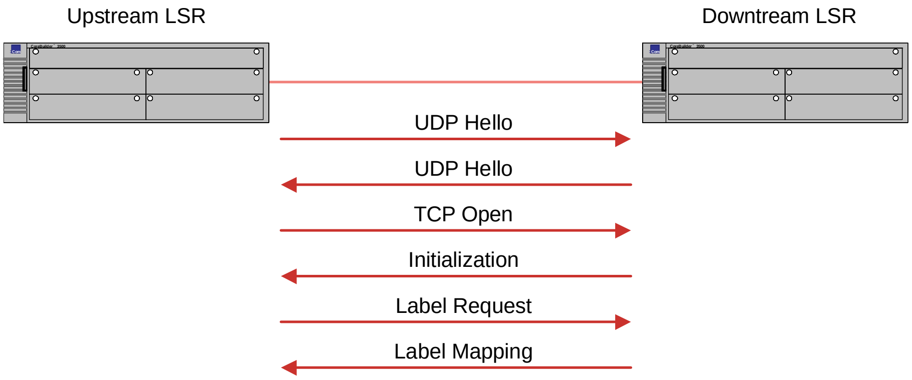
13.3.1. *Label distribution protocol (LDP)*

For an LSR to perform label switching so that the packet can be forwarded to the next LSR, the LSR must have knowledge of the label value expected at the next LSR. To achieve this, a set of signaling protocols called the label distribution protocol (LDP) is used. LDP is used to establish LSPs through a network by mapping network layer routing information directly to the data link layer for switched paths. LDP distributes the routing information among LSRs and label binding procedures used for updating the routing information (required to perform label switching) stored in the forwarding tables (Figure 13.2).

LDP discovery is a mechanism used to discover possible LDP peers[2]. The LDP discovery scheme uses four categories of LDP messages shown in Figure 13.3 [WU 01]:

---

[2] Two LSRs exchanging binding information between them.



LSR: Label Switching Router
TCP: Transmission Control Protocol
UDP: User Datagram Protocol

Figure 13.3. *LDP discovery procedures*

– discovery messages: used to inform and maintain the existence of an LSR;

– session messages: used to establish, maintain, and terminate a session between LDP peers;

– advertisement messages: used to create, modify, and remove label mappings;

– notification messages: used to provide advisory status and error notification.

Using discovery messages, LSRs announce their presence in the network by sending *hello* messages periodically. A *hello* message is transmitted as a UDP packet to all LDP ports at the “all routers on this subnet” group multicast address (i.e. IP address 141.127.0.0). A *hello* message holds the LDP identifier for the label space that the LSR intends to use for the interface. When an LSR sets up a new session with another LSR via the *hello* message, the *hello* message is sent over TCP to initialize the setting up of a session. When an LSR needs a label mapping from its peer LSR, an *advertisement* message for a label request is sent out, and a label mapping is sent back. Accurate LDP procedures depend on the reliable delivery of messages and this can be accomplished using TCP [AND 01].

Currently, several protocols can be used to distribute labels between LSRs including LDP, the Constraint Based Routed Label Distribution Protocol (CR-LDP), and the Resource Reservation Protocol (RSVP). The protocol used for label distribution depends on the underlying network requirements. For instance, if faster packet forwarding is required, LDP can be used to meet the needs of the end-user. However, as more LSPs are built, if stricter QoS requirements are needed, LDP alone cannot deliver such QoS support. To support QoS applications, LDP must be able to properly select and reserve network resources along an LSP. This may be accomplished by using a protocol that can resource reservations and extend label distribution, or to use a protocol that can be used for label distribution and extends it to support resource reservation. An example of a protocol that already supports this type of reservation is the RSVP. As mentioned earlier, LDP alone cannot support strict QoS requirements, so LDP has been extended to support CR-LDP [ASH 02a, JAM 02] which we discuss in more detail below.

13.4. Mobility and MPLS

MIP was designed to provide mobility support at the IP layer and to protect higher layers from terminal mobility. At the IP layer, the IP routing mechanism remains unchanged. Two IP addresses are used in MIP: (1) a MN owns an IP address in its home network, and (2) the MN is also assigned a temporary Care of Address (CoA) while in a foreign network. A Correspondent Node (CN) addresses the MN via its home IP address. MIP introduces two elements to the network: the Home Agent (HA) and the Foreign Agent (FA). Routing is performed by address translation and IP-in-IP address tunneling. If a CN wants to send packets to the MN, packets are first delivered to the home IP address via normal IP forwarding. The HA intercepts the packets and encapsulates the packets using IP-in-IP tunneling and forwards the packets to the FA. The FA decapsulates the packets and forwards them to the MIP host via normal IP forwarding. The whole process is illustrated in Figure 13.4. When the MN communicates with the CN, packets are forwarded to the CN directly without forwarding to the HA first.

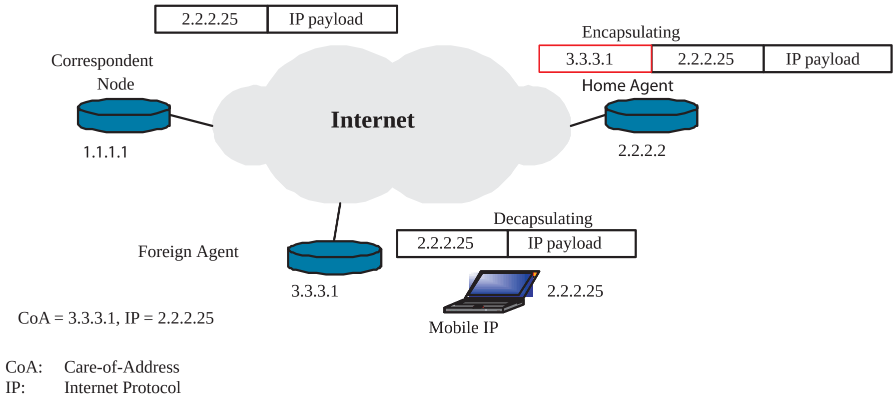


Figure 13.4. *Mobile IP packet forwarding*

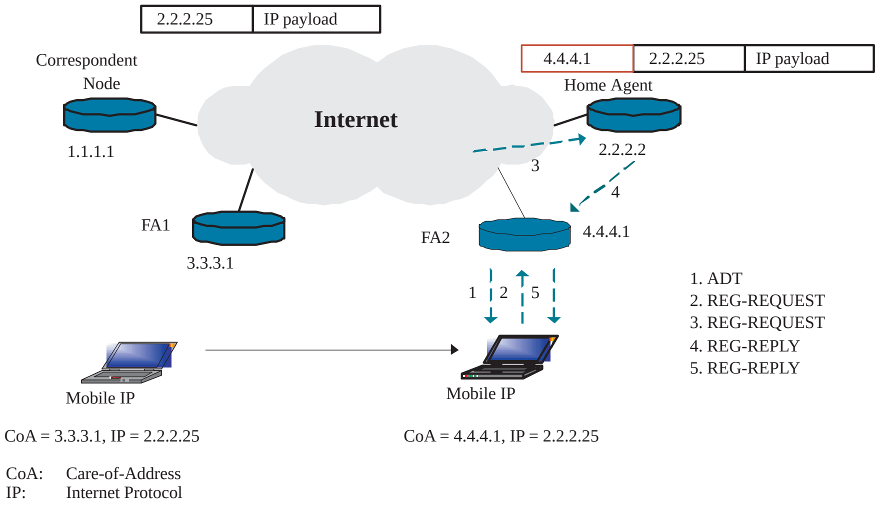


Figure 13.5. *Mobile IP handover*

In MIP, the FA periodically broadcasts MIP Advertisement (ADT) messages to indicate its presence (step 1 in Figure 13.5). When a MN discovers that it has relocated to a different IP subnet and has received a new CoA from the new FA, the MN registers its new CoA with the new FA via a MIP Registration Request (REG-REQUEST) message (step 2 in Figure 13.5). Next, the new FA passes on this new Registration Request to the HA. This allows for the binding between the MN's IP home address and the CoA (step 3 in Figure 13.5). The HA sends a MIP Registration Reply (REG-REPLY) message to the FA (step 4 in Figure 13.5) which forwards it to the MN (step 5 in Figure 13.5). All packets are subsequently delivered to this new CoA. The whole process is illustrated in Figure 13.5.

Several solutions have been proposed to overcome some of the performance limitations of the MIP handover process. One such performance bottleneck occurs when the MN is located far way from the HA, the amount of signaling traffic load (as a result of frequent registrations) increases since changing to a new FA every time requires a MIP registration, even when the handover occurs locally. To reduce the signaling traffic load, hierarchical MIP [CAM 01, GUS 04] (otherwise called IP micro-mobility protocols) has been proposed. In fact, many solutions have been proposed that transform the macro-mobility MIP network into a hierarchical structure creating a micro-mobility network.

13.5. Hierarchical MIP

To reduce the amount of signaling load that results from frequent MIP registration messages when the MN changes its FA, and to decrease the amount of signaling

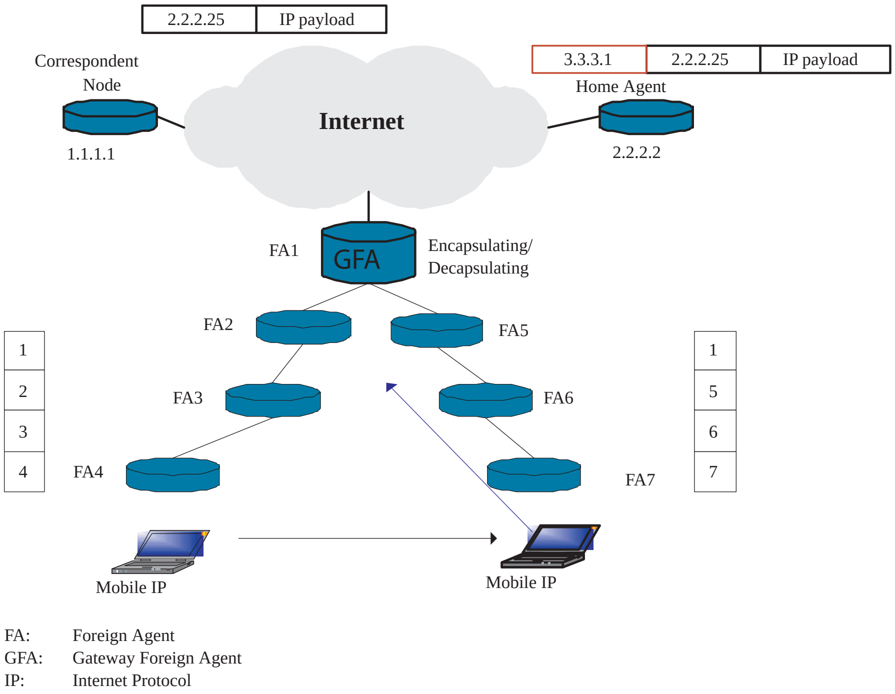


Figure 13.6. *Hierarchical mobile IP regional registration*

from the HA, regional registration [CAM 01, OMA 03, GUS 04] has been proposed to enhance basic MIP. The idea is that hierarchical FAs do not allow the MN in sending MIP registration messages to the HA each time it changes its local attachment point. When a MN first arrives at a foreign network, it performs a MIP home registration (i.e. registration with its HA). During the home registration, the HA registers the CoA of the MN. If the foreign network supports regional registration (hierarchical MIP), the CoA registered with the HA is the routable address of a Gateway Foreign Agent (GFA). This CoA does not change when the MN changes FA under the same GFA. Only when the MN changes GFA does the MN perform a home registration again. When a MN changes FA under the same GFA, the MN performs a regional registration within the visited domain. At each level, a regional foreign agent (RFA) is introduced. The lowest level regional foreign agent announces the RFA hierarchy in its MIP advertisement message. From this advertisement message, the MN knows where it should send the local registration. Figure 13.6 illustrates hierarchical MIP regional registration that occurs when the MN node moves from FA4 to FA7.

