Network Composition using Existing and New Technologies

Cornelia Kappler, Nadeem Akhtar, Rui Campos and Petteri Pöyhönen

Abstract — **4G networks will demand the seamless integration of technology into the user environment. Such networks are envisioned to be an evolution and convergence of mobile communication systems and IP technology, requiring the support for heterogeneity in network access, communication services, and user devices. The Ambient Networks Project aims to solve these heterogeneous networking problems with a uniform process, Network Composition, in a plug&play way. In this paper we consider Network Composition by using two example scenarios to analyze the gaps in today's technology, and highlight the advantages of the Composition process.**

***Index Terms*— Access Networks, Ambient Networks, Internetworking, Network Composition, Personal Area Networks**

I. Introduction

A salient feature of 4G networks will be convenient support for flexible networking. For example, users can easily network their devices to form a Personal Area Network (PAN); PANs of several users may automatically confederate to share the Internet access that one of them can provide; a Café owner may simply attach its WLAN hot spot to the cellular network of a commercial operator; travelers on a train may attach to the train network accessing local servers on the train and the Internet, etc.

In the context of the Ambient Networks Project [1,2], we aim to solve these heterogeneous networking scenarios in a unified framework. We call such networking of networks *Composition*. The heterogeneity arising from the different technologies is embraced such that the composition process appears homogeneous to the users. The vision is to allow composition of networks on-the-fly, transparently and in a plug&play manner, without the need for pre-configuration or offline negotiation.

The examples above illustrate that end users are increasingly not just owners of a terminal or PC, but own and manage a network of devices in their homes, offices, and around their body. Consequently, according to Ambient Networks ideas, users are treated as operators of low-complexity networks. Particularly, we do not differentiate devices and networks. Rather, we regard every device as a network, and the network is the primitive building block of our architecture, allowing all types of networks to be composed into larger networks.

While a lot of effort needs to go into the development of the theoretical concepts, it is also important to verify the composition ideas by real-life examples. In this paper we illustrate composition scenarios in terms of today's technologies. Particularly, we show to what extent composition is already possible today, and where new technology is necessary or will give advantages when the Ambient Networks concepts are fully implemented.

The remainder of this paper is organized as follows: In Sec. II, we describe the Ambient Networks ideas and composition in more detail. In Sections III and IV, two example scenarios are detailed, namely the configuration of a PAN and the extension of an operator's access network. In Sec. V we describe both scenarios as being particular instances of network composition. Finally, in Sec. VI, we summarize our findings and highlight the advantages gained by the composition concept.

II. The Ambient Network Concepts

Composition achieves dynamic automated interworking of networks on the *control plane,* in addition to the data plane cooperation possible today. Data-plane co-operation provides basic addressing and routing services, control plane internetworking encompasses additional capabilities including mobility management, security and QoS control. It generalizes and streamlines many existing basic concepts like attaching a node to a network, mobility of nodes and networks (viewed as changing the composition structure) as well as typical inter-operator network agreements. A detailed description can be found in [3].

Networks capable of composition are called *Ambient Networks* (ANs). An AN requires therefore an identity, a

Manuscript received February 6th, 2005 This document is a byproduct of the Ambient Networks Project, partially funded by the European Commission under its Sixth Framework Programme. It is provided "as is" and without any express or implied warranties, including, without limitation, the implied warranties of fitness for a particular purpose. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the Ambient Networks Project or the European Commission.

Cornelia Kappler, is with Siemens Communications, Berlin, Germany. Tel.: ++49-30-386 32894 (e-mail: cornelia.kappler@siemens.com).

Nadeem Akthar is with the University of Surrey, UK (email: N.Akhtar@surrey.ac.uk).

Rui Campos is with INESC Porto, Portugal (email: rcampos@inescporto.pt)

Petteri Pöyhönen is with Nokia Research, Helsinki, Finland (e-mail: petteri.poyhonen@nokia.com).

common control space known as the Ambient Control Space (ACS), and support for a specific control interface, the *Ambient Network Interface* (ANI). The ACS is an abstraction that consists of all the control plane functions of ANs. At an abstract level, the ACS has a modular structure, with independent - yet interworking - *Functional Areas* (FAs) for each control plane function. Thus there is a QoS Functional Area which contains multiple control functions, e.g. resource configuration, admission control etc.. Beyond this, there are few prescriptions as to how the ACS is realized, e.g. what functionality it actually supports, and how it is implemented. Likewise, the ANI may be distributed over multiple physical network nodes, or it may be implemented by a single physical node.

