A Framework for Mobility and QoS Provisioning in IPv6 DECT Networks

Sarantis Paskalis[1], Georgios Lampropoulos[1],
Dimitris Skyrianoglou[1], and Evangelos Zervas[2]

[1] Communication Networks Laboratory
Department of Informatics and Telecommunications
University of Athens, Greece
{paskalis,glambr,dimiski}@di.uoa.gr
[2] Department of Electronics, TEI of Athens, Athens, Greece
zervas@ee.teiath.gr

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 booming 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, QoS, wireless nodes and addressing issues. We propose a framework for mobility and QoS provisioning in IPv6 DECT networks. Mobile IPv6 is deployed, in conjunction with standard DECT mobility procedures to provide a suitable environment for Internet users on the move. Furthermore, RSVP is utilized to handle QoS signaling.

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 the handheld terminals 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 feature of any mobile device is a generic communication capability. The devices 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 a flexible and adjustable bearer support for the information transmission of various applications. 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

Y. Manolopoulos et al. (Eds.): PCI 2001, LNCS 2563, pp. 368–385, 2003.

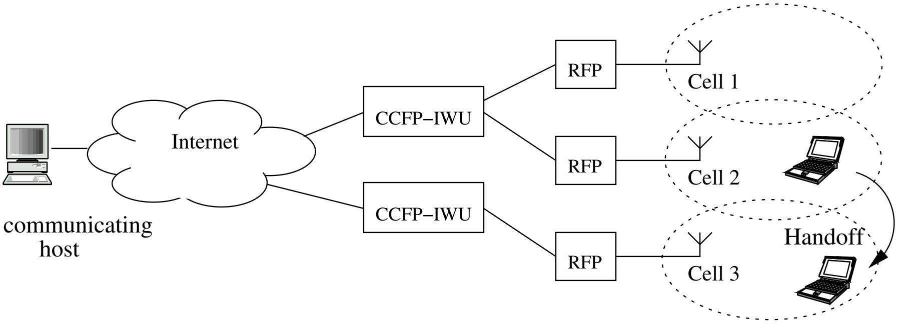

Fig. 1. Network topology

its extensive addressing and mobility extensions, while QoS guarantees can be satisfied through the use of the well established RSVP protocol.

The combination of the aforementioned technologies, however, is a difficult task, given the different focus points. An overview of the involved technologies is given in Section 2. The proposed system architecture is analyzed in Section 3 defining the basic mobility management infrastructure, interconnecting IP and DECT. Section 4 examines the interworking between RSVP and our framework and points out some possible approaches for their integration, while Section 5 concludes this work.

2 Overview

2.1 DECT

DECT (Digital Enhanced Cordless Telecommunications) [8] denotes a radio technology suited for voice data and networking applications with range requirements up to a few hundred meters. DECT mobility entities are separated into Portable Parts (PPs) and Fixed Parts (FPs). A DECT access network consists of an FP with one or more PPs attached to it. The FP encompasses three functional entities: the Radio Fixed Part (RFP), the Common Control Fixed Part (CCFP) and the Inter-Working Unit (IWU) as shown in Fig. 1.

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. Each DECT network is supervised by a CCFP and consists of a number of RFPs, each responsible for a single cell.

The IWU is directly connected to the CCFP, and its role 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 [12].

DECT Connectivity Modes DECT supports three modes of connection, Call Control (CC), Connection Oriented Message Service (COMS), and Connection-Less Message Service (CLMS) [10]. Call Control is the main service instance. It provides a set of procedures that allow the establishment, maintenance and release of switched services, as well as support for call related signaling. COMS offers a point-to-point protocol oriented packet service. On the contrary, CLMS offers a connectionless point-to-point or point-to-multipoint service.

DECT Location Management Three location tracking mechanisms have been specified in DECT: Location Registration, Location Update and Detach [10].

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 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 default Location Area is defined as the PARI field of the RFPI, but it is also possible to define Location Areas by a fraction of the RFPI identity using the Location Area Level (LAL) indicator. In order to initiate the registration process, the PP compares the LA field of the last RFPI kept in its buffer with the LA 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. If the LA values are the same, the PP remains in the same LA, and the registration procedure is similar and named “attach”.

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.

