(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 July 2006 (13.07.2006)

PCT

(10) International Publication Number
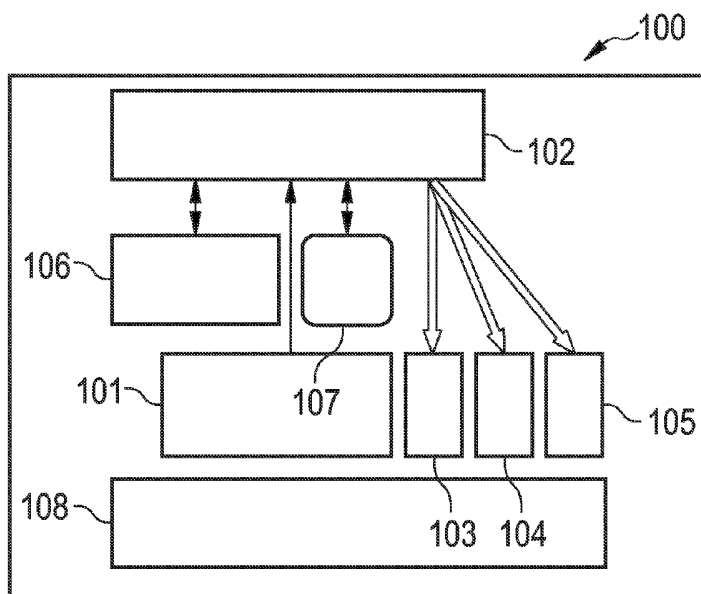**WO 2006/072860 A1**

(54) **Title:** DEVICE CAPABLE OF BEING OPERATED WITHIN A NETWORK AND PROVIDING SERVICES TO THE NETWORK, METHOD OF OPERATING SUCH A DEVICE WITHIN A NETWORK, PROGRAM ELEMENT AND COMPUTER-READABLE MEDIUM

(57) **Abstract:** A device (100) capable of being operated within a network (201) and providing services to the network (201), the device comprising a determining unit (101) adapted to determine the network (201) in which the device (100) is operable, and a selection unit (102) adapted to select, on the basis of the network (201) determined by the determining unit (101), a mode in accordance with which the device (100) provides at least one service to the network (201) when the device is connected in the network (201) determined by the determining unit (101).

For two-letter codes and other abbreviations, refer to the "Guid-
ance Notes on Codes and Abbreviations" appearing at the begin-
ning of each regular issue of the PCT Gazette.

Device capable of being operated within a network and providing services to the network, method of operating such a device within a network, program element and computer-readable medium

The invention relates to a device capable of being operated within a network and providing services to the network.

The invention further relates to a method of operating such a device within a network.

5   The invention also relates to a program element and to a computer-readable medium.

Portable devices are becoming more and more important. Particularly, an

10   increasing number of users buy hard disk-based portable audio/video players, powerful and intelligent cellular phones, and other portable entertainment equipment.

Many portable devices according to the prior art use point-to-point connectivity to a personal computer (PC) to exchange content (for example, through Universal Serial Bus (USB™) or FireWire™). However, many companies are working on

15   the next generation of these products, which will offer more powerful connectivity possibilities. Two important technologies, which may be implemented in the context of such devices, are WiFi and Bluetooth (IEEE 802.15 standard).

Using such technologies, the portable devices will be able to communicate directly with other devices on a network, for example, a home network, and exchange content

20   and control information with them.

In the world of networked home entertainment devices (such as the Philips Streamium™), a standard denoted as UPnP (Universal Plug and Play) can be implemented to realize such a kind of interconnectivity. This UPnP technology defines a "common language" and necessary services for devices to talk to one another. Thus, a user is enabled to stream

25   content from one device, which is located in his home, to another device, as long as both devices are connected to the network.

A standardization body called the Digital Living Network Alliance (DLNA) has specified extra requirements on top of UPnP (for example, codecs, options), in order to guarantee interoperability between all compliant network devices.

As portable devices are now also entering this connected world, they are also moving towards the use of UPnP, as they wish to be connected to all the other devices in the home, once they are connected to the home network. This connection may be direct, for example, when the device uses WiFi. However, interaction is possible even without such a

5   direct network connection. DNLA defines an architecture allowing interactions between such a portable device and the stationary UPnP network, even if WiFi is not used as the main connectivity means, but, for example, Bluetooth is used instead. For that case, it is proposed to include a WiFi-Bluetooth bridge within the network. In any case, UPnP runs on top of all this, and allows inter-device communication.

10   In a UPnP network, a media server may be implemented as a device for hosting content (audio, video, picture, etc.) and for exposing this content on a home network. A media renderer is a device capable of playing back certain types of content, which device is controllable via a UPnP network, that is to say, external devices can track and control the renderer (for example, start playback of a song from a media server). A control point of a

15   UPnP network is a controlling device capable of browsing content available on the network (i.e. on media servers), starting and controlling playback of this or other content on media renderers on the network, and tracking progress on these renderers. Such a control point is also capable of performing actions such as content move between media servers.

Each of these components is logically independent and may reside on different

20   devices, or can be combined to one.

The media renderer and server may offer a service to the network (for instance, a service like "I have content", "I can play content"), whereas a control point is able to use these services.

Documents WO 2004/077791 A1 and US 2004/0083303 A1 disclose methods

25   as to how control points can discover what action they are allowed to perform and access on a media server or a media renderer. Since a control point does not know in advance what it is authorized to do, WO 2004/077791 A1 and US 2004/0083303 A1 describe mechanisms to discover in advance what action is authorized before a user actually presses a button to trigger such an action.

30   Thus, WO 2004/077791 A1 and US 2004/0083303 A1 describe how a controlling device (accessing remote services) can address devices with known authorizations and access rules.