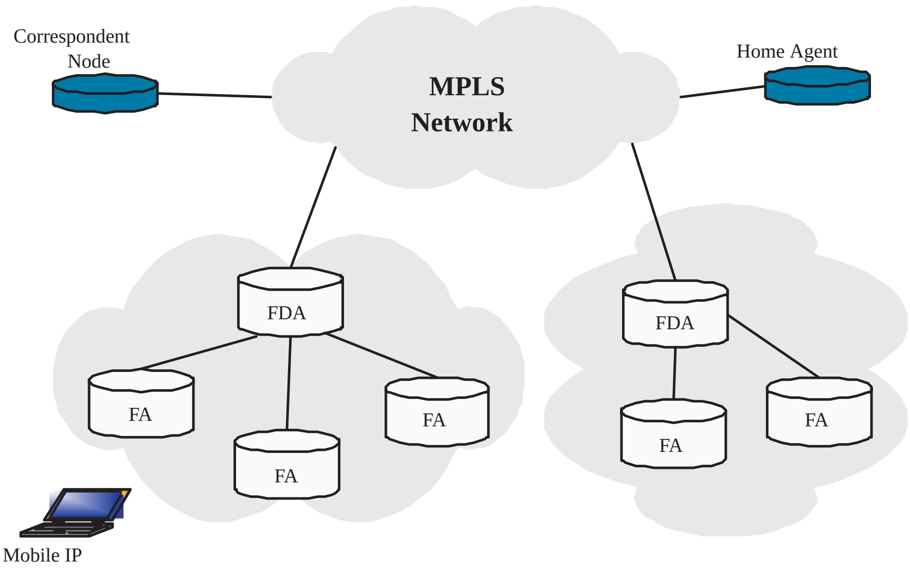
When a CN sends packets to the MN, the packets are first directed to the HA. The HA routes the packets to the GFA. The GFA decapsulates the packets, and then re-encapsulates and routes them to the next regional FA. At each regional FA, packets en-route to a MN are decapsulated and re-encapsulated. As for the lowest level regional FA, packets are simply decapsulated and forwarded to the MN via normal IP routing.

13.6. Extending MPLS from wired networks to wireless networks

We continue to experience explosive growth in wireless networks and the trend is expected to continue at a rapid pace well into the future. Today's wireless networks often extend wired infrastructure to locations that were previously unreachable. Wireless network users often use the wireless link as a last hop when communicating with other hosts residing on the wired Internet. To enable end-to-end QoS spanning both the wired and wireless infrastructure, there has been a growing interest [TAH 05, PAL 05, GUO 02] in the use of MPLS technology over wireless domains as well. Some of the recent approaches proposed to enable MPLS to work over wired-wireless connections include hierarchical mobile MPLS (H-MPLS) [YAN 01], Micro-Mobility with MPLS (MM-MPLS) [YAN 02a], and label edge mobility agent (LEMA) [CHI 02b, CHI 02a] which we discuss below.

13.6.1. *Hierarchical mobile MPLS (H-MPLS) approach*

In the case of conventional mobile MPLS, whenever a MN moves from one FA to another, a new registration message is sent from the FA to the HA. As mentioned in the previous section, this re-registration process increases in latency and traffic load with each handover. As a result, simply using MPLS in conjunction with MIP is not an efficient solution [JAM 02] for mobile users with MPLS. For such wired-wireless networking environments, to minimize frequent registration handover delays incurred in establishing an LSP, the hierarchical mobile MPLS (H-MPLS) [VAS 03, CHI 02a, YAN 01, SET 04] was proposed. With H-MPLS, instead of using a GFA (as in hierarchical mobile IP), a foreign domain agent (FDA) was introduced. The FDA reduces the signaling load that results from frequent MIP registration messages (when the MN changes the FA) and also decreases the amount of signaling from the HA (as in Hierarchical MIP). In the H-MPLS approach, the LSP between the HA and the regional FDA is unaffected when the MN moves. When the MN performs a handover to another FA, a new LSP is created between the new FA and the FDA. Thus, only the FDA and the FA will be affected (Figure 13.7). Consequently, there is decrease in the delay when re-establishing a new path while the MN roams in a regional subnet [YAN 01, YAN 02b].



FA:	Foreign Agent
FDA:	Foreign Domain Agent
MPLS:	Multi-Protocol Label Switching

Figure 13.7. *Hierarchical mobile MPLS*

13.6.1.1. *MN registration procedure*

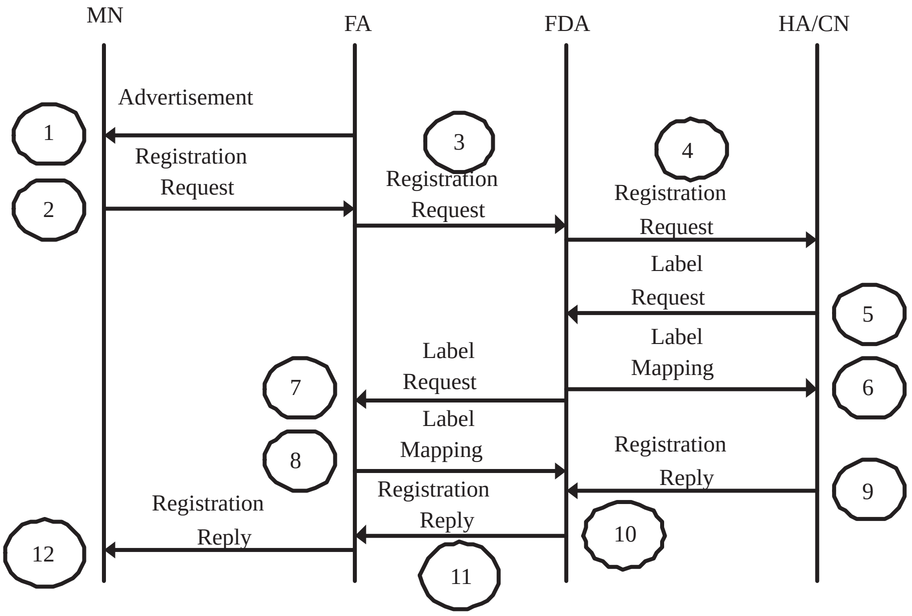
In H-MPLS-based networks, the MIP registration protocol can be used to set up an LSP for the MN. The FA periodically broadcasts MIP advertisement messages to all MNs. Upon receipt of an advertisement message, the following steps are followed (Figure 13.8):

1) For an H-MPLS-based network, the MN determines whether it is in the home domain or in a foreign domain when it receives advertisement messages broadcast by the FA.

2) The MN acquires a temporary CoA from the FA and sends a Registration Request to the FA.

3) The FA forwards this Registration Request to the FDA (traditionally, the Registration Request would be forwarded to the HA).

4) The FDA then forwards this Registration Request to the HA.



CN:	Correspondent Node
FA:	Foreign Agent
FDA:	Foreign Domain Agent
HA:	Home Agent
MN:	Mobile Node

Figure 13.8. *MN first register in H-MPLS*

5) When the HA receives the Registration Request and knows the IP address of the FDA, the HA sends a Label Request using the LDP protocol to the FDA with the IP address of the FDA as the FEC[3].

6) The FDA replies with an LDP Label Mapping message back to the HA, resulting in the establishment of an LSP from the HA to the FDA.

7) The FDA sends a Label Request to the FA of the sub-network where the MN is currently located.

---

3. The FEC is a set of packets which will be forwarded in the same manner on an LSP (e.g., over the same path with the same forwarding treatment).

8) The FA replies with an LDP Label Mapping message back to the FDA. When this message arrives at the FDA, the LSP from the FDA to the FA is established.

9) The HA searches the label table until it finds the MN's home address when it changes the outgoing port and outgoing label to the same values as those for the LSP from the HA to the FDA. Next, the HA sends a Registration Reply to the FDA along the LSP from HA to the FDA.

10) The FDA forwards this Registration Reply to the FA along the LSP from the FDA to the FA.

11) When the FA receives the Registration Reply, it puts the incoming Registration Reply's label value and port number into the "In label field" and "incoming port field" of the table.

12) The FA sends a Registration Reply back to the MN.

13.6.1.2. *MN handover procedure*

When a MN performs a handover from one FA to another within the same foreign domain, the new FA station informs the FDA, via the MIP registration request message, using the following steps (Figure 13.9):

1) The MN determines whether to perform a handover to a new FA based on advertisements from the new FA.

2) When the MN makes a handover from one sub-network to another sub-network within the same foreign domain, it sends a Registration Request to the new FA.