2.2 IPv6

IP version 6 (IPv6) [6] 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 the address self configuration task for those devices. Multicast is 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 need to be always on-line.

2.3 IPv6 Addressing Issues

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), are unique for that link, and should be assigned prior to any other IPv6 address [16]. A link-local address is constructed by a specific prefix indicating local use only (FE80::/64), and an interface identifier that could be based on the EUI-64 [17]. In order to avoid any duplicate addresses, the “Duplicate Address Detection” mechanism is performed on all addresses before assignment. After a node is assigned a link-local address, it can proceed with stateful (DHCPv6) or stateless (IPv6 Stateless Auto-configuration) mechanisms to obtain a global IPv6 address.

DHCPv6 In DHCPv6 [7], the allocation of addresses to nodes follows the client-server paradigm. The mobile node acts as a DHCP client requesting an address (or other configuration parameters) from a DHCP server. The client sends a solicitation message to the multicast address of all DHCP agents (FF02::1:2) in order to find a DHCP server that could provide the requested configuration parameters.

Each server identifies the client by a DHCP Unique Identifier (client DUID) contained in the solicitation message and replies with an advertisement message including the server DUID. The DUID (both client and server) is of variable length and constructed into one of four possible formats: Link-layer address plus time, Vendor-assigned unique ID based on domain name, Vendor-assigned unique ID based on Enterprise Number or Link-layer address.

The solicitation and the advertisement messages also contain an option field called Identity Association (IA), which is a construct for identification, grouping and management of addresses assigned to a client interface. It is characterized by an IA identifier (IAID), chosen by the client to be unique among the IAIDs for the particular client. According to the suitability of the advertisement messages received regarding the IAs, the client choses the fittest server. DHCP servers may not be located on the client's physical link for scalability and economy reasons. In such cases, a DHCPv6 relay agent is placed in the client's subnet and is responsible for forwarding messages from client to server and vice versa.

After a specific server is chosen, the communication between the client and the particular server continues with the exchange of request-reply messages. The client sends a request message to the server, asking for resources. The request message includes the client identifier (DUID), the server identifier (DUID) and one or several IAs. 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 client. The allocation procedure is based on the link to which the client is attached, the DUID supplied by the client and other information supplied by the client or the relay agent. During this process, a binding between each interface of the client and the allocated IPv6 addresses for that interface is built. This binding is indexed by the tuple <DUID, IA-type, IAID>, where the DUID is the client DUID, the IA-type is the address type of the IA (for example temporary) and the IAID is the identifier for the IA that requests DHCP resources from the server. 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 requesting interface. Each IPv6 address assigned to an IA has a specific expiration time (lease), which is included in the reply message and may be renewed later.

IPv6 Stateless Auto-Configuration IPv6 provides a stateless configuration mode [27] for IPv6 nodes. In this mode, the assignment of IPv6 addresses is simplified and there is no need for servers. After an interface is assigned a link-local address, the node tries to construct a global IPv6 address. The global address is formed by substituting the link-local prefix with the subnet prefix in the link-local address. In other words, the IPv6 address is formed with the addition of the advertised subnet prefix to the interface identifier.

The powered-on node discovers the subnet prefix, by means of Router Advertisements (broadcast periodically) or by sending a Router Solicitation to the all-routers multicast group [20]. The Router Advertisements contain the subnet prefix and additional information, such as the lifetime values which indicate how long the addresses remain valid. Since the delay for a Router Advertisement is critical for the performance of stateless configuration, the node may generate a link-local address and send a Router Solicitation in parallel in order to speed

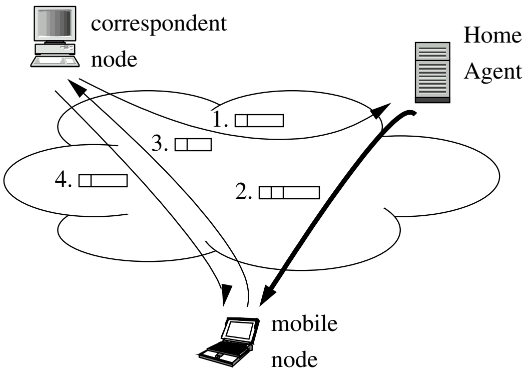

Fig. 2. Mobile IPv6 functionality

the process. This procedure may save time when the Router Advertisement is not received a short time after the assignment of the link-local address.

