R. Bars, J. Gomez, M. Mahdi, C. Alcaraz and R. Roman, "Digital Home Networking: Standards", *Digital Home Networking*, vol. 7130, pp. 60-96, 2011.
NICS Lab. Publications: https://www.nics.uma.es/publications

Chapter 4

Standards

4.1. Introduction

The main goal of this chapter is to describe the major standards used in the home, i.e. UPnP and Zigbee, and the main solutions that have been proposed by the different standardization forums to enable the Remote Access (RA) to Homes.

Regarding Digital Living Network Alliance (DLNA), it seeks to create new products that are compatible using open standards and widely available industry specifications. DLNA does not define standard but defines how to use it, and then certifies products to guaranty to the end user the compatibility of the different devices used in his/her home.

As for the two major standards described in this chapter, they do not address the same use case, even if sometimes both are trying to manage same kind of equipment. UPnP addresses content management, home gateway management, and telephony, when Zigbee focuses on the solution to offer home automation.

4.2. Standards used in the home

4.2.1. *DLNA: Digital Living Network Alliance*

Digital Living Network Alliance® began in 2003 when a collection of companies from around the world agreed that they all provide better products when those products are compatible. As of 2010, more than 245 companies comprise

Chapter written by Remi BARS, Jorge GOMEZ, Mohamed MAHDI, Cristina ALCARAZ, Rodrigo ROMAN

DLNA. They include consumer electronics, computer, and mobile device manufacturers. DLNA also includes many components and software developers.

Figure 4.1. *DLNA logo*

These DLNA member companies seek to create new products that are compatible by using open standards and widely available industry specifications. In fact, as of May 2010, more than 8,000 different devices had obtained the "DLNA Certified" status, indicated by a logo on their packaging and confirming their interoperability with other devices. This logo can be found on various kinds of products, such as personal computers (PCs), mobile devices, televisions (TVs), digital cameras and printers, personal electronic devices, and many more.

This DLNA Certified logo tells us that the product is in compliance with the DLNA certification testing requirements. That means it has proven it can connect with other DLNA Certified devices. To be compliant DLNA provides the DLNA Interoperability Guidelines, which are the collection of open standards that enable this new generation of devices to be networked. Note that DLNA do not define any standard, as it only defines how to use these existing standards to provide an interoperable solution.

DLNA guidelines can be thought of as an "umbrella standard" that defines how the home network interoperates at all levels. In addition to defining how different standards will interoperate and how data will be handled at each level, it also narrows down the number of standards a device must support. DLNA guidelines define both mandatory and optional standards for each of the different networking layers. Devices must support all mandatory standards to be compliant.

DLNA approach to standards is critical for a cost-effective implementation of content sharing. Rather than bogging down cost and increasing device complexity by requiring devices to support a myriad of standards – both in terms of engineering effort and licensing investment – DLNA has defined a small set of mandatory standards that devices must support (the device model used by DLNA is derived from the UPnP Forum fundamental device model – see www.dlna.org). This not only simplifies development, but also ensures that consumers will be able to share all of their contents among all of their devices.

The DLNA certified device classes are separated as follows:

– *Home Network Devices*

Digital Media Server (DMS): These devices store content and make it available to networked digital media players and digital media renderers. Some digital media servers can also help protect your content once stored. Examples include PCs and network attached storage (NAS) devices.

Digital Media Player (DMP): These devices find content on DMS and provide playback and rendering capabilities. Examples include TVs, stereos and home theaters, wireless monitors, and game consoles.

Digital Media Renderer (DMR): These devices play content received from a digital media controller, which will find content from a DMS. Examples include TVs, audio/video receivers, video displays, and remote speakers for music.

Digital Media Controller (DMC): These devices find content on DMS and play it on DMR. Examples include Internet tablets, Wi-Fi enabled digital cameras, and personal digital assistants (PDAs).

Digital Media Printer (DMPr): These devices provide printing services to the DLNA home network. Generally, DMP and DMC with print capability can print to DMPr. Examples include networked photo printers and networked all-in-one printers.

– *Mobile Handheld Devices*

Mobile Digital Media Server (M-DMS): These wireless devices store content and make it available to wired/wireless networked mobile digital media players (M-DMP), DMR, and DMPr. Examples include mobile phones and portable music players.

Mobile Digital Media Player (M-DMP): These wireless devices find and play content on a DMS or M-DMS. Examples include mobile phones and mobile media tablets designed for viewing multimedia content.

Mobile Digital Media Uploader (M-DMU): These wireless devices send (upload) content to a DMS or M-DMS. Examples include digital cameras and mobile phones.

Mobile Digital Media Downloader (M-DMD): These wireless devices find and store (download) content from a DMS or M-DMS. Examples include portable music players and mobile phones.

Mobile Digital Media Controller (M-DMC): These wireless devices find content on a DMS or M-DMS and send it to DMR. Examples include PDAs and mobile phones.

4.2.2. *UPnP*

By considering current scenarios where home and (small) office networks interconnect several electronic devices, intelligent appliances, mobile devices, and PCs, the UPnP Forum emerged as one of the most important initiatives proposing technologies and standards for the seamless interconnection and the interoperability of homes based on Internet Protocol (IP)-based network devices.

Indeed, consumer requirements have evolved and nowadays people ask for the transfer of video/audio from a media server to a TV to control home appliances from a work place, to print directly from a camera, and to manage every possible home device from a mobile phone or a universal-wide remote control. To enable those scenarios, the UPnP Forum has published several specifications through several working committees such as, for example, the UPnP Device Architecture, UPnP Audio Visual (AV), UPnP IGD, and the UPnP QoS specifications.

The UPnP Forum technology is based on the UPnP Device Architecture specification (UDA) [UPnP DA 08] which is designed to extend the plug and play concepts to network devices and services (i.e. gateways, AV devices, cameras, telephones, printer, game console, and electrical appliances). To support zero-configuration, "invisible" networking, and the automatic discovering of all devices, UDA defines protocols for the communication between UPnP control points and controlled devices.

4.2.2.1. *UPnP committees*

The UPnP has many working committees which focus on subjects like security, device management, telephony, image printing, and low power, among others. In the following, we will introduce the UPnP AV and UPnP QoS specification, as these are the most important in the scope of this book. They will be explained in more detail in section 4.2.2.3. and Chapter 7, respectively. We will also briefly mention the UPnP Internet Gateway Device specification.

4.2.2.1.1. UPnP AV

In the particular context of multimedia, the UPnP AV specification [UPnP AV 02] has defined a set of UPnP devices and service templates that specifically targets devices interacting with entertainment content such as movies, music, and still image. Three main logical entities constitute the AV Architecture: media

servers, media renders, and control points. In the UPnP AV Architecture, the media servers have access to multimedia content and can send it to other UPnP devices through the network. Media renderers are able to receive external content from the network and present it on its local hardware. Finally, the control points coordinate the overall operation and provide the interface to the end user. Owing to its importance in the context of the digital home, this specification will be explained in more detail in section 4.2.2.3.

4.2.2.1.2. UPnP QoS

The UPnP QoS specification [UPnP QoS] deals with QoS aspects in UPnP networks. Even in home or small office networks, it is necessary to consider time constrains when rendering multimedia information. To do so, UPnP Forum has published three versions of QoS DCP (Device Control Protocol). The first two versions provide priority-based Quality of Service (QoS) solution to ensure better performance for multimedia content delivered on a congested network. Nonetheless, in scenarios where priority- based protocols are not enough, e.g. high-definition video transmission in a congested network, the QoS version 3 DCP defines an IP reservation-based QoS protocol in order to reserve the amount of bandwidth necessary. Chapter 7 of this book gives a detailed explanation of the UPnP QoS Architecture.

4.2.2.1.3. UPnP Internet Gateway Device

To solve the complexity in configuring network settings, the UPnP Internet Gateway Device (IGD) specification [UPnP IGD 01] defines how to control the parameters of the home gateway. The main defined functions are as follows:

– Save the public IP address of the router.

– Manage the list of redirected ports.

– Add and delete a port redirection in the saved list rules (lifetime of these rules is configurable).

This stack is widely used by the gateways of the Internet service providers. In September 2010, the UPnP Forum published the version 2 of the IGD, including important security and access control functions.

4.2.2.2. *UPnP basic architecture*

4.2.2.2.1. UPnP devices

The main concepts of the UPnP architecture are devices and services. A device is an equipment that offers one or multiple services. A service is the smallest control

unit in UPnP. It proposes actions and is described using state variables. There are two types of devices:

Controlled device or device: This component offers a set of services to the equipment connected to the networks. Devices can also embed a list of logic devices that offers (each of them) a set of services.

Control point: This component is responsible for connecting controlled devices to each other. It can be embedded in a device component.

A UPnP device is installed in an equipment offering resources. It proposes services reusable by the control point. The device publishes information describing its services. The XML language is used to present this information. Control points can retrieve the services with a simple HTTP GET request, since each UPnP device embeds a little web server.

A service is created by a set of actions, which modify its states variables. These services use the registration concept. Indeed, a control point that is registered to a service is notified of all the state changes of the device. The device should provide the description of its actions and states in an XML format. Figure 4.2 illustrates the composition of a device.