However, it is a shortcoming of the prior art that it does not teach how a device containing content to be offered may be configured so as to be properly operable in a plurality of different networks in which it may be operated during its lifetime.

5

It is an object of the invention to enable a device to be used flexibly and securely in a plurality of different networks.

In order to achieve the object defined above, a device capable of being operated within a network and providing services to the network, a method of operating such

10   a device within a network, a program element and a computer-readable medium as defined in the independent claims are provided.

According to the invention, a device is provided which is capable of being operated within a network, and which comprises a determining unit adapted to determine the network in which the device is operable, and a selection unit adapted to select, on the basis of

15   the determined network, a mode in accordance with which the device provides at least one service to the network when the device is connected in the network determined by the determining unit.

The invention further provides a method of operating such a device within a network, wherein the network is determined in which the device is operable. Furthermore,

20   based on the determined network, a mode is selected in accordance with which the device provides at least one service to the network when being connected in the determined network.

A program element is also provided, which, when being executed by a processor, is adapted to carry out a method of operating a device within a network in accordance with the above-mentioned method steps.

25   Moreover, a computer-readable medium is provided, in which a computer program is stored which, when being executed by a processor, is adapted to carry out a method of operating a device within a network in accordance with the above-mentioned method steps.

The operation of the device within a network can be realized by a computer

30   program, i.e. by software, or by using one or more special electronic optimization circuits, i.e. in hardware or in a hybrid form, i.e. by means of software components and hardware components.

The characteristic features according to the invention particularly have the advantage that the device determines by itself which network/networks is/are currently

available for access. For instance, the device may detect whether there is a WLAN (wireless local area network) present at a location at which the device is operated, via which the device might intercommunicate with other nodes of the network. After having determined a network that is accessible by the device (or would allow the device to join the network), the device

5   self-configures its service-providing mode. In other words, the device internally determines if, and in what manner, services which may be provided by the device to other nodes of a network will in fact be provided to the nodes of the determined network in which the device is interconnected. For instance, if a detected available network is ranked to be secure (for instance, in the case of a home network environment), the service-providing mode may be

10   configured in such a way that all nodes of the "secure" network have full access to all services provided by the device to the network. If, for instance, a network is considered to be not secure (for example, the Internet), no service at all may be provided to all other nodes to the network. In this scenario, the selection unit may configure the device in such a way that no other Internet computer may use the device having a camera functionality such as a web

15   cam. Another service-providing mode of the device might partly allow and partly prohibit access to services provided by the device, for instance, allowing services only below a predetermined service bandwidth threshold, or allowing only computers with particular IP addresses to access the services of the device.

              Thus, particularly for an application of the device as a portable connectable

20   device having an audio or video jukebox functionality, it is advantageous that the device can enter a plurality of networks during its lifetime, and that, whenever the device enters a new network, the mode of the service provided may be adapted or updated accordingly.

              Thus, according to measures of the invention, a network-based content-sharing service is realized which may be fully automated and integrated in the device.

25   According to the invention, a selective activation and configuration of device services based on a specific network is allowed. With portable devices, such as cellular phones and portable audio/video jukeboxes, gaining connectivity capabilities, they may become an integral part of the home network of entertainment services (such as the Philips Streamium™ product range). All of these connected home products may use Universal Plug

30   and Play (UPnP) and related services as interconnectivity technology. The system according to the invention overcomes the shortcoming that these technologies as yet provide no security feature, i.e. if content is locally exposed via UPnP, there is no access control mechanism, and everybody on the network is able to access the content. Such a free access may be fine in some applications which are limited to a pure home network. However, in the case of

portable devices, which are connectable to a variety of other networks outside the home, this is no longer a desirable situation. To overcome this security problem, it is taught according to the invention to activate and configure specific UPnP services (for example, defined by a user, by the manufacturer or by some intelligent process) depending on the network the

5   device is currently connected to.

UPnP is a standard that facilitates inter-device communication, but it has no security or access control features available, that is to say, once on the network, everybody can access all the content exposed by UPnP media server, or use other services offered by a UPnP device. The system according to the invention significantly improves the security

10   situation, because it allows flexible adaptation of the mode of accessing its services in dependence upon the network or network type in which a service-providing device is to be interconnected.

In other words, in a home context, access control is not such a problem in some cases, as all the family members are probably allowed to access this content. However,

15   serious problems arise when portable devices become part of such a home network. As described above, they can also use UPnP to expose content or services to the network, making, for instance, personal pictures available for other devices on the network. Such portable devices will frequently leave the home and connect to various other networks (for example, a corporate network, a public WiFi hotspot, a hotel room network, etc.).

20   Unless the user specifically disables the network services (for example, UPnP services) time after time, the devices according to the related art will also expose content in this situation, which is probably not what a user desires. The system according to the invention overcomes this problem by automatically selecting a network-dependent service provision mode without requiring the user to change settings manually every time.

25   According to one aspect of the invention, a portable device with network connectivity is provided with the ability to offer some services on a network, for example, using UPnP. This device may use means that allow detection of the network the device is logged in to. Depending on the actual network (or the type of the actual network), the device automatically enables/disables or configures the services it wants to offer, for example, via

30   UPnP.

According to an aspect of the invention, a device is provided which comprises wireless networking means (for example, Bluetooth or WiFi) for establishing and connecting to a network, servicing means for servicing content to the network using a connectivity technology (such as, for example, UPnP), detection means for detecting or characterizing the

network in which the device is interconnected, and configuring means for configuring the servicing means in that different services are available in dependence upon the detected or characterized network the device is part of.