Addressing Schemes Assessment The two ways of IPv6 addressing configuration offer different advantages according to the configuration needs.

The use of stateless auto-configuration minimizes the signaling required before an address is assigned to an interface. Thus, stateless auto-configuration is attractive in cases where the need for extra configuration parameters is legible and the domain is not particularly concerned with the exact addresses used by hosts.

DHCPv6 instead, is not only a "stateful" version of stateless auto-configuration, but it extends the configuration parameters supported. With DHCPv6, the administration of IPv6 addresses is very flexible. The use of Dynamic Updates to Domain Name Servers (DNS) for auto-registration is also possible. DHCPv6 capabilities move beyond the usual addressing issues and may include load balancing mechanisms between DHCP servers [28] or security enhancements [13]. The drawback of the DHCPv6 approach is the accurate addressing issues, the necessity to keep several identifiers on persistent storage and the increased signaling exchanged. This implies the presence of servers with certain hardware capabilities.

2.4 Mobile IPv6

Mobile IPv4 [23] was developed as a mobility extension for IPv4 [24]. 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 [18]. 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 in 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 Home Address of the PP and its respective Care-of Address in any other IPv6 host that communicates with that mobile. An analytical signaling exchange is illustrated in Fig. 2.

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 a packet destined to the mobile node's IPv6 Home Address. The Home Agent intercepts it by means of IPv6 Network Discovery [20]. 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.

2.5 Quality of Service

Quality of Service (QoS) is an ambiguous concept with different interpretations. In the Internet community, two schools of thought have gained ground for the provision of QoS: the Integrated Services Architecture [4] and the Differentiated Services Architecture [3]. The common aspect in both architectures is the effort undertaken to treat certain packets preferentially, so as to "guarantee" their on-time delivery. They are mainly targeted to real-time applications such as Voice-over-IP or streaming video.

RSVP [5] is a protocol implementation of the Integrated Services Architecture. It provides a well defined means to specify a data flow and to reserve resources in the communication path of the flow. It is designed to deal end-to-end with unidirectional flows, facilitating QoS requests throughout the communication route. Its flexibility stems from the fact that it does not deal directly with QoS service details or flow specification, but merely interacts with the respective "packet scheduler" and "packet classifier" at each node to ensure provision of the necessary QoS and flow identification. In our study, we will use the Fixed Filter reservation style, suitable for unicast applications. The two fundamental RSVP message types are Resv and Path.

Each RSVP sender host transmits RSVP "Path" messages downstream along the route provided by the routing protocol, following the paths of the data. These Path messages store "path state" in each node along the way. This path state includes at least the unicast IP address of the previous hop node, which is used to route the Resv messages hop-by-hop in the reverse direction.

Each receiver host sends RSVP reservation request (Resv) messages upstream toward the senders. These messages must follow exactly the reverse of the path(s) the data packets will use, upstream to the sender host. They create and maintain "reservation state" in each node along the path(s). Resv messages must finally be delivered to the sender host, so that the host can set up appropriate traffic control parameters for the first hop.

The Integrated Services architecture is best applied to access networks due to its fine-grained classification, whereas core networks can scale better when the Differentiated Services architecture is applied. In our study, we assume that QoS reservations are performed with RSVP in the access network. The core network can support either kind of QoS architecture. If it only supports Differentiated Services, then some interworking scheme can be employed [1]. If the core network supports RSVP, then no extra components need to be added.

2.6 Related Work

IP transportation over DECT is an issue that is generally covered by the DPRS specification [12]. The provision, however, of efficiency and flexibility is the goal of ongoing research work. Mobility between different DECT access networks and DECT interworking with Mobile IP is dealt with in [19]. The efficiency of IP transportation over DECT is examined in [30]. QoS in the light of interworking with the service classes of 3G networks is approached in [15]. Our work aims to provide an integrated framework, in which DECT terminals can be used as fully fledged QoS-aware IPv6 terminals.