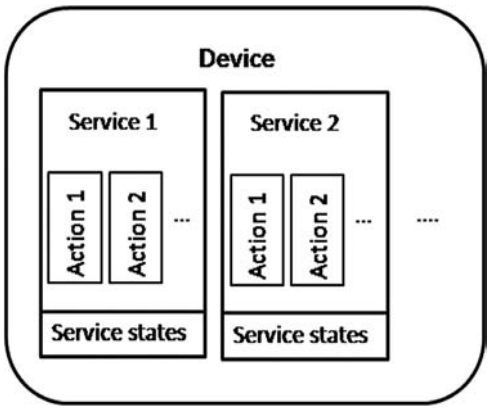

Figure 4.2. *UPnP device composition*

A UPnP control point is simpler than a controlled device. It does not hold services. It is just in charge of subscribing to services published by the devices of the network. So, whenever the states of these services change, the control point will be notified about the change. And thus, the control point can react to these changes.

4.2.2.2.2. How UPnP works

The communication between the controlled devices and a control point is carried out in six steps. The following paragraphs detail them one by one.

Addressing: This step allows UPnP components to acquire an IP address. By default, the component uses a Dynamic Host Configuration Protocol (DHCP) [DRO 97] client. If the DHCP request fails, the component uses an automatic IP addressing (mechanism returning an arbitrary IP address). Once the device obtains a valid IP address, it begins the second step (discovering).

Discovering: This procedure is based on the use of the SSDP protocol (Simple Service Discovery Protocol) [CAI 99]. This protocol offers methods for the devices (NOTIFY) to advertise their capabilities, and to the control point (M-SEARCH) to discover the devices available in the network.

In fact, when a new device is added to the network, it sends periodically multicast advertising messages. These messages define the essential information about the device, such as its type, its identifier, and a pointer (URL) to its XML-detailed description document. In addition, each device, and each service embedded in this new device, sends an advertising message to indicate their capabilities.

So, all control points in the network listen to the standard multicast address and port (239.255.255.250:1900) that devices use to send their advertisements, and then they know all connected devices. Besides, control points can also send a multicast message (M-SEARCH) to force the devices to announce themselves.

Description: After the discovery step, the control point has only the information about devices and services available in the network. To learn more details about their capabilities, the control point retrieves the file describing the devices and services from the locations indicated by the advertise messages. An HTTP GET request is sent for that purpose. The response will be processed by the web server embedded in the device. Note that the description of a device contains some vendor information, the definitions of all embedded devices, the URL for the presentation file of the device, and an enumeration of all services, including their URLs for control and events. The files describing the services include the information about the offered actions (name, input arguments, and output arguments) and their states variables.

Control: Since the control point knows all needed information about devices and services, it can use the actions provided by the device services through Simple Object Access Protocol (SOAP) [HAD 03] requests, sent to the URL dedicated to their control. By invocating service actions, a control point aims to change service

state variables. At the end of the action process, the service sends the result to the control point. The action result can be an error code or the new value of the service states.

Eventing: We call eventing the process that the device uses to publish the value of variables that describe the state of its services. This process uses the General Event Notification Architecture (GENA) [COH 98] technique to publish the eventing messages. In fact, whenever a control point wishes to follow the change of a device states, it can subscribe to the eventing service of such device. Then, each time the values of these variables change, the publisher service will send a notification message to the list of subscribed control points.

Presentation: If a device offers an HTML page to present its status, it can be browsed by a standard Internet browser. The location of this page is declared during the description step. The presentation page can also offer to the user the possibility to control the device.

Finally, Figure 4.3 represents a sum up of the six steps that are involved in the interaction between a control point and a device.

4.2.2.3. *UPnP AV*

Because UPnP AV is one of the most used technologies for Audio/Video communication in a home network, the following sections present a detailed explanation of it.

4.2.2.3.1. UPnP AV goals

There is a simple scenario in which a user can watch a film or listen to a song by easily selecting its content from a media server and choosing the device (render) where the content will be played with the help of a remote control. UPnP Forum has published the UPnP AV Architecture with the goal of enabling such kind of scenario by allowing an easy sharing of multimedia contents between UPnP connected devices.

The UPnP AV Architecture defines two sets of devices: media servers and media renders, and a specific control point. These components interact in order to transport AV content between UPnP servers and renders using non UPnP transfer protocols and content formats. Figure 4.4 shows the UPnP AV Architecture and the interactions between its components.

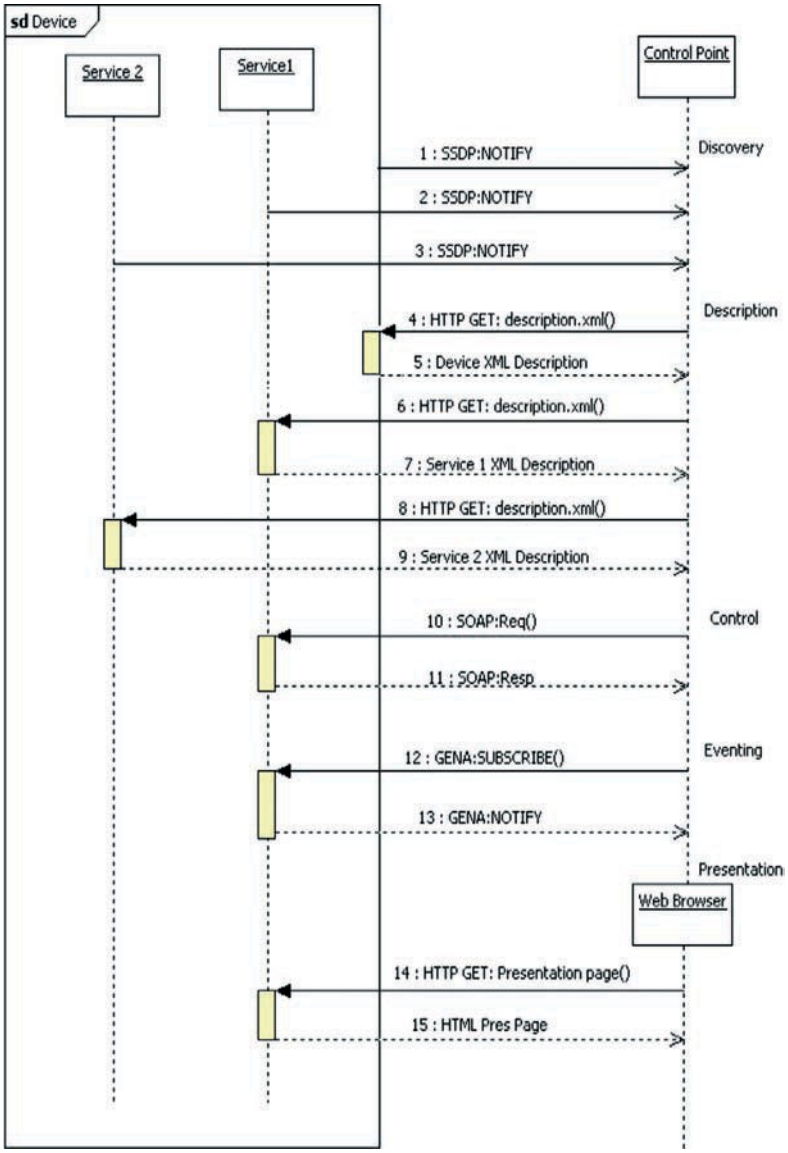

Figure 4.3. *Device and control point interaction*

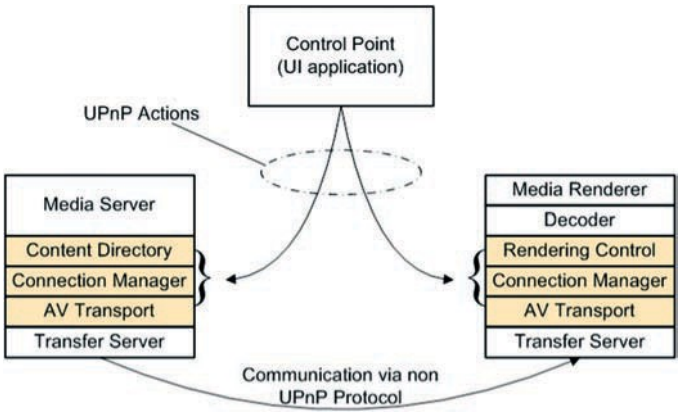

Figure 4.4. *The UPnP AV architecture*

AV control point: Usually, a user interacts with an AV control point's user interface (UI) in order to set the multimedia session between the media server and the media renderer. In this sense, the control point invokes services or actions from UPnP devices (multimedia server and renderer) in order to:

– browse the multimedia content;

– obtain a list of transfer protocols and data formats supported by the renderer and the server;

– select a transfer protocol and the data format supported by both the media server and renderer;

– configure the server and renderer for content transmission;

– and finally select the item to be transmitted.

In the "three box model" the UPnP AV Architecture defines the control point as located outside the media server and renderer. On the other hand, the control point can be implemented within a device: either a media server or a media renderer. The UPnP AV Architecture names those cases as the "two box model". No matter the location of the control point, its role and those of the media server and renderer are well defined by the AV specification.

Media server: The media server contains the multimedia content to be browsed by the control point. The media server has three services: the content directory service (CDS), the connection manager (CM) service , and the AV transport service (AVTS).

The CDS provides the actions that allow the control point to obtain the information about each item that the media server can share in the UPnP network. By using this service, the control point can get the meta-information about each content item, such as its name, size, and date created. Also, the control point can obtain the transport protocols and data formats supported by the media server for a particular item. In this way, the control point will know if a media renderer is able to play that item.

As its name indicates, the CM service manages the connections with a particular device. In order to manage several connections at a time, the CM must implement an optional action (CM::PrepareForConnection) that prepares the media server for an upcoming transfer. However, when this action is not implemented, the control point is only able to support a single renderer at a given time.

