Mobility Management in DECT/IPv6 Networks

Sarantis Paskalis[1], Georgios Lampropoulos[1], and Georgios Stefanou[1]*

Department of Informatics and Telecommunications
University of Athens, Greece

Abstract. The Internet Protocol suite is emerging as the ubiquitous communication platform for almost every conceivable information exchange. Hence, a worldwide effort to support IP functionality over any existing link technology has started, including the dramatically increasing wireless industry. DECT is a well-standardized wireless access network technology, supporting high bitrate digital communications. Moreover, IPv6, the emerging Internet Protocol version, extends support for mobility, wireless nodes and addressing issues.
In this paper, a mobility management architecture is proposed. Mobile IPv6 is deployed, in conjunction with standard DECT mobility procedures to provide a suitable environment for Internet users on the move.

1 Introduction

Wireless devices are constantly enhanced with new capabilities that open up a great window of opportunity for their exploitation. Whereas the size of those handhelds continues to shrink, their processing power continues to increase. Nowadays, handheld devices posses more computing power than many workstations some years ago. Since the mobile devices are serving well to many of everyday productivity tasks, they are posed with more challenging missions.

The most important capability mobile devices should acquire is the communication infrastructure. They should be able to connect to other networks wherever they are. DECT is a well-standardized wireless access network specification with an extensive user base in residential and business wireless telephony. It can provide the necessary bearer support for the information transmission. Since the Internet Protocol suite is the dominant network architecture, a wireless device should exhibit an IP stack in order to be able to communicate globally. The IPv6 standard supports mobile devices through its extensive addressing and mobility extensions.

2 System Architecture

The system architecture of the integration of DECT with Mobile IPv6 is based on the standard functionality of DECT's mobility procedures with some extensions regarding Mobile IPv6. As such, mobility entities are separated into Portable Parts (PPs) and Fixed Parts (FPs). A DECT network consists of an FP with one or more PPs attached

* This work and its dissemination efforts have been partially supported by the General Secretariat for Research and Technology of Greece under grant 99PENED-192.

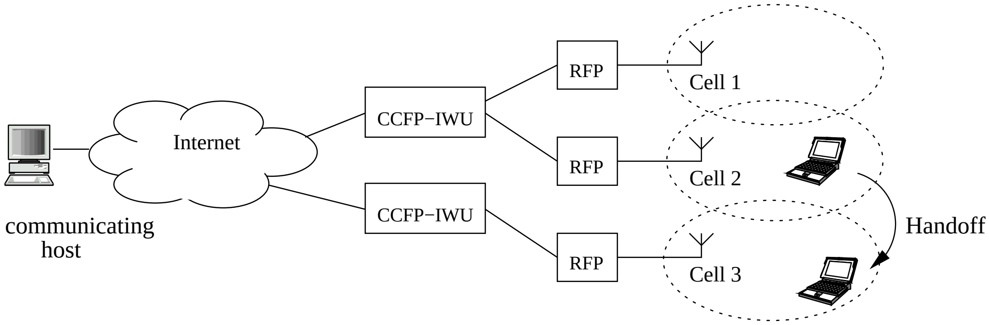

Fig. 1. Network topology

to it. The FP functionality consists of PP control and their interconnection to outside networks. The FP encompasses three functional entities: the Radio Fixed Part (RFP), the Common Control Fixed Part (CCFP) and the Inter-Working Unit (IWU).

The RFP controls the radio interface to the PPs. It contains all the radio endpoints that are connected to a single system of antennas and its coverage area represents a single cell in a cellular system. Concerning the protocol stack functionality, the RFP implements the Physical (PHY) and the Medium Access Control (MAC) layer procedures of DECT, while a Data Link Control (DLC) relay capability is included in order to make the exchange of DLC frames between the CCFP and the PP feasible.

CCFP is in a higher hierarchical position compared to the RFP. It is the core of the FP functionality and only one CCFP can be present in each FP. It supports both the DLC and Network (NWK) layers for communication with several RFPs. Its PP peer entity regarding the exchange of DLC frames is the DLC relay. The CCFP is directly connected to the IWU in order to provide Internet connectivity.