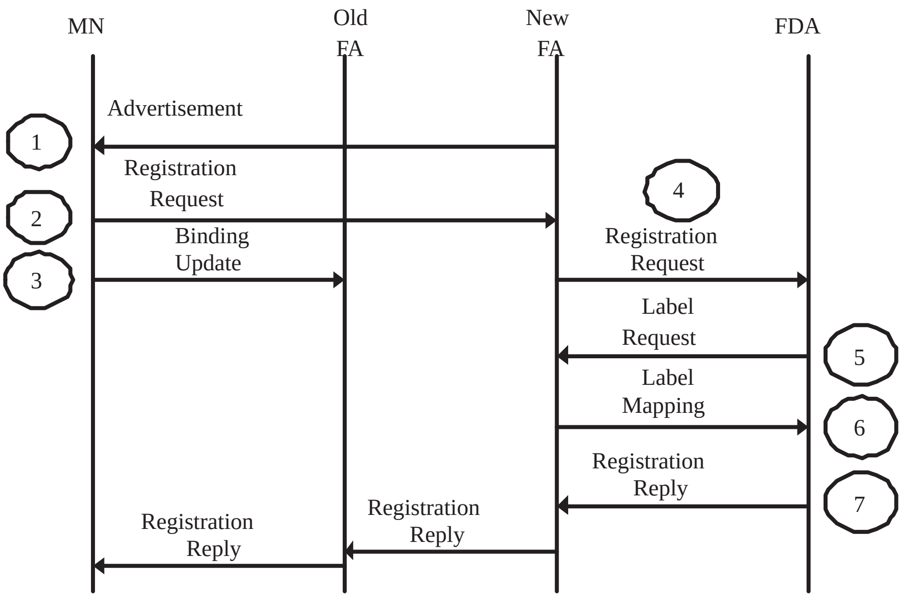
3) During the handover, the MN may also notify the old FA of its new CoA, by sending a binding update message. This allows the previous FA to cache the new binding of the MN. If the FDA later forwards a packet to the MN using an out-of-date cache entry, the old FA will receive the packet, sets up an LSP to the new FA, and then sends the packet to the new FA through the LSP.

4) The new FA forwards the Registration Request to the FDA.

5) The FDA sends a Label Request message back to the new FA.

6) The new FA receives the label request and responds with a Label Mapping message back to the FDA. This results in the establishment of a new LSP from the FDA to the new FA.

7) Finally, a Registration Reply is forwarded to the new FA, the old FA, and the MN from the FDA.



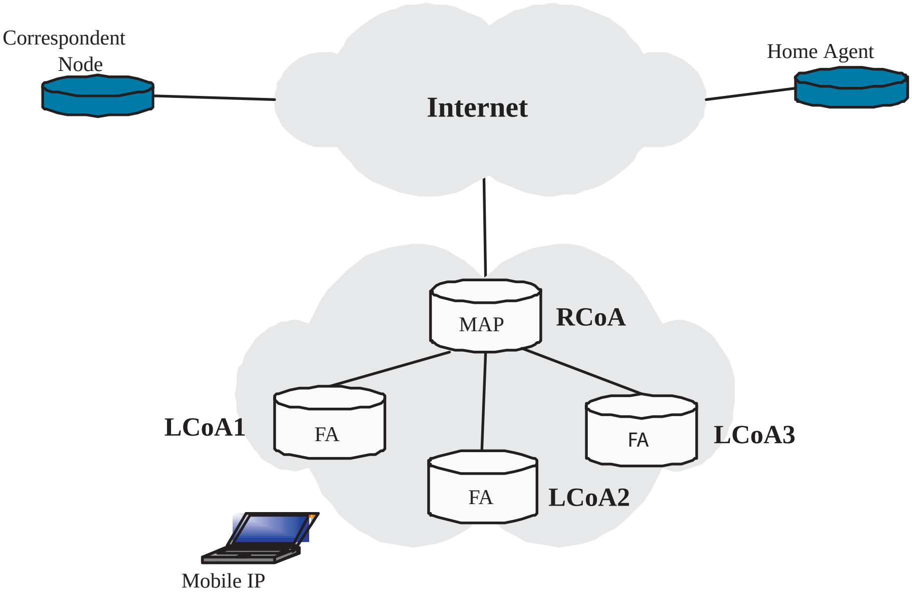
FA: Foreign Agent
FDA: Foreign Domain Agent
MN: Mobile Node

Figure 13.9. *MN handover in the same domain procedure*

13.6.2. *Hierarchical mobile IPv6 with MPLS*

In this section we first briefly present an overview of Hierarchical Mobile IPv6 (HMIPv6) and then we discuss MPLS support with HMIPv6. In the case of HMIPv6, the FDA is known as the Mobility Anchor Point (MAP) and a MN is assigned two CoAs instead of only one. The addresses are called Regional Care of Address (RCoA) and On-Link Care of Address (LCoA) [HAB 06, MON 02, SOL 05]. The MN obtains the RCoA from the visited network and it is an address on the MAP's subnet. The LCoA (as with the CoA of MIPv6) is the address of the Access Router (AR) in the MAP domain.

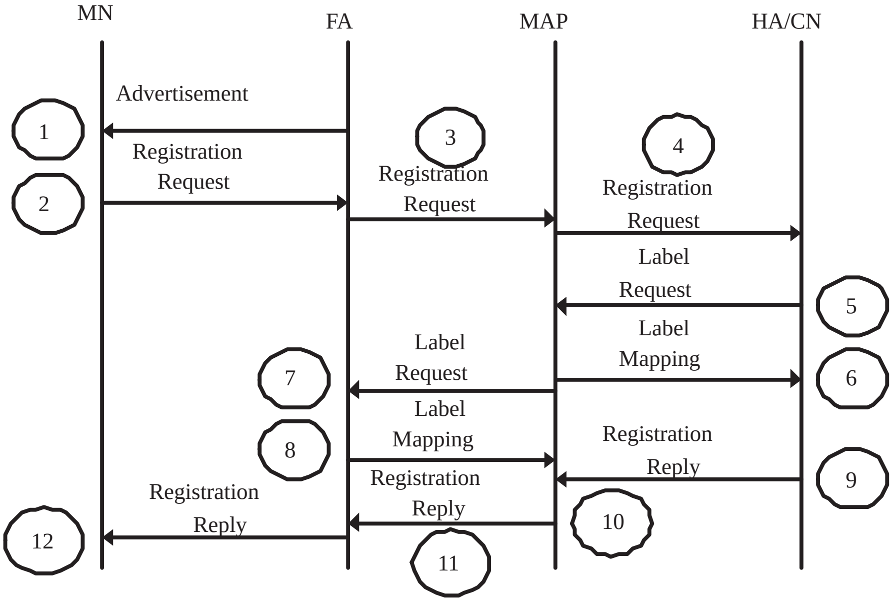
When the MN enters a new network site, it receives Router Advertisements (RAs) from the AR. The RAs informs the MN about the available MAPs and their distances from the MN. After selecting a MAP, the MN receives the RCoA on the MAP domain and the LCoA from the AR. At the same time the MN sends binding update messages to the MN's HA and to the CN with which the MN is interacting with to bind the RCoA and its HA.



FA: Foreign Agent
LCoA: On-Link Care-of-Address
MAP: Mobility Anchor Point
RCoA: Regional Care-of-Address

Figure 13.10. *HMIPv6*

When the MN moves within the same MAP domain, it should only register its new LCoA with its MAP. In this case, the RCoA remains unchanged. When the CN or HA sends messages to the MN's RCoA, they are received by MAP, which tunnels them to the MN's based on the LCoA using IPv6 encapsulation. However, the MN is able to send data directly to the CN. When the CN and MN are both located in the same domain, the CN sends data packets directly to the MN without any MAP intervention. Figure 13.10 illustrates a configuration that can be used by HMIPv6. The operation of MPLS with HMIPv6 is similar to MPLS with Hierarchical Mobile IPv4 (HMIPv4), except for some additional elements such as LCoA and RCoA. The FA periodically broadcasts MIP advertisement messages to all MNs. Upon receipt of the advertisement message, the following procedure is adhered to (as shown in Figure 13.11) [KUB 04, VAS 03]:



CN: Correspondent Node
FA: Foreign Agent
HA: Home Agent
MAP: Mobility Anchor Point
MN: Mobile Node

Figure 13.11. *The mobile node first registers on HMIPv6 with MPLS*

1) In an H-MPLS based network, the MN determines whether it is in the home domain or in a foreign domain when it receives advertisement messages broadcasted by the FA.

2) The MN acquires two CoA (RCoA and LCoA) and sends a Registration Request to the FA.

3) The FA forwards this Registration Request to the MAP (normally, the Registration Request would be forwarded to the HA).

4) The MAP forwards this Registration Request to the HA or to the CN which the MN is interacting with.

5) When the HA/CN receives the Registration Request and knows the RCoA address of the MAP, the HA/CN sends a Label Request, using the LDP, to the MAP using the RCoA of the MAP as the FEC.

6) The MAP replies with an LDP Label Mapping message sent back to the HA/CNs, resulting in the establishment of an LSP from the HA/CN to the MAP.

7) The MAP sends a Label Request to the FA of the sub-network in which the MN is currently located.

8) The FA replies with an LDP Label Mapping message back to the MAP. When the MAP receives this message, the LSP from the MAP to the FA is established.

9) The HA/CN searches the label table. When it finds the MN's home address, it changes the outgoing port and outgoing label to the same values as those for the LSP from the HA/CN to the MAP. The HA/CN sends a Registration Reply to the MAP over the LSP from the HA/CN to the MAP.

10) The MAP forwards this Registration Reply to the FA over the LSP from the MAP to the FA.

11) When the FA receives the Registration Reply, it puts the incoming Registration Reply's label value and port number into the "in label field" and "incoming port field" of the table.

12) The FA sends the Registration Reply back to the MN.

When the MN performs a handover from one FA to another within the same foreign domain, the new FA station informs the MAP via the MIP registration request message using the following steps (Figure 13.12):

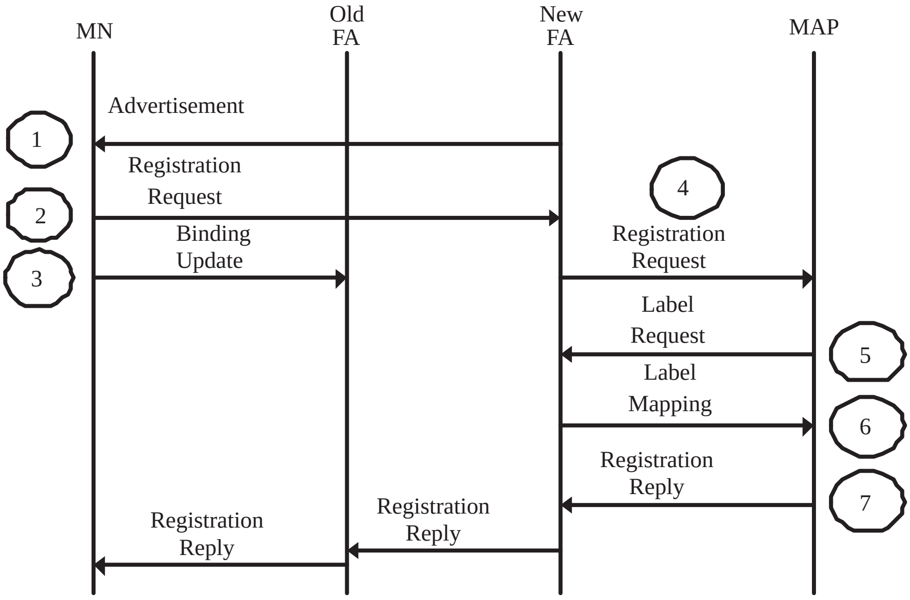
1) The MN determines whether to perform a handover to a new FA based on the advertisements received from the new FA.