Depending on the supported transport protocols and/or data formats, the control point may be able to, e.g. pause, stop, resume, and seek the content that the media server is transferring. The AVTS is an optional service offered by the media server and the media renderer.

Media render: The media renderer is the device that will play the media content. The media renderer allows the control point to determine the transfer protocol and the data format as well as the way to control the content flow, i.e. play, pause, and resume. The media renderer includes a rendering control service (RCS), a CM service, and an AVTS.

The RCS allows the control point to control rendering characteristics, such as brightness, contrast, volume, and mute. However, to support multiples instances of this service, the CM service must implement the CM::PrepareForConnection.

The CM service is used to manage the connections with the media renderer. In this context, the CM allows the control point to obtain information about the transfer protocols and data formats supported by the renderer. In consequence, the control point knows if the renderer will be able to play the selected content. When the media renderer implements the CM::PrepareForConnection action, it also allows the control point to control the flow of the content (play, pause, resume, etc.), as well as the rendering characteristics such as brightness, volume, and mute.

The AVTS is an optional service used by the control point to control the flow of the content being transferred, i.e. play, pause, and seek. In the context of the media renderer, the CM::PrepareForConnection enables the creation of several AV transport instance IDs to distinguish between the several connections and instances of this service. In this way, the media renderer can simultaneously handle multiple content items.

Figure 4.5 shows a common exchange between the control point, the media server, and the media renderer in the three box model.

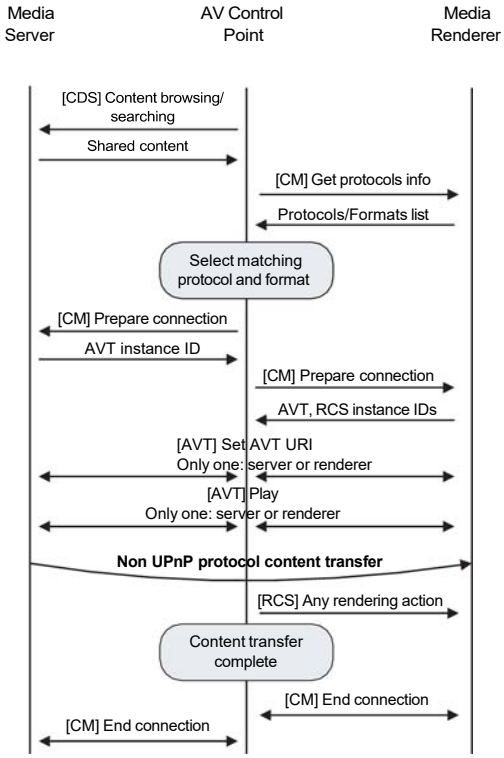

Figure 4.5. *Interactions between the control point, media server, and media render in the three box model*

4.2.3. *ZigBee*

ZigBee is an open specification defined by the ZigBee Alliance, which was founded in 2002 to define communication protocols for networks with low-power consumption, low-data-rate and short-range wireless communication. The Alliance comprised a set of relevant manufacturers and vendors, which are classified by promoters, participants, and adopters. Independent of their levels of membership, all of them afford a wide range of certified products within the today's market, providing attractive automation and remote control applications. The certification comprises a compliance and an interoperability process under the supervision of the ZigBee Qualification Working Group belonging to the Alliance.

The first ZigBee release, currently obsolete, was ratified in 2004 to offer home automation applications for medium networks using a tree topology and a restricted number of nodes. This led to a significant change in the specification published in ZigBee-2006 to handle large networks through a dynamic addressing scheme. Although this was a significant improvement, a new update was again considered to define two new protocol stacks known as ZigBee-2007 (simply ZigBee) and ZigBee-PRO. As of 2011, these two specifications are available and provide enhanced functions and backward compatibility with respect to ZigBee-2006.

Generally speaking, all ZigBee releases have certain objectives and features in common. For example, all of them try to achieve:

– interoperability and coexistence with other technologies;

– communication reliability and security; and

– cost-effective solutions.

To be more explicit, ZigBee-2006/2007/PRO specifications try to extend diverse (hardware and software) solutions that provide a high cooperation among different types of technologies with low installation and maintenance costs. Regarding its topological and functional features, ZigBee supports mesh, star, and cluster-tree networks, whose protocol stack depends on the IEEE 802.15.4-2006 standard for Low-Rate Wireless Personal Area Networks (LR-WPANs) and optionally on the IEEE 802.15.4-2003 (a previous release, also known as IEEE 802.15.4b). This standard will be explained in section 4.2.3.1.2.

As for the markets that can take advantage of the benefits of ZigBee comprise both commercial and industrial applications, which are illustrated in Figure 4.6 and are listed as follow:

– *Smart Energy*™ for energy management and efficiency through demand response, network metering, advanced metering infrastructure (AMI), and supervisory control and data acquisition (SCADA).

– *Remote control*™ for electronic devices and multimedia, such as TV, VCR, DVD/CD, video camera, PC, and peripherals.

– *Personal health care*™ for patient monitoring and fitness monitoring.

– *Home automation*™ for security and access control, as well as lighting and HVAC (heating, ventilation, and air conditioning) management.

– *Telecommunication services*™ for e-commerce, information services, and object interaction (Internet of things).

– *Building automation*™ for security and access control, lighting and HVAC management, and advanced meter reading (AMR).

– *ZigBee retail*™ for the management and modernization of the retail experience from point-of-manufacture to point-of-sale. Some applications are related to collect in-store information from customers and establish a wireless network for in-home shopping and assistance using, for example, voice devices.

Figure 4.6. *Current applications profiles*

4.2.3.1. *ZigBee platform and network architecture*

ZigBee devices are defined by the Alliance as the combination of radio, microcontroller, memory, and the ZigBee protocol stack. Most devices provide 4–300 MHz microcontrollers with 8–512 KB RAM and 8–256 KB of flash memory. Each of these hardware devices is attached on a unique development board with an IEEE 802.15.4 compliant transceiver using Advanced Encryption Standard (AES)-128 bit under the CCM* security mode and additional functional modules. These modules usually consist of sensors to measure physical events of a determined context (e.g. light, humidity, temperature, and noise), power supplies (e.g. AA batteries), and peripherals. An example of this configuration is represented in Figure 4.7 on the right side.

4.2.3.1.1. ZigBee protocol stack

The ZigBee protocol stack follows the Open System Interconnect (OSI) model so as to provide a wireless networking protocol based on layers. This type of design facilitates individual updating of the layers without requiring significant changes in the whole stack. Observing Figure 4.7, it is possible to notice that the ZigBee Compliant Platform is basically based on four main layers: the physical layer (PHY), the link layer (MAC), the network layer (NWK), and the application layer (APL).

The two bottom layers follow the IEEE 802.15.4 standard (detailed in section 4.2.3.1.2), whereas the NWK, the APL, and even the security layer (also illustrated in Figure 4.7) have been established by the same Alliance. The general mission of each layer is to perform and provide a set of services to the adjacent layers through special interfaces known as service access points (they are represented as gray points in Figure 4.7). Some of these services are described below.

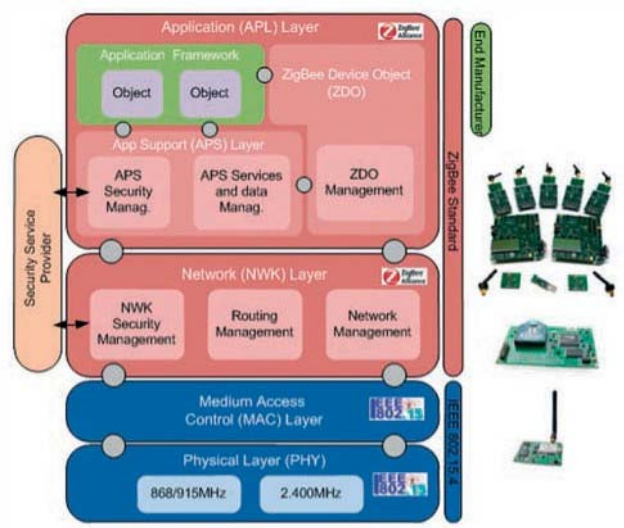

Figure 4.7. *ZigBee compliant platform and a few ZigBee hardware modules*

– The *PHY layer* is responsible for activating the transmission radio and sending/receiving data packets through the most suitable radio frequency (RF). The signal is modulated under a low spectral power density using the Direct Sequence Spread Spectrum (DSSS) method provided by the IEEE 802.15.4 standard.

– The *MAC layer* is responsible for providing secure connectivity with other network devices. In particular, this layer is based on an access control list (ACL) to protect the system against unauthorized accesses and on the Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA) protocol to manage packet collisions. Moreover, the MAC layer offers synchronized accesses into the communication channels by using the guarantee time slots (GTS) protocol using centralized medium access times.

– The *NWK layer* is in charge of network management by using specific services as joining/rejoining, routes management, packet routing, and key management services.

– The *APL layer* is responsible for specifying the application context and has the capability to define application profiles, which are based on interoperability agreements (i.e. software, hardware, actions, and formats) among different devices that come from different vendors. The APL layer comprised two main sublayers: the Application Support (APS) and the ZigBee Device Object (ZDO), and by an

Application Framework manufacturers can individually specify and implement their respective application profiles. The *APS sublayer* manages group addresses, message formats, forwarding, and binding to the endpoints. A binding task consists of establishing logical links between associated devices or applications through relationship tables, known as binding tables. The *ZDO sublayer*, in contrast, is in charge of defining and managing the roles for new devices, discovering nodes and services, and providing security services. Finally, the Application Framework manages application objects to customize the functions of a device under a certain application context.