3 Proposed Framework

3.1 System Architecture

The system architecture for the integration of DECT with Mobile IPv6 and RSVP is based on the standard functionality of DECT mobility procedures. As

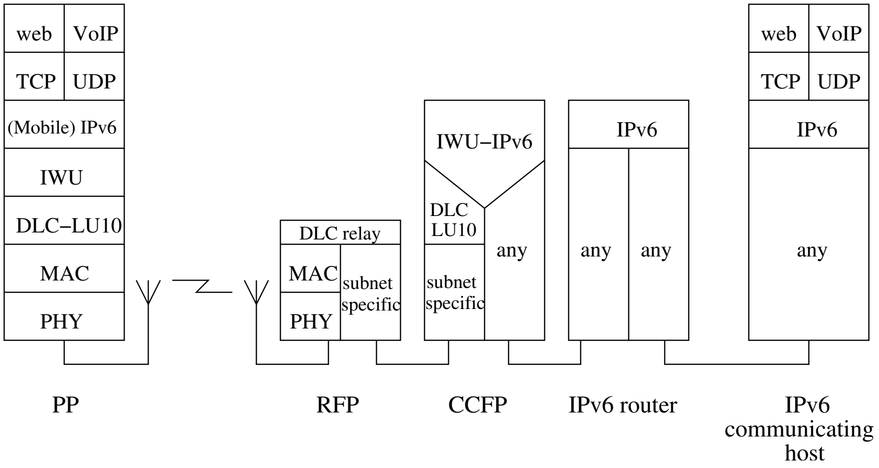

Fig. 3. System Protocol Stack – User Plane

shown in Fig. 1, the DECT access network is considered 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 CCFP is directly connected to the IWU in order to provide Internet connectivity. 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

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 format service [9] of the DLC layer [12]. The essential entity for the data transfer is the IWU, placed between the DLC and IPv6 layers. The set of IWU functions is realized as a separate sublayer which is already defined in [12]. The CCFP-IWU is the border between DECT and IPv6 procedures, as illustrated in Fig. 3.

Regarding the signaling information transfer, the Control Plane is extended with the NWK layer functionality compared to the User Plane as illustrated in Fig. 4. 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.

3.2 IP Transportation over DECT Connections

After careful analysis of the functionality provided by the DECT connection modes in Section 2.1, CC seems to be more suitable to support IP traffic with

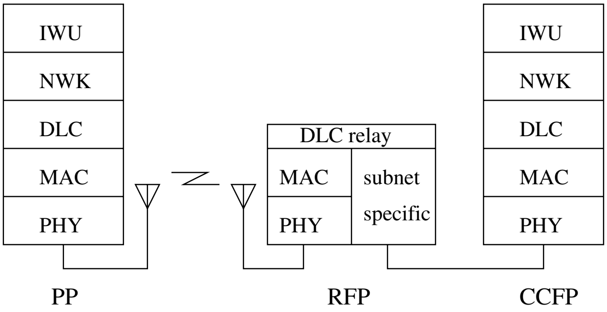

Fig. 4. DECT Protocol Stack – Control Plane

QoS provisioning. Specifically, CLMS is not quite suitable due to its limitation in supporting bandwidth demanding applications. COMS does not offer advanced connection modes which allow negotiation of the bandwidth allocated for the specific instance. Therefore, the remaining approach was to utilize the CC service that supports an extended functionality for service negotiation.

In CC procedures, each independent service is a "call" and is controlled by an independent instance of the CC. CC represents a group of procedures covering all aspects of call establishment, modification and release. In our proposed framework, the procedure of initiating a CC connection executes upon the terminal's power-on. Following this initiation sequence, the DECT enabled device has a setup IP communication route as soon as possible after the power-on.

3.3 DECT–Mobile IPv6 Location Management – Registration

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.

