3
Background

This chapter summarizes the Mobile IPv6 (MIPv6) [7] functionality and its two main enhancements defined to minimize latency and packet loss during a L3 handover process known as HMIPv6 [8] and FMIPv6 [9]. It also presents the MIH architecture proposed by IEEE 802.21 [5], which specifies a solution to optimize L2 heterogeneous handover (L2 vertical handover).

3.1 MIPv6 Functionality

In Mobile IPv6 (MIPv6), any mobile station can be, at any time, attached to its original network (or *Home Network – HN*) or it can be away, visiting some other domain or network (generically known as a *Foreign Network – FN*). Whenever a station moves from one network to the other, it has to change its point of attachment in a process that involves many procedures including: the acquisition of a new valid address, the registration and authentication in the new domain, etc. The handover is completed when all these required procedures are completed and the station is again capable of communicating with other devices. In order to describe the steps involved during mobility and handover procedures, the MIPv6 specification defines the following functional entities:

- *Mobile Node (MN)* – represents a host that changes its point of attachment from one network or subnetwork to another.
- *Home Agent (HA)* – represents a router on the mobile node's home network (HN), which intercepts packets addressed to the MN's home address (IP address with HN prefix). Whenever intercepted, these packets are encapsulated by the HA and tunneled to the MN when it is away from home. In or-

der to perform these functions, the HA has to maintain what is called a *Binding Cache*, that stores up to date information about MN's current location (address).

- *Access Router (AR)* – represents a router on a Foreign Network, which provides routing services to the MN while registered. For packets sent by the MN, the AR may serve as a default router for registered MNs.
- *Correspondent Node (CN)* – A peer node with which a MN is communicating. The CN may be either a mobile or a stationary node.

In MIPv6, whenever a MN is attached to some foreign link, it can be reached by what is defined as its *Care-of Address* (CoA), which is an IP address associated to the MN that has the subnet prefix of that particular FN. The MN can acquire its CoA through conventional IPv6 mechanisms, such as stateless [11] or stateful auto-configuration (e.g. DHCPv6 [13]). As long as the MN stays in a foreign network, packets addressed to its CoA will be routed to the MN.

Whenever the MN changes its point of attachment, it needs to register its new CoA at the HA. A registration message, known as a *Binding Update* message, is sent by the MN to the HA. In response, a confirmation message, called *Binding Acknowledgement,* is sent by the HA to the MN.

There are two possible communication modes between MN and CN in MIPv6 (Figure 1): (i) bidirectional tunneling; and (ii) route optimization.

3.1.1 Bidirectional Tunneling

Bidirectional tunneling, as described in [7], is available even when the MN does not register its current binding with the CN and does not require any mobility support from the CN. Packets from the CN are routed to the HA and then tunneled to the MN. Packets to the CN are tunneled from the MN to the HA (*reverse tunneled*) and then routed normally from the HN to the CN. In this mode, the HA uses proxy Neighbor Discovery to intercept any IPv6 packets addressed to the MN's home address on the home network. Each intercepted packet is tunneled to the MN's primary care-of address. This tunneling is performed using IPv6 encapsulation [12]. As a result, this mode offers a compatible mechanism that allows

CNs without the mobility binding cache support to communicate to MNs without any modification or adaptation to their functionality.