The role of the IWU is mainly to transform any kind of control or data information in a proper format for transmission over different types of networks and vice-versa. A direct interworking of DECT with Ethernet, Token Ring, PPP and IP has already been specified by ETSI [1]. However, there is a continuous work for methods to support Quality of Service (QoS) [2] and mobility [3] in DECT/IP networks.

As presented in Fig. 1, the DECT access network can be mapped as the subnet link in the DECT/Mobile IPv6 architecture. Each DECT network (subnet) is supervised by a CCFP and consists of a number of RFPs, each responsible for a single cell. The PP is always identified by two unique addresses: the IPv6 Home Address in the IPv6 network and the DECT International Portable User Identity (IPUI) in the DECT access network.

An internal table inside the CCFP-IWU is keeping the binding between the IPUI and the IP address the mobile currently uses. If the mobile is locate in in its home network, the IP address will be its Home Address. If the PP is roaming in a foreign network, the binding will contain the Care-of IP Address.

The overall architecture is divided into two planes: The Control Plane (C-Plane) and the User Plane (U-Plane). The U-Plane includes the PHY, MAC and DLC layers. It is used for transmission of IP packets over the DECT links using the LU10 frame

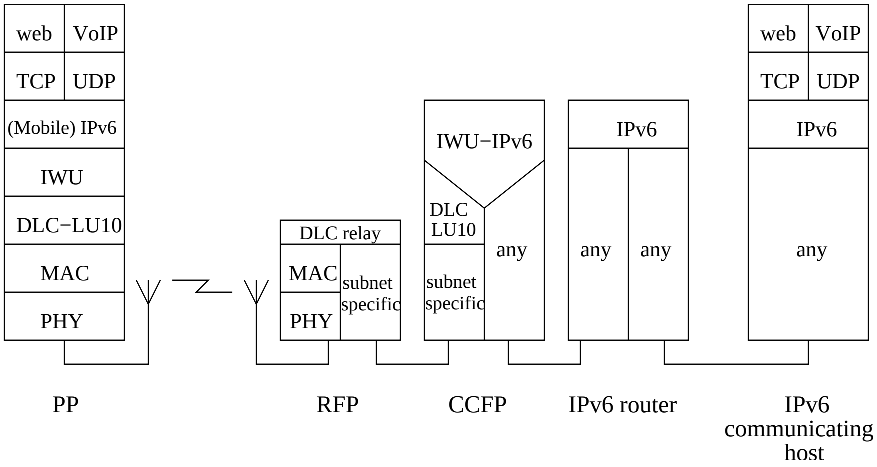

Fig. 2. System Protocol Stack – User Plane

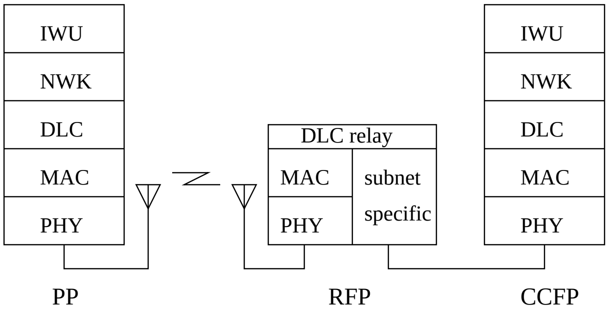

Fig. 3. DECT Protocol Stack – Control Plane

format service [4] of the DLC layer [1]. The essential entity for the data transfer is the IWU placed between the DLC and the Mobile IPv6 layers. The set of IWU functions is realized as a separate sublayer which is already defined in [1]. The CCFP-IWU is the border between DECT and IPv6 procedures, as illustrated in Fig. 2.

Regarding the signaling information transfer, the Control Plane—illustrated at Fig. 3—is extended with the NWK layer functionality compared to the User Plane. The use of the PHY, MAC, DLC layers and IWU is similar to that in the U-plane. In order to establish, negotiate, modify and release a connection, the Call Control (CC) entity procedures are used, while the Mobility Management (MM) entity describes the steps needed for the treatment of each type of location tracking and handoff.