4.2.3.1.2. IEEE 802.15.4 standard

The IEEE 802.15.4 standard provides ZigBee with useful services and mechanisms for wireless remote control and network management. In particular, it mainly provides network and device discovery mechanisms, energy control through frequent changes of states (i.e. low-duty cycles), and security and interference/noise control in communication channels. This standard operates at different unlicensed Industrial, Scientific and Medical (ISM) radio frequency bands. In particular, it is able to work at 2.4 GHz (worldwide) with sixteen 250 kbps transmission channels, 868–868.8 MHz (Europe) with one 20/100/250 kbps transmission channel, and 902–928 MHz (North America) with thirty 40/250 kbps channels over an action range around 10–100 m.

The standard makes use of the DSSS method to spread the signal properly. Specifically, this method is responsible for modulating the information before its transmission using a low spectral power density in order to assure an interference reduction in frequency channels. The standard also defines three types of modulation systems that preserve the DSSS approach: (i) Binary Phase Shift Keying (BPSK), (ii) Offset Quadrature Phase Shift Keying (O-QPSK), and (iii) Parallel Sequence Spread Spectrum (PSSS). In particular, ZigBee modulates its signals with BPSK when the network works at 868—928 MHz and O-QPSK when it works at 2.4 GHz.

With regard to security, IEEE 802.15.4 affords a set of security services to ensure the confidentiality, integrity, and authenticity of the messages. In particular, confidentiality and integrity are obtained by using AES-128 security primitives and Message integrity code (MIC)/Message authentication code (MAC) messages with 32/64/128 bits, respectively. The MIC/MAC messages are mainly based on a frame control, an auxiliary security control, and a data payload.

As for authentication, IEEE 802.15.4 allows ZigBee to refuse the communication to unauthorized devices using an ACL. This list includes the addresses belonging to trustworthy devices, a key with 128 bits, a security policy (e.g. AES-CTR), a last initial vector (IV), and a replay counter to guarantee freshness in the messages.

4.2.3.1.3. ZigBee network devices

There are three different types of devices in the ZigBee network architecture: (i) a ZigBee coordinator (ZC), (ii) ZigBee routers (ZR), and (iii) ZigBee end-devices (ZED).

– *ZC devices* act as an IEEE 802.15.4 PAN-coordinator (a full-function device, FFD) with capability of performing the main role in the network. Generally, the coordinator behaves like a trust center, which is able to manage the deployment (such as, for example, configuring device groups through PAN identifiers or choosing an RF before the deployment), synchronization, maintenance, and control processes on the whole network.

– *ZR devices* are an optional type of device that may act as an IEEE 802.15.4 coordinator (FFD) having the capability needed for allocating/deallocating local addresses, participating in multihop routing scenarios and managing its own ZEDs.

– *ZED devices* are a type of end-devices that is neither a ZC nor a ZR, with reduced resources and functions for applications that are extremely simple. For example, they might be associated to washing machines, lamps, air-conditioning equipment, water heaters, light switches, passive infrared sensors, TVs, and smart metering devices.

4.2.3.1.4. ZigBee network topologies

Depending on the ZigBee specification (Table 4.1) the communication can follow a different topology based on a cluster-tree network, a mesh network, or a many-to-one network. A *cluster-tree network* is composed by a hierarchical structure where leaves devices (i.e. ZEDs) have to route their messages to their parents (e.g. a ZR) until they reach the root, and vice versa. Then, the depth of the tree is going to depend on the number of hops to reach. In contrast, a *mesh network* is a no-hierarchical network where different devices are able to establish one-hop and/or multi-hop connections among them. In addition, as this type of networks has implemented the Ad Hoc On Demand Distance Vector Routing (AODV) protocol, it is dynamically possible to select alternatives paths.

In contrast with the previous topology, a *many-to-one network* consists of devices subsets whose nodes are capable of reaching in one-hop their respective parent nodes (either ZR or ZC). Therefore, it is not necessary to store a complex route table. An example of this type of configuration is found in a star network topology. Here, the ZC and ZR establish connectivity with the ZEDs and other ZCs/ZRs, while a ZED can only establish it with a ZC/ZR. So far, this type of topology is provided by the ZigBee-PRO standard.

4.2.3.2. *Current services offered by ZigBee*

Many commercial and industrial applications are extending the ZigBee technology day-by-day because of two main reasons. First, most of the applications

require wireless communication with capability of supporting large networks. Second, these networks must provide a set of suitable services that ensure a reliable and secure communication. Most of these services are summarized in Table 4.1, in which X means that the function is available and described in detail throughout this section.

Feature Set	2006	2007	PRO
	Communication and Routing		
Communication	Cluster-tree, Mesh	Cluster-tree, Mesh	Mesh, Many-to-one, star
Centralized data collection	X	X	X
Routing	Symmetric	Asymmetric	Asymmetric
Route aggregation			X
Source routing			X
Low-power routing			X
	Addressing and Messages		
Addressing scheme	Hierarchical	Hierarchical	Stochastic
Group addressing	X	X	X
Fragmentation and reassembly		X	X
	Interoperability and Reliability		
Addressing scheme	Hierarchical	Hierarchical	Stochastic
Frequency agility	X optional	X mandatory	X mandatory
Coexistence	X	X	X
	Security		
Standard mode security	X	X	X
High mode security			X
128-AES, MIC and freshness	X	X	X
Entity-Authentication			X
Trust center	ZC	ZC	Any Device
	Application and Compatibility		
Scalability	Tens to hundreds	Tens to hundreds	Hundreds to thousands
Application context	Residential	Residential	Residentia, Commercial
Backward compatibility		ZigBee-2006	ZigBee-2006

Table 4.1. *Comparative table of the ZigBee-2006/2007/PRO standards that includes compatibilities, features and services*

4.2.3.2.1. Routing and communication services

Both ZigBee-2007 and Zigbee-PRO offer asymmetric routing capability for dynamically and autonomously identifying routes with the best link quality in either direction. This type of selection enables the network to face anomalous situations, avoiding, for example, congested paths because of a noise or a threat (such as denial of service attack, flooding attack, or jamming attacks), favoring the reliability and robustness in the communication. Moreover, this service improves the symmetric routing mechanism, since it does not require location awareness to define particular routes between a source device and a destination device.

It is important to highlight that ZigBee-PRO includes in its specification other interesting routing services for many-to-one networks, such as the identification of low-power ZRs to efficiently route messages toward them, route aggregation, and source routing. A route aggregation service is a mechanism that allows devices to reach a route on the way to the coordinator using a simple routing table with a single entry. In the case in which the coordinator wants to respond to a source node, it will have to call the second service, i.e. source routing. To this end, it will be necessary to remember the used path from the source node to the coordinator. This process consists in explicitly including the path within the message header.

Another special feature offered by ZigBee-PRO is the scalability control for large networks through an identity conflict resolution mechanism. In other words, while ZigBee-2006/2007 addresses are automatically assigned by using a hierarchical distributed scheme, ZigBee-PRO offers a stochastic scheme. This scheme consists of assigning previously a unique random address to each device. If the address is in conflict with the identity of another network device, the network stack assigns a different address by applying a conflict resolution mechanism using the IEEE MAC address of the device. Although this feature is relevant, it is important to comment that the three specifications are also able to manage groups of nodes by implementing a group addressing scheme, whose addresses are based on single frames in order for reducing overhead in the communication.

Concerning noise control, the three ZigBee releases are capable of reacting against both high and persistent interferences in the communication channels. This is carried out by implementing the frequency agility technique (as an optional service in ZigBee-2006 and a mandatory service in ZigBee-2007/PRO). The technique consists automatically changing the RF channel when the current channel experiences noise or obstacles. Typical situations are, for instance, when different wireless technologies try to share the same frequency band for the same application (this is known as coexistence, cf. section 4.2.3.3.). In ZigBee-PRO, this technique has been assigned to a dedicated device, known as network channel manager. This manager is able to change the frequency channel when it receives from end-

devices or routers a considerable number of reports about the interference level. However, the exclusive use of this technique in a network does not ensure a suitable coexistence and interoperability among technologies. It is necessary to take into account other additional services and mechanisms.

4.2.3.2.2. Security services

With regard to security, two security modes are nowadays available in ZigBee: (i) security standard mode and (ii) security high mode. The latter mode is only supported by ZigBee-PRO, and it introduces some additional security services, such as tunneling, peer-to-peer key establishment using a master key, and entity-authentication. All the security process, like, for example, the key management, is regulated through a security policy and is supervised by a trustworthy device known as trust center. This entity does not have to be necessarily represented by the coordinator such as in ZigBee-2006/2007. Its role can be performed by any other device in the network.

The security in the standard mode is based on two main keys: link-key and network-key. The link-key is a unique and optional key shared between two nodes and used to encrypt the messages in the application layer. On the contrary, the network-key, provided by the trust center, is used to encrypt the communications at network level, and is shared by the whole network. There are two different ways of acquiring the network-key: (i) preconfiguring the link-key in the new nodes to encrypt the network-key or (ii) transmitting the network-key without encryption from the trust center. It is clear that the second option is not very recommendable for certain applications that require a high confidentiality and integrity of messages.

