UPNP STANDARDS & ARCHITECTURE

About UPnP

Effective January 1, 2016, UPnP Forum assigned their assets to the Open Connectivity Foundation (OCF). UPnP Forum was originally formed in October 1999 as an industry initiative who gained more than 1000 leading companies in computing, printing and networking; consumer electronics; home appliances, automation, control and security; and mobile products.

UPnP technology allows devices to connect seamlessly and to simplify network implementation in the home and corporate environments. Toward this end, UPnP Forum members worked together to define and publish UPnP device control protocols built upon open, Internet-based communication standards.

The UPnP architecture offers pervasive peer-to-peer network connectivity of PCs of all form factors, intelligent appliances, and wireless devices. The UPnP architecture is a distributed, open networking architecture that leverages TCP/IP and the Web to enable seamless proximity networking in addition to control and data transfer among networked devices in the home, office, and everywhere in between.

Click here to download all UPnP Specifications (67 MB)

Broad in Scope

UPnP technology targets home networks, proximity networks and networks in small businesses and commercial buildings. It enables data communication between any two devices under the command of any control device on the network. UPnP technology is independent of any particular operating system, programming language, or network technology.

Zero Configuration and Automatic Discovery
The UPnP architecture supports zero-configuration and automatic discovery whereby a device can:

- Dynamically join a network
- Obtain an IP address
- Announce its name
- Convey its capabilities upon request
- Learn about the presence and capabilities of other devices
- Leave a network smoothly and automatically without leaving any unwanted state information behind
  DHCP and DNS servers are optional and are used only if they are available on the network.

Technology Benefits

- Media and device independence. UPnP technology can run on any network technology including Wi-Fi, coax, phone line, power line, Ethernet and 1394.
- Platform independence. Vendors can use any operating system and any programming language to build UPnP products.
- Internet-based technologies. UPnP technology is built upon IP, TCP, UDP, HTTP, and XML, among others.
- UI Control. UPnP architecture enables vendor control over device user interface and interaction using the browser.
- Programmatic control. UPnP architecture enables conventional application programmatic control.
- Common base protocols. Vendors agree on base protocol sets on a per-device basis.
- Extendable. Each UPnP product can have value-added services layered on top of the basic device architecture by the individual manufacturers.

Standardized Device Control Protocols

Like the creation of Internet standards, the UPnP initiative involves a multi-vendor collaboration for establishing standard Device Control Protocols (DCPs). Similar to Internet-based communication, these

are based on protocols that are:

Declarative
Expressed in XML
Communicated via HTTP

See below for more information on UPnP technology.

Download all of the UPnP specifications here.

Interested in Certifying Devices?

Visit here for more information on how to qualify for access to the official UPnP certification test tool and to submit devices for UPnP certification.

About UPnP

Resources

Certification

Presentations & White Papers

Standards: Device Control Protocols

These are the specifications, produced by specific UPnP Task Groups, which have been standardized. The standardization process includes obtaining three sample implementations of the Device Control Protocol (DCP) to pass the UPnP Certification Test Tool, circulating the specification for a mandatory OCF member review and comment period, and obtaining the approval of the UPnP Work Group and OCF Board to become a Standardized DCP. Standardized DCPs are available to the public.

Download all of the UPnP specifications in a single .zip file here.

Device Categories

Audio/Video

- MediaServer:4 and MediaRenderer:3
- MediaServer:3
- MediaServer:2 and MediaRenderer:2
- MediaServer:1 and MediaRenderer:1

Basic

- Basic Device:1

Cloud

- CloudProxy:1

Device Management

- Manageable Device:2
- Manageable Device:1

Home Automation

- SolarProtectionBlind:1
- Digital Security Camera:1
- HVAC:1
- Lighting Controls:1

IoT Management and Control

- IoT Management And Control:1

MultiScreen

- MultiScreen:1
- MultiScreen:2

Networking

- Internet Gateway:2
- WLAN Access Point:1

Printer

- Printer Enhanced:1
- Printer Basic:1

Remote Access

- RAServer:2 and RADiscoveryAgent:2
- RAClient:1, RAServer:1 and RADiscoveryAgent:1

Remoting

- Remote UI Client:1 and Remote UI Server:1

Scanner

- Scanner:1

Sensor Management - RENAMED to IoT Management and Control

- IoT Management And Control:1

Telephony

- Telephony:2
- Telephony:1

Add-on Services

- DataStore:1
- DeviceProtection:1
- EnergyManagement:1
- FriendlyInfoUpdate:1
- Low Power:1
- ContentSync:1
- Quality of Service:2
- Quality of Service:1
- BasicManagementService:2
- BasicManagementService:1
- ConfigurationManagementService:2
- ConfigurationManagementService:1

- Device Security:1 and Security Console:1
- Quality of Service:3
- SoftwareManagementService:2
- SoftwareManagementService:1

Referenced Specifications

The following specification is referenced in UPnP Device Architecture Version 1.0 and is provided here because it is no longer available from its original source.