In the next section issues raised by the integration of DECT MM procedures with Mobile IPv6 are discussed. The allocation of an IPv6 address during the initialization phase through DHCPv6 (Dynamic Host Configuration Protocol) is incorporated into the sequence of the signals exchanged between the control entities for a more detailed description of mobility in DECT/IPv6 networks.

3 DECT/IPv6 Interworking

IPv6 IP version 6 (IPv6) [5] is the new version of the Internet Protocol, which contains many enhancements over the current version (IPv4) that is deployed in today's Internet. A communication protocol that was designed a few decades ago could not foresee all the needs for the highly evolving computer industry. In that respect, IPv6 offers improvements in those areas that exhibited scalability or other types of problems. Some of these are:

- Enhanced addressing scheme. The most visible and needed feature of IPv6 is the expansion of the address space from 32 to 128 bits, that provides support for a huge number of hosts, most of which are expected to be mobile. It also simplifies greatly the address self configuration task for those devices. Multicast is also improved and the "anycast" address is specified to send a packet to any one of a group of nodes.
- Header simplification. Although the header size increases significantly (128 from 32 bits), the default header fields are reduced in number, resulting to more flexible processing in the intermediate routers.
- Extensibility. The header fields restructuring has resulted in a more flexible header option processing manner. New header fields can be added without causing significant processing overhead.
- Discrimination of packet flows. The Flow Label field added in the IPv6 header allows the distinction of packets according to their traffic "flows" and their potential preferential treatment.

Mobile IPv6 is a solid migration path from today's Internet to next generation networks, where mobile nodes and terminals are supposed to be always on-line.

DHCPv6 In IPv6 environments, a node may communicate through several interfaces. All interfaces are required to have at least one IPv6 address, their link-local address. Link-local addresses are used for communication between nodes in the same link (subnet), and are unique for that link [6]. A link-local address is constructed by a specific prefix indicating local use only, and an interface identifier that could be based on the EUI64 [7], or most possibly in the case of DECT, on the E.164 format [8].

After a node is assigned a link-local address, it can proceed with DHCPv6 mechanisms in order to obtain a global IPv6 address [9]. In DHCPv6, the allocation of addresses to nodes follows the client-server model. The mobile node acts as a DHCP client requesting an address (or other information like routing or OS installation information) from a DHCP server. Specifically, the client sends a request to the multicast address of all DHCP agents (FF02::1:2) and waits for replies, if the DHCP server address is unknown. A specific server is chosen by the client, according to the received replies. DHCP servers may not be located on the client's link for scalability and economy reasons. In such cases, a DHCPv6 relay must be placed in the client's subnet and is responsible for forwarding messages from client to server and vice versa.

The communication between the client and the server is based on the exchange of request-reply messages. If the address of the DHCP server is known, the client sends a request message to that server, asking for a pool of addresses for each of its

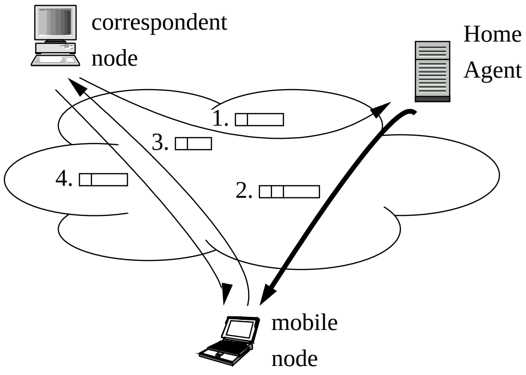

Fig. 4. Mobile IPv6 functionality

interfaces. This message includes the client's link-local address (the link-local address of the interface for which the client is using DHCP), the server's address and an option field called Identity Association (IA). The IA is a construct through which a server and a client can identify, group and manage IPv6 addresses. Each IA is associated with one of the client's interfaces and the client uses the IA to obtain IPv6 addresses for that interface from a server. An IA consists of a 64-bit field DUID (DHCP Unique Identifier), that identifies uniquely each interface, and a list of associated IPv6 addresses.