2) When the MN performs a handover from one sub-network to another sub-network within the same foreign domain, it sends a Registration Request to the new FA.

3) During the handover, the MN may also notify the old FA of its new LCoA, by sending a binding update message. This allows the previous FA to cache the new MN binding. If the MAP subsequently forwards a packet to the MN using an out-of-date cache entry, the old FA receives the packet, sets up an LSP to the new FA, and sends the packet to the new FA through the LSP.

4) The new FA forwards the Registration Request to the MAP.

5) The MAP sends a Label Request message back to the new FA.



FA: Foreign Agent
MAP: Mobility Anchor Point
MN: Mobile Node

Figure 13.12. *MN handover in the same domain on HMIPv6 with MPLS*

6) The new FA receives the Label Request and responds with a Label Mapping message back to the MAP. This results in the establishment of a new LSP from the MAP to the new FA.

7) Finally, a Registration Reply is forwarded to the new FA, the old FA, and the MN from the MAP.

Before setting up an MPLS connection, the underlying network connection must be established. Part of the underyling network for HMIPv6 uses LCoA. Before using the LCoA for a MN, the MAP performs Duplicate Address Detection (DAD) as part of the auto configuration mechanism. The DAD mechanism is used to prevent address duplication. However, this requirement to execute DAD limits the performance of HMIPv6 [HAB 06, MON 02, MON 05, SOL 05] but does not affect the MPLS performance except during the initial establishment of LSP.

Fast Handover for Mobile IPv6 (FMIPv6) [MON 02, KOO 05] was introduced to minimize the amount of service disruption during handovers. Keeping the handover latency to a minimum is important for multimedia traffic. Fast Handover for Hierarchical MIPv6 (FHMIPv6) uses bi-casting for fast handovers. Bi-casting allows the MN to simultaneously register with several ARs. This causes a problem for MPLS since packets destined for the MN need to be duplicated and sent to several potential locations. Packets duplication increases the delay incurred in establishing several LSPs and also causes additional traffic to be generated. Under high loads with many MNs performing handovers, the MAP will be heavily loaded. Moreover, with bi-casting, duplicating and sending packets to several potential ARs, there is also a decrease in number of available labels for use by other MNs.

13.6.3. *Micro-mobility with MPLS (MM-MPLS) approach*

Micro-mobility in MPLS-based wireless networks (henceforth referred in this chapter as Micro-MPLS based networks) has three advantages [XIE 03]:

1) It allows for constraint-based routing and the support of traffic engineering in wireless networks.

2) Within the wireless network, only the LSR deals with label switching and base stations (HA or FA) need to be aware of the mobility of the MN.

3) It improves network reliability through the use of path protection and restoration schemes (e.g. fast reroute).

In the case of Micro-Mobility with MPLS (MM-MPLS), a crossover LSR is inserted between the FA and the FDA. The crossover LSR is the LSR closest to the MN, which is at the intersection of two paths; one SR is between the FDA and the previous FA, and the other LSR is between the FDA and the new FA (A is the crossover LSR in Figure 13.13). When a request arrives at the crossover LSR, a new LSP is set up to the new FA using the MN's home address as FEC [YAN 02a].

When the MN first moves into a foreign domain, the exchange of messages involved are similar to those in H-MPLS: the MN sends a Registration Request message to the nearest FA (e.g. node D in Figure 13.13). The key difference between H-MPLS and MM-MPLS however is the establishment of an LSP between the FDA and the current FA using the Resource Reservation Protocol-Traffic Engineering (RSVP-TE) feature of MM-MPLS. RSVP-TE allows soft-state location management on MNs within the MM-MPLS domain. The FDA sends an RSVP PATH message to the current FA. An important feature of MM-MPLS is that the MN's home address is used as FEC instead of the current FA's address when establishing an RSVP path from the FDA to the FA. When the current FA receives the RSVP PATH message containing a LABEL_REQUEST, it responds by transmitting a Reservation (RESV)

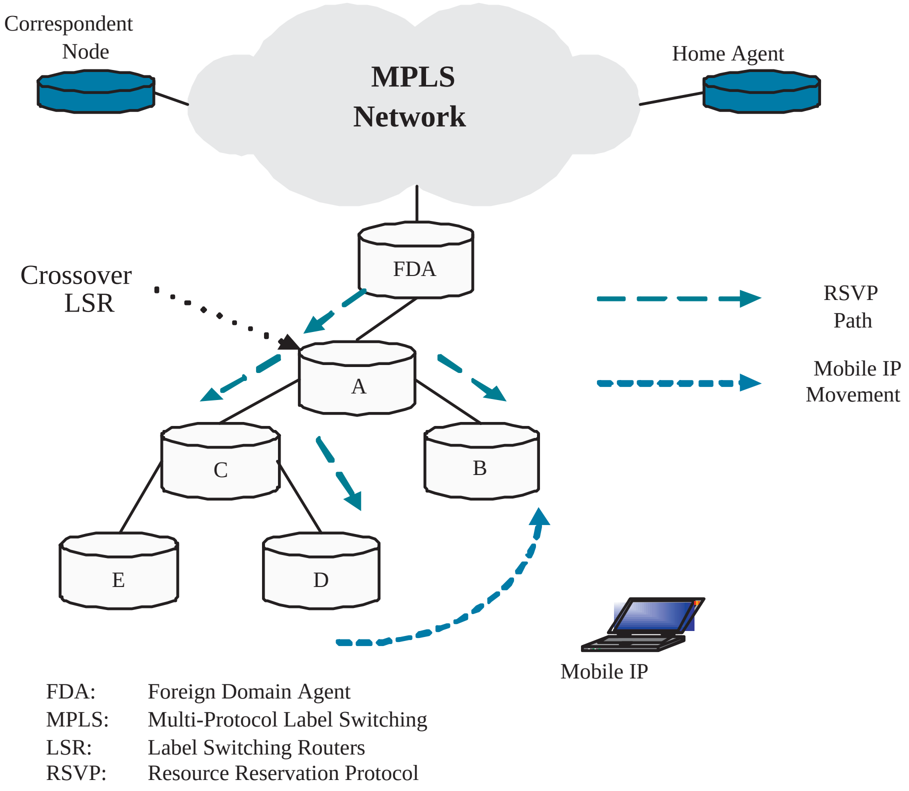


Figure 13.13. *MM-MPLS architecture*

message which contains the label binding that the downstream LSR communicates to its upstream neighbor. The RESV message is forwarded upstream towards the FDA along the same path. Once the RESV message arrives at the FDA, the LSP between the FDA and the current FA is established. Finally, the FDA relays the Registration Replay message sent from the HA to the MN along the LSP between the FDA and the current FA [YAN 02a].

When the MN makes a handover from one FA to a new FA within the same foreign domain, it sends a Registration Request to the new FA. Next, the new FA (i.e. node B in Figure 13.13) relays the Registration Request to the FDA. Every LSR between the new FA and the FDA will confirm whether there is an entry possible for the MN (this is done by checking whether the MN home address (FEC) is in the LSR label table). Finally, the Registration Request message reaches an upstream LSR (depicted in node A of Figure 13.13) and becomes a crossover LSR (with a forwarding entry for the

MN). In the worst case, the crossover LSR will be the FDA. A crossover LSR is the LSR closest to the MN and is at the intersection of two paths connecting the FDA with the old FA and the new FA. Once the crossover LSP receives the Registration Request, it establishes a new LSP for the new FA. After the new LSP from the crossover LSR to the new FA has been established, the crossover LSR changes its label table and redirects the LSP (with the MN home address as FEC) to the new FA. The crossover LSR then intercepts PATH messages from the FDA to the old FA, and generates a RESV message containing the new EXPLICIT_ROUTE OBJECT (ERO). The ERO defines the new path from the FDA to the new FA, and returns the newly generated RESV message back to the FDA. All subsequent PATH messages in RSVP-TE sent by the FDA will include the new ERO and are forwarded through the new LSP by the crossover LSR to the new FA. Finally, since RSVP-TE periodically sends a refresh message, nodes along the old path (nodes A → C → and D in Figure 13.13) will timeout, resulting in the MN's home address (as FEC) being deleted from the LSR table [YAN 02a]. However, RSVP sends periodic refresh messages to maintain the LSP, and this results in additional traffic being injected into the network.

13.6.4. *The label edge mobility agent (LEMA) approach*

The label edge mobility agent (LEMA) [CHI 02a, CHI 02b] approach was proposed to enhance label edge routers (LERs). The idea was to create a hierarchical overlay network that directly inherits the basic features of MPLS in terms of LSP redirection, traffic engineering, advanced IP services, and fast restoration [CHI 02a, CHI 02b]. In the case of LEMA, there are pre-established LSPs because as packets traverse this network, the LEMA examines their network layer addresses to map the each packet's address to an outgoing label. When an intermediate LSR encounters a packet, it simply performs label switching. The major difference with the LEMA approach compared with other hierarchical architectures is that the host (or the AR[4] on its behalf) has the flexibility to create its own hierarchy of agents based on its mobility pattern, the bandwidth availability in the network and other factors [CHI 02a, CHI 02b].

When the MN has AR 1 (Figure 13.14) to communicate, it registers with the chain (1, 7, 8) (note that node 8 is the FA). AR 1 receives an advertisement containing the sub-tree (1, (7, (6, 8))) with AR 1 as root. After executing a selection algorithm, AR 1 chooses the chain (1, 7, 8) for registration. When the MN moves from the scope of AR 1 to that of AR 2, the MN receives a new advertisement message and AR 2 (AR 2 is the host) receives an advertisement containing the sub-tree (2, (7, (6, 8))). AR 2 recognizes that a handover has to be initiated and compares the current chain (1, 7, 8) with the new sub-tree. After running the selection algorithm again, AR 2 creates a new chain

---

[4] The responsibility of the AR is to keep track of various access points.