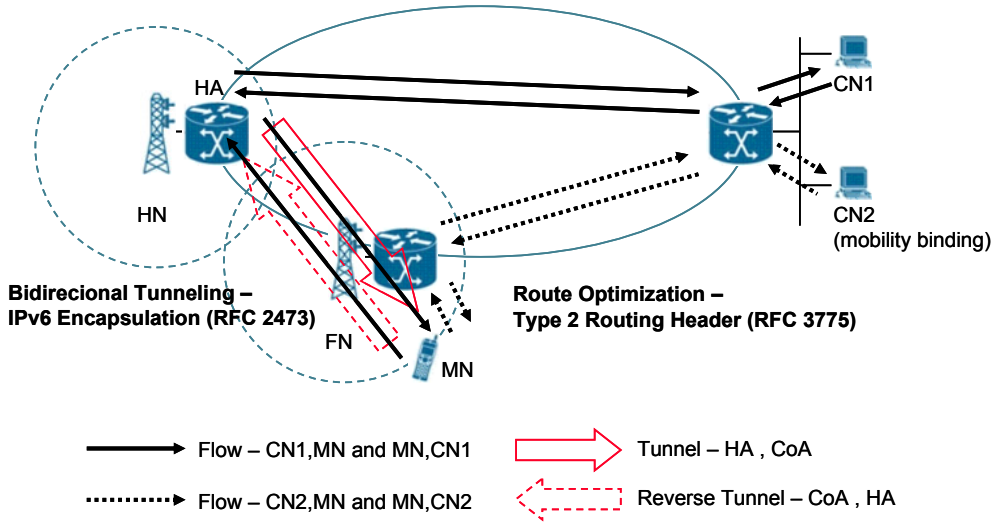

Figure 1– Modes for communication in MIPv6

3.1.2 Route Optimization

Route optimization, as described in [7], requires the MN to register its current CoA at the CN. So, it also requires mobility binding cache support from the CN. In order to be able to execute the registration process, the MN must execute the *return routability procedure* to receive a set of security information that are required to build the Binding Update message (that must be sent to CN to update its binding cache with the new CoA of the MN).

In this mode, packets from the CN can be routed directly to the CoA of the MN. When sending a packet to any IPv6 destination, the CN checks its cached bindings for an entry for the packet's destination address. If an entry for this destination address is found, the node uses a new type of IPv6 routing header, known as *Type 2 Routing Header* [7], to route the packet to the MN using the the CoA indicated in this binding. The Destination Address in the IPv6 header is set to the CoA found in the binding cache and the new Type 2 Routing Header is set to the MN's home address. This routing schema allows the shortest communications path to be used and also eliminates congestion at the MN's HA and home link. In

addition, the impact of any possible failure of the HA (or networks on the path to or from it) is reduced.

Similarly, packets from the MN can be directly routed to the CNs. To do so, the MN sets the Source Address in the packet's IPv6 header to carry its current CoA and adds a new *IPv6 Home Address Destination Option* [7] to carry its home address. The inclusion of home addresses in these packets makes the use of the CoA transparent above the network layer (e.g., at the transport layer).

3.1.3 Optimization Proposals to Reduce Handover Latency

There are optimization proposals to MIPv6, such as HMIPv6 [8] and FMIPv6 [9], that aim to minimize latency and reduce the loss of packets during the handover procedure. In general, these proposals contain solutions to: (i) minimize the time related to CoA registration; (ii) minimize the time related to the change of point of attachment; and (iii) minimize the loss of packets. The following subsections summarize HMIPv6 and FMIPv6 functionalities and contributions.

3.1.3.1 Hierarchical Mobile IPv6 Mobility Management (HMIPv6)

One of the well-known problems that affect mobile communication on MIPv6 is the latency related to the registration of the new CoA. This procedure has a high latency (compared with a registration in a local network) [1] because it requires the MN to exchange signaling messages with components located outside the new network, such as the HA and the CNs that support route optimization.

In order to minimize registration latency, the hierarchical handover schema divides mobility into two categories: (i) *micro-mobility* (generally intra-domain); and (ii) *macro-mobility* (generally inter-domain). The central element of this schema is a conceptual entity known as the *Mobility Anchor Point* (MAP) [8]. The MAP defines a *MAP domain* composed of one or more networks. The movement of a MN between networks of the same MAP domain determines a micro-mobility while a movement of a MN between networks of different MAP domains determines a macro-mobility.

Each of the networks inside a MAP domain has an Access Router (AR) that corresponds to the default router of the MNs located within its covered area. The presence of the MAP of the domain the AR belongs to is announced by the *Router Advertisement* message. Therefore, the change of a MAP domain is perceived by the MN when an announcement with a new (different) MAP is received by the MN.

