Home Networking with Universal Plug and Play

Brent A. Miller, IBM Corporation
Toby Nixon, Microsoft Corporation
Charlie Tai, Intel Corporation
Mark D. Wood, Eastman Kodak Company

ABSTRACT

In this article we present an overview of the Universal Plug and Play (UPnP™) technology and the UPnP Forum, the multicompany organization that develops parts of the architecture. A technical description of the technology is presented, followed by three illustrative usage cases where it could be applied in home networking environments. Finally, the authors describe the benefits UPnP technology can provide in home networking and briefly discuss potential future work in this area.

INTRODUCTION

All sorts of devices — PCs, mobile phones, cameras, handheld computers, and so on — are increasingly connecting to networks, and they are using a multitude of connectivity methods to do so. This trend increases the need for self-configuring networks that allow devices to easily and automatically join and leave networks, and learn about other connected devices. Home networks, automotive networks, and similar environments demand new technologies that can automate device and service discovery and control, obviating the need to administer these networks.

The Universal Plug and Play (UPnP) architecture enables pervasive peer-to-peer network connectivity of PCs of all form factors, intelligent appliances, and wireless devices. It is a distributed, open networking architecture that leverages TCP/IP and Web technologies to enable seamless proximity networking in addition to control and data transfer among networked devices in the home, office, and everywhere in between. Figure 1 depicts an example UPnP networking topology, illustrating multiple device types and multiple connectivity methods.

What is *universal* about the UPnP architecture?

- It uses common protocols rather than vendor-specific device drivers.
- It is independent of the underlying physical media and transports.
- UPnP devices can be implemented using any programming language, and on any operating system.
- The UPnP architecture leverages HTTP and other Internet technologies such as XML and SOAP.
- UPnP technology enables vendor control over device user interface and interaction via a browser.
- It also enables conventional application programmatic control.
- Vendors agree on UPnP control protocols on a per-device-class basis.
- Vendors can unilaterally extend the basic control protocols as needed.

UPnP architecture supports zero-configuration networking and automatic discovery of devices. Network infrastructure such as DHCP and DNS servers are optional; they may be used if available on the network but are not required. Furthermore, a device can leave a network smoothly and automatically without unwanted state information remaining behind. The UPnP architecture learns from the Internet's success and heavily leverages its components, including IP, TCP, UDP, HTTP, SOAP, and XML.

THE UPNP FORUM

Universal Plug and Play is not only a technology, it is also a cross-industry initiative. The *UPnP Forum* is the embodiment of that initiative, and its primary mission is to develop *device control protocols* (DCPs) that describe standard methods for device interaction. For more information about the UPnP Forum, see [1].

Formed in 1999, the Forum now has more than 350 member companies from many industries, including consumer electronics, home automation and security, computers and peripherals, networking, appliances, semiconductors, and others.[1] General membership requires completion of a membership agreement[2] but is free of charge. Forum members receive a license to the intellectual property necessary to implement the UPnP specifications and may participate in the development of those specifications.

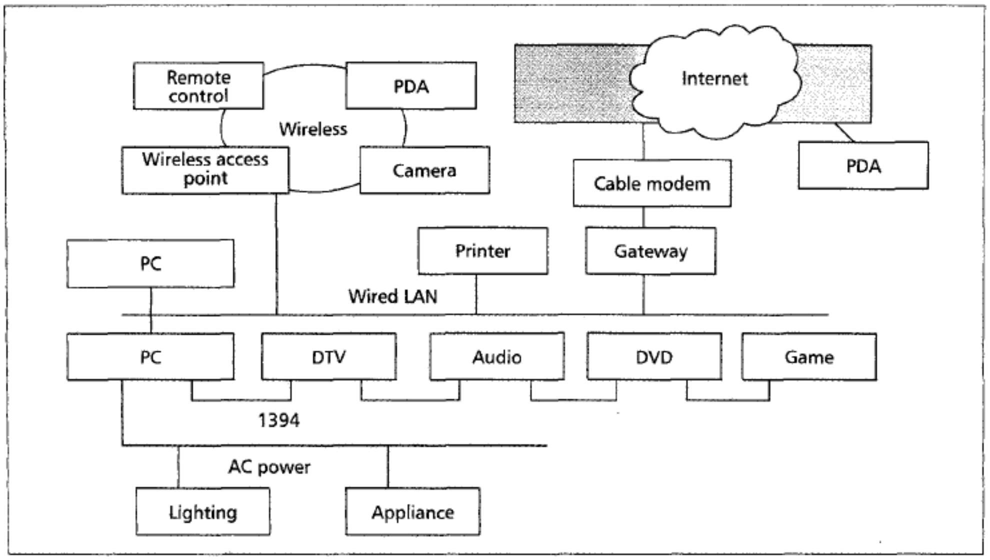
Working committees produce the DCPs. In 2001, working committees were developing DCPs for audio-visual devices, home automation

UPnP is a trademark of the UPnP Implementers Corporation.