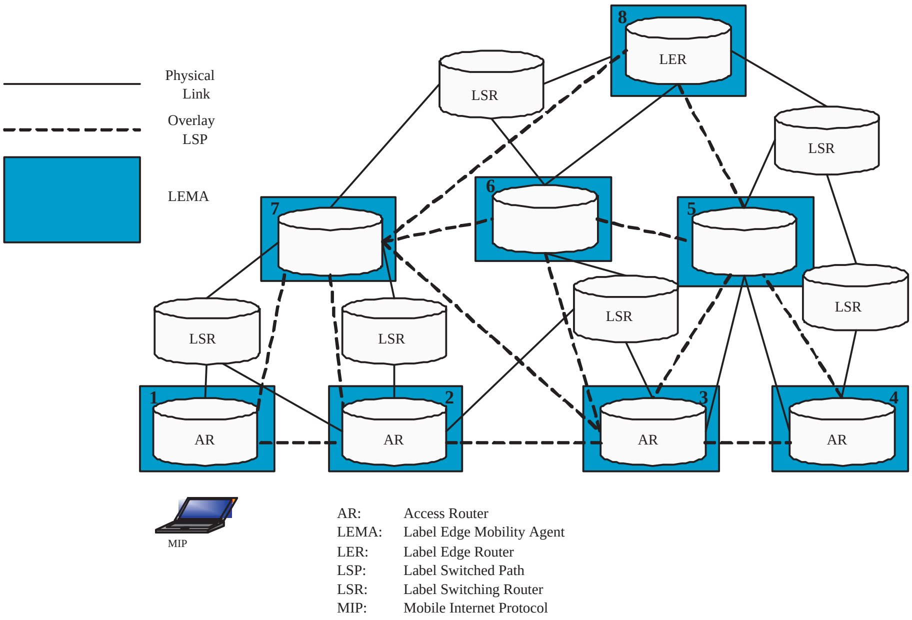


Figure 13.14. *An example of a LEMA network*

(2, 7, 8). The MN registers its identifying address with LEMA 2 and issues a redirect message to LEMA 7 in order to change its mapping to the LSP that points to LEMA 2. Any change in the top-level LEMA (for example from LEMA 8) will require the FA to re-register with the HA. However, the algorithm for selecting a LEMA for a MN is complex and is still a subject of investigation [LAN 05]. In addition, maintaining pre-established LSPs requires further network resources, limiting the deployment of this approach.

13.7. Multimedia support over MPLS-based networks

The wide range of multimedia services that are being deployed over the Internet are pushing ISPs to provide a network that is dependable and offers reliable network performance. Although MPLS is a connection-oriented label swapping technology, and does offer new possibilities in addressing some of the limitations of QoS over IP-based systems, combining MPLS with other, previously deployed QoS techniques, can make MPLS a powerful technology for QoS provisioning in IP backbone networks [LIN 02]. Common QoS techniques that have recently been explored with the hope of providing support for MPLS include differentiated services (DiffServ), the RSVP, and the CR-LDP.

MPLS-based wireless approaches	Disadvantages	Advantages
HMIPv6 with MPLS	• The use of DAD in the address auto-configuration mechanisms does not affect the performance of MPLS. MPLS performance is affected only when the initial LSP needs to be established and DAD for the LCoA has not been completed. • Bi-casting needs time to establish several LSPs. • Bi-casting increases traffic delays due to the increased traffic generated from the various LSPs. • Bi-casting causes heavy loading on MAP when a large number of mobile nodes are simultaneously performing handovers. • Bi-casting causes duplication with packets sent to several access routers, resulting in a decrease in the number of available labels for other mobile nodes.	• Compatible with IP-based networks. • Combines performance and traffic management capabilities of the data link layer (Layer 2) with the scalability and flexibility of network layer (Layer 3) routing (such as OSPF, BGP and IS-IS extensions). • Faster network transit of packets. • Extended support for QoS along with the ability to provide differentiated services.
MM-MPLS	• RSVP sends periodic refresh messages to maintain LSPs, injecting additional traffic into the network. • RSVP failures from the crossover router to the FA affects the end-to-end QoS.	• Decrease in handover delays. • Resource reservation for individual traffic flows. • End-to-end QoS signaling.
LEMA	• LEMA examines packets at the network layer to map the packets' addresses to outgoing labels. • The algorithm for selecting a LEMA for a mobile node is complex and is still being investigated. • Maintaining pre-established LSPs requires additional network resources limiting deployment of the approach.	• BS or AR has the flexibility to create its own hierarchy of agents based on mobility pattern and bandwidth availability in the network.

Table 13.1. *Disadvantages and advantages of HMIPv6-MPLS, MM-MPLS, and LEMA for MPLS-based wired-wireless networks*

13.7.1. *MPLS support in DiffServ*

DiffServ provides edge-to-edge QoS, while MPLS provides a fast forwarding mechanism that is designed to work with current Internet routing protocols. The combination of DiffServ and MPLS [FAU 02, FAU 03] presents an attractive strategy for backbone network service providers, as a support of scalable QoS and fast packet switching technologies.

DiffServ is a scalable technique that can provide QoS support to multimedia traffic. DiffServ supports three different types of per hop behavior: expedited forwarding (EF[5]) [JAC 99], assured forwarding (AF[6]) [HEI 99] and best-effort (BE[7]). Unfortunately, there is no response from the client to determine whether the QoS requirements are being met for the traffic. Thus, a sender may not know whether a particular service state is being delivered to the application. Moreover, the lack of end-to-end signaling from the sender to the client (or from the client to the sender) makes the DiffServ approach impossible to operate in isolation within any environment. Using the QoS object in IPv6 or HMIPv6 enables certain parameters (representing QoS requirements and traffic characteristics for a QoS flow) supported by DiffServ, but implementing QoS requirements for the QoS objectives with MPLS needs further investigation. In addition, HMIPv6 suffers from other limitations, in the forms of bi-casting and DAD, as mentioned earlier. End-to-end signaling using RSVP or CR-LDP also introduces further issues that will be discussed later.

There are two major issues in providing MPLS support to DiffServ. First, the differentiated services code point (DSCP[8]) is carried in the IP header, but the LSRs only examine the MPLS label header. Second, the DSCP has 6 bits but the experimental (EXP) field (field in MPLS header dedicated to selecting per hop behavior (PHB)) has only 3 bits. There are two ways to handle these issues, EXP-Inferred-PHB scheduling class LSP (E-LSP) or label-only-inferred-PHB scheduling class LSP (L-LSP).

13.7.1.1. *EXP-inferred-PHB scheduling class LSP (E-LSP)*

E-LSP refers to a single LSP but can be used to support one or more ordered aggregates (OAs[9]). Such LSPs are capable of providing up to eight behavior

---

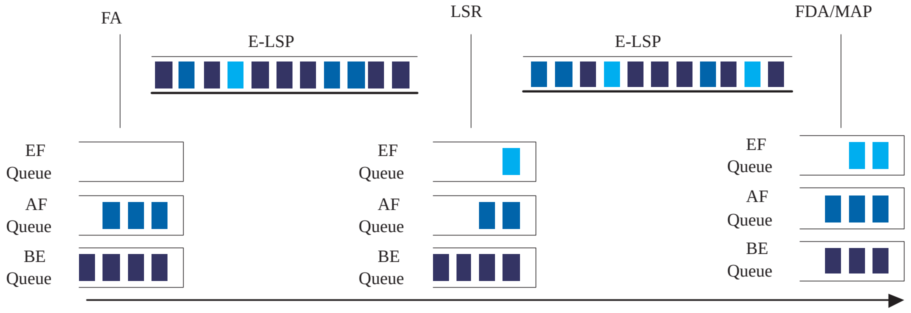
[5] EF: receives the best treatment that is available on the network, thus providing low loss, low latency and low end-to-end jitter service.

[6] AF: receives better than best effort service, hence there is some level of forwarding assurances.

[7] BE: delivers as many packets as possible, as soon as possible. There is no guarantee as to timeliness or actual delivery.

[8] DSCP: replaces the existing definitions of the Type of Service (ToS) in IPv4 or the traffic type in IPv6 for the DiffServ information.

[9] OA: a set of behavior aggregates share an ordering constraint.



AF:	Assured Forwarding
BE:	Best Effort
EF:	Expedited Forwarding
E-LSP:	EXP-Inferred-PHB Scheduling Class LSP
FA:	Foreign Agent
FDA:	Foreign Domain Agent
LSR:	Label Switching Router
MAP:	Mobile Anchor Point

Figure 13.15. *E-LSP supporting Diffserv*

aggregates (BAs) for a given FEC and are referred to as E-LSPs, since the PHB of a label transported on this LSP depends on the EXP field value in the MPLS header. This includes both the PHB scheduling class (PSC[10]) and the drop preference. Figure 13.15 illustrates how a single E-LSP supports three different PHBs as it transports an aggregate flow from the ingress LSR to the egress[11] LSR. The mapping from the PHB field to the EXP (i.e. to PSC and drop precedence) for a given LSP can be either pre-configured or explicitly signaled during the E-LSP establishment.

E-LSP offers several benefits when supporting MPLS over DiffServ [FAU 02, JUN 06b, JUN 06a]. Some of these benefits include:

– the approach is similar to DiffServ over IP. Each packet is arranged and tagged at the ingress. Each LSR examines the EXP to determine the PHB that should be applied to the MPLS packet;

– when EXP is used, this allows the LSR to determine the PHB;

– no modification to the existing signaling and LDP protocols is required;

– a maximum of 8 PHB over a single E-LSP can be supported;

---

[10] PSC: a set of one or more PHBs can be applied to the behavior aggregate(s) belonging to a given OA.

[11] Egress: the exit point of the MPLS domain.

– E-LSP may be used with L-LSP if PHBs are needed;

– support for various PHBs on a single E-LSP simplifies network management (by reducing the number of LSPs) and LSP maintenance (by efficiently managing the limited label space).