A preferred application of the invention is portable network entertainment equipment, such as audio/video network hard disk-based audio/video jukeboxes. Other applications relate to cellular phones with Bluetooth or WiFi connectivity. Other preferred applications of the invention are portable network devices exposing services to the network using a technology such as UPnP, which devices are expected to connect to various different networks.

Thus, the system according to the invention provides access control verification or conditional access, which access may also be implemented in the frame of a UPnP standard.

An idea of the invention starts from a scenario of devices offering services (for example, host content as a media server), which services are or may be networked. Examples are WiFi-enabled mobile phones wanting to share pictures, or portable audio/video jukeboxes with WiFi capabilities. Such devices can encounter many networks (due to their mobile and nomadic nature). Without the precautions taken by the invention, the services offered by the devices will act the same on all of these networks, for example, all of its content will be exposed. The system according to the invention adapts such a device in such a manner that the device finds out what network it is actually on (there are several techniques to do this), and, based on this determination, configures all of the services it has available. It could totally shut down its media server, or only expose part of its content, or expose (for example, at home) all of its content.

It is to be noted that UPnP is not limited to only audio/video, but also has specifications for imaging, etc. This means that a camera function of a cellular phone could also be made controllable from the network. This may be desirable in a home or in an office (since one might use the cellular phone as a web cam), but not in a general public situation. Another example is that a user wishes a cellular phone to offer SMS capabilities on the home network, but of course not on a public network. Such a service can be realized within UPnP, but actual configuration or switching on/off depending on the network may still be left to the user.

Thus, the invention teaches how devices that offer services can adapt the configuration of the services depending on the network situation they are in. Such an automatic configuration of services (for example, UPnP services), especially on portable

devices, depending on the situation and/or the network and/or the location they are in are important for flexible and secure use of these devices.

The device of the invention may be realized as in integrated circuit, particularly as a semi-conductor integrated circuit. In particular, the system can be realized as

5   a monolithic IC, which may be fabricated in silicon technology.

Referring to the dependent claims, further preferred embodiments of the invention will be described hereinafter.

Preferred embodiments of the device of the invention will now be described. These embodiments may also apply to the method of operating a device within a network, the

10   program element and the computer-readable medium.

The device may comprise a storage unit adapted to store data according to at least one service which the device is capable of providing to a network. Such a storage unit may be a hard disk, a ROM-memory, a RAM-memory, a flash memory or an optical storage medium such as a DVD., The storage unit is preferably erasable and (re-)programmable to

15   allow updating of stored service data. Such a storage unit may contain, for instance, control information for a camera used as a web cam, audio, video or picture data, etc.

Selecting a mode by the selection unit may include selecting a security mode. Based on the detected or discovered network or type of network, the device may, for instance, classify the identified network as highly secure, medium secure, or low secure

20   (alternatively, any other classification scheme may be implemented), so that the provision of services by the device and the exchange of control information can be performed on a corresponding security level.

Selecting a mode by the selection unit may also include selecting one of a plurality of access control modes. Based on the determined network or a type of network, the

25   control of access of other nodes of the network to the device for using a service provided by the device is thus controlled. For instance, access of all network nodes or only a part of the network nodes to the services of the device may be enabled.

Selecting a mode by the selection unit may include at least one of the group consisting of completely enabling at least one service to at least one node of a network,

30   completely disabling at least one service to at least one node of a network, and partly enabling/partly disabling at least one service to at least one node of a network.

This embodiment will be illustrated by way of some examples. Taking, for instance, explicit user input, factory settings, or some other intelligent mechanism into account, the device may detect how desirable its available services are in this network. For

example, the device may detect that it is connected to a home network of a user via a WiFi network. In this home setting, all the device services can be safely enabled. Alternatively, the device may be connected to a home network, but via Bluetooth. Although all the services might be enabled from a security point of view, the media server may be automatically

5   configured to only expose sound and pictures, since the available bandwidth in the present network is insufficient to host movies. According to another alternative, the device may be connected to a corporate network of a user: in such a scenario, a user may specify that, in this specific network, only the media server service is to be enabled, hosting only one specific directory of content. According to another scenario, the device may be connected to an

10   anonymous public WiFi hotspot. In such an environment, the exposure of all services of the device may be disabled. Based on such knowledge, the device may select and configure an appropriate service for this network situation.

The selection unit may be adapted to select the service provision mode on the basis of at least one of the group consisting of a user-defined selection rule, a pre-stored

15   selection rule, and a selection rule transmitted to the device via a network in which the device is currently operated.

Regarding the intelligence to know which services are to be started at a given network, this could be realized in one of the following ways.

For instance, whenever a user enters a new network, the device may prompt

20   him to specify what services should be started and how they should be configured (preferably with a minimal template, for example, start no service, acting as default). The device characterization can be performed at the same time. The service information/configuration may then be stored together with the network characterization, and the next time this network is encountered, the correct services may be started and configured in accordance with the

25   relevant profile.

Alternatively, the user may be enabled to configure which service is to be started and configured manually, but the user does this offline, without actually being on the specific network. This may be a service offered by a company like Philips™, wherein a consumer who has bought a portable player can log on to a website (for instance,

30   my.philips.com) and configure the behavior the user desires for his device in a specific environment. This back-end could already have a characterization of all the networks that any connected Philips™ device owned by this user is on (for example, the user has a Streamium™ radio in his office, and a Streamium™ TV in his home, and both of these devices are connected with a Philips™ back-end, and can report on specific network

information, thus allowing the back-end to create such network profiles). For each of these networks, the user could then state specifically the manner in which he desires his portable device to behave. Whenever a portable device enters a different network, it may contact the Philips™ back-end, and request the specific profile for this network. It can use this

5   information to configure itself correctly. This has the advantage that a user only needs to create such a central profile once, which profile can then be shared with all his devices.