In contrast, the high security mode basically adds one key more to the previous set, known as master-key. This master-key has to be preconfigured in each new device to generate the link-key using the Symmetric-Key-Key-Exchange (SKKE) algorithm. This algorithm requires a transaction process mainly based on nonces to guarantee freshness in communication. At the moment at which the link-key is generated, the network-key is transmitted encrypted it with the corresponding device. The network-key is frequently updated using a unicast message encrypted with the link-key by the trust center. This updating process improves the updating process of the standard mode, as such mode updates the network-key using a broadcast message encrypted with the old network-key.

ZigBee-PRO provides an additional mechanism to recover the current network-key for both security modes. In fact, the standard allows a network device to obtain the current network-key when it passes from a sleeping state to the awake state. For the transmission of the current network-key, the link-key established between the trust center and the new awake node must be used. This last characteristic

suggests us that the specification tries to provide a balance between security and energy consumption, aiming to increase the lifetime of low-power devices.

Finally, ZigBee-PRO includes in its specification special commands and services to offer entity authentication. However, this security service involves carrying out two additional communication steps: (i) the involved devices have to share a unique security key and (ii) they individually have to generate a 16-octet random string, called random challenge. The generated value has to be transmitted to the other end of the communication, since it is required as an input parameter for the Symmetric- Key-Entity-Authentication scheme.

4.2.3.3. *Coexistence in ZigBee, a great challenge*

In a digital home scenario, a wide range of multimedia devices as well as information communication systems and technologies coexist in one single household. An example of this is illustrated in Figure 4.8, where diverse electronic devices (such as TVs, DVD/CD radios, cellular mobiles, PCs, laptops, security systems, and headphones) are available in an application context with the goal of improving personal comfort and safety. Within this context, it is very important to highlight the ZigBee technology, since it offers solutions for both remote control and multimedia, as well as solutions related to both home automation and energy management systems.

Unfortunately, most ZigBee multimedia devices operate at a same frequency band (2.4 GHz) than other typical electronic and electro-domestic devices, such as microwave ovens, cordless phones, Bluetooth headphones, TVs/radios, smart meters, lighting, washing machines, water heaters, air conditioning, heating, and ventilation (check Chapter 3 for a list of wireless standards that operate in the 2.4 GHz. Range of the spectrum). Normally, these electronic and electro-domestic devices are randomly distributed in a closed environment and in the proximity to digital and multimedia devices (see Figure 4.3). As they belong to different wireless communication systems, their management and synchronization policies, their medium access control and their routing schemes are also different. This might lead to a serious problem, since several of these systems can transmit concurrently and at the same frequency. As a result, the probability of packet conflict on the communication channels is relatively high. For this reason, one of the main proposals of ZigBee is to provide system with mechanisms, services, techniques, and procedures in order to ensure the coexistence and reliability in communication channels.

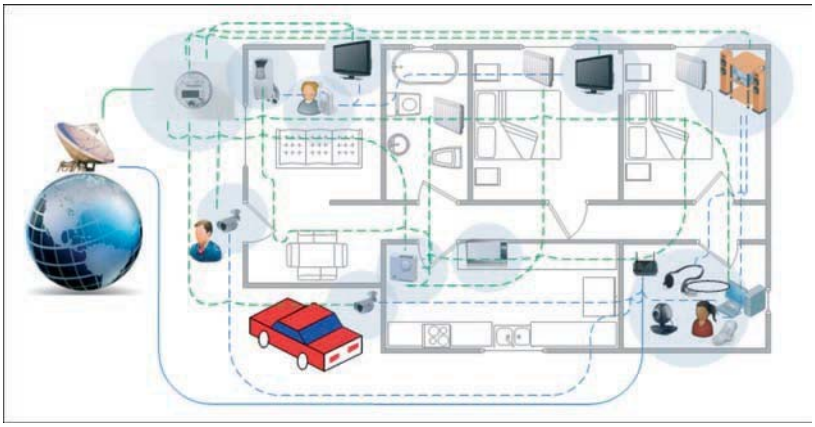

Figure 4.8. *Connectivity among different electronic devices in a close environment*

Coexistence can be defined as the ability to work in a same area with different wireless network devices. To this end, ZigBee provides two main approaches: (i) a collaborative method and (ii) a noncollaborative method. Specifically, a collaborative method is based on a set of mechanisms to allow the whole network to synchronize and gain access to the medium. However, this method requires having knowledge of the operating mechanisms belonging to the involved communication systems. It also demands some type of connectivity with ZigBee networks to carry out collaboration tasks.

In the noncollaborative approach, these requirements are not necessary. This approach basically consists of additional mechanisms – some of them already mentioned in section 4.2.3. – to help network devices to manage and face anomalous situations whenever needed, such as congestion or jamming in the communication channels.

Some of the mechanisms are as follows:

– Use of the *CSMA/CA protocol* to efficiently access the medium. Its function allows any node to observe the medium before transmitting in order to check whether another network device is using the channel. This service is really useful when the channel presents noise and the communication systems do not implement specific mechanisms to change by themselves the RF.

– *Change the RF output power* to a lower output power. This is feasible by dynamically adjusting the transmitter to a level that ensures the expected reliability in communication. As a consequence, the probability of conflicts among signals can

be reduced with a positive effect over the battery lifetime. Similarly, a dynamic RF channel selection can also be possible through the frequency agility service, which is managed and supervised by the network coordinator. Note that, as already commented in section 4.2.3.2.1., ZigBee-PRO assigns this service to the channel manager node, thus reducing the load of the coordinator.

– Use of an *automatic packet (APSDU) length selection* mechanism to avoid large packet losses. In some cases, such as when the channel suffers a high congestion and/or noise, large packets might not reach their respective destination nodes properly. Then, under these circumstances, it is almost preferable to ensure that a certain percentage of information reaches a destination node using small APSDU packets. Note that some research experiments have shown that these changes are not very recommendable, since they could not always result in a better performance.

– Use of a *selection mechanism of alternative routes* for mesh networks. Such mechanism is based on the analysis of the interference levels for each path before the transmission of information. Such analyses require a link-cost function whose input might depend, for example, on the information related to the location of the neighbor nodes, residual battery levels, or even to a link quality indicator (LQI). A LQI is a specific indicator to measure the quality of a received packet. In our case, we could use the received signal strength as an indicator.

– Finally, it is important to highlight that *energy control mechanisms* could also aid in reducing packet conflicts. In our case, ZigBee provides a low duty cycle process in order to offer a persistent state change in network devices. These state changes might mean an important decrease in signal conflicts and a better availability of the medium.

4.2.3.4. *Current ZigBee solutions for digital home*

The ZigBee Alliance provides a multitude of standards, solutions, and products. In fact, as of 2011, the Zigbee Alliance has officially published seven standardized applications profiles and five technical documents. Some of these profiles can be used to create attractive digital home scenarios, where different technologies and communication systems could be integrated. For example, a digital home scenario could include solutions for home automation, smart energy, remote control, telecom, or health care.

The idea is to create a smart wireless environment where users can easily find their comfort, social well-being, safety, and security. This means that the system has to be able to transparently cover any kind of users' need, while ensuring the physical and logical security of the household, independently of the user geographic location. Some examples of ZigBee devices for home environments are hand-held remote

controllers, wireless switches, plasmas/TVs, DVDs, radios, smart meters, climate control, security, and lighting systems.

One specific example of ZigBee devices is the home security devices. Such devices are usually equipped with sensors that can detect anomalous events (e.g. gas escape or fire). Other devices include cameras and software mechanisms that enable local and remote control. These devices can, for example, turn on/off a security system, open/close windows, lock/unlock doors, detect smoke, etc. Another application of the ZigBee standard provides users with mechanisms to efficiently control energy consumption (gas, water, and thermal). The autonomous and intelligent devices that enable this functionality are known as advanced meter reading (AMR) systems. More specifically, AMRs have the capability of measuring and managing energy in real-time detecting failures or malfunctioning (e.g. leaks). They even can provide intelligent solutions to resolve anomalous situations, such as stopping the service and warning the central security system. Its network topology is usually based on wireless mesh networks with a wide coverage across residential complexes and with connectivity to AMI. These infrastructures are in charge of collecting and analyzing energy usage obtained from a specific residential complex.

So far, there are several companies that provide ZigBee solutions for smart home environments. For example, Eaton's Home Heartbeat is one of the worldwide leaders in home automation and power distribution using the ZigBee standard. Likewise, AMX provides advanced control systems for homes whose main target is to offer performance and interoperability with other wireless communication systems. There are other companies and research centers, such as Cefriel, that are pursuing the development of novel digital home applications using ZigBee. Examples are solutions for lighting (light, windows, and tent management), heat and conditioning (remote activation, programmable power on/off), kitchen automation (programmable working time, diet and menus management, ordering management), intrusion detection and domestic safety (remote home control, physical security, intrusion detection), life and wellness (heart and vital sign control, elderly people monitoring, people vigilance with disability), expert remote assistance (vital sign monitoring, wellness check up, remote heart auscultation), and others.

4.3. Remote access to homes

Because of the technological developments in both telecommunications and computing fields, users express their interest to share their personal experience through multimedia (holiday pictures, birthday video, films, songs, etc.). That is why we find a huge number of services offering multimedia content sharing, mainly in the Internet (DailyMotion and YouTube) and by some P2P frameworks (Bittorent and Emule). Besides, several works try to provide network solutions to RA since the

protocols used in the home network, mainly UPnP and DLNA, are not originally designed for this issue. In fact, RA presents challenges, especially security and QoS to be provided to the end users. The aim of this section is to provide a concise but detailed description of some existing RA strategies.