As described in [8], when the MN moves to a new MAP domain, it must bind its new CoA, known as *Local CoA* (LCoA), to an address in the MAP subnet, known as *Regional CoA* (RCoA), which, in general, corresponds to the MAP address. The MAP acts as a local HA and intercepts all packets addressed to the MN in order to tunnel them directly to the MN's LCoA. If the MN moves to another network on the same MAP domain, it only needs to register its new LCoA at the MAP by sending a Binding Update message. If the MN moves to a different MAP domain, a registration of its RCoA at the HA and at its CNs (by sending a Binding Update message to each of them) is also needed. The RCoA is not modified if the MN moves along the same MAP domain. So, MN's micro-mobility is seamless to HA and CNs. Figure 2 illustrates the hierarchical MIPv6 schema.

In order to optimize handover and reduce packet loss, the MN must send a Binding Update message to its previous MAP informing its new LCoA. Packets that are in transit to the previous MAP will be, then, forwarded to the new LCoA. The MNs are also allowed to send Binding Update messages with their LCoA (instead of their RCoA) to CNs present on the same visited network allowing packets within the same network to be directly forwarded without passing through the MAP.

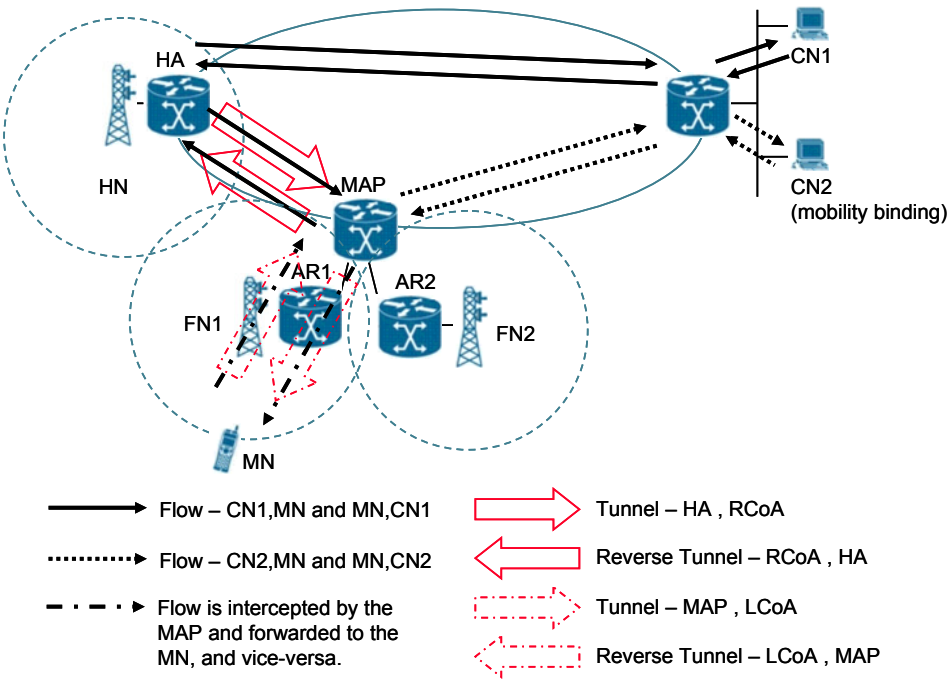

Figure 2 – Hierarchical MIPv6 Schema

3.1.3.2 Fast Handovers for Mobile IPv6 (FMIPv6)

The ability of a MN to start sending packets when it enters a new subnet depends on the latency of the IP connectivity reestablishment, which in turn depends on the movement detection and new CoA configuration latency [9]. Once the IP connectivity of the MN is restored, it can send the Binding Update message to the HA and to all of the CNs. Once its correspondents successfully process the Binding Update message, which typically involves the execution of the return routability procedure to each CN [7], the MN becomes able to receive packets at its new CoA. Therefore, the ability to receive packets at the new CoA depends on the Binding Update latency as well as on the IP connectivity latency.

The FMIPv6 enables the MN to quickly detect movements between networks by providing information about the new point of attachment (PoA) and new subnet prefix while the MN is still connected to the current network. The current default router becomes the *Previous Access Router* (PAR). For example, the MN can discover available PoAs using link layer mechanisms (e. g., WLAN scan operation) and then request information about the subnet prefix of one or more discovered PoAs. This request is made by sending a *Router Solicitation for Proxy*

Advertisement (RtSolPr) to the default router. The MN may do this after performing router discovery or at any time while connected to its current router.