Alternatively, the device can maintain a list of "friendly" devices. Consequently, when the device discovers one of these friendly devices on the network, the device may assume that the network is secure, and thus assume a certain configuration. For

10   instance, when the device identifies that another known device belonging to the same user has a (number of) given service(s) running, the device can decide to launch similar services with similar configurations. For instance, if the device discovers the presence of the home media server, it can start up its own media server with all of its content shared. When the device discovers the user's laptop with the media server on the network with only a

15   "corporate" folder shared, the device can decide to act similarly. Kids at school could "pair" their devices, i.e. build a community, and when one device encounters one or more of these other "paired" devices, the device can start up the media server and host the "school content share". Further network restrictions could be applied, for example, "only do this when on a private ad-hoc network with no other devices present", or "only do this when on a 'class'

20   sub-network", etc.

Depending on the type of services available on the network, it can be decided which services are started in a given network. For example, the user may have configured his portable device to start up the media server, and host a "presentations" folder whenever it is on a sub-network which is part of his corporate network with a UPnP projector on it.

25   The device of the invention may further comprise a networking unit adapted to operate the device in one of a plurality of different types of networks. Thus, a network stack or software unit may be implemented in the device, which stack or software unit allows the device to be operated in a plurality of different networks.

The networking unit may be adapted to operate the device in at least one of a

30   Bluetooth network and a WiFi network. Bluetooth is an industrial specification for wireless personal area networks (PANs) formalized by the Bluetooth Special Interest Group (SIG). WiFi, short for "Wireless Fidelity", is a set of standards for wireless local area networks (WLAN) based on the IEEE 802.11 specification. WiFi is intended to be used for wireless devices and LANs, but may also be used for Internet access. WiFi enables a person with a

wireless notebook or desktop computer or personal digital assistant (PDA) to connect with the Internet when he is in the proximity of an access point called a hot-spot.

In the device, the networking unit may be adapted to operate the device to communicate in accordance with a Universal Plug and Play protocol (UPnP). UPnP is a protocol for making several home network devices having different standard specifications interface mutually. UPnP allows a plurality of devices to connect and to simplify the implementation of networks in a home incorporate environment. UPnP achieves this by defining and publishing UPnP device control protocols. Since UPnP technology is independent of media devices, it can run on any medium including a phone line, a power line, an Ethernet, or by a transmission of radio frequency radiation (for example, WiFi, Bluetooth). Particularly, the device of the invention may be realized as a media server in the frame of a UPnP architecture.

The determining unit may be adapted to determine a network based on determining whether at least one reference network node is present in a network. For instance, in a home network, the address of a particular network node expected to be present in the network allows the determining unit to determine that the present network is in fact the particular home network.

Additionally or alternatively, the determining unit may be adapted to determine a network based on at least one network-access characteristic. For instance, a network name or an encryption key required to enter the network, or the combination of both, may serve to securely determine a particular network.

Additionally or alternatively, the determining unit may be adapted to determine a network based on at least one network configuration characteristic. Such a network configuration characteristic may include the information which proxy server or what DNS servers are used, or what IP address has been assigned to the device.

Additionally or alternatively, the determining unit may be adapted to determine a network based on at least one network-service characteristic. For instance, a network time server, a number of network printers or a UPnP server with a specific UDN may be interpreted as such a network service characteristic to be used to identify the present network.

Thus, the device of the invention may have some mechanism for characterizing the network it is part of. This characterization can be performed in various ways including those simply based on the SSID and encryption settings of a WiFi network, a

MAC address of the access point, or the availability of certain devices or services on the network.

Different examples of approaching the network characterization of the invention will now be explained.

5   Once a portable device is connected to a network, it could try and see if a number of reference unique hardware devices and/or characteristics are present on this specific network. An example is the access information for a wireless network (if the connection is made via WiFi). This includes settings like the SSID (i.e. the network name) or the encryption key (for example, WEP or WPA key). Without these settings, a WiFi device

10   cannot join the network. It is up to the user to enter them (for example, on-the-spot, or store them in some profile). For this purpose, the combination of the SSID and the encryption key suffices to securely and (almost) uniquely identify a network.

Alternatively or additionally, unique data on some of the networking equipment may be used for the network characterization. Each component connected to the

15   network has a MAC address assigned to it, i.e. a low-level address through which it is addressable on the network. Such a MAC address is globally unique and can thus serve to uniquely identify a device. A portable device can see if one or several networking components with specific MAC addresses are present on this network. If so, it can conclude that it is on a specific network. Prime candidates of devices to do such a presence test based

20   on MAC addresses are access points, gateways, some networked storage, or any other device that is assumed to be always on, and always present on this network.

For the sake of network characterization, the device could also look for specific configuration information that is deemed to be unique for the network. Examples of such information include the proxy server that is used by the network. For instance, when the

25   device detects that a Philips™ proxy is used on the network, it can deduce that it is on the Philips™ corporate network. Alternatively or additionally, the device may discover what DNS servers are used. Also alternatively or additionally, the device could discover its IP address. Some ranges are private, and thus do not provide any information (for example, the 192.168.*.* range, often used in home networks), but other addresses in the public range do

30   provide useful information. For instance, if the device is told that it gets an address in the 130.145.*.* range, it can assume that it is on the Philips™ Intranet.

The device of the invention could also look for the presence of specific services on the network, i.e. a network time-server, a number of network printers, and/or a UPnP server with a specific UDN (i.e. a unique characterization of a service in UPnP). Using

12

this method, if the device finds a "home server" with which it always synchronizes content on the network, it can assume that it is on the home network. The same applies to other UPnP services (for example, a renderer, a security camera, a gateway with UPnP IGD service, etc.).