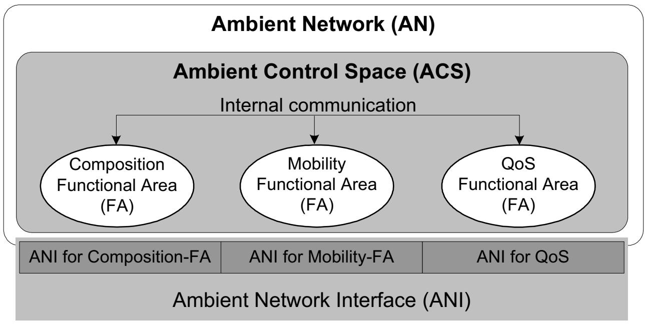
Ambient Network (AN)
Ambient Control Space (ACS)
Internal communication
Composition Functional Area (FA)
Mobility Functional Area (FA)
QoS Functional Area (FA)
ANI for Composition-FA
ANI for Mobility-FA
ANI for QoS
Ambient Network Interface (ANI)

Fig. 1: The modular structure of the Ambient Control Space and the ANI

When ANs compose, they communicate across the ANI to negotiate a Composition Agreement and create a composed AN. This process is orchestrated by the Composition FA. Composing ANs agree on joint control of all or a subset of their individual resources and on all policies that they are going to follow in order to coordinate their control planes. A composed AN consists of all logical and physical resources that each constituent AN contributes. It has its own ACS controlling all its resources and communicating directly to the outside with its own identifier and via its own ANI. The ANI of a composed AN does not reveal its internal structure. This means composition is a recursive process that is always the same. It does not matter whether the composing ANs are themselves already the result of a composition. The ACS and the composition process are illustrated in Figs. 1 and 2.

An important feature of ANs is that they can be single nodes. Treating nodes as networks allows unification of the composition concept. However, it implies that support of ANI and composition must scale from small sensor nodes to large networks by constructing ANI and the composition procedure in a modular, extensible fashion.

The Generic Ambient Network Signaling (GANS) is the open base set of protocols enabling transport of signaling messages between FAs via the ANI. It is important to emphasize that GANS does not replace standard or de-facto standard protocols, which are used for instance to exchange routing information or for mobility support. GANS is used to exchange information currently not sufficiently covered by generally accepted protocols – e.g. Service Level Specification (SLS) negotiation between QoS FAs.

Composition proceeds according to well-defined rules and steps, which schematically look as follows. After discovering one another, ANs decide, possibly policy driven, under what conditions composition is desirable. Then follows an authentication and authorization phase. Subsequently, the ANs negotiate the composition agreement. They agree on joint resources, e.g. on a dynamic SLS for QoS, and on how mobility and other functionalities are handled. The new composed AN is then created by selecting an ID, creating the common ACS, and enabling the common ANI.

III. 1ST Scenario: Configuration of a PAN

We now present the first example scenario, configuration of a PAN. It should be emphasized that there are several technical solutions to both scenarios presented in this paper, and for each scenario we describe only one of them. Furthermore, many technical details need to be considered when setting up such systems. In this paper, we only highlight some of them.

A. Scenario Description

John is on his way home carrying his Personal Digital Assistant (PDA) and a mobile phone. He decides to switch on his PDA and use it to access the Internet. While the PDA only has a Bluetooth interface and hence cannot provide Internet access, the mobile phone has interfaces for Bluetooth and UMTS (Universal Mobile Telecommunications System). When John launches the browser on the PDA, the PDA automatically discovers that the mobile phone provides Internet access and composes with it to create a PAN. Now the PDA can access the Internet via the mobile phone's UMTS interface, as illustrated in Fig. 3. When John arrives at home he powers up his laptop. The laptop has Internet connectivity over ADSL (Asymmetric Digital Subscriber Line) provided by a local Internet Service Provider. Additionally it has a Bluetooth interface activated. John's PAN discovers automatically the laptop using the Bluetooth network. The laptop joins the PAN and the ongoing session on the PDA is routed via the cheaper and faster ADSL access, see Fig. 3.