There are also shortcomings [FAU 02, JUN 06a, JUN 06b] associated with E-LSP, some of which are listed below:

– when a higher priority LSP preempts a lower LSP, all service classes on the lower LSP are affected;

– we need to calculate LSPs that meet the constraint of multiple PHBs rather than calculating LSPs that optimize the constraints of a single PHB;

– we can merge a single E-LSP only if the E-LSP uses the same EXP values in the label;

– E-LSP can only support 8 PHBs. If more than 8 PHBs are required for an FEC, alternative methods must be explored;

– the amount of bandwidth allotted to a queue is different from the LSP. For example, an EF queue with a capacity of 10 Mbps over a 100 Mbps LSP. To avoid congestion on an EF queue, all traffic must be less or equal to 10 Mbps. This is difficult to police due to the heterogenity of the LSP on an MPLS network.

13.7.1.2. *Label-only-inferred-PHB scheduling class LSP (L-LSP)*

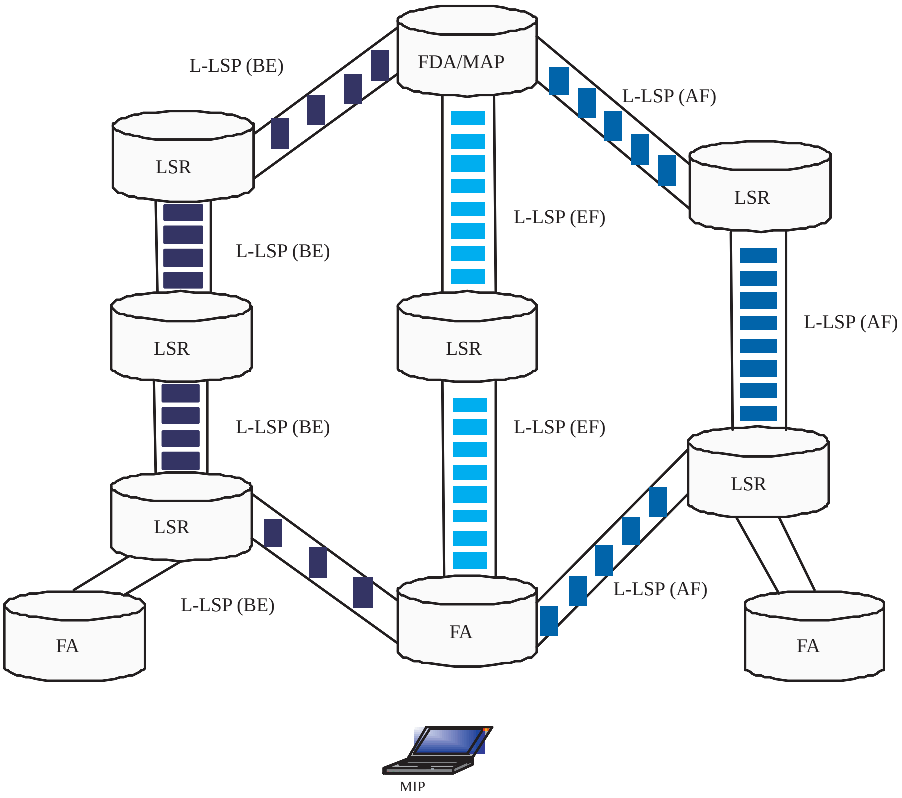
As an alternative to establishing only a single LSP between the ingress LSR (also known as LER) and the egress LSR (also known as LER), an ingress LSR can establish multiple LSPs between itself and a given egress LSR. This means that a separate LSP can be established for a single ⟨FEC and OA⟩ pair. Thus, each LSP can be configured to support the particular requirements of the aggregated flow. This is referred to as L-LSP since each LSR along the path uses the label to decide where the packet should be sent and the specific PHB to be applied to the label. With L-LSP, the PHB scheduling class can be fully inferred from the label regardless of the EXP field value in the MPLS header.

Figure 13.16 illustrates one L-LSP setup for the three different classes used in DiffServ (explicated, assured and best-effort forwarding). The ingress LSR uses the destination IP address and the DSCP in the IP packet header to determine the label to use, allowing for the appropriate L-LSP to be selected [FAU 02, JUN 06a, JUN 06b].

Some of the benefits associated with the L-LSP approach include:

– it allows support up to 64 PHBs the following ;

– it enables the ingress LSR to configure the path related to the traffic flow;



AF:	Assured Forwarding
BE:	Best Effort
EF:	Expedited Forwarding
L-LSP:	Label-Only-Inferred-PHB Scheduling Class LSP
FA:	Foreign Agent
FDA:	Foreign Domain Agent
LSR:	Label Switching Router
MAP:	Mobile Anchor Point
MIP:	Mobile Internet Protocol

Figure 13.16. *One L-LSP supporting three different PHBs*

– it needs only a single PHB per LSP;

– with thorough planning and good configuration, an L-LSP can provide good throughput, jitter, and delay guarantees for multimedia traffic.

Some of the limitations of L-LSPs include the following:

– L-LSPs can only be merged if they use the same PHB;

– L-LSP may complicate network management when there is an increase in the number LSPs that need to be set up, as well as maintaining application constraints;

– binding between the label, FEC and the PHB is not supported by the current IGP and LDP without modifications or extensions;

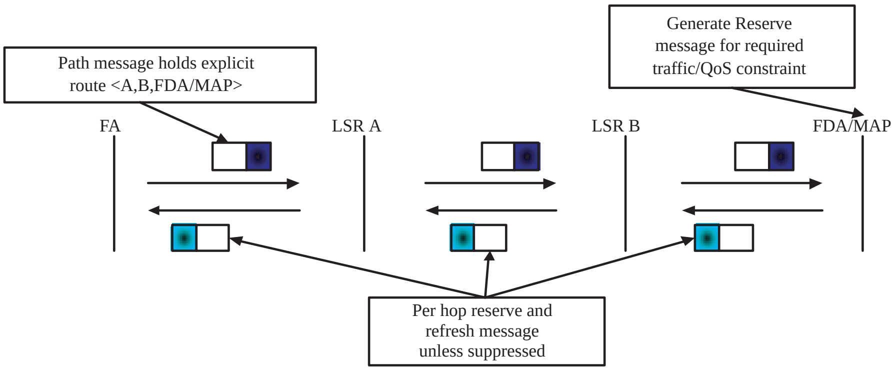
– physical configuration to support traffic guarantees is difficult.

13.7.2. *Resource reservation protocol traffic engineering (RSVP-TE) with MPLS*

RSVP [BRA 97] was engineered to accomplish the creation and maintenance of distributed reservation states across a network.

By exploiting RSVP-TE, MPLS traffic engineering extends the original RSVP protocol, adding new capabilities to support an MPLS domain. RSVP-TE enables the establishment of an LSP over MPLS to meet the QoS requirements for end-user applications. As mentioned earlier, RSVP communicates with two basic types of messages: PATH and RESV messages. PATH messages flow from a sender to the receiver. When the receiver admits the PATH message, it sends an RESV message back to the sender and reserves network resources for an explicitly routed LSP (ER-LSP). To maintain resource reservations and the LSP, refresh messages must be re-transmitted. Figure 13.17 illustrates the flow of RSVP messages in establishing an ER-LSP. It is also worth noting some of the limitations of RSVP/ER-LSP:

– it is not scalable, as the number of RSVP LSP increases with the number of soft states;



FA:	Foreign Agent
FDA:	Foreign Domain Agent
LSR:	Label Switching Router
MAP:	Mobile Anchor Point
QoS:	Quality of Service

Figure 13.17. *Extension to RSVP for an ER-LSP*

– the soft state protocol characteristic of RSVP/ER-LSP requires periodic refreshing of the states, which increases the traffic load on the network.

13.7.3. *Constraint-based routed label distribution protocol (CR-LDP)*

CR-LDP is based on LDP. The difference from LDP is that CR-LDP supports explicit routes and resources allocation. It does not require the implementation of an additional protocol [ASH 02a, JAM 02]. For instance, an LSP can be established based on explicit route constraints or QoS constraints to meet traffic engineering requirements. These requirements are met by extending LDP to support constraint-based routed label switched paths (CR-LSPs) [JAM 02, ROS 01b].

As mentioned earlier, CR-LDP supports explicit routes (list of nodes that the LSP must traverse). CR-LDP supports both strict and loose explicit routes [ASH 02a, JAM 02]. If CR-LDP is marked as strict, then it must include only network nodes from the strict node in the explicit route. Conversely, if an abstract node is marked as loose, then any next hop along the path to the destination node may be taken. Thus, strict routes allow complete control of the nodes traversed by an LSP, while loose routes provide significant local flexibility in selecting the nodes that comprise selected portions of the path. CR-LDP allows for explicit routes, using both strict and loose hops, providing maximum flexibility in building specific paths through the network. Figure 13.18 illustrates the establishment of CR-LDP to a LSP.

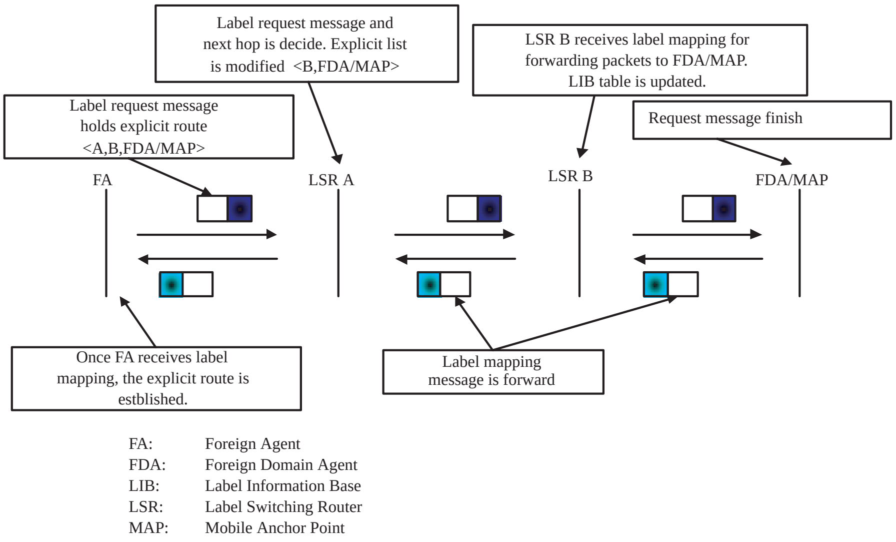


Figure 13.18. *Operation of CR-LDP*

Constraint-based routing computes routes that are subjected to constraints and is an important tool for traffic engineering and for providing QoS. Constraint-based routing relies on state information specifying resource availability at network nodes and links, and uses it to find paths with enough free resources to accommodate new flows. With constraint-based routing, there is a constant change in the amount of available resources because of the termination of existing routing flows and successful completion of other routing flows. This constant change in the available resources causes considerable amounts of inaccuracy in the information required to identify and select optimal network paths. This selection becomes particularly challenging for large-scale networks, where it takes a significant amount of propagation delay for a local state adjustment to be transmitted to other nodes. Also the link state protocol updates the status periodically or only when a noticeable state change is identified.