The server, upon reception of a request message, examines an internal table, where the configuration parameters for each interface are kept, and allocates IPv6 addresses to the interface requested. The allocation procedure is based on the building of a binding between each interface and the allocated IPv6 addresses for that interface. This binding is indexed by the tuple <prefix, DUID>, where the prefix is the client's link prefix, and the DUID is the one contained in the request message. After the allocation mechanism is completed, a reply is sent back to the client, indicating successful or unsuccessful binding, i.e IPv6 addresses are allocated or not to the requested interface. Each IPv6 address assigned to an IA has a specific expiration time (lease), which is included in the reply message.

Mobile IPv6 Mobile IPv4 [10] was developed as a mobility extension for IPv4 [11]. It introduced the concept that a mobile node should be always reachable through a single IP address, independently of its actual location. To achieve this goal, new entities and terms were introduced and existing components were enhanced. The main concept is that any mobile node should always be reachable by means of a single IP address, its Home Address.

Since the Internet Protocol was not designed for mobile hosts, Mobile IPv4 had to work around many problems in suboptimal manners. Triangular routing, extensive tunneling and firewall problems are but a few. IPv6, on the other hand, is a new protocol that takes into account the expected growth in the number and capabilities of mobile devices. The respective mobility extension for IPv6 is Mobile IPv6 [12]. Mobile IPv6, in contrast to Mobile IPv4, takes advantage of the infrastructure IPv6 offers to support mobile hosts and enables a more efficient communication path for mobile computers.

The philosophy behind Mobile IPv6 has remained the same as Mobile IPv4. Each mobile node is always identified by its Home Address, regardless of its current point of attachment to the Internet. When it is located away from its home network, the mobile node has also a Care-of Address indicating its current location. Any packets destined to the Home Address are rerouted to its Care-of Address. IPv6 supports bindings between the mobile's Home Address and its respective Care-of Address in any other IPv6 that communicates with that mobile. An analytical signaling exchange is illustrated in Fig. 4.

The mobile node is roaming in a foreign network and has informed its Home Agent with a Binding Update about its current Care-of Address previous to the presented packet exchange. In the first step an IPv6 capable host across the Internet is sending an IPv6 destined to the mobile node's IPv6 Home Address. The Home Agent intercepts it by means of IPv6 Network Discovery [13]. It figures out that the mobile node is not attached to its home link, but it roams in a foreign network and has acquired the Care-of Address. The second step is the transmission from the Home Agent to the Care-of Address of the mobile node of an encapsulated packet, that contains the original packet as payload and an additional header consisting of the current Care-of Address. The mobile node decapsulates it and, wishing to establish a direct communication to the correspondent host, transmits to the correspondent host a Binding Update, that informs it about the <Home Address, Care-of Address> binding (packet 3). The correspondent host, on the reception of the Binding Update, creates a cache binding for the Home and Care-of Address of the mobile host and transmits any remaining packets directly to the Care-of Address (packet 4) bypassing the home network altogether. The procedure is transparent to the higher layers (above IPv6) and the application need not know that the communicating node is not attached to its home network.

3.1 Location Management (IPv6)

In every mobile environment, it is important for the network to keep track of the position of each terminal, in order to set up and route properly incoming calls, connections or packets. Issues of determining and finding the mobile hosts are covered through the Location Management procedures.

DECT Location Management Three location tracking mechanisms have been specified in DECT: Location Registration, Location Update and Detach [14].

The Location Registration mechanism is used by the PP to indicate to the FP its current location in terms of Location Areas (LAs). The LA usually consists of part of one or several DECT systems and may cover several RFPs. The PP initiates the registration mechanism after it figures out that it has moved to a new LA. The RFP in each cell broadcasts periodically the cell identity to its associated PPs. This is a Radio Fixed Part Identifier (RFPI). It consists of a Primary Access Right Identity (PARI) field and a Radio Fixed Part Number (RPN) field. A cell inside a LA is uniquely identified by the RPN field while the PARI field is similar for all cells in the same