This scenario is realized by a mixture of old and new technology. When the browser is launched on the PDA, PDA-internal logic must exist that examines the routing table and finds Internet connectivity does not exist. Therefore over the BlueTooth interface the PDA attempts to discover an Ambient Network offering Internet connectivity. Once the mobile

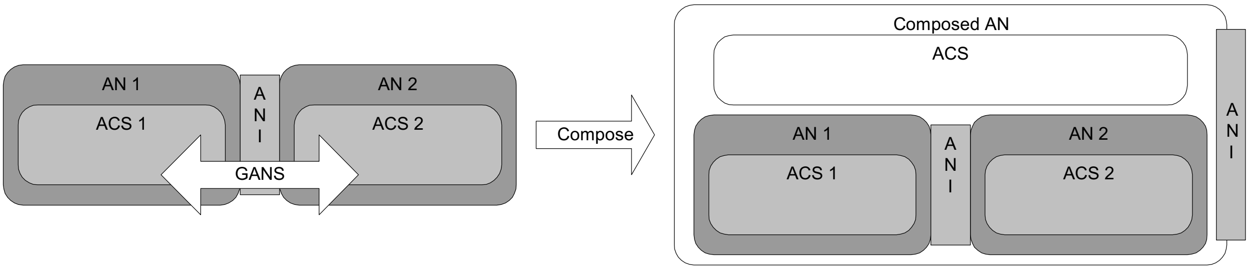

Fig. 2 The formation of a new ACS upon composition.

phone is found, the devices mutually authenticate, realize they know each other and even have a preconfigured Composition Agreement stating that the PDA may use the UMTS Internet access of the mobile phone. They compose over the Bluetooth interface, using the Bluetooth PAN Profile that emulates an Ethernet link over Bluetooth and enables IP-based networking between Bluetooth devices.

Now addressing and routing needs to be configured. For this scenario we assume John has a fixed home IPv6 prefix from his home network, and mobility of the PAN is supported in accordance with the NEMO solution [8]. In this case, the mobile phone acts a Mobile Router, masking the mobility to the PDA and ensuring reachability from the outside. Reachability could also be achieved with SIP and IMS [15]. However, since the IMS is currently only accessible from a UMTS network, we adopted the MIPv6/NEMO approach to support alternative access methods like ADSL. The mobile phone advertises its home IPv6 prefix to the PAN by using a Router Advertisement (RA) message of the Neighbour Discovery (ND) protocol [6]. The BlueTooth interfaces of both phone and PDA auto-configure their IPv6 addresses [5]. The mobile phone now receives a temporary IPv6 prefix from the UMTS network. Based on the temporary prefix it autoconfigures an IPv6 address for its UMTS interface and updates it as Care-of-address (CoA) in its home agent [8]. Now, any traffic addressed to the home IPv6 prefix is tunneled to the PAN from John's home network.

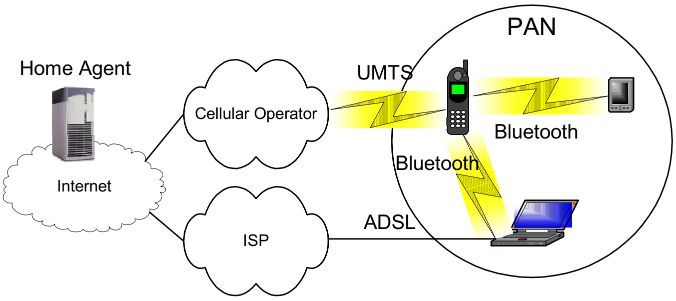

Fig. 3. Configuration of a PAN

A DNS service is made available by the cellular operator. The mobile phone provides a Stateless Dynamic Host Configuration Protocol Service [7] to the PAN to distribute DNS server address(es). This service does not require the maintenance of any dynamic state in the mobile phone. Alternative methods to configure DNS server address(es) are defined in [12]. Finally, routing tables are configured in the mobile phone and Internet access is available.

When John powers up his laptop, the laptop advertises availability of ADSL on its Bluetooth interface on a regular basis. Upon receiving such an advertisement, the PAN decides, based on policy, to use ADSL rather than UMTS for Internet access. Using the same procedure as before, the laptop and PAN compose. The IP addresses of the devices that already are in the PAN remain unchanged. The current state and configuration information of Mobile Router functionality is transferred to the laptop that updates its current global IPv6 address as new CoA to John's Home Agent. The user's ongoing session is now using the laptop's ADSL access instead of mobile phone's UMTS access.