UUIDs and GUIDs

This specification defines the format of UUIDs (Universally Unique IDentifier), also known as GUIDs (Globally Unique IDentifier).

A UUID is 128 bits long, and if generated according to the one of the mechanisms in this document, is either guaranteed to be different from all other UUIDs/GUIDs generated until 3400 A.D. or extremely likely to be different (depending on the mechanism chosen).

UUIDs were originally used in the Network Computing System and later in the Open Software Foundation's Distributed Computing Environment. (February 1997)

Back to top

Architectural Documents

Here are the fundamental documents that anchor the UPnP architecture. Device architecture and template guidelines provide a blueprint for the UPnP Task Groups. When a Task Group is finished with its device and services specifications, the checklist provides a thorough accounting of milestones required to propose a specification for standardization.

PORTIONS OF THIS APPROVED SPECIFICATION WERE COMPLETED PRIOR TO THE COMBINATION OF UPNP INTO THE OPEN CONNECTIVITY FOUNDATION. FOR PORTIONS OF THE SPECIFICATION THAT WERE PUBLISHED ON OR PRIOR TO FEBRUARY 20, 2015 THE FOLLOWING APPLIES: ALL LICENSES, INTELLECTUAL PROPERTY RIGHTS, AND OTHER RIGHTS, RESPONSIBILITIES, OBLIGATIONS, STANDARDS, AND PROTOCOLS ASSOCIATED WITH PORTIONS OF THIS APPROVED SPECIFICATION THAT WERE PUBLISHED ON OR PRIOR TO FEBRUARY 20, 2015 ARE SUBJECT TO THE UPNP BYLAWS AND FORUM MEMBERSHIP AGREEMENT.

UPnP Device Architecture version 2.0
Document Revision Date: April 17, 2020

This latest revision adds the following text to section 4.1.1:

The subscription request containing a delivery URL not on the same network segment as the fully qualified event subscription URL shall not be accepted. For private networks this means that the delivery URL provided will adhere to the following IP ranges:

- *10.0.0.0 - 10.255.255.255 (10/8 prefix)*
- *172.16.0.0 - 172.31.255.255 (172.16/12 prefix)*
- *192.168.0.0 - 192.168.255.255 (192.168/16 prefix)*

The UPnP Device Architecture (formerly known as the DCP Framework) contained herein defines the protocols for communication between controllers, or control points, and devices.

The UPnP Device Architecture (UDA) V2.0 is the basis for UPnP+ which enhances the UPnP experience so that any device can securely interact anywhere. Here is a summary of the changes between the UDA V1.1 and the new UDA V2.0:

- Annex A (IPv6) has been updated to be compliant with the latest IETF recommendations.
- Annex C (UPnP Cloud Architecture) has been added.
- Support for Control Point identification.
- Subscription support for individual state variables.
- A clarification was made that UDA 2.0 control points shall be backwards compatible with UDA 1.x devices.
- Version mapping clarification.
- Initial bye-bye clarification.
- M-search responses clarification.
- Various language editorial changes for consistency.

An archive of previously published versions of the UPnP Device Architecture is available for historical reference.

IP Declarations from last UDA 2.0 revision published February 20, 2015

UPnP Vendor's Implementation Guide

This document contains clarifications to v1.0 of the UPnP Device Architecture that are likely to be of specific interest to vendors implementing control points and/or devices.

Legal Disclaimer

NOTHING CONTAINED IN THESE DOCUMENTS SHALL BE DEEMED AS GRANTING YOU ANY KIND OF LICENSE IN ITS CONTENT, EITHER EXPRESSLY OR IMPLIEDLY, OR TO ANY INTELLECTUAL PROPERTY

Back to top

UPnP+ Initiative

UPnP+ Certification is now available. Read here for more details.

For Training and Resources on UPnP+ implementation please see below.