The mobility management procedures in DECT and Mobile IPv6 described earlier point out that the interworking between DECT and Mobile IPv6 has to be very efficient so as not to affect the current functionality of the two technologies. The efficiency can be accomplished by considering two levels of mobility: A DECT mobility level and a Mobile IPv6 mobility level. The former is responsible for any movement inside a single DECT network, whereas 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 used to determine the address configuration policy for a non-configured host [20]. In our proposed system, advanced configuration and security features are desirable and, thus, DHCPv6 is deemed

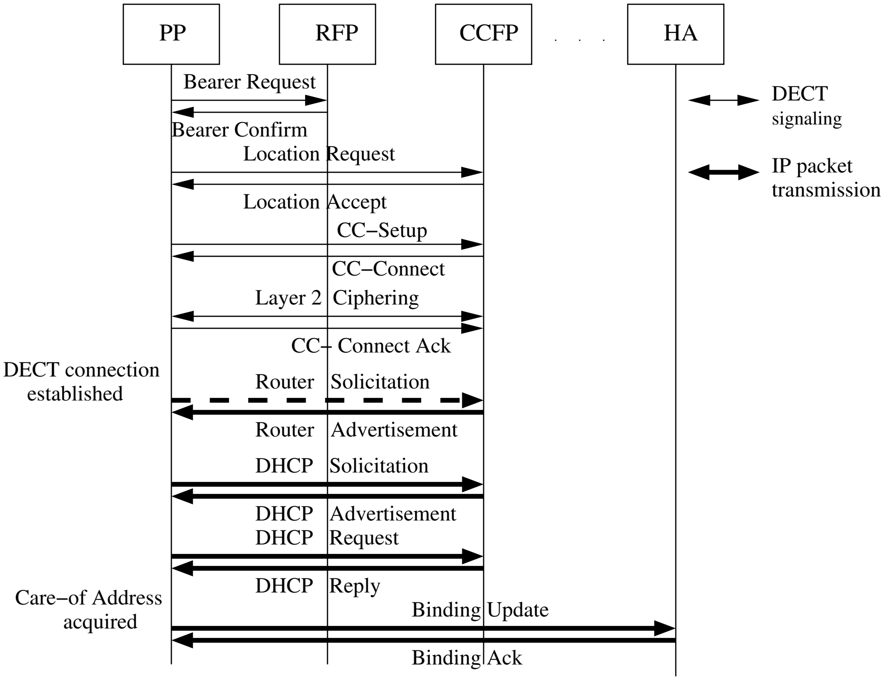

Fig. 5. Location registration for an IPv6 enabled DECT terminal

appropriate. The DHCPv6 server can be included in the CCFP functionality, whereas the PP can 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. Since the PP has recently moved to the new location 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. A Location Accept message is returned from the CCFP. At this point 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. Afterward, a NWK layer set-up process is initiated between the PP and the CCFP. A CC-Setup message is sent to the CCFP indicating a new connection and a response is sent back from the CCFP through the CC-Connect message. The communication between the two entities can be ciphered (Layer 2 Ciphering messages) for enhanced security. The new connection establishment is finished with a CC-Connect Ack sent from the PP to the CCFP.

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 [11]. The IPUI is zero-padded in order to build a 64-bit interface identifier [17]. 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 DHCPv6 is used. If DHCPv6 is the preferred configuration protocol, the PP will send a Solicitation message to the multicast address of all DHCP Agents in order to discover a proper DHCPv6 server. The Solicitation message should contain a Link-layer type DUID and particularly the 40-bit type N IPUI in the place of the client DUID for unique identification. DHCPv6 servers (CCFP) reply with Advertisement messages containing the offered resources (addresses or other parameters) and the server DUID. In order to avoid any conflict between clients' and servers' DUIDs, the servers' DUIDs are selected to be different than any DECT IPUI. After receiving Advertisement messages, the PP selects a DHCPv6 server (the server located on the CCFP is recommended for minimum signaling traffic) and sends a Request message to the selected server (CCFP). The DHCPv6 server (CCFP) updates its internal resource tables, selects an IPv6 address and sends a Reply message to the PP. After the PP receives the Reply, it may immediately use an 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 credentials of the mobile and if the authentication is successful, it replies with a Binding Ack. After that message exchange, the mobile is globally reachable through its Home Address.

3.4 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.

The internal handoff case is handled exclusively through DECT mobility procedures [10]. 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.