Network characterization can be performed by focusing on one of the above-

5   mentioned (or other) features exclusively, or by combining (for example, doing a Fuzzy match on) a number of these features (for example, require three out of five defined features to be true).

The device of the invention may be realized as a portable device, which may be connected to and disconnected from a particular network, transported physically to

10   another network and interconnected to this other network.

The device of the invention may be realized as a device which is operable in a network in a wireless manner. For instance, the device may communicate with other nodes of a network via the exchange of electromagnetic radiation, for example, RF. Particularly, the device may be operated within a WLAN. The invention may thus be implemented

15   particularly advantageously in the frame of a wireless network. Although this will be the likely means of communication for a portable device, it is noted that the invention also applies to wired connections to the network (for example, ethernet, or even USB). Every network that supports the IP protocol can also support UPnP, thus including wired ones. Consequently, the device of the invention may be realized as a device which is operable in a

20   network in a wired manner.

The device may be realized as a device providing at least one functionality of the group consisting of audio recording, audio replay, video recording, video replay, image recording, image replay and telecommunication. For instance, the device may be a portable entertainment device such as an audio/video jukebox or a cellular phone. The device should

25   have some networking capabilities, for example, Bluetooth or WiFi. The device has some service on board, which it can expose to the network using a connectivity technology such as UPnP. The service could be, for example, the exposure of local pictures.

These and other aspects of the invention are apparent from and will be elucidated with reference to the embodiments described hereinafter.

30

The invention will be described in more detail hereinafter with reference to non-limiting examples of embodiments.

Fig. 1 shows a network-compatible device according to a preferred embodiment of the invention.

Fig. 2 shows a network including a device according to the invention.

Fig. 3 shows another network including a device according to the invention.

The illustrations in the drawings are schematic. In the different drawings, similar or identical elements are denoted by the same reference numerals.

A network-compatible device 100 according to a preferred embodiment of the invention will now be described in detail with reference to Fig. 1.

The network-compatible device 100 is capable of being operated within a network and comprises a determining unit 101 adapted to determine a network in which the device 100 is currently operable, and a selection unit 102 adapted to select, on the basis of the determined network, a mode in accordance with which the device 100 provides different items of service to the network when being connected in the network which has previously been determined by the determining unit 101. The device 100 further comprises a first service storage unit 103, a second service storage unit 104 and a third service storage unit 105. The storage units 103 to 105 are adapted to store data according to three different services, which services the device 100 may provide to nodes (for example, other devices such as computers, PDAs, mobile phones, etc.) of a network. The selection unit 102 is adapted to select a mode based on a user-defined selection rule as stored in a user-defined configuration storage unit 107 and/or based on a selection rule transmitted to the device 100 via a network in which the device 100 is currently operated, wherein such information is stored in an interaction module 106. The device 100 further comprises a network stack 108 adapted to operate the device 100 in one of a plurality of different (types of) networks.

The determining unit 101, which may also be denoted as a network identification module, identifies one or more networks being present in the environment in which the network-compatible device 100 might be interconnected and is ready to be joined by the device 100 as a further network node. The network stack 108 is a software library containing software needed to enter one of a plurality of networks.

When the device 100 has entered or intends to enter a particular network, the determining unit 101 determines and characterizes the current network. Then, the selection unit 102 determines what services are to be initiated and how they are to be configured. According to the described embodiment, this initiation and configuration is performed by

14

applying some heuristic, by referencing some user configuration files stored on the device 100 itself, or by accessing some back-end server containing such information. This information is then used to configure the individual services and the way in which they will be accessible by other devices of the network.

5   For this purpose, the interaction module 106 contains information from some back-end server with configuration and identification information, for example, "my.philips.com".

        The user-defined configuration storage unit 107 contains predetermined configuration information which is input by a user and stored on the device 100. The

10   selection unit 102 selects a mode in accordance with which the services (corresponding to data which are stored in the service storage units 103 to 105) will be provided to other nodes of the network in which the device 100 is interconnected.

        According to the described embodiment, the first service storage unit 103 contains content to be shared by other nodes, for instance, picture data, video data or audio

15   data.

        The second service storage unit 104 provides a web cam function. In other words, the device 100 can be used as a web cam, while pictures locally captured by a camera (not shown) included in the device 100 can be transmitted to a remote node of the network which, for instance, may illustrate the captured pictures on a homepage on the Internet.

20   The third service storage unit 105 may include a security service. According to the security scheme of the device 100, and if the network to be joined by the device 100 is a home network, the selection unit 102 controls the device 100 to provide all services stored in the first to third service storage units 103 to 105 to all other nodes of the home network without any restriction or limitation. If the determining unit 101 detects that the current net is

25   the Internet, it is prevented/prohibited that any of the services, which may be provided by the first to third service storage units 103 to 105, is in fact provided to any of the connected Internet computers.

        The networking capabilities as provided by the content of the network stack 108 include Bluetooth and WiFi.

30   In summary, when the device 100 is switched on in an environment in which it has not been operated before, the determining unit 101 determines a network to be accessed subsequently. Depending on which network shall be joined, the selection unit 102 adjusts a service access scheme, i.e. it formulates a set of rules defining a manner in accordance with

which other nodes of the joined network are allowed to access any of the services as provided by the service units 103 to 105.

A network system 200 in which the network-compatible device 100 is operated will now be described with reference to Fig. 2.

5   In Fig. 2, the network system 200 includes a home network 201 and the Internet 207.

In the home network 201, UPnP devices 100, 204, 205 (namely, the device 100, a UPnP refrigerator 204 and a UPnP personal computer 205) and a UPnP control point device 203 are connected with each other. The UPnP devices 100, 204, 205 are connected to

10   the Internet 207 through a home gateway 206, for instance, to receive various Internet services. The portable device 100 has a camera functionality, i.e. it is adapted to capture pictures of its environment and to store captured pictures according to any standard, for example, as JPEG files.