Evolution

- Full integration of IPv6 with seamless backwards compatibility to IPv4
- Improved interoperability baseline incorporating the latest specifications, including AV, Device Protection, and Energy Management

Revolution

- Discovery of cloud services and content as well as secure sharing of devices across the Internet
- Data-based definition of new devices
- Expandable protocol bridging using REST based methodologies

- Features that drive UPnP devices to the core of the Internet of Things
- Enabling Social Media interactions

The UPnP+ certification program uses new and existing UPnP device control protocols (DCPs) and UPnP architecture enhancements to provide UPnP protocols focused on delivering new technical capabilities enhancing functionality and increase customer satisfaction in today's ever-changing market of always-on connectivity. UPnP+ technology is an evolution of previous UPnP capabilities that will assist devices trying to integrate new paradigms like mobile connected computing, cloud-based service delivery, smartphone content sharing, and the Internet of Things.

Key areas UPnP+ addresses include:

- Interoperability
- Security
- Evolving standards (HTML5, IPv6, etc.)
- Cloud-based features
- New services

UPnP+ supports a wide range of functions, ensuring future connectivity and makes new services possible, in areas such as health and fitness, energy management, security and sustainability. UPnP+ allows devices from different manufacturers to work together seamlessly, based on a single underlying technology, which is backwards-compatible with existing products and easy to deploy.

UPnP Device Architecture

The UPnP Device Architecture V2.0 (UDA 2.0) is the basis for UPnP+ certification enhancing the UPnP experiences towards the cloud and in a secure way. The UDA 2.0 is backwards compatible with UDA 1.x devices, enables additional features including IPv6, cloud based sharing, event subscriptions to individual state variables, and includes a number of clarifications. Access the UDA 2.0 here.

UPnP+ Training and Resources

- Why You Should Upgrade to UPnP+ (February 17, 2015)
  YouTube recording | Presentation slides only
- UPnP+ demo at IBC (September 2014) - YouTube video
- Leveraging UPnP+: The Next Generation of Universal Interoperability (April 2015)
  Full Whitepaper | Short Marketing Brief
- UPnP+ Certification Overview and Requirements Matrix
- UPnP Internet of Things Overview
- UPnP AV Tutorial

- UPnP Device Architecture Tutorial
- Cloud Demo Source Code
- UPnP+ Implementation Guide (Coming Soon!)

UPnP+ Certification Requirements

View UPnP+ Certification Information and the Requirements Matrix. The process to certify a UPnP+ product is the same as standard UPnP products.

If you have any questions, feel free to contact us!

UPnP+ Certification Requirements

In order to improve UPnP technology implementations and encourage the use of the latest version of UPnP specifications, UPnP Forum has created the UPnP+ certification level. UPnP+ certified products will be more reliable, more secure and will have increased functionality.

The benefits include improved features and performance in:

- Interoperability
- Security
- Evolving standards (HTML5, IPv6, etc.)
- Cloud-based features
- New services

In support of this effort, OCF has updated the UPnP Certification Test Tool (UCTT) for enhanced testing and expanded its testing program to improve the quality of open source implementations.

The following are the requirements for UPnP+ certification compared to UPnP certification for all UPnP certified devices.

Specification	UPnP Certification	UPnP+ Certification
UDA	• UPnP version 1.0 is a minimum requirement, • UPnP version 1.1 is optional	• UPnP version 2.0 is a minimum requirement

IPv6 Annex	• UPnP certification requires IPv4 support • IPv6 support is optional and the currently published IPv6 annex is out of date	• UPnP+ certification requires dual-stack (IPv4/IPv6) implementation as described in the new UPnP UDA annex
UDA Cloud Annex	• UDA V1.0 devices cannot be certified as cloud devices, however legacy UDA V1.0 devices can be bridged to the cloud using a UPnP+ certified CPDev Cloud Proxy device	• UPnP cloud device support (UCCD) is mandatory for UPnP+ device certification • UPnP cloud control point support (UCC-CP) is mandatory for UPnP+ control point certification

The following are the requirements for UPnP+ certification compared to UPnP certification for floating services. These services can be added to other device types.