[1] *A complete current membership list is available at http://www.upnp.org/forum/members.htm*

[2] *See http://www.upnp.org/membership.htm for UPnP Forum membership information.*

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.



■ **Figure 1.** *An example UPnP topology.*

and security equipment, appliances, printers, cameras and other imaging devices, and Internet gateways. The steering committee governs the overall business of the Forum, establishing working committees, ratifying DCPs, and guiding the Forum in general. Steering committee members are elected by the Forum's members.[3]

For UPnP v. 1, the Forum has completed or will complete dozens of DCPs for various classes of UPnP devices. As DCPs are ratified, they are published on the Forum's Web site at http://www.upnp.org.

Technical Description

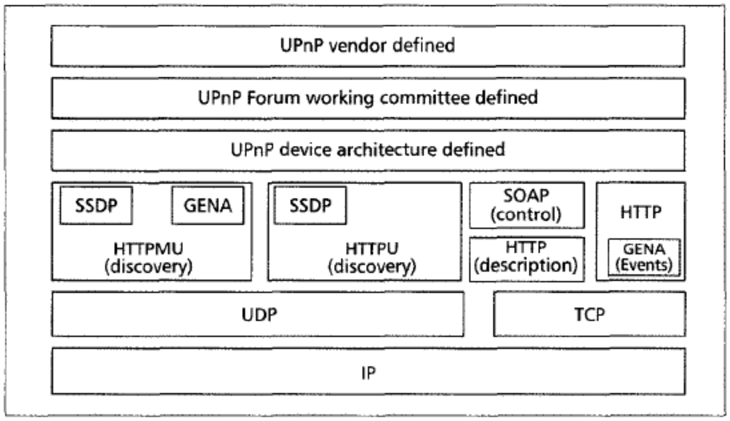
Overview

The UPnP Device Architecture [2] defines the protocols for communication between UPnP *control points* and *devices*. These protocols are illustrated in Fig. 2, taken from [3], and described further in following sections. The architecture specifies six phases of interaction:

- *Addressing*, by which devices obtain an IP address
- *Discovery*, by which control points become aware of the existence of devices
- *Description*, by which control points learn details about devices and their services
- *Control*, in which control points invoke service actions
- *Eventing*, by which devices notify control points of changes in state
- *Presentation*, by which devices can present Web pages to control points allowing for status and control interactions

Addressing

Every UPnP device incorporates a Dynamic Host Configuration Protocol [4] client and searches for a DHCP server when initially connected to the network. A device first requests an IP address via DHCP. If a response is received before a prescribed timeout, the device uses the dynamically assigned address.



■ **Figure 2.** *The UPnP protocol stack.*

If no DHCP server responds, the device uses automatic IP addressing [5]. It randomly chooses an address in the 169.254/16 range, and tests it using an Address Resolution Protocol [6] probe to determine if it is already in use. If so, another address is chosen and tested until an unused address is found. It then periodically checks for the existence of a DHCP server; if a server responds, the device uses the assigned address, and stops using the address selected by Auto-IP after a period of parallel use to complete interactions in progress.

In addition to numeric IP addresses, names can be used to access devices if they are identified in a Domain Name Service (DNS) server [7, 8]. Device names could be registered manually, dynamically according to [9], or by the DHCP server.

Discovery

Devices advertise their services to control points on the network using the UPnP discovery protocol, which is based on the Simple Service Discovery Protocol [10]. Control points also may use SSDP to search for devices of interest on the

[3] *The Steering Committee consists of up to 20 member companies. A complete list of current Steering Committee members can be found at http://www.upnp.org/forum/memberstatements.htm*

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

Formed in 1999, the Forum now has more than 350 member companies from many industries, including consumer electronics, home automation and security, computers and peripherals, networking, appliances, semiconductors, and others.

network. The fundamental exchange in both cases is a discovery message containing a few specific attributes of the device or one of its services: its type, a unique identifier, and a pointer to more detailed information.

Devices multicast, using a well-known address and port, several NOTIFY messages advertising the availability of embedded devices and services [11]. Control points monitor this standard multicast address for notifications that new capabilities are available.