As can be seen in Fig. 2, the network-compatible device 100 comprises a

15   microprocessor (CPU) 202 for carrying out a method of operating the device 100 within the network system 200.

When the portable device 100 having the camera functionality is switched on in the home network 201, the detection unit 101 detects the presence of the UPnP-based home network 201 which is ready to be joined by the device 100. The service resources (for

20   instance, the camera) included in the device 100 can then be accessed by any of the nodes 203, 204, 205 within the UPnP-based home network 201, in accordance with a mode of such an access defined by the selection unit 102 for the operation of the device 100 within the UPnP-based home network 201.

For instance, the UPnP personal computer 205 may use the camera of the

25   device 100 as a web cam, and can transfer the corresponding pictures via the Internet 207 to other nodes anywhere in the world.

A network system 300 in which the network-compatible device 100 is operated will now be described with reference to Fig. 3.

The network system 300 is a WLAN (wireless local area network) in which a

30   first WLAN computer 301, a second WLAN computer 302 and a third WLAN computer 303 are interconnected.

The device 100, which has previously been operated within the network 200, is disconnected from the network 200, migrated to the network 300 and switched on in the network 300 so as to be connected to the WLAN computers 301 to 303 in a wireless manner.

When the portable device 100 having the camera functionality and, additionally, a media server functionality hosting a specific directory of content is switched on in the WLAN network 300, the detection unit 101 detects the presence of the WLAN network 300 which is ready to be joined by the device 100. The services of the device 100 are configured in accordance with the specific network 300 in which the device 100 is on at that moment. According to the described example, the camera service is not made available for the WLAN computers 301 to 303, but the media server hosting a specific directory of content is made available for the WLAN computers 301 to 303.

It should be noted that use of the verb "comprise" and its conjugations does not exclude the presence of elements or steps other than those stated in the claims, and use of the indefinite article "a" or "an" preceding an element or step does not exclude the presence of a plurality of such elements or steps. Moreover, elements described in association with different embodiments may be combined.

It should also be noted that reference signs in the claims shall not be construed as limiting the scope of the claims.

CLAIMS:

1.   A device (100) capable of being operated within a network (201) and providing services to the network (201), the device (100) comprising:

-          a determining unit (101) adapted to determine the network (201) in which the device (100) is operable;

5   -   a selection unit (102) adapted to select, on the basis of the network (201) determined by the determining unit (101), a mode in accordance with which the device (100) provides at least one service to the network (201) when the device is connected in the network (201) determined by the determining unit (101).

10   2.   The device (100) according to claim 1, further comprising a storage unit (103, 104, 105) adapted to store data in accordance with at least one service which the device (100) is capable of providing to a network (201).

3.   The device (100) according to claim 1, wherein the selection unit (102) is
15   adapted to select a security mode or an access control mode.

4.   The device (100) according to claim 1, wherein the selection unit (102) is adapted to select a mode by including at least one of the group consisting of completely enabling at least one service to at least one node of a network (201), completely disabling at
20   least one service to at least one node of a network (201), and partly enabling/partly disabling at least one service to at least one node of a network (201).

5.   The device (100) according to claim 1, wherein the selection unit (102) is adapted to select a mode based on at least one of the group consisting of a user-defined
25   selection rule, a pre-stored selection rule, and a selection rule transmitted to the device (100) via a network (201) in which the device (100) is currently operated.

6.   The device (100) according to claim 1, further comprising a networking unit (108) adapted to operate the device (100) in a plurality of different types of networks (201).

7.   The device (100) according to claim 6, wherein the networking unit (108) is
adapted to operate the device (100) in at least one of a Bluetooth network and a WiFi
network.

5

8.   The device (100) according to claim 6, wherein the networking unit (108) is
adapted to operate the device (100) to communicate in accordance with a Universal Plug and
Play protocol.

10   9.   The device (100) according to claim 1, wherein the determining unit (101) is
adapted to determine a network (201) based on determining whether at least one reference
network node is present in a network (201).

10.   The device (100) according to claim 1, wherein the determining unit (101) is
15   adapted to determine a network (201) based on at least one of the group of at least one
network access characteristic, at least one network configuration characteristic, and at least
one network service characteristic.

11.   The device (100) according to claim 1, realized as a portable device.

20

12.   The device (100) according to claim 1, realized as a device (100) which is
operable in a network (201) in a wireless manner.

13.   The device (100) according to claim 1, realized as a device (100) providing at
25   least one functionality of the group consisting of audio recording, audio replay, video
recording, video replay, image recording, image replay and telecommunication.