To establish an explicit route computed by constraint-based routing, it is not adequate to simply reserve resources along that route for QoS, some kind of path setup is also needed. To achieve this, two methods can be used namely, RSVP and CR-LDP. The hard-state protocol of CR-LDP makes it a suitable choice and scalable in terms of the signaling traffic volume in the network as the number of CR-LDPs increases.

After a CR-LSP is established, its bandwidth reservation may need to be changed by the network operator. This is because new requirements made of the traffic carried on that CR-LDP may demand the re-establishment of a new CR-LDP, resulting in a service disruption [ASH 02b].

If a routing request with constraints needs to be established, and the LSP conflicts with other existing LSPs (for example, these LSPs occupy the same link and the capacity of the link is below the aggregate bandwidth of these two LSPs), the LSP with low priority will be rerouted. However, re-routing a CR-LDP LSP would cause re-routing of another CR-LDP LSP. Consequently, re-routing of various other CR-LDP LSPs may occur. This makes the management of network resources difficult.

Other limitations of CR-LDP [ASH 02a, JAM 02] include:

– CR-LDP only supports unidirectional (allowing flow in only one direction) LSP setup;

– the CR-LDP specification only supports direct links between two LSRs (point-to-point) for LSPs, with no point-to-multi-point support;

– CR-LDP only supports a single label allocation per LSP setup.

13.8. Emerging trends of MPLS-based networks

Several issues still need to be resolved to provide a consistent and scalable end-to-end QoS solution that can deliver different types of service (including multimedia) with different requirements to mobile users. As the number of mobile users continues to increase, the scalability of QoS and traffic engineering solutions becomes crucial. In addition, wireless networks have become widely ubiquitous and are increasingly being connected to wired networks. Therefore, it is important that traffic engineering solutions such as MPLS are able to extend their QoS support to wireless networks connected to wired networks. MPLS is a promising solution, offering scalable qualities designed to address the end-to-end QoS challenge over heterogenous wired-wireless networks. To reduce the signaling load, micro-mobility was proposed. Such a scheme is well suited for fast handovers since it minimizes the signaling overhead and the latency caused by wide-area mobility protocols in macro-mobility (which occurs when the MN move globally from one FDA/MAP to another FDA/MAP) environments, and transient packet loss associated with high mobility. Micro-MPLS-based network handover techniques are unable to guarantee QoS for a connection as a MN moves to a new FA or a new FDA/MAP. More research is needed to explore new approaches that minimize the impact of handovers on end-to-end QoS for MPLS-based wired-wireless networks. Efficient solutions will enable seamless roaming without the difficulties involved in configuring devices, inputting authentication parameters, and reconfiguring QoS parameters.

Next generation wireless devices will be expected to provide mobile users with seamless handovers, and end-to-end QoS support among different networks using multimodal wireless devices. The task of managing authentication among mobile users and configuration of QoS over MPLS-based networks should be transparent to the user. This is a highly desirable goal, and much work remains to make this goal a reality. We present some of the issues such as end-to-end QoS and security that need to be addressed in future MPLS-based networks.

13.8.1. *Label management of MPLS*

The use of MPLS over IP-based networks provides several benefits over conventional network layer forwarding. For example, the ingress may insert additional information into the packet and thereby route it differently to satisfy specific QoS requirements. With MPLS, explicit LSP may be performed, making it easier to carry out traffic engineering compared to conventional routing schemes [GUP 03]. As MPLS is deployed over wireless networks, label allotment becomes an important issue. The management of bandwidth, label, and QoS requirements will become more complex in the LSR when the number of labels increases. In addition, label space cannot exceed 2^{20} on an LSR. Increasing the label size is not a practical solution, since having a small label space reduces the size of the forwarding table, which lowers the memory requirements of such tables and enables faster packet routing. In [ROS 01a, ROS 01b] the label stack concept was introduced into MPLS to support efficient label management. The label stack was introduced into MPLS to allow multiple LSPs to be aggregated into a single LSP tunnel. It is worth pointing out that there are scalability and performance related reasons for reducing the label size. As mentioned previously, the label space cannot exceed 2^{20} and to achieve scalability the label space must be used efficiently. Small label sizes are critical for enabling better scalability and performance. Unfortunately, having a small label sizes results in the use of expensive, deep stacks which are detrimental since each stack entry (the label) causes an increase in the space requirements of IP packet headers. Thus, label management needs to address scalability given that the label space cannot exceed 2^{20}.

13.8.2. *MPLS support over heterogenous networks*

In the past few years, wireless networks have become widespread. Wireless devices, such as wireless laptops, PDAs (e.g. palm pilots), cell phones, etc., have become an integral part of our daily lives. Having a wide technological diversity raises another major issue related to heterogenity. Next generation heterogenous systems will be expected to provide end-users with a usage model for wireless devices that will allow them to roam seamlessly among different networks, using multimodal wireless devices [SID 05]. To be able to access different types of network technology, it is essential to develop MPLS-aware multimode terminals that can adapt to various technologies with different operational frequencies, data rate, access technology, etc.

13.8.3. *MPLS security*

The existence of heterogenous wireless access systems makes it very difficult to provide a uniform security level for data flows. We should not assume that the core MPLS network provides a high security level [BEH 06]. Protection against an insecure core is required, since the core network is part of the end-to-end path. Suitable cryptographic protocols that protect the MPLS header and thus prevent ISP services thefts are essential. The use of such cryptographic protocols should not interfere with the QoS that an ISP provides on MPLS networks. For example, adding 128 bits to each MPLS header makes the header four times larger than the original, which increases the packet's processing overheads.

Standard secure protocols such as IP security (IPSec) protocol operates at layer 3 compared to MPLS which operates at layer 2. Some designs require the exchange of labeled packets, which makes it possible for a third-party to introduce labeled packets which if correctly crafted might be associated with certain virtual private networks (VPNs) over MPLS networks. Incorporation of a secure LDP remains an unresolved issue that requires further investigation [BEH 06].

13.8.4. *QoS support over MPLS-based networks*

Providing efficient, scalable QoS means more than just fast forwarding packets. To support end-to-end QoS requires satisfactory bandwidth, throughput, reliability and low jitter, all of which present major challenges. When MPLS is used, there is an information exchange when establishing an LSP. Hence mobility management over MPLS-based networking environments present issues such as timely service delivery, and QoS negotiation during handovers since there is increased information exchange when establishing an LSP. The main challenge in providing QoS in a mobile MPLS environment is that we need efficient support for both QoS and mobility management so that the QoS delivered is not affected during operations such as handovers.

13.8.5. *Fast handovers across MPLS-based wired-wireless networks*

The Micro-MPLS-based approach was proposed to enable mobile MPLS support over wireless networks connected to wired networks. Performance evaluation shows that, with Micro-MPLS-based networks, the delay the MN experiences during handovers is considerably lower when compared with the delay obtained when conventional mobile MPLS is used [XIE 02, YAN 01]. When the MN performs a handover to another FA with the same FDA/MAP, it sends the registration request to the new FA. The new FA relays the message towards the FDA/MAP which sets up an LSP between itself and the current FA. These steps are repeated every time the MN changes FA in the FDA/MAP domain. Future research should investigate techniques that minimize or eliminate the need to re-establish completely new LSPs between the new FA and the FDA/MAP. Moreover, with Micro-MPLS-based networks, bottlenecks may occur on the FDA/MAP when a large number of MNs need to establish a connection or several handovers occur simultaneously. With the increasing proliferation of wireless devices handling delay-sensitive traffic (such as voice and VoIP), it is essential to provide low end-to-end delays when establishing the LSP during handovers since traffic delays may result in QoS degradations.

13.9. Conclusion

Multimedia support over networks has been extensively studied over the last decade. Several QoS approaches and protocols have been proposed and implemented. However, few of these proposed approaches have been incorporated into commercial products. This is because many of these solutions were too cumbersome to implement and could not adequately satisfy various QoS characteristics. As a result, many previous QoS solutions have not been widely deployed. However, one of the latest traffic engineering technologies that has gained wide acceptance over the last couple of years is MPLS, which is currently supported by many commercial switches and routers on the market. Initially, MPLS was introduced as a fast forwarding mechanism designed to work with existing Internet routing protocols such as OSPF or BGP. Recently, extensions have been made to MPLS to support features such as constraint-based routing. The Internet continues to grow at a rapid pace and part of that growth can be attributed to the rapid proliferation of wireless networks, many of which connect to the wired Internet infrastructure. Along with these developments, users are becoming increasingly mobile and they expect their services to be delivered uninterrupted with high QoS anywhere, anytime. To satisfy these challenging demands we need QoS technologies and protocols that are effective end-to-end, spanning wired-wireless network paths. We discussed various approaches (H-MPLS, MM-MPLS, LEMA) that have been recently proposed as means of enhancing QoS support over MPLS-based wired-wireless networking domains. We identified several QoS implementation issues and challenges that still need to be addressed to firstly enable and then maintain end-to-end QoS for mobile users. We argue that additional efforts are needed to solve challenging research issues in the areas mobile QoS management, label management, fast handovers, and security for MPLS-based networks.

13.10. References

[AND 01] ANDERSSON L., DOOLAN P., FELDMAN N., FREDETTE A. and THOMAS B., "LDP specification", *RFC3036*, January 2001.

[ASH 02a] ASH J., GIRISH M., GRAY E., JAMOUSSI B. and WRIGHT G., "Applicability statement for CR-LDP", *RFC3213*, January 2002.

[ASH 02b] ASH J., LEE Y., ASHWOOD-SMITH P., JAMOUSSI B., FEDYK D., SKALECKI D. and LI L., "LSP modification using CR-LDP", *RFC3214*, January 2002.

[BEH 06] BEHRINGER M., "Analysis of the security of BGP/MPLS IP virtual private networks (VPNs)", *RFC4381*, February 2006.

[BRA 97] BRADEN E.R., ZHANG L., BERSON S., HERZOG S. and JAMIN S., "Resource reservation protocol (RSVP) – version 1 functional specification", *RFC2205*, September 1997.