B. *Enhancement of current technology*

While a lot of building blocks exist to realize this scenario today, a number of additional features are necessary. As a first step, all devices must be capable of screening their environment for devices that offer Internet access and mobile router functionality. Vice versa, these devices must advertise their capability. Furthermore, the mobile phone first acts as a mobile router, and the mobile router functionality is later transferred to the laptop. Additionally, the mobile phone automatically starts up the stateless DHCPv6 service to enable a synchronization of different configuration frameworks (UMTS and PAN). Whenever UMTS provides new or updated configuration parameters (e.g. DNS server addresses) they are automatically injected to the local DHCPv6 service to be distributed for the use of the PAN.

Related, however simpler features, are offered by UPnP (Universal Plug and Play) [16]. It supports autoconfigured networking of devices in protected environments, and both discovery and advertisement of the services these devices can offer (e.g., a printing service). Furthermore, the UPnP architecture allows an event-based invocation of these services by other devices in the network. Services are typically application-layer bound to a single device. However, in the example presented here, invocation of the "Internet connectivity" service on the PAN triggers services also on other layers (e.g., a mobile router service and a stateless DHCPv6 service on the network layer), on several devices (mobile phone and laptop), and the service trigger may provoke actions also in the future (e.g., service is transferred to another device as John powers up the laptop).

IV. 2ND Scenario: Extension of an Access Network

A. *Scenario Description*

Another example scenario is a café that wants to offer Internet access to its customers. The café sets up a WLAN network that lets customers access its network. Furthermore, the café has established an agreement with a network operator and is connected to the public network via one or more

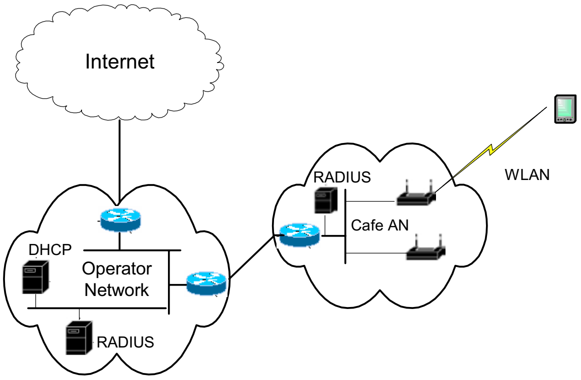

Fig. 4. Extension of an operator's access network

backhaul links. The café hence extends access to the public network to its customers, as illustrated in Fig. 4.

We discuss two possible models for providing access to the customer. In the first case (1) the café sells a pre-paid card, and customers directly log in to the public operator. Online-charging is performed by the operator. This approach roughly corresponds to one of the 3GPP proposals for 3G-WLAN interworking [9], where the WLAN is integrated as another Radio Access Network. The agreement between the café AN and the public operator might allow for hiding the identity of the café AN and the café users hence only sees the identity of the public network. The second case (2) is where the customer logs in to the café network and is charged by the café itself. Café and operator have an agreement that all café customers may access the operators network. This agreement may also guarantee a certain QoS to the Café customers.

The WLAN network of the café consists of a set of access points that form an Extended Service Set (ESS) and have the same Service Set ID (SSID). The access points are controlled by an access router (AR) that is connected to the operator's network. This configuration falls in the category of Centralized WLAN Architecture, following the classification proposed by the IETF CAPWAP Working Group [10]. In the following, we describe the sequence of steps that takes place when a customer wants to get access to the public network.

