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 paper, we present an overview of the Universal Plug and Play (UPnP^{TM}) technology and the UPnP Forum, the multi-company 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 that UPnP technology can provide in home networking and briefly discuss potential future work in this area.

1 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 to 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.

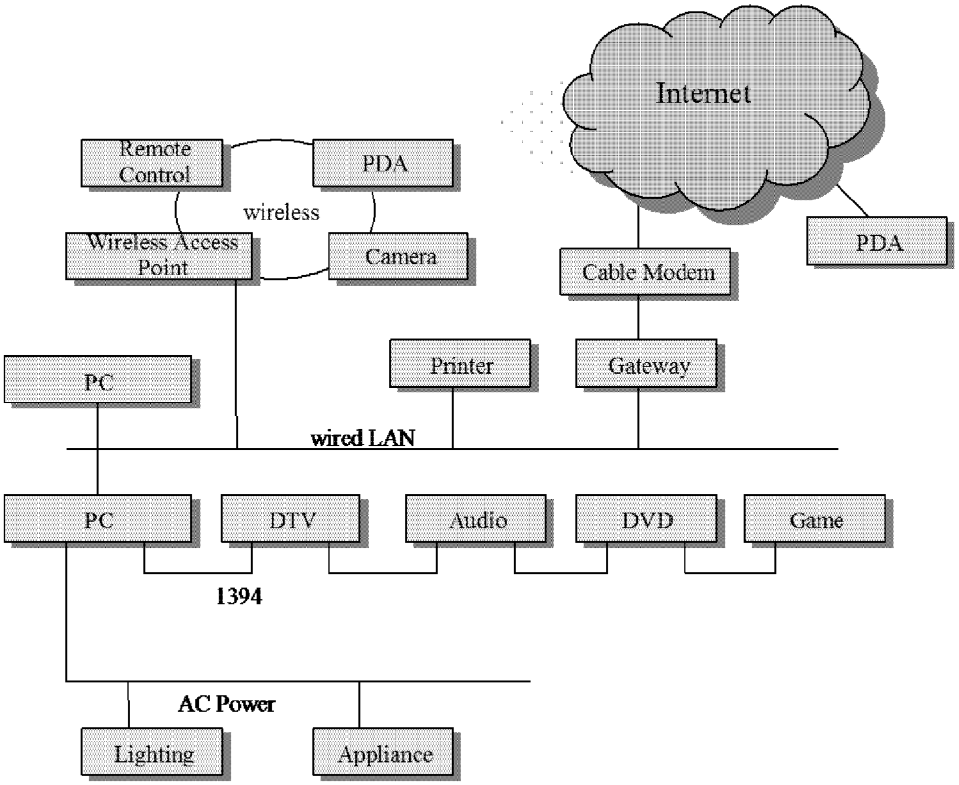

Figure 1. Example UPnP topology.

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.

2 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 [FORUM99].

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 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 version 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.

3 Technical Description

3.1 Overview

The UPnP Device Architecture [DEVARCH00] defines the protocols for communication between UPnP *control points* and *devices*. These protocols are illustrated in Figure 2, taken from [FORUMWP], 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; and
- *Presentation*, by which devices can present Web pages to control points allowing for status and control interactions.

[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.
[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.

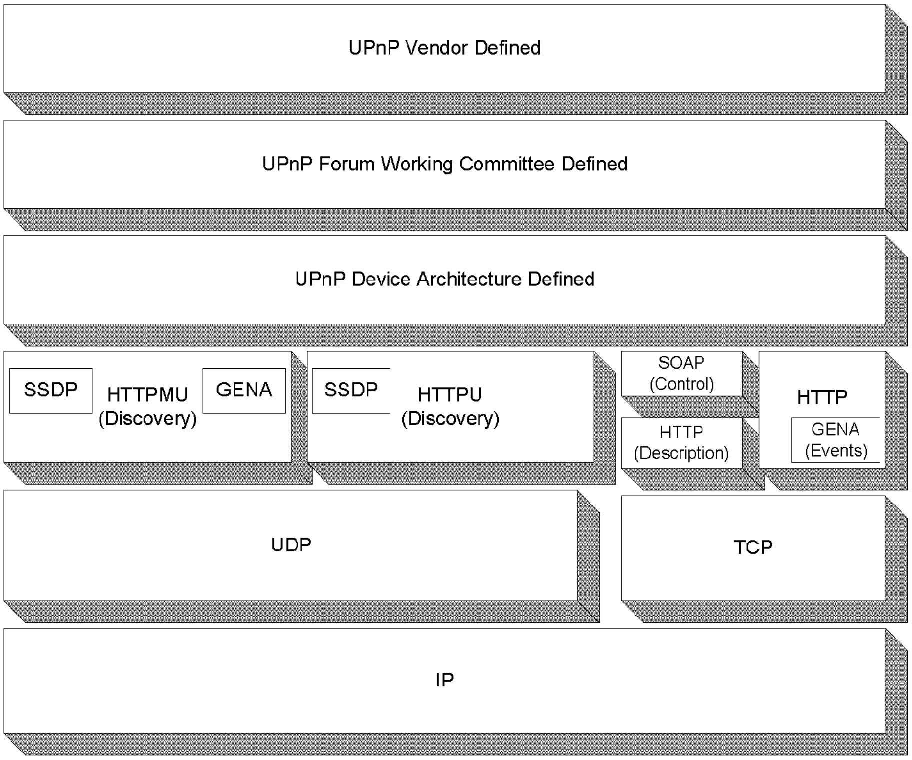

Figure 2. UPnP protocol stack.

3.2 Addressing

Every UPnP device incorporates a Dynamic Host Configuration Protocol [DHCP] 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.

If no DHCP server responds, the device uses automatic IP addressing [Auto-IP]. It randomly chooses an address in the 169.254/16 range, and tests it using an Address Resolution Protocol [ARP] 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 [RFC1034, RFC1035]. Device names could be registered manually, dynamically according to [RFC2136] or by the DHCP server.

3.3 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 [SSDP]. Control points also may use SSDP to search for devices of interest on the network. The

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.