[CAM 01] CAMPBELL A.T. and GOMEZ J., "IP micro-mobility protocols", *ACM SIGMOBILE Mobile Computer and Communication Review*, vol. 4, p. 45–54, October 2001.

[CHI 02a] CHIUSSI F.M., KHOTIMSKY D.A. and KRISHNAN S., "A network architecture for MPLS-based micro-mobility", *IEEE Wireless Communications and Networking Conference (WCNC)*, 2002.

[CHI 02b] CHIUSSI F.M., KHOTIMSKY D.A. and KRISHNAN S., "Mobility management in third-generation all-IP networks", *IEEE Communications Magazine*, p. 124–135, September 2002.

[FAU 02] FAUCHEUR F.L., WU L., DAVIE B., DAVARI S., VAANANEN P., KRISHNAN R., CHEVAL P. and HEINANEN J., "MPLS support of differentiated services", *RFC3270*, May 2002.

[FAU 03] FAUCHEUR F.L. and LAI W., "Requirements for support of differentiated services-aware MPLS traffic engineering", *RFC3564*, July 2003.

[GUO 02] GUO Y., ANTONIOUS Z. and DIXIT S., "IP Transport in 3G radio access networks: an MPLS-based approach", *IEEE Wireless Communications and Networking Conference (WCNC)*, March 2002.

[GUP 03] GUPTA A., KUMAR A. and RASTOGI R., "Exploring the trade-off between label size and stack depth in MPLS routing", *INFOCOM*, March 2003.

[GUS 04] GUSTAFSSON E., JONSSON A. and PERKINS C., "Mobile IPv4 Regional Registration", *draft-ietf-mobileip-reg-tunnel-09.txt*, June 2004.

[HAB 06] HABAEBI M., "Macro/micro-mobility fast handover in hierarchical mobile IPv6", *Computer Communications*, Elsevier Science, vol. 29, p. 611–617, March 2006.

[HEI 99] HEINANEN J., BAKER F., WEISS W. and WROCLAWSKI J., "Assured forwarding PHB group", *RFC2597*, June 1999.

[JAC 99] JACOBSON V., NICHOLS K. and PODURI K., "An expedited forwarding PHB", *RFC2598*, June 1999.

[JAM 02] JAMOUSSI B., ANDERSSON L., CALLON R., DANTU R., WU L., DOOLAN P., WORSTER T., FELDMAN N., FREDETTE A., GIRISH M., GRAY E., HEINANEN J., KILTY T. and MALIS A., "Constraint-based LSP setup using LDP", *RFC3212*, January 2002.

[JUN 06a] JUNIPER NETWORKS WHITE PAPERS, "MPLS DiffServ-aware traffic engineering", *[ONLINE]* http://www.juniper.net/solutions/literature/white_papers/200048.pdf, March 2006.

[JUN 06b] JUNIPER NETWORKS WHITE PAPERS, "Supporting differentiated service classes: multiprotocol label switching (MPLS)", *[ONLINE]* http://www.juniper.net/solutions/literature/white_papers/200039.pdf, March 2006.

[KOO 05] KOODLI E.R., "Fast handovers for mobile IPv6", *RFC4068*, July 2005.

[KUB 04] KUBINIDZE N., O'DROMA M. and GANCHEV I., "Integrated algorithm of HMIPv6 & MPLS for ns to support next generation wireless networks", *Telecommunications Quality of Service: The Business of Success (QoS 2004)*, p. 156–159, March 2004.

[LAN 05] LANGAR R., TOHME S. and GRAND G.L., "Micro mobile MPLS: a new scheme for micro-mobility management in 3G all-IP networks", *IEEE Computers and Communications (ISCC)*, p. 301–306, June 2005.

[LIN 02] LIN Y.-D., HSU N.-B. and HWANG R.-H., "QoS routing granularity in MPLS networks", *IEEE Communications Magazine*, vol. 40, p. 58–65, June 2002.

[MET 01] METZ C., "Layer 2 over IP/MPLS", *IEEE Internet Computing*, vol. 5, p. 77–82, July 2001.

[MON 02] MONTAVONT N. and NOEL T., "Handover management for mobile nodes in IPv6 networks", *IEEE Communications Magazine*, vol. 40, August 2002.

[MON 05] MONTAVONT N. and NOEL T., "Improving handoff performance in wireless overlay networks by switching between two-layer IPv6 and one-layer IPv6 addressing", *IEEE Journal on Selected Areas in Communications*, vol. 23, November 2005.

[NOR 01] NORTEL NETWORKS WHITE PAPERS, "MPLS-An introduction to multiprotocol label switching", *[ONLINE]* http://cnscenter.future.co.kr/resource/networking/qos/mplsintro.pdf, April 2001.

[OMA 03] OMAE K., INOUE M., OKAJIMA I. and UMEDA N., “Handoff performance of mobile host and mobile router employing HMIP extension”, *IEEE Wireless Communications and Networking Conference (WCNC)*, March 2003.

[PAL 05] PALMIERI F., “An MPLS-based architecture for scalable QoS and traffic engineering in converged multiservice mobile IP networks”, *Computer Networks*, Elsevier Science, vol. 4, p. 257–269, February 2005.

[PER 02] PERKINS C., “Mobile IP”, *IEEE Communications Magazine*, vol. 40, p. 66–82, May 2002.

[ROS 01a] ROSEN E., TAPPAN D., FEDORKOW G., REKHTER Y., FARINACCI D., LI T. and CONTA A., “MPLS Label Stack Encoding”, *RFC3032*, January 2001.

[ROS 01b] ROSEN E., VISWANATHAN A. and CALLON R., “Multiprotocol Label Switching Architecture”, *RFC3031*, January 2001.

[SET 04] SETHOM K., AFIFI H. and PUJOLLE G., “Wireless MPLS: a new layer 2.5 micromobility scheme”, *MACM Press*, p. 64–71, October 2004.

[SID 05] SIDDIQUI F. and ZEADALLY S., “Mobility management across hybrid wireless networks: Trends and challenges”, *Computer Communications*, Elsevier Science, October 2005.

[SOL 05] SOLIMAN H., CASTELLUCCIA C., EL-MALKI K. and BELLIER L., “Hierarchical Mobile IPv6 mobility management (HMIPv6)”, *RFC4140*, August 2005.

[TAH 05] TAHA A.-E. and HASSANEIN H., “Extensions for Internet QoS paradigms to mobile IP: a survey”, *IEEE Communications Magazine*, vol. 443, p. 132–139, May 2005.

[VAS 03] VASOS V., OWEN H.L., BARLOW D., SOKOL J., HUTH H.P. and GRIMMINGER J., “M-MPLS:Micromobility-enabled Multiprotocol Label Switching”, *IEEE International Conference on Communications(ICC)*, vol. 1, p. 250–255, August 2003.

[WU 01] WU J., MONTUNO D., MOUFTAH H., WANG G. and DASYLVA A., “Improving the reliability of the label distribution protocol”, *IEEE Conference on Local Computer Networks*, November 2001.

[XIA 00] XIAO X., HANNAN A., BAILEY B. and NI L., “Traffic engineering with MPLS in the internet”, *IEEE Network Magazine*, vol. 14, p. 28–33, March 2000.

[XIE 02] XIE K. and LEUNG V., “A MPLS Framework for macro and micromobility management”, *IASTED Wireless and Optical Communications*, July 2002.

[XIE 03] XIE K., WONG V. and LEUNG V., “Support of micro-mobility in MPLS-based wireless access networks”, in *Proceedings of IEEEWireless Communications and Networking*, vol. 2, p. 1242–1247, March 2003.

[YAN 01] YANG T. and MAKRAKIS D., “Hierarchical mobile MPLS: supporting delay sensitive applications over wireless Internet”, *International Conference on Info-Tech & Info-Net*, October 2001.

[YAN 02a] YANG T., DONG Y., ZHANG Y. and MAKRAKIS D., "Practical approaches for supporting micro mobility with MPLS", *International Conference on Telecommunications (ICT)*, June 2002.

[YAN 02b] YANG T., DONG Y., ZHANG Y. and MAKRAKIS D., "Mobility support for differentiated service in next generation MPLS-based wireless network", *International Conference on Communication Circuits and Systems (ICCCAS)*, June 2002.

13.11. Appendix – list of acronyms

3G	3rd Generation
4G	4th Generation
ADT	Advertisement
AF	Assured Forwarding
AR	Access Router
BAs	Behavior Aggregates
BE	Best Effort
CN	Correspondent Node
CoA	Care of Address
CR-LDP	Constraint Based Routed Label Distribution Protocol
CR-LSPs	Constraint-based Routed Label Switched Paths
DAD	Duplicate Address Detection
DiffServ	Differentiated Services
DSCP	Differentiated Services Code Point
EF	Expedited Forwarding
E-LSP	EXP-Inferred-PHB
ER-LSP	Explicitly Routed LSP
ERO	EXPLICIT_ROUTE OBJECT
EXP	Experimental
FA	Foreign Agent
FDA	Foreign Domain Agent
FEC	Forwarding Equivalence Class
FHMIPv6	Fast Handover for Hierarchical MIPv6
FMIPv6	Fast Handover for Mobile IPv6
GFA	Gateway Foreign Agent
HA	Home Agent
HMIPv4	Hierarchical Mobile IPv4
HMIPv6	Hierarchical Mobile IPv6
H-MPLS	Hierarchical Mobile MPLS
IP	Internet Protocol
IPSec	IP Security
ISPs	Internet Service Providers
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6

LCoA	On-Link Care-of-Address
LDP	Label Distribution Protocol
LEMA	Label Edge Mobility Agent
LER	Label Edge Router
LIB	Label Information Base
L-LSP	Label-Only-Inferred-PHB Scheduling Class LSP
LSP	Label Switched Path
LSRs	Label Switching Routers
MAP	Mobility Anchor Point
MIP	Mobile IP
MM-MPLS	Micro-Mobility with MPLS
MN	Mobile Node
MPLS	Multi-Protocol Label Switching
OA	Ordered Aggregates
PDA	Personal Digital Assistants
PHB	Per Hop Behavior
PSC	PHB Scheduling Class
QoS	Quality of Service
RAs	Router Advertisements
RCoA	Regional Care-of-Address
REG-REQUEST	Registration Request
RESV	Reservation
RFA	Regional Foreign Agent
RSVP	Resource Reservation Protocol
RSVP-TE	Resource Reservation Protocol-Traffic Engineering
ToS	Type of Service
VPNs	Virtual Private Networks