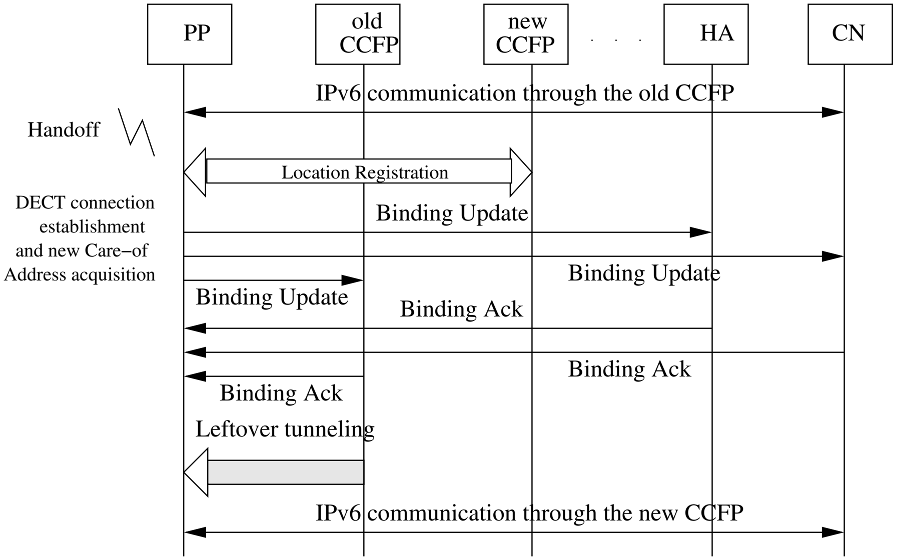

Fig. 6. IPv6 signaling exchange after a handoff

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. 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 QoS Provisioning

A DECT network constituted by portable parts and fixed parts, comprises a characteristic example of access network. Due to the rather limited available bandwidth and the foreseen demand for QoS with strict requirements, the Integrated Services architecture and the RSVP signaling protocol form the basis for the preferred QoS framework.

4.1 DECT–RSVP Interworking

The Integrated Services Architecture supports the following QoS traffic classes:

– Controlled Load Service Class [29]. Controlled-load service provides a data flow with a quality of service closely approximating the QoS that the same flow would receive from an unloaded network element. It uses admission control to assure that this service is received even when the network element is overloaded.
– Guaranteed Service Class [25]. Guaranteed service provides firm (mathematically provable) bounds on end-to-end datagram queuing delays. This service makes it possible to provide a service that guarantees both delay and bandwidth.
– Null Service Class [2]. Null service is intended for applications that require some form of prioritized service, but cannot quantify their resource requirements. The requirements specification is left to the network administrator.

These classes along with the Best Effort service class should be supported by DECT. One method is to use the different DECT Layer 3 services such as Call Control (CC), Connection Oriented Message Service (COMS) and Connection-Less Message Service (CLMS) to support the QoS classes as suggested in [15]. A more efficient method is to explore the extended functionality offered by CC, to accommodate the IP service requirements.

To this end, we assume that the PP has already established a connection with CCFP, using the CC service. A DECT connection is setup at power-on so that the portable can configure an IP address and various other network characteristics as described in the previous section. This connection is used by the portable as a default route for its IP traffic from and to the outside IP networks. It should be always up, although it may be configured to reduce its bandwidth in idle periods. This is the route for all the non-QoS traffic for the Portable Part, i.e. its best-effort connection. The actual QoS provisioning procedures depend on whether the DECT terminal includes RSVP functionality or not, as will be described in the following sections.

4.2 DECT Terminals with RSVP Functionality

If an application, running at the mobile terminal with RSVP functionality, wishes to establish a QoS connection with the outside IP network, it will issue a Path message toward the CCFP. This RSVP message will reach CCFP through the established best effort connection and it will be forwarded to the outside IP network. On the return path, the CCFP receives a corresponding Resv message, with parameters denoting the availability of the outside routers to support the requested QoS reservation. This Resv message has to be forwarded to the mobile terminal, which is unaware of the available radio resources, which are generally known at the fixed terminal side. Hence, the CCFP may alter the Resv parameters in such a way, that traffic requirements can be met. The modified Resv message is forwarded to the mobile terminal, through the established best effort CC connection. A new CC instance is initiated for the aforementioned QoS demanding flow.

Alternatively, the CCFP upon reception of the Resv message from the outside IP network, may issue a CC-setup toward the PP, with attributes denoting the supporting capabilities, before forwarding the Resv message to the mobile terminal. The Resv message can be delivered to the PP either through the newly established connection or, through the default best effort route. Both alternatives require a proactive behavior of the RSVP entity at the CCFP.