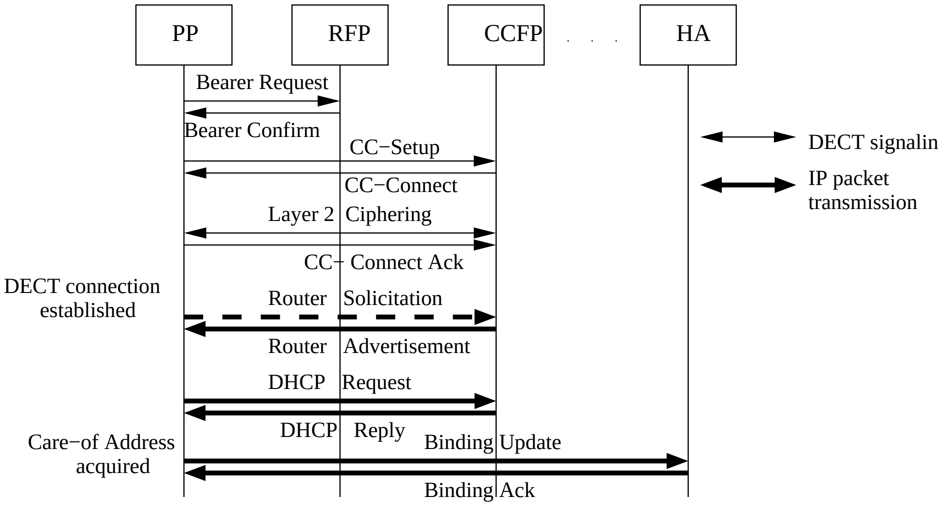

Fig. 5. Location registration for an IPv6 enabled DECT terminal

LA. In order to initiate the registration process, the PP compares the PARI field of the last RFPI kept in its buffer with the PARI field of the current RFPI. If these are different, the PP sends a Location Request message to the FP including its IPUI. The FP responds with a Location Accept message in case of successful registration or with a Location Reject message otherwise. The registration procedure when the PP has not changed LA is called attach and is similar to the case of new LA.

Location Update is used by the FP to inform the PP of a modification of the LAs. Detach is the process whereby a PP informs the FP that it is not ready to receive incoming calls.

DECT-Mobile IPv6 Location Management – Registration From the mobility management procedures in DECT and Mobile IPv6 described earlier, it is clear that the interworking between DECT and Mobile IPv6 has to be quite efficient in order not to affect the current functionality of the two technologies. This can be accomplished by considering two levels of mobility: A DECT mobility level and a Mobile IPv6 mobility level. The former is responsible for the movement inside a single DECT network, while the latter deals with cases where mobility is extended beyond the boundaries of a single DECT island.

Based on the architecture presented in Fig. 1, the CCFP can be considered as an edge router related to the DECT network. It is responsible for forwarding messages outside the DECT boundaries and generating proper Router Advertisement messages. The advertisements are quite valuable for determining the address configuration policy for a non configured host [13]. Since DHCPv6 is selected as the main configuration protocol, the CCFP must also possess the functionality of a DHCPv6 server, whereas the PP must act as a DHCPv6 client. The necessary signaling flow for the location registration case is illustrated in Fig. 5.

After the PP determines a change regarding the LA, it tries to establish a physical connection with the RFP in its current area. This is accomplished by the Bearer Request and Bearer Confirm messages. Right after receiving the Bearer Confirm message, a NWK layer set-up process is initiated between the PP and the CCFP. A CC-Setup message is sent to the CCFP indicating new connection and a response is sent back in case of success from the CCFP through the CC-Connect message. For security reasons the communication between the two entities may be ciphered (Layer 2 Ciphering messages). The new connection establishment is finished with a CC-Connect Ack sent from the PP to the CCFP. Since the PP has recently moved to the current area, it is important to register its position. This is done with the exchange of DECT Location Registration messages. A Location Request message is sent from the PP to the CCFP, including the IPUI of the PP, and a Location Accept is received at success. This is the point where the DECT mobility functionality stops and IPv6 procedures take over in order to establish a communication path for IPv6 packets to be received from and transmitted outside the DECT network.