Advertisement messages indicate the lifetime of the advertisement. If a device remains available, it retransmits its advertisements well before the lifetime expiration. If a device or service becomes unavailable and an orderly shutdown is possible, previous advertisements are cancelled by sending cancellation messages; otherwise, advertisements eventually expire on their own. The lifetime for advertisements is selected to balance the need to minimize network traffic with the desire to maximize the currency of device status.

Control points may search for devices or services of interest by multicasting an SSDP M-SEARCH message. Responses from devices contain information essentially identical to advertisement messages, but responses to search requests are unicast directly to the requesting control point.

The time to live (TTL) field in the IP header of multicast discovery messages is set to a small value to reduce propagation of UPnP messages beyond the boundaries of the local network, hence limiting the scope of advertisement.

DESCRIPTION

After a control point has discovered a device, it uses a URL contained in the discovery message to request a UPnP description from the device. The description includes a *device description* and one or more *service descriptions*.

The device description includes vendor-specific information such as the model name and number, serial number, and manufacturer name. For each service included in the device, the device description lists the service type, name, and URLs for the service description, control, and eventing. A device description may include descriptions of embedded devices and a URL to access a presentation page.

A service description includes a list of actions the service responds to, arguments for each action, and a list of state variables. The variables model the state of the service at runtime and are described in terms of their data type, range, and event characteristics.

UPnP descriptions use XML syntax and are based on a standard UPnP *device template* or *service template* [12]. Device and service templates are produced by the UPnP Forum and derived from the UPnP *template language*. The template language itself is written in XML syntax and is derived from an XML schema language [13]. Because the template language, templates, and descriptions are all machine-readable, automated tools can be used to ensure that the latter two have all required elements, are correctly nested, and have values of the correct data types.

UPnP vendors can differentiate their devices by extending services, embedding other devices, and including additional UPnP services, actions, or state. When a control point retrieves a device's description, these added features are exposed to the control point for control and eventing.

Retrieving a UPnP device description is simple: the control point issues a GET request on the URL in the discovery message, and the device returns the device description in the body of an HTTP response [14]. Retrieving a UPnP service description is a similar process that uses a URL within the device description.

CONTROL

Having obtained knowledge of a device and its services, a control point can ask those services to invoke actions. Invoking actions is a form of remote procedure call; a control point sends the action to the device's service, and when the action has completed (or failed), the service returns any results or errors.

Actions are invoked by sending a message to the control URL for the service. Control messages are expressed in XML using the Simple Object Access Protocol [15] and sent via HTTP requests; results and errors are received via HTTP responses. The effects of the action, if any, are modeled by changes in the variables that describe the runtime state of the service and may be reflected in event messages.

EVENTING

A UPnP service description includes a list of actions to which the service responds and a list of variables that model the state of the service at runtime. The service publishes updates, in the form of event messages, when these variables change and a control point may subscribe to receive this information.

To subscribe to event notification, a control point sends a subscription message to the subscription URL specified in the device description and provides a delivery URL to which event notifications should be sent. The subscription message is a request to receive all event messages; no mechanism is provided to subscribe to a subset of evented state variables. All subscribed control points receive all event messages regardless of why the state variable changed.

If the subscription is accepted, the device responds with a unique identifier for the subscription and the duration of the subscription. The device then sends an initial event message to the control point that includes the names and current values for all evented variables.

When an evented state variable changes, the service notifies subscribed control points by sending event messages. These messages are GENA NOTIFY messages, sent using HTTP, that contain within their body an XML structure that specifies the names of one or more state variables and the new values of those variables. Event messages are sent as soon as possible after the state changes so that control points receive accurate and timely information about the service, allowing them to display a responsive user interface. Control points acknowledge receipt of event messages by responding with an HTTP OK message. Event notifications contain sequence numbers to allow detection of lost or out-of-order messages.

Some state variable values might change too rapidly for eventing to be useful. Event notifica-

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

tions for such state variables may be filtered; devices send notifications only when the degree of change exceeds a limit or a specified amount of time has elapsed since the last notification. The parameters for these filters are specified in the service description.

To keep a subscription active, the control point sends a message to renew the subscription before it expires. The renewal message is sent to the same URL as the subscription message, and specifies the subscription identifier received when the subscription was accepted. The response for a renewal message is the same as one for a subscription message, updating the lifetime of the subscription. Should a subscription expire, the device stops sending event messages to that control point; any attempt to renew the expired subscription is rejected.

When a control point no longer needs event notifications from a particular service, it cancels its subscription by sending an appropriate message to the subscription URL.