In the case that an IP node wishes to establish a QoS connection with the PP, the RSVP message Path will reach the PP through the best effort connection. Upon reception of this message, the PP may negotiate the connection characteristics with the CCFP through a CC-setup message and standard DECT procedures. A successfully established connection may generate a local Resv message at the CCFP, which proceeds as usual by issuing a Resv message toward the requested IP node. Alternatively, the Resv message can be sent by the PP through the newly established connection.

4.3 DECT Terminals without RSVP Functionality

The DECT terminals are widely deployed as simple telephone devices and may not possess a fully operational IP stack, not to mention RSVP capabilities. Hence, for the low end of the DECT terminal capabilities spectrum, we propose that the CCFP-IWU can take over the role of a RSVP Proxy [14].

In the case of incoming flows (toward the DECT network), the CCFP acts as a RSVP Receiver Proxy. The CCFP intercepts incoming Path messages and originates Resv messages in response to them. It also performs all the necessary state keeping as if the CCFP were the endpoint of the reservation request. Furthermore, it establishes internal DECT connections to the PP that is the destination of the data flow as bearers for the data flow. Alternatively, the CCFP may re-configure the existing CC-instance, adjust its bandwidth allocation and perform scheduling to the incoming data packets to ensure QoS guarantees for the particular data flow to the PP, while leaving some space for the default best effort traffic.

In the case of outgoing flows, the CCFP should possess the functionality of a RSVP Sender Proxy. The Sender Proxy could be triggered by external filters that examine the outgoing IP packets and determine whether the identified flows need any kind of resource reservation. Obviously, the decision for flow classification and reservation for the respective flows is a matter of policy and, therefore, it is possible that a policy server be contacted before any reservation request is made. In every case, if the RSVP reservation succeeds in the external IP network, the CCFP should provide the necessary QoS guarantees inside the DECT access network. The CCFP might install a new CC-instance for the new flow, but this approach requires extra signaling to indicate to the PP the reason for this DECT connection setup, i.e. that the newly discovered data flow from the PP should be transmitted over the new instance.

In that case, the preferable solution is the adjustment of the existing CC-instance provided to serve best-effort traffic from the PP. Thus, the PP will be able to transmit the data flow with QoS guarantees through its default route (the adjusted default CC-instance) in the DECT network and with RSVP signaled guarantees through the outside IP networks.

4.4 Clustering DECT–IPv6 Access Networks

Through our analysis in the previous sections, we have proposed some methods to provide QoS support through RSVP signaling in DECT access networks. Whereas RSVP-enabled QoS could be considered adequate for such an access network, it falls short in cases where multiple DECT networks are located in a greater domain, that handles mobility through Mobile IPv6. In such cases, interworking problems arise between Mobile IP and RSVP [26]. The core of the problem lies in the observation that RSVP marks each QoS "session" by the triplet <Destination Address, Destination Port (or Flowlabel in IPv6), Protocol Type>. If a mobile moves within the area controlled by the same CCFP, only DECT mobility procedures will apply and its IP address will remain the same.

If the DECT terminal moves to an area controlled by a different CCFP, it will perform the procedures described in Section 3.4. In that case, through Mobile IPv6 procedures, a new Care-of Address will be assigned to the terminal and the RSVP session will be incorrect (or at least unusable) in the new context. One possible solution would be to enhance the edge IP router with some extra functionality. Bearing in mind, that the edge router already deal with Mobile IPv6 and RSVP, an interworking between the mobility and QoS functionalities could be deployed to eliminate the incompatibilities. Such a solution is proposed with the RSVP Mobility Proxy concept in [21] and [22].

5 Conclusions

A DECT/IPv6 interworking framework was presented, that overcomes the limited mobility and QoS capabilities DECT offers. The extended features were realized through the exploitation of Mobile IPv6 and RSVP QoS signaling protocol respectively.

In order to specify the exact interaction between DECT and Mobile IPv6 location management procedures, 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, while mobility was demonstrated by means of Mobile IPv6. Moreover, guidelines were set for the interworking between the RSVP QoS signaling protocol and DECT procedures for allocating resources in the wireless medium. The Interworking Unit, 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.