1) Customers log-in directly to operator network

In this case, the operator is responsible for allocating IP addresses, for authentication and authorization of clients, as well as for accounting and billing. Thus, the operator maintains a DHCP server [14] and a RADIUS (Remote Authentication Dial In User Service) server [15]. The access points of the café network are already registered with the RADIUS server. Furthermore, a set of identities and passwords are reserved for the prepaid cards with the RADIUS server. When a customer wants to access the Internet in the café, the following steps take place:

- The customer is sold a prepaid card with a temporary identity and password by the café.
- The customer accesses the WLAN using normal procedures, i.e. the wireless client attempts to detect an Access Point (AP) by listening to the beacons being transmitted by the access points. After an access point is found, an association is established between the wireless client and the AP
- The client enters the password on a login page. This information is received by the AP who sends it to the RADIUS server. The authentication procedure takes place according to the IEEE802.1x protocol.
- The wireless client sends a DHCP request, and the DHCP server of the operator replies with a globally routable IP address assigned to the client.
- The customer negotiates QoS guarantees for the wireline links to the Internet and resources are reserved corresponding to the QoS guarantees agreed upon. The café network itself has agreed upon certain QoS guarantees with the network operator beforehand.
- The customer can now access services and applications across the Internet with the accounting information collected by the RADIUS server.

2) Customers log-in to café network

In this case, customers log on to the café network first and are then allowed to access the public network. Furthermore, billing and charging is taken care of by the café network, which is also responsible for allocating IP addresses and for authentication and authorization of clients. The café's access points are registered with the operators' network such that any traffic originating from them is accepted. The café network has a DHCP server as well as (access to) a RADIUS server. Accessing the network proceeds along similarly as described before except that the café now sells temporary IDs together with a password, and customer is served by RADIUS and DHCP servers local to the café network. In addition to online-charging, in this case off-line charging, i.e. paying after service usage, is feasible.

B. Enhancement of current technology

While the operation of the café's access network can be realized with current technology, the initial configuration must be performed manually. It is not possible to install a dynamic, automatic agreement between café's owner and the operator, detailing who is responsible for allocating addresses, authentication, accounting etc. This obviously is expensive and, furthermore, restricts the flexibility of the set-up. Likewise, the QoS reservation between café and operator is hard to adapt. As we will see in the next section, when the association between café network and operator network is regarded as a composition, the entire process can become automatic and dynamic, and moreover similarly in structure to the creation of the PAN described above.

V. Scenarios in Terms of Composition

Now we show how both scenarios just introduced can be described as compositions. For Scenario I we now look at how the composition between mobile phone (AN A) and PDA (AN B) is created. For Scenario II we look at the composition between the operator network (AN A) and the café WLAN network (AN B) with delegation of control to the operator network (case 1). Composition means the devices / networks in question are networked automatically.

In both scenarios, we assume the Ambient Networks composing are able to mutually authenticate and authorize. In a first step, a discovery phase is triggered by AN B, (upon activation of the browser or upon physically connecting to the Internet access providing network) The ANs, and specifically their Connectivity Functional Areas send solicitation messages, advertising their AN identity and the services they are searching for, namely Internet Access (or Internet access plus delegation of control functionality for the second scenario). The Connectivity FA at the receiving AN A (mobile phone or. operator) receives the solicitation and replies and with a message advertising its own identity and the services offered. AN B decides to attempt composition. Subsequently, the Connectivity FAs of AN A and AN B negotiate connectivity parameters for further communication. AN A and AN B mutually authenticate. Now, AN B offers a Composition Agreement to AN A. It is expected that these agreements are "off-the-shelf", i.e. pre-installed in the case of the PAN, and corresponding to a subscription package selected by the café prior to this procedure.

The Composition Agreement may include (for example) the IDs of the composing ANs, the ID of the composed AN (which may be the ID of one of the composing ANs), services included (e.g. Internet Access, DHCP-based IP address allocation), identifier and location of control functions (e.g. DNS server, mobile router etc.), and a QoS Service Level Specification. The Composition Agreement is modular, with separate sections for each Functional Area. Upon reception, each FA inspects its section of the Composition Agreement, e.g. the QoS FA inspects the Service Level Specification and possibly negotiates changes with the corresponding FA in the other AN. Unless suitable protocols exist, this negotiation is performed using the GANS protocol across the ANI. Depending on a specific FA implementation; centralized vs. distributed, an FA is either directly negotiating with its peer FA in another AN or alternatively the Composition FA may negotiate on its behalf. Subsequently, the consistency of the Composition Agreement is checked, e.g. to make sure the QoS FA did not agree on more bandwidth than made available by the Connectivity FA.

Finally, the Composition Agreement is realized, by e.g. assigning IP addresses, configuring routing tables, configuring DHCP servers etc.