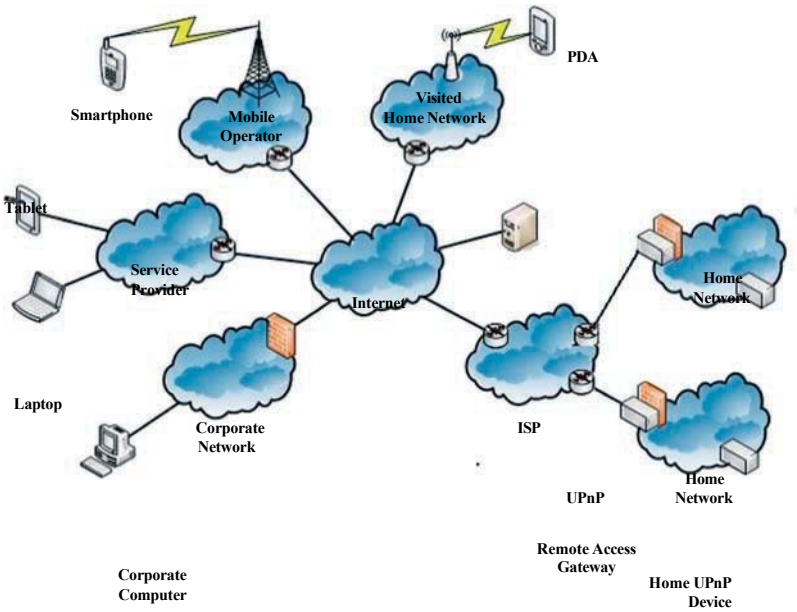

Figure 4.9. *Network description*

4.3.1. *P2P and web service*

A large number of content sharing services exist in the Internet. Examples of these services are YouTube for video sharing and Picasa for picture sharing. These services are usually dedicated to one content type and as of 2011 there is no service offering a sharing for all multimedia types (note that we consider Facebook mainly as a content aggregator: video content can be linked, but not stored). Also, the contents shared by these services are stored in a central server, and the fact that the contents are stored outside the users' home is quite troublesome in terms of privacy. Besides, Web solutions and P2P solutions (Weezo and Bittorent) do not offer real security and authentication features in their services to allow the end user to control with whom he/she shares his/her contents. Final shortcoming that we can mention about these solutions is the QoS miss in the content transfer phase, as the P2P and Web service providers have no agreement with the network operator to make resources reservation to support their traffic.

4.3.2. *UPnP remote access*

UPnP RA describes an architecture that allows generic UPnP devices, services, and control points deployed in remote physical devices to interact with the corresponding UPnP devices, services, and control points physically attached to the home network. The mechanisms defined in this architecture allow people to extend the home network so that it will logically include remote devices. As a result, all devices can communicate among themselves using the UPnP Forum defined mechanisms, e.g. UDA. The desired behavior of the interactions between the remote and home devices is envisioned to be similar with the behavior expected as if all devices were located in the same local area network (LAN): remote devices will be able to follow the same steps (e.g. IP addressing, discovery, description, control, and eventing) as any UPnP device present in a home network.

UPnP technology was envisioned to be deployed in LANs. This initial design goal led to some challenges when trying to expand the original scope of the UPnP technology beyond the physical boundaries of LANs such as those found at home. For example, the discovery step described in the UPnP Device Architecture v1. 0 involves multicast messages, which will be difficult to forward beyond the home network because of the fact that a typical Internet router will discard such messages. In addition, the overall user experience might be degraded due to the limitations induced by external factors (e.g. network latencies and bandwidth).

To make the vision of the Remote Access Architecture possible, there are two main mechanisms: (i) a transport channel which provides the security for UPnP Device Architecture protocols, and for any associated protocols that are used in the context of various DCPs (e.g. RTP [RFC 3550]) and (ii) a Discovery Agent, which enables a UPnP device or service to be visible from a remote location and that controls the visibility of these devices according to some filters configured by the homeowner. Using these mechanisms, the experience provided by the Remote Access Architecture is similar to the experience encountered at home, although with certain limitations due to the available bandwidth on the path between the remote device and the home network.

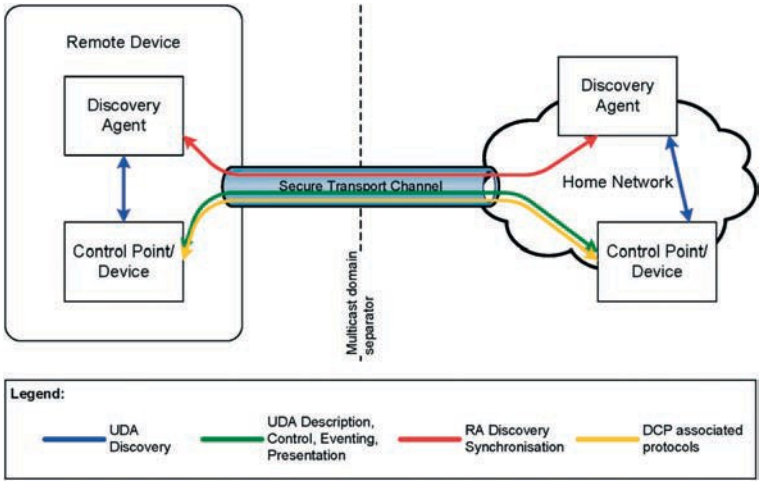

Figure 4.10. *UPnP RA RA Architecture*

In more detail, the role of the Remote Access Discovery Agents (RADA) is to expose a UPnP Service interface to facilitate in-band synchronization with other discovery agents. Each RADA will register itself with the other Discovery Agents in the remote connection by providing information about itself such that it can be notified of changes in the device aggregation tree.

The Location URL for the UPnP Service exposed by the Discovery Agent is fixed and will always be bound to Transmission Control Protocol (TCP) port 1900 on the established path link between the two networks, negating any need to "discover" the other RADA. A Discovery Agent simply needs to download the description document from this URL in order to determine the Control and Event URLs.

Whenever a UPnP Device is added or removed from the aggregation tree, the Discovery Agent will notify other Discovery Agents by invoking the appropriate action on the UPnP Service exposed by the remote Discovery Agent.

During the SSDP synchronization process, the information about the UPnP Devices and services that are maintained in the local branch of one Discovery Agent is transferred to the remote branch of the corresponding remote Discovery Agent. Before transferring the local branch information, the Discovery Agent may apply some filters defined by the user in order to restrict the visibility of some of the local devices from remote entities.

4.3.3. *HGI remote access*

Home Gateway Initiative (HGI) proposes a new architecture for providing a standardized RA to the residential home gateways (HG). The architecture proposes solutions for establishing a media tunnel between the remote device and a device in the home. HGI defines two approaches for the RA, and these approaches define four new blocks in the HG, dedicated to the RA feature:

– "Device Discovery" in the home;

– "RA-config" to manage an ACL which designates remote caller rights to access to the local devices;

– "Synchronization" to synchronize the remote devices with the HG services; and

– "Remote Access Transport" to forward the data traffic between remote and local devices.

The first approach reuses the IP Multimedia Subsystem (IMS) framework to interconnect the two remote HGs. This approach inspired many works to extend the use of UPnP for remote sharing. It uses Session Initiation Protocol (SIP) to exchange UPnP signaling. In those solutions, the HG embeds a SIP User Agent (SIP UA) and a SIP/UPnP Adapter. Once the SIP UAs have established the session between the remote HGs, the SIP/UPnP Adapter acts as a proxy. The adaptation comes to handle the differences between the UPnP and SIP protocol stacks: UPnP uses HTTP as a control and transport protocol, while SIP uses UDP and RTP. The SIP/UPnP Adapter translates all signaling messages going to and coming from the HG (HTTP ↔ SIP). Another adaptation is made during the media delivery phase (HTTP ↔ RTP) to transport multimedia packets. More information about IMS and SIP is included in Chapter 8.

The relevant drawback is the memory and CPU consumption in the HG. Indeed, an HG has memory and processor constraints as it is a small network device (i.e. a Customer Premise Equipment) and its main function is routing. It is not normally designed for such services adaptation.

The second approach proposed by HGI for RA is a web-oriented approach. In this solution, the remote device looks for the public IP of the residential HG using a Domain Name Server (DNS) server. Then, it logs in a web server embedded in the HG using his/her login/password. Thus, the remote device will be able to access to the authorized devices in the home through the web server in the HG.

4.3.4. *TISPAN remote access (based on UPnP RA:1)*

The Telecommunications and Internet converged Services and Protocols for Advanced Technologies (TISPAN), a standardization body of the European Telecommunications Standards Institute (ETSI), defines two types of RA architectures. The first is based on a virtual private network (VPN) solution and the second is based on using a proxy. In TISPAN the following terms are used:

– CND: Customer Network Device;

– CNG: Customer Network Gateway;

– CPN: Customer Premises Network; and

– Remote UE: Remote User End Service.

The first solution (based on VPN) only describes how to establish a secure tunnel between two homes in order to be able to use a UPnP RA solution.

Let us describe first a procedure by which an RA connection is established: in this procedure, the information of which CNDs are registered in the CNG (and therefore accessible through RA) is retrieved by the remote UE. The UE provides an application linking the procedures for RA services. The initial setup establishes the connection between the two peers: the Remote UE and the CNG.