The result of resolving an identifier associated with a PoA is a [PoA-ID, AR-Info] tuple, where PoA-ID is the PoA identification and AR-Info is composed of the L2 address of the router, the IP address of the router and a valid prefix on the subnet of the PoA. The information is delivered to the MN by the *Proxy Router Advertisement* (PrRtAdv) message sent by the PAR.

With the information provided, the MN formulates a prospective *New CoA* (NCoA) and sends a *Fast Binding Update* (FBU) message when a link-specific handover event occurs. The purpose of the FBU is to authorize the PAR to bind the *Previous CoA* (PCoA) to the NCoA, so that arriving packets can be tunneled to the new location of the MN. Whenever feasible, the FBU should be sent from PAR's link. When it is not feasible, the FBU is sent from the new link. By executing the described procedure, the latency due to new prefix discovery subsequent to handover is eliminated as well as the packet loss is reduced.

As a response to the FBU, the PAR should send a *Fast Binding Acknowledgement* (FBack) message. Depending on whether an FBack is received on the previous link, there are two modes of operation:

1. The MN receives an FBack on the previous link. This means that packet tunneling is already in progress by the time the MN handovers to NAR. The MN should send the *Fast Neighbor Advertisement* (FNA) immediately after attaching to NAR, so that arriving and buffered packets can be forwarded to the MN right away. Before sending an FBack to an MN, the PAR can determine whether the NCoA is acceptable to the NAR through the exchange of *Handover Initiate* (HI) and *Handover Acknowledgement* (Hack) messages. When using assigned addressing (i.e., when addresses are assigned by the router), the proposed NCoA in the FBU is carried in HI, and the NAR may assign the proposed NCoA. Such an assigned NCoA must be returned in HAck, and the PAR must in turn provide the assigned NCoA in the FBack. If there is an assigned NCoA returned in the FBack, the MN must use the assigned address (and not the proposed address in the FBU) upon attaching to NAR.

2. The MN does not receive the FBack on the previous link because the MN has not sent the FBU or the MN has left the link after sending the FBU (which itself may be lost), but before receiving an FBack. Without receiving an FBack in the latter case, the MN cannot ascertain whether PAR has successfully processed the FBU. Hence, it (re)sends an FBU as soon as it attaches to NAR. To enable NAR to forward packets immediately (when FBU has been processed) and to allow NAR to verify whether NCoA is acceptable, the MN should encapsulate the FBU in the FNA. If NAR detects that NCoA is in use when processing the FNA, for instance while creating a neighbor entry, it must discard the inner FBU packet and send a *Router Advertisement* with the *Neighbor Advertisement Acknowledge* (NAACK) option in which NAR may include an alternate IP address for the MN to use. This discarding avoids the rare and undesirable outcome that results from address collision.

The scenario in which an MN sends an FBU and receives an FBack on PAR's link is known as *predictive* (*anticipated*) mode of operation and is illustrated in Figure 3.