PRESENTATION

In addition to the functional interface provided by control and eventing, devices may also provide a presentation URL for a "Web" interface, accessible from a standard Web browser. If such a URL is provided in the device description, the control point can use an HTTP GET request to retrieve an HTML page from this URL, load the page into a browser, and allow a user to control the device and view device status. The degree to which control and status monitoring can be accomplished depends on the specific capabilities of the presentation page and device.

Unlike the UPnP device and service descriptions, the contents of a presentation page are completely specified by the UPnP vendor. A presentation page need not be present, but if present it must be an HTML page and should be written in HTML v. 3.0 or later. The architecture does not define further requirements for presentation pages, but certain design characteristics are recommended.

USAGE SCENARIOS

Consumers are interested in the usage cases enabled by the UPnP architecture. As home networks become more widespread, consumers increasingly will appreciate the value of sharing and accessing many devices via a home network. UPnP technology permits devices to be used anywhere within a home network. With the advent of low-cost wireless communication methods such as IEEE™ 802.11 and Bluetooth™ technologies, the network's reach might extend to the entire house and yard. Devices can be located where it is most convenient and controlled from any UPnP control point, including PCs, Internet appliances, and mobile devices.

Ease of use is critical to the success of the home network. Home networking is intended to make life easier for consumers, enabling them to share resources and access devices from any location. These benefits are realized only if devices are easy to use; the success of home networking could be severely limited if device and network configuration is required. To foster ease of use, the UPnP Forum is actively defining DCPs for more than a dozen devices, enabling several popular usage cases. Here we describe some usage cases that are likely to benefit from the use of UPnP technology.

USAGE CASE 1: UPNP INTERNET GATEWAYS

With the proliferation of multiple-PC households and the wide deployment of broadband services, Internet gateways are becoming popular as consumers seek to share their high-speed Internet connection among multiple devices.

Internet gateways typically employ Network Address Translation (NAT) function to allow multiple home PCs and other Internet devices to share the external IP address that is assigned by the Internet service provider. The UPnP Internet gateway can help to solve a problem that often confronts home and small business users: peer-to-peer applications such as videoconferencing, IP telephony, and online gaming don't work with NAT because devices that share a single IP address cannot be identified uniquely over the Internet.

Consider a hypothetical user, Paula, who initially has a PC in the den with a 56K modem connection to the Internet. Paula recently purchased a second PC to browse the Web and run other Internet applications while she is in the kitchen. She installs a wireless home network and an Internet gateway to allow both PCs to share a new asynchronous digital subscriber line (ADSL) broadband connection. Paula discovers that the online gaming and peer-to-peer applications that worked well with only one PC no longer work. Even after calling the technical support hotline, Paula, like most consumers, still could not figure out how to manually set up the gateway's port mapping table to make the non-UPnP gateway work as she would like. When Paula learns that her online gaming and peer-to-peer applications already have UPnP capability, she installs a new UPnP Internet gateway and her applications run as expected, without any configuration.

UPnP technology automates the processes of discovering the Internet gateway and configuring the port mapping function that maps applications running in the home to unique external port numbers that are visible to external peers. A UPnP Internet gateway can also generate event notifications when the connection speed changes or a connection is lost. Applications might take advantage of this information and adjust themselves accordingly. The UPnP architecture allows control points to work seamlessly with Internet gateways without user intervention. Hence, Paula can enjoy Internet browsing and online gaming with friends and get the most out of her home network and high-speed Internet connection.

USAGE CASE 2: THE PRINTER

Another device approaching final standardization in the UPnP Forum is the printer. The standard UPnP printer definition enables a control point to print to any UPnP printer without prior configuration. Traditionally, a user wishing to share a printer among different PCs needs to install the appropriate printer driver on each PC. If a printer is a network printer, prior knowledge of either the printer or a print server's identity is required. UPnP technology automates the discovery and configuration processes.

Unlike the UPnP device and service descriptions, the contents of a presentation page are completely specified by the UPnP vendor. A presentation page need not be present, but if present it must be an HTML page and should be written in HTML version 3.0 or later.

Bluetooth is a trademark of the Bluetooth Special Interest Group, Inc.

IEEE and IEEE 802 and its derivatives are registered trademarks of the Institute for Electrical and Electronics Engineers, Inc.

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

To enable complete interoperability, agreement on data formats is required for devices such as printers. The UPnP architecture does not prescribe a specific data transfer format; however, the UPnP printer working committee has standardized basic formats to ensure interoperability.