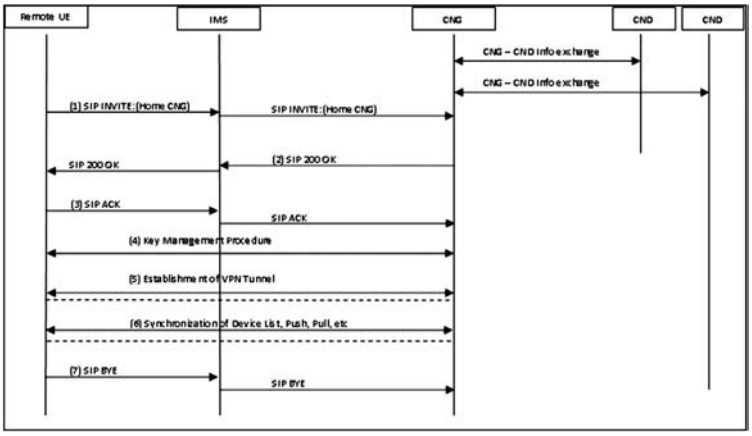

Figure 4.11. *TISPAN Remote Access*

Initially, in order to have a not empty device list, the CNDs in the CPN have to be registered (e.g. using UPnP) to the CNG before the following steps take place:

1) The UE, using the RA menu, initiates a SIP INVITE toward the home CNG. The request is granted by the IMS core and sent to CNG.

2) CNG checks whether the request shall be granted. It initiates the mapping of addresses and ports and prepares the RA procedures by returning SIP 200 OK.

3) SIP ACK is sent to acknowledge the RA session setup.

4) If no keys for the tunnel were distributed in the SDP part, the key management procedures starts by agreeing on keys and tunnel type.

5) A secure tunnel is set up between the remote UE and the CNG enabling the RA services.

6) After tunnel establishment, any side may send synchronization messages. The traffic is now enabled and will be transferred between the two peers using the established tunnel connection carrying both the UPnP signaling and the UPnP media transfer.

7) If the RA session is to be terminated, a SIP BYE is sent.

One major issue of this solution is the potential address conflict, as the home networks usually use the same address range in the LANs.

4.3.5. *TISPAN RA using UPnP proxy*

This section explains in detail the concepts introduced in the previous section by describing an architecture for RA between two CPNs or between a Remote UE and a CPN using the UPnP functionalities. The solution is based on two new functions in the CPN, which could be part of the CNG-PPF (Plug and Play), the UPnP Reverse Proxy (RP), and the UPnP Virtual Media Server (VMS). We define these two new functions (RP and VMS) for allowing privacy for the shared house and usability for Remote UE.

The aim of the UPnP RP is to filter UPnP Requests using a directory, but also to filter actions for a Remote UE. For example, in the case of a content sharing between two CPNs (User B accessing remotely User A content), the UPnP RP in User A CPN will enable to browse and get content actions from the Remote UE but forbid actions such as delete, move, etc.

On the other side (Remote UE CPN), the role of the UPnP VMS is to announce the CPNs in which a user is sharing something for the Remote UE. UPnP VMS is compliant with UPnP A/V Media Server [MediaServer:3 Device Template Version 1.01].

Two kinds of ACL are introduced in which:

– sharing rules authorize User A to establish a session with User B. These rules are setup by User B.

– filtering rules govern which folders/files User B share with User A. These rules are also setup by User B.

Both sharing and filtering rules are stored in User B UPnP RP. Only sharing rules are exported to the RA AS functionality.

The RA AS functionality could be a dedicated AS, a presence AS or located in the CNG. Indeed, when User A shares a content with User B, it can be seen as a presence, as User A content is available for User B. The RA AS has the following functionalities:

1) Presence, by publishing a list of contents available for User B (see procedure no.1 in Figure 4.12), according to User A sharing rules. This functionality could be part of the CNG or be located in the IMS Network.

2) CPN Access Control, by deciding whether or not a Remote UE is allowed to connect to a CPN. This functionality could be part of the CNG or be located in the IMS Network.

3) Check service rights (see procedure no. 3 in Figure 4.12). This functionality must be located in the IMS Network.

In the Figure 4.12, the whole functionalities of the RA AS are colocated in the IMS network.

The procedures in Figure 4.12 are the following:

1) User A, who wants to share a content, has to select a repository on a CND and add filtering and sharing rules to the CNG UPnP RP.

2) CNG UPnP RP notifies the RA AS that User A wants to share a content with User B. These actions could be implemented by means of SIP presence messages if the RA AS implements the Presence service. In this case, the users first subscribe to the RA Service, then when User A publishes a new sharing rule with User B, the RA AS notifies the User B with a RA proposal from User A. Alternatively, these actions could also be implemented by means of HTTP if the RA AS supports web-based service (HTTPserver). In other words, the CNG UPnP RP could send sharing rules to the RA AS using the HTTP protocol. In that case, a notification to User B is not needed because User B directly asks the RA AS for the list of the available content.

3) Prerequisites: the UPnP VMS has the list of all CPNs sharing content with User B (using a presence enabler or dedicated requests from the RA AS). When

User B browses UPnP VMS, all Remote CPNs are displayed on his/her UPnP Media Player (MP) as directories of UPnP VMS. User B selects User A directory. Alternatively, when User B browses UPnP VMS the UPnP VMS retrieves accessible CPN and contents list from the RA AS (sent to User B CPN by CPN), and all the available contents on the User A Remote CPN are displayed on the User B UPnP MP.

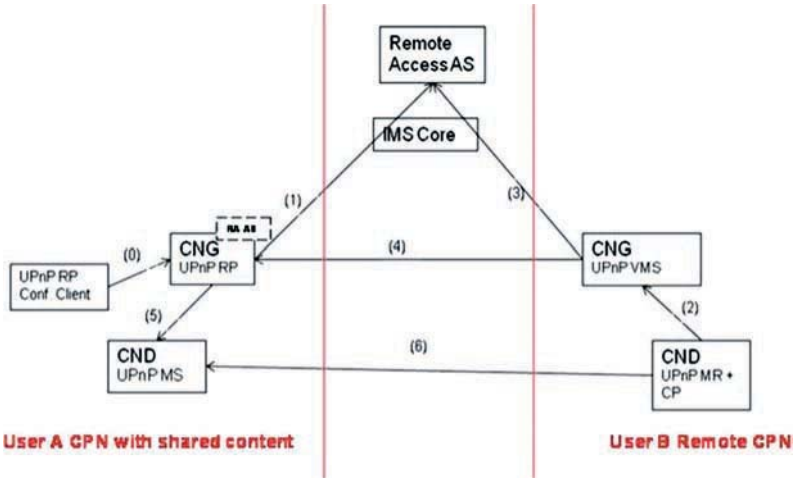

Figure 4.12. *Remote Access using UPnP functionalities, with the Remote Access AS functionalities colocated in the NGN network*

4) A SIP INVITE is sent from CNG B to CNG A to establish a new media session between User A and User B. The IMS Network checks if CNG B and CNG A have the RA service rights (e.g. the operator or owners may have the ability to switch on/off this functionality). Then the IMS Network triggers the RA AS (located in the IMS Network), which checks if that User B can access the CPN of User A. If yes a SIP session is opened between CNG B and CNG A, so as to identify User B, and negotiate HTTP parameters. Note that media flows are exchanged between CNG B and CNG A using HTTP so as to avoid HTTP/RTP translation (in case RTP would be used to convey media flows through the IMS Network).

5) UPnP VMS sends a browse request to User A CNG (based on the SIP session defined before). UPnP RP sends back a UPnP answer with all shared directories for User B. On his/her CND, User B selects a directory. Request is forwarded by the UPnP VMS to the UPnP RP.

6) Based on filtering rules, UPnP RP forwards the request to the appropriate CND in the User A CPN.

7) User B selects a content to play, then a Re-INVITE SIP session may be sent, from CNG B to CNG A, to negotiate the media to be shared (and send back the content URL to User B) and possibly the QoS parameters. In the case where a media/QoS negotiation is not needed, the content URL could be sent to User B during the browsing session, thus there is no need to send the RE-INVITE message.

Figure 4.13 describes the Remote Browsing, i.e. a procedure that can be used to establish an RA browse session between two CPNs, particularly the procedure where shared folders are delivered from a UPnP Reverse Proxy to the Remote UE CND. The prerequisites for this Remote Browsing is that the SIP User A must be already registered by means of a SIP REGISTER message in the IMS Network, so that it can be directly contacted through its sip URI. Presence enabler could be used to inform about presence of shared content from contacts.

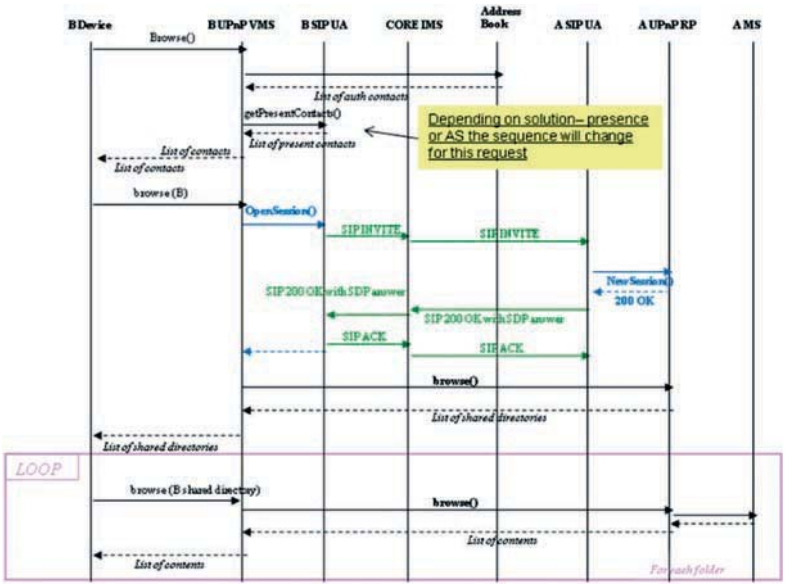

Figure 4.13. *Remote browsing from User B on User Media Server*

4.4. Bibliography

[ALC 10] ALCARA Z.C., LOPEZ J., "A security analysis for wireless sensor mesh networks in highly critical systems", *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews*, vol. 40, no. 4, pp. 419–428, July 2010.