Finally, the enhanced functionality placed on the DECT controller is justified by the seamless, QoS enabled, wireless Internet access for DECT/IPv6 terminals.

References

[1] Y. Bernet. RFC 2996: Format of the RSVP DCLASS object, November 2000. 375

[2] Y. Bernet, A. Smith, and B. Davie. RFC 2997: Specification of the Null Service Type, November 2000. 381

[3] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss. RFC 2475: An architecture for differentiated services, December 1998. 374

[4] R. Braden, D. Clark, and S. Shenker. RFC 1633: Integrated services in the Internet architecture: an overview, June 1994. 374

[5] R. Braden, Ed., L. Zhang, S. Berson, S. Herzog, and S. Jamin. RFC 2205: Resource ReSerVation Protocol (RSVP) — version 1 functional specification, September 1997. 375

[6] S. Deering and R. Hinden. RFC 2460: Internet Protocol, Version 6 (IPv6) specification, December 1998. 370

[7] R. Droms (ed.), J. Bound, M. Carney, C. Perkins, T. Lemon, and B. Volz. Dynamic Host Configuration Protocol for IPv6 (DHCPv6). Internet Draft, October 2002. Work in Progress. 371

[8] ETSI. Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); part 1: Overview. ETSI EN 300 175-1, January 2002. 369

[9] ETSI. Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); part 4: Data link control (DLC) layer. ETSI EN 300 175-4, January 2002. 376

[10] ETSI. Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); part 5: Network (NWK) layer. ETSI EN 300 175-5, February 2002. 370, 379

[11] ETSI. Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); part 6: Identities and addressing. ETSI EN 300 175-6, January 2002. 379

[12] ETSI. Digital Enhanced Cordless Telecommunications (DECT); DECT Packet Radio Service (DPRS). ETSI EN 301 649, October 2002. 370, 375, 376

[13] P. Flykt, C. Perkins, and T. Eklund. AAA for IPv6 Network Access. Internet Draft, March 2002. Work in Progress. 373

[14] S. Gai, D. G. Dutt, N. Elfassy, and Y. Bernet. RSVP Proxy. Internet Draft, March 2002. Work in Progress. 382

[15] A. Gyasi-Agyei. Mobile IP–DECT Internetworking Architecture Supporting IMT-2000 Applications. *IEEE Network*, pages 10–22, November 2001. 375, 381

[16] R. Hinden and S. Deering. RFC 2373: IP version 6 addressing architecture, July 1998. 371

[17] IEEE. Guidelines for 64-bit global identifier (EUI-64) registration authority, March 1997. 371, 379

[18] D. Johnson, C. Perkins, and J. Arkko. Mobility Support in IPv6. Internet Draft, June 2002. Work in Progress. 374

[19] 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. 375

[20] T. Narten, E. Nordmark, and W. Simpson. RFC 2461: Neighbor discovery for IP Version 6 (IPv6), December 1998. 372, 374, 377

[21] S. Paskalis, A. Kaloxylos, E. Zervas, and L. Merakos. RSVP Mobility Proxy. Internet Draft, December 2001. Work in Progress. 383

[22] S. Paskalis, A. Kaloxylos, E. Zervas, and L. Merakos. An Efficient RSVP–Mobile IP Interworking Scheme. *Journal on Special Topics in Mobile Networking and Applications (MONET)*, 8(3), June 2003. 383

[23] C. Perkins. RFC 2002: IP mobility support, October 1996. 373

[24] J. Postel. RFC 791: Internet Protocol, September 1981. 373

[25] S. Shenker, C. Partridge, and R. Guerin. RFC 2212: Specification of guaranteed quality of service, September 1997. 381

[26] M. Thomas. Analysis of Mobile IP and RSVP interactions. Internet Draft, February 2001. Work in Progress. 383

[27] S. Thomson and T. Narten. RFC 2462: IPv6 stateless address autoconfiguration, December 1998. 372

[28] B. Volz. Load balancing for DHCPv6. Internet Draft, July 2002. Work in Progress. 373

[29] J. Wroclawski. RFC 2211: Specification of the controlled-load network element service, September 1997. 381

[30] 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. 375