Before acquiring a global IPv6 address, the PP must have a link-local address for communication inside the subnet (a single interface per IPv6 node is assumed). The interface identifier for a link-local address can be for example the 40-bit type N IPUI, which is the residential default IPUI. It is a unique type, as mandated by [15]. The IPUI is zero-padded in order to build a 64-bit interface identifier [7]. After acquiring a link-local address, the PP must get a global address. The PP may optionally generate a Router Solicitation message in order to check the presence of a router. If a Router Advertisement is received, the PP can decide for the use of DHCPv6 or the Stateless Autoconfiguration based on the contents of the message. If no Router Advertisement is received, the absence of a router is assumed and the DHCPv6 is used.

If DHCPv6 is the preferred configuration protocol, the PP will send a DHCP Request to the multicast address of all DHCP Agents. The request message contains the 40-bit type N IPUI in the place of the 64-bit IA DUID for unique identification. After receiving a DHCP Request, the CCFP updates its internal resource tables, selects an IPv6 address and sends a DHCP Reply to the PP. The PP may receive more than one replies, and should select the closest CCFP DHCP Server, to reduce signaling traffic. If there are no addressing conflicts in the subnet of the PP with other PPs, the IPv6 address assigned to the PP is finally considered a valid IPv6 address and Mobile IPv6 Registration procedures follow.

The PP will send a Binding Update to its Home Agent (HA) indicating its new Care-of Address. The Home Agent checks the mobile's credentials and if the authentication is successful, it replies with a Binding Ack. After this message exchange, the mobile is now globally reachable through its Home Address.

3.2 Handoff

A handoff occurs when the PP switches to a different point of attachment (RFP). Two handoff cases exist, the internal and the external handoff. In the former case the two successive RFPs, onto which the PP attaches, are controlled by the same CCFP (Cells 1 and 2). In the latter case, the PP switches to an RFP that is controlled by a different CCFP.

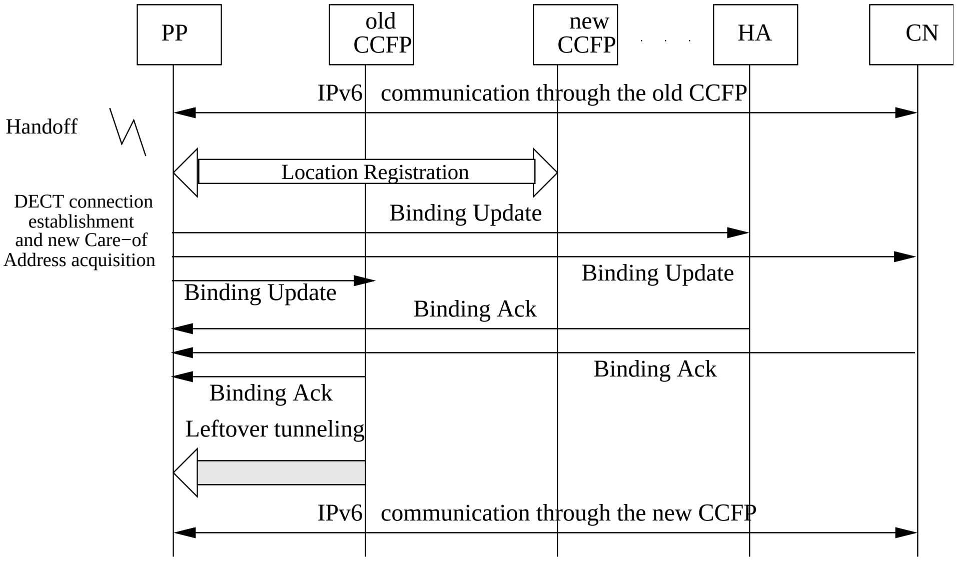

Fig. 6. IPv6 signaling exchange after a handoff

The internal handoff case is handled exclusively through DECT mobility procedures [14]. Hence, no interaction with IP takes place when a PP is moving solely inside a DECT access network that is controlled by a single CCFP.