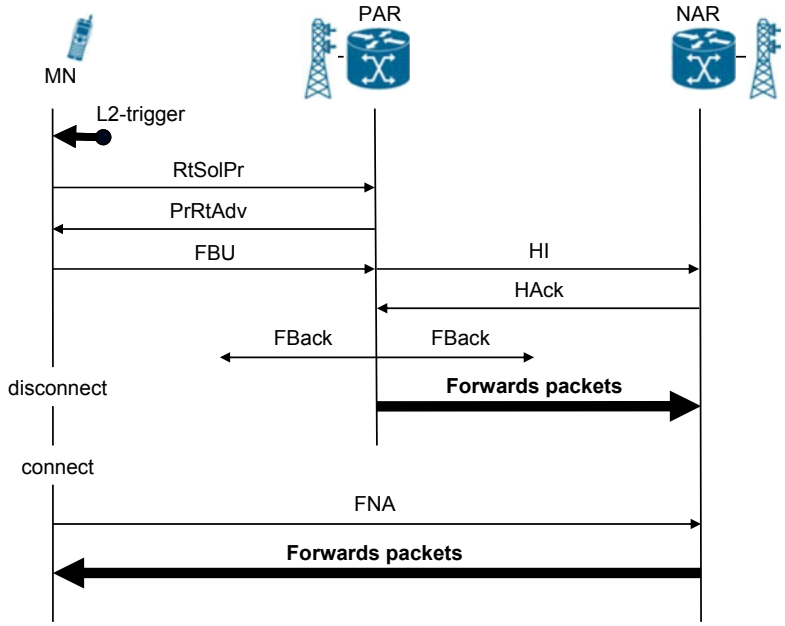

Figure 3 – Fast Handover: predictive mode of operation

The scenario in which the MN sends an FBU from NAR's link is illustrated in Figure 4. For convenience, this scenario is characterized as a *reactive* mode of operation. This mode also includes the case in which an FBU has been sent from PAR's link but an FBack has not been received yet.

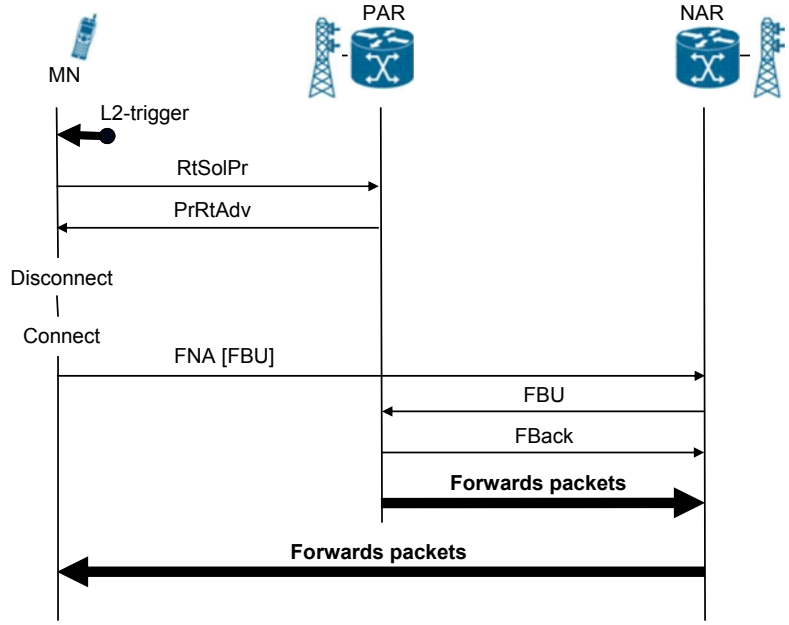

Figure 4 – Fast Handover: reactive mode of operation

Finally, the PrRtAdv message may be sent unsolicited (i.e., without the MN first sending a RtSolPr message). This message can keep the MN informed about geographically adjacent networks, which in turn reduces the amount of traffic necessary to obtain the neighbor topology map of links and subnets.

Concerning HI and Hack messages, they can be used to carry information regarding network context, such as access control, QoS and header compression, as well as handover information.

3.2 Media Independent Handover (MIH)

Media Independent Handover (MIH) – IEEE 802.21 Draft Standard [5] defines methods and functionalities to enable a seamless L2 handover between multiple physical layer network links. This standard provides capabilities to detect and initiate handover from one network to another, but does not define how to treat the handover procedure.

IEEE 802.21 defines a MIH Function (MIHF) between layer 2 and 3 and provides three basic services: (i) *Media Independent Event Service* (MIES); (ii) *Media Independent Command Service* (MICS); and (iii) *Media Independent Information Service* (MIIS). MIHF architecture is illustrated in Figure 5.