14.   A method of operating a device (100) within a network (201) and providing
services to the network (201), the method comprising the steps of:
30   -   determining the network (201) in which the device (100) is operable;
-          selecting, on the basis of the determined network (201), a mode in accordance
with which the device (100) provides at least one service to the network (201) when being
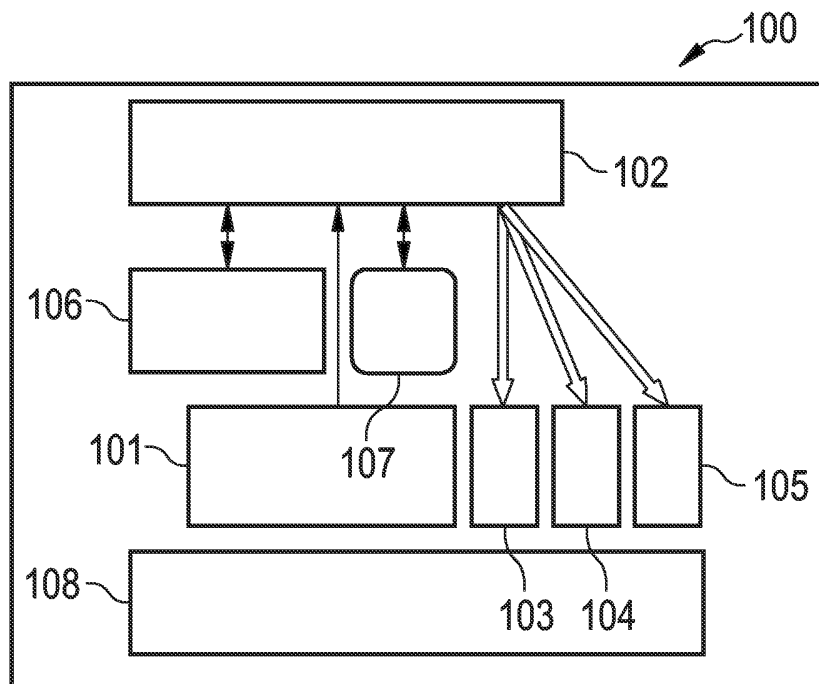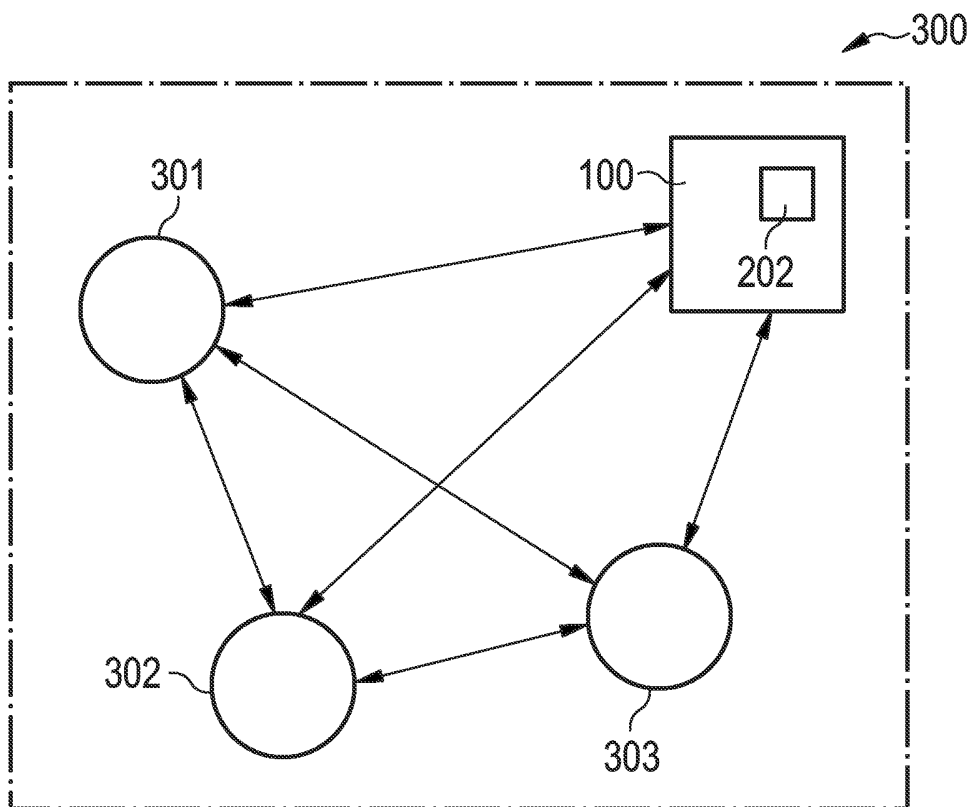connected in the determined network (201).

15.   A program element, which, when being executed by a processor (202), is adapted to carry out a method of operating a device (100) within a network (201) and providing services to the network (201), the method comprising the steps of:

-           determining the network (201) in which the device (100) is operable;