VI. Conclusion

Network composition is a new concept for dynamic and instantaneous interworking of networks on the control plane. In this paper we aimed at giving a practical illustration of network composition. We depicted two distinct scenarios in terms of today's technologies and highlighted were technology needs to be augmented to allow plug&play internetworking of networks. Then, we showed how both scenarios, while very different at first sight, can be described as particular instances of the same concept, network composition.

We argue that network composition gives a more coherent and simplified framework for future control architectures:

- With composition, control functions can be explicitly assigned and distributed. Control functions, their state and configuration information can be re-located transparently.
- Internetworking of mobile networks needs a much larger variety of control plane interworking options than possible with static network agreements and fixed protocol solutions.
- Dynamic internetworking is simplified if the procedure is independent of the nature of the entities involved. It shouldn't matter whether a single device, a PAN or the mobile network of a train (itself containing terminals and PANs) are attached to an access network: An Ambient Network can be a single node, a network, or a network of networks. Composition always proceeds according to the same procedure.
- The configuration of control-plane interaction becomes a self-configuring process, because it is very complex and yet needs to be realized on-the-fly. Composition is thus almost transparent to the user, and human interaction in network management and configuration tasks is minimized.

Ongoing and future work on network composition includes both practical work such as demonstrators (some to be shown at the IST Summit) and design work, particularly on the GANS protocol.

Acknowledgment

The authors would like to thank the colleagues from the Ambient Networks Project. This paper is founded on joint work in the project. Fruitful discussions with Frank-Uwe Andersen and Louise Burness are gratefully acknowledged.

References

[1] N. Niebert, A. Schieder, H. Abramowicz, G. Malmgren, J. Sachs, U. Horn, Ch. Prehofer and H. Karl, *Ambient Networks: An Architecture for Communication Networks beyond 3G*, IEEE Wireless Communications, April 2004.

[2] www.ambient-networks.org

[3] C. Kappler, P. Mendes, P. Pöyhönen, C. Prehofer, D. Zhou, *A Framework for self-organized Network Composition*, Proc. 1st IFIP TC6 WG6.6 International Workshop on Autonomic Communication (WAC 2004), Springer LLNC Series, Berlin, Okt. 2004.

[4] Christos Politis, Toshikane Oda, Sudhir Dixit, Andreas Schieder, Hong-Yon Lach, Michael I. Smirnov, Sami Uskela, and Rahim Tafazolli, *Cooperative Networks for the Future Wireless World*, IEEE Communications Magazine, vol. 42, pp. 70-79.

[5] S. Thomson, T. Narten, *IPv6 Stateless Address Autoconfiguration,* RFC2462, December 1998.

[6] T. Narten, E. Nordmark, W. Simpson, *Neighbor Discovery for IP Version 6 (IPv6)*, RFC2461, December 1998.

[7] R. Droms, *Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6*, RFC3736, April 2004.

[8] Vijay Devarapalli, Ryuji Wakikawa, Alexandru Petrescu, and Pascal Thubert, *Network Mobility (NEMO) Basic Support Protocol*, draft-ietf-nemo-basic-support-03, work in progress (expired Internet-Draft), June 2004.

[9] 3GPP TR 22.934, *Feasibility study on 3GPP system to Wireless Local Area Network (WLAN) interworking (Release 6)*, v 6.2.0, September 2003.

[10] L. Yang, P. Zarfos, E. Sadot, *Architecture Taxonomy for Control and Provisioning of Wireless Access Points (CAPWAP)*, draft-ietf-capwap-arch-06 (work in progress), November 2004.

[11] Tony Jeffree, et. al, *IEEE Std 802.1X-2001 IEEE standard for local and metropolitan area networks - Port-based network access control*, IEEE, 2001.

[12] J. Jeong, Ed., *IPv6 Host Configuration of DNS Server Information Approaches*, Internet-Draft, September 2004.

[13] R. Droms, *Dynamic Host Configuration Protocol*. RFC2131, March 1997.

[14] C. Rigney, S. Willens, A. Rubens, W. Simpson, *Remote Authentication Dial In User Service (RADIUS)*, RFC2865, June 2000.

[15] 3GPP TS 23.228,, IP Multimedia Subsystem (IMS)" v6.8.0, Jan. 2005.

[16] UPnP Forum, "UPnP Device Architecture V1.0", June 2000, available from www.upnp.org.