[ALL 06a] ALLIANCE Z., "Vision for the home, ZigBee wireless home automation", *Zig-Bee Alliance*, November 2006.

[ALL 06b] ALLIANCE Z., "ZigBee Specification 053474r13", https://www.zigbee.org, December 2006.

[ALL 07] ALLIANCE Z., "ZigBee and wireless radio frequency coexistence", *ZigBee WhitePaper* (retrieved from ZigBee Website), June 2007.

[ALL 10a] ALLIANCE Z., "ZigBee automation building", https://www.zigbee.org, 2010.

[ALL 10b] ALLIANCE Z., "ZigBee automation industrial", https://www.zigbee.org, 2010.

[ALL 10c] ALLIANCE Z., "ZigBee health care", https://www.zigbee.org, 2010.

[ALL 10d] ALLIANCE Z., "ZigBee home automation", https://www.zigbee.org, 2010.

[ALL 10e] ALLIANCE Z., "ZigBee remote control", https://www.zigbee.org, 2010.

[ALL 10f] ALLIANCE Z., "ZigBee retail", https://www.zigbee.org, 2010.

[ALL 10g] ALLIANCE Z., "ZigBee RF4CE", https://www.zigbee.org, 2010.

[ALL 10h] ALLIANCE Z., "ZigBee smart energy", https://www.zigbee.org, 2010.

[ALL 10i] ALLIANCE Z., "ZigBee specifications", *http://www.zigbee.org/*, 2010.

[ALL 10j] ALLIANCE Z., "ZigBee telecom services", https://www.zigbee.org, 2010.

[AMX 10] AMX, "AMX", http://www.amx.com/, 2010.

[ATM 10] ATME, "ZigBit 2.4 GHz module product data", http://www.atmel.com/dyn/resources/prod_documents/doc8226.pdf, 2010.

[CAG 06] CAGENIUS T et. "Evolving the TV experience: anytime, anywhere, any device", *Ericsson Review*, 2006.

[CAI 99] CAI T., LEACH P., GU Y., GOLAND Y., "Simple service discovery protocol/1.0M", *http://www.ietf.org/proceedings/44/I-D/draft-cai-ssdp-v1-00.txt*, February 1999.

[CEF 10] CEFRIEL, http://www.cefriel.it/, 2010.

[CHA 08] CHAN M., ESTÈVE D., ESCRIBA C., CAMPO E., "A review of smart homes – present state and future challenges", *Comput Methods Programs Biomed*, Elsevier North-Holland, Inc., vol. 91, no. 1, pp. 55–81, 2008.

[CHI 08] CHINTADA S. et al., "Converged services for Home using a SIP/UPnP software bridge solution", *IEEE Consumer Communications & Networking Conference*, 2008.

[COH 98] COHEN J., AGGARWAL S., *Internet-Draft GENA Base*, July 1998.

[DLNA 04] DIGITAL LIVING NETWORK ALLIANCE, DLNA Home Networked Device Interoperability Guidelines v1.0, June 2004.

[DRO 97] DROMS R., Dynamic host configuration protocol RFC 2131, March 1997.

[EMB 10] EMBER, "EM357 product datasheet", http://www.ember.com/pdf/ember-EM300.pdf, 2010.

[ETSI 09] ETSI, "Open … for business", *http://www.etsi.org*, 2009.

[FAS 08] FASBENDER A., GERDES M., HJELM J., KVARNSTRÖM B., PETERSSON J., SKOG R., "Virtually at home: high-performance access to personal media", *Ericsson Review*, November 2008.

[FRE 10] FREESCALE, "MC13213 product datasheet", http://cache.freescale.com/files/rf_if/doc/data_sheet/MC1321x.pdf?pspll=1,2004,2010.

[GOL 06] GOLMIE N., Coexistence in wireless networks, challenges and system-level solutions in the unlicenced bands, University Press, Cambridge, 2006.

[GOU 07] DE GOUVEIA F.C., MAGEDANZ T., GOOD R., VENTURA N., "The role of open IMS testbeds in complex service delivery platforms", *AFRICON 2007*, September 2007.

[HAD 03] HADLEY M., MENDELSOHN N., MOREAU J., NIELSEN H., GUDGIN M., "SOAP version 1.2 part 1: messaging framework", *W3C REC REC-soap12-part1-20030624*, June 2003.

[HEA 10] HEARTBEAT H., "Home heartbeat", http://www.Homeheartbeat.com/HomeHeartBeat/index.htm, 2010.

[HGI 08a] HGI, HGI guideline paper remote access v1.01, May 2008.

[HGI 08b] HGI, Home gateway requirements: residential profile, Home gateway initiative, April 2008.

[IEE 02] "IEEE STANDARD, 802.15.4-2003, WPAN Task Group 4b, TG4b, Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)", *http://www.cmi.ac.in/~sdatta/ networks/standards/802.15.4-2003.pdf*, 2002.

[IEE 06] "IEEE Standard, 802.15.4-2006, Telecommunications and information exchange between systems – local and metropolitan area networks – Specific requirements, Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (LR-WPANs)", *http://standards.ieee.org/getieee802/download/802.15.4-2006.pdf*, September 2006.

[INT 10] INTERNATIONALD, "ZigBee and RF modules", http://www.digi.com/products/embeddedsolutions/zigbeesolutions/, 1996-2010.

[IYE 01] IYER P., WARRIER U., *UPnP Forum, UPnP Internet Gateway Device:1*, November 2001.

[JEN 10] JENNIC, "JN5148 product datasheet", http://www.jennic.com/download_file.php?brief=JN-DS-JN5148-1v2.pdf, 2010.

[KUM 06] KUMAR B., RAHMAN M., "Mobility support for Universal Plug and Play (UPnP) devices using Session Initiation Protocol (SIP)", *IEEE Consumer Communications & Networking Conference*, 2006.

[LEE 07] LEE J-S., SU Y-W., SHENC C-C., "A comparative study of wireless protocols: bluetooth, UWB, ZigBee, and Wi-Fi", *IECON, 33rd Annual Conference on IEEE Industrial Electronics Society*, Taipei, Taiwan, pp. 46–51, November 2007.

[LOP 09] LOPEZ J., ROMAN R., ALCARAZ C., "Analysis of security threats, requirements, technologies and standards in Wireless Sensor Networks", *On Foundations of Security Analysis and Design*, vol. LNCS 5705, pp. 289–338, 2009.

[MAA 09] EL MAARABANI M., ADALA A., HWANG I., CAVALLI A., "Interoperability testing of presence service on IMS platform", *Testbeds and Research Infrastructures for the Development of Networks & Communities and Workshops*, April 2009.

[MES 10] MESHNETICS, "ZigBit 900 mModule with balanced RF output", *http://www.meshnetics.com/zigbee-modules/zigbit900/*, 2010.

[MIS 09] MISCHLER D., TOUTAINT L, DIRAISON B., "SYSTERMIN@L: consumer devices for IMS/TISPAN deployment", *IEEE International Symposium on Broadband Multimedia Systems and Broadcasting*, Bilbao, May 2009.

[MOT 06] MOTOROLA, "X-Internet", http://www.motorola.com/innovators/pdfs/X-Internet-WhitePaper.pdf, July 2006.

[NET 10] NET4HOMES, "ZigBee devices for home", http://www.tradett.com/product_list/u32129/all-products.html, 2009–2010.

[OPENWRT] http://www.openwrt.org.

[PJSIP] http://www.pjsip.org.

[RIT 02] RITCHIE J., KUEHNEL T., UPnP AV Architecture for universal plug and play version 1.0, UPnP forum, 2002.

[SHU 06] SHUAIB K., BOULMALF M., SALLABI F., LAKAS A., "Co-existence of Zigbee and WLAN – a performance study", *2006 IFIP International Conference on Wireless and Optical Communications Networks*, p. 5, 2006.

[STA 09] "Smart Grid Cyber Security Strategy and Requirements", *OF STANDARDS N. N. I. Technology, Draft NISTIR 7628*, The Cyber Security Coordination Task Group, September 2009.

[TISPAN A] *TISPAN TS 185 003* (CNG Architecture).

[TISPAN P] *TISPAN TS 185 010* (Protocols).

[UPnP 02] UPnP FORUM, *UPnP AV Architecture V1.0*, June 2002.

[UPnP 08] UPnP FORUM, *UPnP Device Architecture V1.1*, October 2008.

[UPnP 09a] UPnP FORUM, *Remote Access Architecture V1.0*, September 2009.

[UPnP 09b] UPnP FORUM, *RAClient V1.0*, September 2009.

[UPnP 09c]UPnP FORUM, *RAServer V1.0*, September 2009.