5   -   selecting, on the basis of the determined network (201), a mode in accordance with which the device (100) provides at least one service to the network (201) when being connected in the determined network (201).
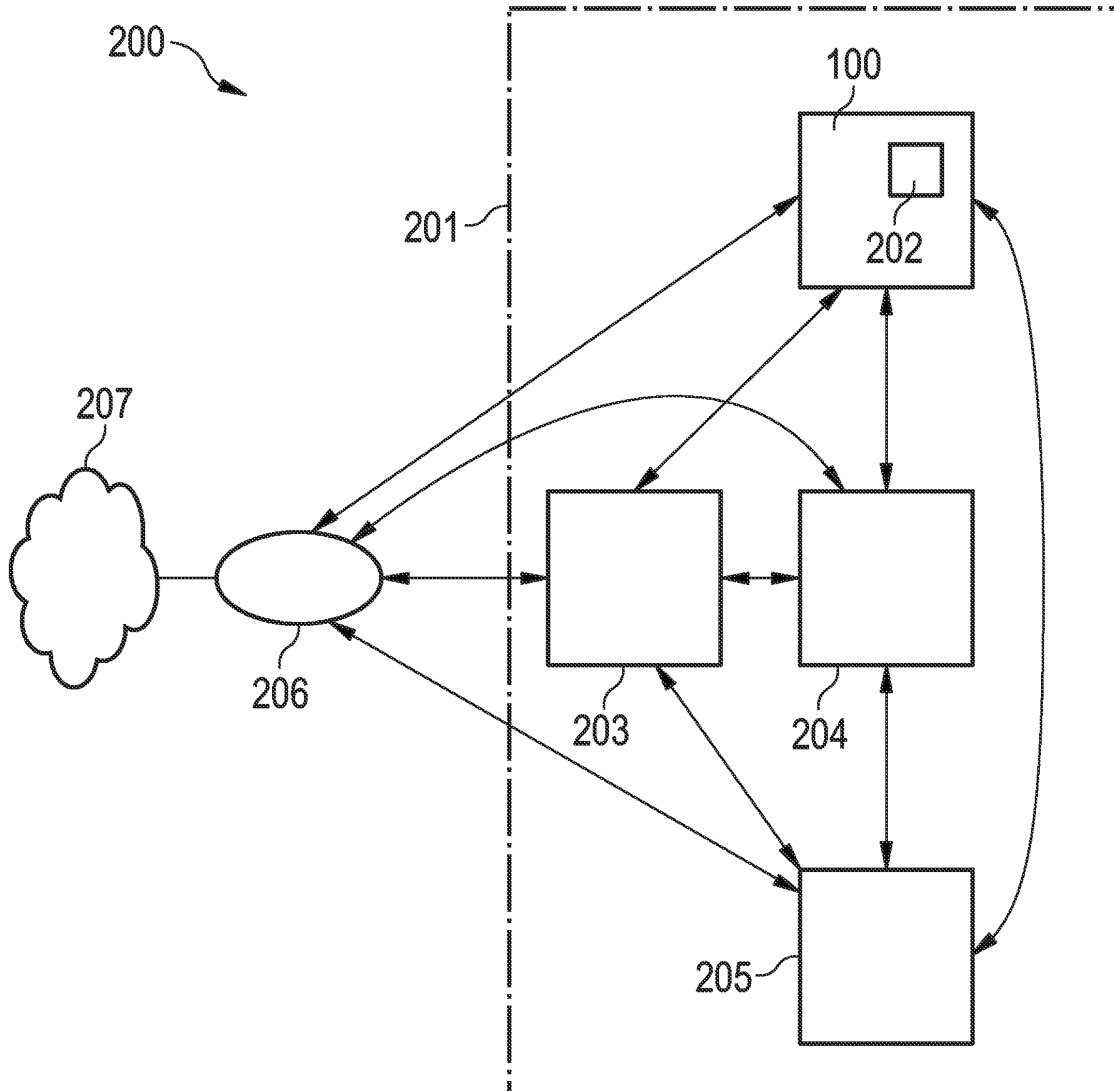

16.   A computer-readable medium, in which a computer program is stored which, when being executed by a processor (202), is adapted to carry out a method of operating a device (100) within a network (201) and providing services to the network (201), the method comprising the steps of:

-           determining the network (201) in which the device (100) is operable;

-           selecting, on the basis of the determined network (201), a mode in accordance with which the device (100) provides at least one service to the network (201) when being connected in the determined network (201).

FIG 1

FIG 2

2/2

FIG 3

INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L12/28   H04Q7/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	MOTTE S: "Avoiding a partially connected home: building further upon the UPnP<TM> framework" CONSUMER ELECTRONICS, 2004 IEEE INTERNATIONAL SYMPOSIUM ON READING, UK SEPT. 1-3, 2004, PISCATAWAY, NJ, USA,IEEE, 1 September 2004 (2004-09-01), pages 545-550, XP010755931 ISBN: 0-7803-8527-6	1-3,6-8, 11-16
A	abstract page 546, left-hand column, line 47 - right-hand column, line 5 page 548, left-hand column, line 41 - right-hand column, line 19	4,5,9,10

-/--

| X | Further documents are listed in the continuation of Box C. | | X | See patent family annex. |

Date of the actual completion of the international search	Date of mailing of the international search report
22 May 2006	30/05/2006

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Ramenzoni, S

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JUN LI ET AL: "Mobile content delivery through heterogeneous access networks" PERSONAL, INDOOR AND MOBILE RADIO COMMUNICATIONS, 2003. PIMRC 2003. 14TH IEEE PROCEEDINGS ON SEPT. 7-10, 2003, PISCATAWAY, NJ, USA,IEEE, vol. 1, 7 September 2003 (2003-09-07), pages 182-186, XP010681581 ISBN: 0-7803-7822-9 abstract page 183, left-hand column, line 51 - right-hand column, line 42 page 186, right-hand column, line 25 - line 34	1,6,7, 11-16
X	US 2004/235463 A1 (PATEL ASHISH RAOJIBHAI) 25 November 2004 (2004-11-25) paragraphs [0004], [0007], [0017]	1,2,5-16
X	EP 0 865 188 A (NOKIA CORPORATION) 16 September 1998 (1998-09-16) abstract page 2, line 27 - line 54 page 5, line 19 - line 29	1,6, 11-16
P,X	EP 1 505 811 A (NEC CORPORATION) 9 February 2005 (2005-02-09) abstract paragraphs [0002] - [0038]	1,2,4,6, 7,10-16
A	HANNIKAINEN M ET AL: "Trends in personal wireless data communications" COMPUTER COMMUNICATIONS, ELSEVIER SCIENCE PUBLISHERS BV, AMSTERDAM, NL, vol. 25, no. 1, 1 January 2002 (2002-01-01), pages 84-99, XP004321158 ISSN: 0140-3664 paragraphs 2.3.3 and 3	1-16

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 2004235463	A1	25-11-2004	EP	1625764 A2	15-02-2006
			WO	2004105415 A2	02-12-2004
EP 0865188	A	16-09-1998	GB	2323245 A	16-09-1998
			US	2002107009 A1	08-08-2002
EP 1505811	A	09-02-2005	CN	1581880 A	16-02-2005
			JP	2005057525 A	03-03-2005
			US	2005032502 A1	10-02-2005