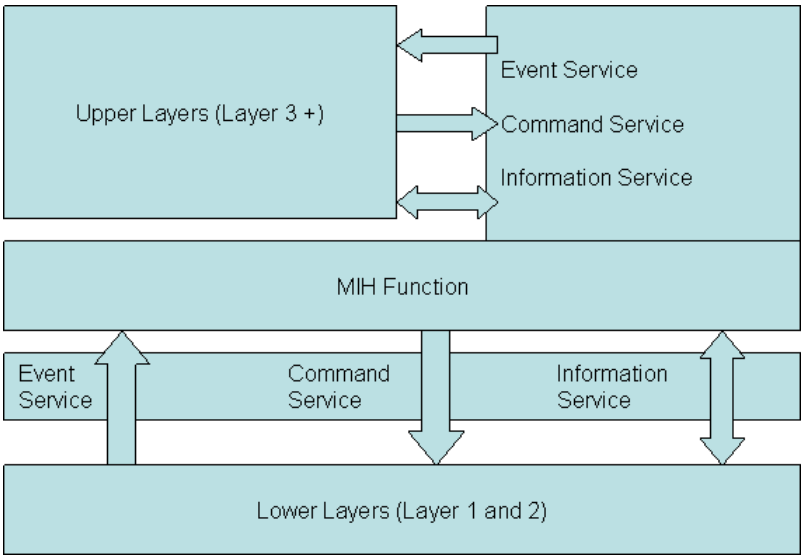

Figure 5 – MIH Function Architecture [5]

MIES provides *event classification*, *event filtering* and *event reporting* corresponding to dynamic changes in link characteristics, link status and link quality. MIH Function must register to link layer in order to be notified by *Link Events* and any upper layers entities in either a local or remote stack (*Point of Access* – PoA – acting as a *Point of Service* – PoS) can register for an *MIH Event notification*, either in groups or with predetermined thresholds. The lower layers will generate a *Link Event* and send it to the MIH Function which will report it to any entity that has registered either an *MIH Event* or a *Remote MIH Event*. Link Events and MIH Events fall into six categories: administrative, state change, link parameter, predictive, link synchronous and link transmission. More details about these events are discussed in [3].

MICS enables MIH users to manage and control link behavior relevant to handovers and mobility. The *MIH Commands* originate from the upper layers and are propagated down to the MIH Function. From there they either become a *Remote MIH Command* to a remote protocol stack or otherwise they continue down

to the lower layers as a *Link Command* from the MIH Function. Link Commands are specific to the access network being used and are local only.

MIIS provides the capability for obtaining the necessary information for handovers including neighbor maps, link layer information, and availability of services. Essentially, this service provides a two way path for all the layers to share information elements (IEs) used to make handover decisions. These IEs are categorized in five groups of information: *General Information* (e.g., operators), *Access Network Information* (e.g., cost, security, QoS), *PoA Information* (e.g., location, data rate, channels), *Upper Layer Service Information* (e.g., subnet information) *and Other Information* (e.g., vendor specific).

Four main concerns should be noted regarding these information:

(i) Access neighbor maps for networks in a geographic area from any network entity may be informed. As an example, Wi-Fi hotspot can be informed about cellular towers and vice versa.

(ii) Static link layer informational parameters may be informed, as QoS support and restricted networks.

(iii) Reports may be used to allow efficiency. As an example, channel range prevents the need for scanning.

(iv) Vendor specific features may be informed, as prioritize networks and network labels.

This service is used to quickly transfer data with very little decoding complexity. Two formats for transferring the reports can be used: (i) *Type-Length Value* (TLV), used by default and illustrated in Figure 6; and (ii) *Resource Description Framework* (RDF) schema, which is represented in Extensible Markup Language (XML).

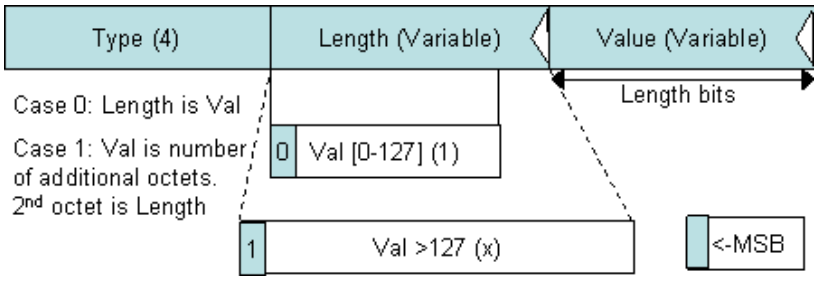

Figure 6 – TLV format for MIH Information Element representation [5]

There are two communication types in MIH Function: (i) between adjacent layers, via *Service Access Points* (SAPs), as defined by the standard; and (ii) between MIH Function entities located in different peers, via the *MIH Protocol*, which encapsulates MIH Frames to be sent over the physical link.