For example, suppose Paula has a printer attached to her wireless network. She comes home from work one day and turns on the television to watch the news. During a commercial, she wishes to print an e-mail from her PDA. UPnP technology enables Paula's PDA to discover the available printers in the home. Paula selects one and prints her document. The UPnP architecture provides a standard control protocol for interacting with the printer and alerts her to abnormal conditions such as paper jams. If Paula's home network consisted of a mixture of wired and wireless networks, UPnP technology would allow her PDA to find the printer regardless of the physical network to which it is attached.

To enable complete interoperability, agreement on data formats is required for devices such as printers. The UPnP architecture does not prescribe a specific data transfer format; however, the UPnP printer working committee has standardized basic formats to ensure interoperability. All UPnP printers must support an XHMTL-based page description language and JPEG-encoded images. Other document and image formats may be supported at the manufacturer's discretion.

USAGE CASE 3: MULTIMEDIA APPLICATIONS

An exciting range of multimedia applications for consumer electronic devices, PCs, and even some mobile devices could be enabled by specifications being cooperatively developed by the UPnP Forum's audio, audio-visual, camera, and electronic picture frame working committees. The goal is to enable users to store, play, and view audio and video content across this range of device classes.

Consider again our hypothetical user Paula, and suppose that she purchases a UPnP camera with a networked docking station. When Paula returns home from her son Ben's soccer match and docks the camera, her PC-based image management application notes that the camera is now available on the network. The application queries the camera, finds new content, and automatically retrieves the new soccer match pictures. Later that night, when Paula checks her e-mail, she already has at her fingertips the favorite photos of the day, which she then e-mails to Ben's grandfather. She also programs her electronic picture frame to include one particular favorite in its repeating slideshow for the next week.

While checking her e-mail, Paula learns that a new recording by her favorite artist is available. Paula visits the recording label's Web site, purchases a copy of one of the songs, and initiates a download of the song to her new audio player in the family room. Later that night Paula decides to listen to the song on her home entertainment system. Using her remote control, she selects the new recording from her audio player and plays it on her stereo.

Several key factors empower these usage cases and many others. Beyond the basic discovery, descriptive and control capabilities provided by the UPnP architecture, work is in progress to define a standard model for a multimedia storage service, leveraging emerging XML-based frameworks such as MPEG-21. Moreover, by developing common mechanisms to establish and manage data transfer, different multimedia devices could interoperate. In addition to supporting IP-based protocols such as HTTP and RTSP, working committees are defining support for non-IP-based mechanisms such as IEEE 1394 and direct analog connections. Although control information by necessity uses an IP-based network, data transfer need not do so.

Note that some devices could act as both UPnP controlled devices that implement one or more UPnP DCPs, and UPnP control points. For example, a digital camcorder might control other UPnP devices. Vendors are free to implement whatever control functionality is appropriate; a camcorder might allow a user to send video directly from the camcorder to a picture frame or digital television. A camcorder also might allow the user to print still snapshots on a printer. Although UPnP control points can discover any UPnP device, they can only interact with or control those devices or services for which they have prior knowledge of the interaction model.

UPNP TECHNOLOGY BENEFITS FOR HOME NETWORKING

STANDARDS-BASED

Universal Plug and Play builds on existing protocols and technology (including IP, TCP, UDP, HTTP, HTML, SOAP, and XML) whenever practical. The Internet provides highly proven, well understood, and open networking technology that is easy to use. IP internetworking is well suited for UPnP because it has proven its ability to span different physical media, enable real-world multivendor interoperation, and achieve synergy with the Internet and many home and office intranets. Mixed-media multivendor networks are likely to become common in the future, and the UPnP architecture has been designed explicitly for these environments.

UNIVERSALITY

By leveraging Internet protocols, UPnP technology is ideally suited for cross-device cross-network deployment. It can work with any underlying networking technology that supports IP traffic, but it does not require all devices to include an IP stack. Cost, technology, or legacy might preclude IP traffic for some media and devices. By using *UPnP protocol bridges*, devices that communicate with non-IP protocols can participate in UPnP networks.

Furthermore, the UPnP architecture is based on the notion of sending only data, not executable code, between control points and devices. Data is transmitted in a platform-independent manner, allowing vendors to select the most appropriate operating system and language for device and control point implementation.

Although the UPnP architecture provides a mechanism for universal control, it does not stipulate universality of data transfer. Instead, common data formats within certain domains and usage cases may be agreed on, such as the previously described example of XHTML and JPEG formats for UPnP printers. In some scenarios, the control point and controlled device might use UPnP control protocols at runtime to negotiate mutually supported formats for data transfer.

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**

fastcase®
Smarter legal research.