The interesting case is the external handoff. When the PP switches to an RFP that is controlled by a different CCFP, it can no longer maintain the same address for roaming in that network. For illustration purposes, we assume the generic case, where the PP is already roaming in a foreign network, has acquired a Care-of Address, and is communicating with another host on the Internet.

When the PP detects that a neighboring cell offers better communication conditions, the PP hands off to the new RFP. The new RFP is assumed to be controlled by a different CCFP. Since no communication mechanisms are defined in DECT for CCFP–CCFP interaction and we are dealing with IPv6 enabled devices, Mobile IPv6 is activated and its mobility procedures are applied.

Figure 6 illustrates the signaling exchange for a handed off PP. The RFP entities are omitted, since they just relay the data to the respective CCFPs. When the PP hands off, it begins the location registration procedure detailed in Fig. 5. The only difference in the handoff case is that the DHCP Request message is replaced by the DHCP Confirm message. After the DECT location registration procedure, and the Care-of Address configuration is completed, the PP sends a Binding Update to its Home Agent to inform it about the Care-of Address modification. Since it is already engaged in an IPv6 communication with a correspondent node (CN), it issues a Binding Update to it as well. Additionally, the PP may send a Binding Update to the previous CCFP. The old CCFP acts as a Home Agent for the previous Care-of Address and forwards any incoming packets toward the new Care-of Address.

Any entity that received a Binding Update (Home Agent, Correspondent Node, old CCFP) should respond with a a Binding Ack to indicate the reception and successful processing of the Binding Update. After this mobility signaling, the communication with the correspondent node can continue through the new Care-of Address.

4 Conclusions

The system architecture for the DECT/IPv6 interworking was analyzed and the necessary protocol stacks were defined. The location management procedures were pointed out for DECT as well as for the IPv6 domain and mobility was demonstrated by means of Mobile IPv6. The IWU, located on the border between the DECT access network and the IP layer was identified as the essential communication entity that deals with any interaction between DECT and IPv6. We have presented a DECT/IPv6 interworking scheme that overcomes the limited mobility DECT offers through the exploitation of Mobile IPv6. The enhanced functionality placed on the DECT controller is justified by the seamless wireless Internet access for the DECT/IPv6 terminals.

References

1. ETSI. Digital Enhanced Cordless Telecommunications (DECT); DECT Packet Radio Service (DPRS). EN 301 649, February 2001.
2. D. Ziotopoulou, D. Skyrianoglou, K. Orfanakos, and E. Zervas. A DECT-IP interworking for quality of service support. In *8th Panhellenic Conference on Informatics*, Nicosia, Cyprus, November 2001.
3. A. Lo, W. Seah, and E. Schreuder. An efficient DECT-Mobile IP interworking for mobile computing. In *IEEE Vehicular Technology Conference*, Tokyo, Japan, May 2000.
4. ETSI. Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); part 4: Data link control (DLC) layer, ed. 2. ETS 300 175-4, September 1996.
5. S. Deering and R. Hinden. RFC 2460: Internet Protocol, Version 6 (IPv6) specification, December 1998.
6. R. Hinden and S. Deering. RFC 2373: IP version 6 addressing architecture, July 1998.
7. IEEE. Guidelines for 64-bit global identifier (EUI-64) registration authority, March 1997.
8. ITU-T. Recommendation E.164: The international public telecommunication numbering plan, May 1997.
9. J. Bound, M. Carney, C. Perkins, and R. Droms. Dynamic Host Configuration Protocol for IPv6 (DHCPv6). Internet Draft, March 2001.
10. C. Perkins. RFC 2002: IP mobility support, October 1996.
11. J. Postel. RFC 791: Internet Protocol, September 1981.
12. D. Johnson and C. Perkins. Mobility support in IPv6. Internet Draft, November 2000. Work in Progress.
13. T. Narten, E. Nordmark, and W. Simpson. RFC 2461: Neighbor discovery for IP Version 6 (IPv6), December 1998.
14. ETSI. Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); part 5: Network (NWK) layer, ed. 3. ETS 300 175-5, December 1997.
15. ETSI. Radio Equipment and Systems (RES); Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); part 6: Identities and addressing, ed. 2. ETS 300 175-6, September 1996.