Service	UPnP Certification	UPnP+ Certification
DeviceProtection	• DeviceProtection:1 is optional	• DeviceProtection:1 is required for UPnP+ certification • http://sourceforge.net/projects/upnpdm/ - an open source implementation from Orange (includes DeviceProtection, DeviceManagement: BMS & CMS & SMS)
FriendlyInfoUpdate	• FriendlyInfoUpdate:1 support is optional	• FriendlyInfoUpdate:1 support is mandatory for UPnP+ certification

EnergyManagement	• EnergyManagement:1 is optional	• EnergyManagement:1 support is mandatory in UPnP+ certification • EnergyManagement proxy is mandatory for mains powered devices
BasicManagementService	• BasicManagementService:1 is optional	• BasicManagementService:2 is mandatory
ConfigurationManagementService	• ConfigurationManagement Service:1 is optional	• ConfigurationManagementService:2 is optional
SoftwareManagementService	• SoftwareManagement Service:1 is optional	• SoftwareManagementService:2 is optional
QOS	• QOS:2 is optional	• QOS:2 is optional
QOS	• QOS:3 is optional	• QOS:3 is optional

The following are the requirements for UPnP+ certification compared to UPnP certification for individual Device Control Protocols. If a particular DCP is used, the UPnP+ requirements for that device must be met for UPnP+ certification. DCPs not listed in this table have no additional requirements for UPnP+ certification.

Specification	UPnP Certification	UPnP+ Certification

IGD	• IGD:1	• IGD:2
AV	• AV:1	• AV:4
MediaServer	• MediaServer:1	• MediaServer:4 • MULTI_STREAM feature • CONTAINER_SHORTCUTS feature • CDS Search() • MULTI_STREAM properties are conditionally required • Relaxed Tracking Changes Option • TCO properties are conditionally required
MediaRenderer	• MediaRenderer:1	• MediaRenderer:3 • Trickmode Pause() is required • SetStaticPlaylist(), SetStreamingPlaylist() and GetPlaylistInfo() are required • GetRendererItemInfo() is required • GetAllowedTransforms(), GetTransforms(), SetTransforms() and GetAllAvailableTransforms() are required

Back to top

UPnP IoT

Who should implement UPnP IoT?

For vendors that already implement UPnP in their devices, we provide a way to discover and manage IoT devices. Read below for more about the UPnP IoT Management and Control Device Control Protocols (DCPs). Bridges between OCF and UPnP have been built and an open source implementation should be available in the coming months.

For vendors that do not implement UPnP, it is recommended that you use OCF directly because of its native RESTful architecture that is very scalable. View the OCF resources here.

UPnP IoT Management and Control

UPnP+ Cloud is built on mature technology (UPnP, Internet Protocols, XMPP...) that caters to tomorrow's connectivity requirements, removing boundaries and enabling full device and network compatibility. UPnP+ provides a solid, future-proof basis for integration of Cloud content and services. One important and fast-growing user requirement is accessing devices from remote locations, often using a mobile device. Home connectivity from outside the home (or workplace) allows for the development of new integrated capabilities, use cases and business models. Security is a vital element in the design of such applications, UPnP Cloud standards have this 'built in', along with access control configurability.

UPnP+ Cloud allows you to connect any number of home devices, mobile devices and cloud services across the Internet in "rooms." You can control and synchronize any UPnP activities with just the people you want. None of your devices are actually shared until you specify with whom and under what conditions. It's simple and secure sharing with the people you want on your terms. To access the Cloud DCPs and Implementation Guides, click here.

The strategy in creating UPnP+ uses new and existing UPnP device control protocols (DCPs) and UPnP architecture enhancements in order to provide UPnP protocols specifically for IoT applications. UPnP core technology provides a base for IoT, creating bridges to both wide-area networks and non-IP devices. There are already published UPnP DCPs for lights, thermostats, automatic blinds and security cameras, and UPnP has defined dozens of data models to support new IoT devices, specifically those with constrained resources.

The UPnP bridging concept allows different local networks to interact. This includes existing device network protocols such as Bluetooth or Zigbee. Entirely new domains, introduced as a result of the rise of the Internet of Things and Cloud computing, which couldn't previously have been accommodated within UPnP are now enabled with UPnP+ IOT extensions.

Beyond physical bridging, the UPnP device data modelling approach allows devices from different ecosystem to agree on a common messaging format. Translations to this format ensures common operation between any ecosystems. UPnP has developed a tool to allow theses device data models to

be crowd-sourced. UPnP scales at the rate of the Internet of Things.

In summary, UPnP IoT:

- Builds upon UPnP core technology that already provides a base for IoT (billions of devices deployed!)
- Uses commonly used web technologies to create secure communication between devices
- Bridges local UPnP networks together through the Internet
- Supports simple, data-based device descriptions to include resource constrained devices
- Enables existing UPnP specifications & devices to be Cloud-capable
- Provides a path for low-risk, rapid implementation of UPnP Cloud solutions
- Enables device and service discovery through the Cloud
- Combines UPnP and XMPP ecosystems to enable new IoT possibilities

Resources:

- UPnP IoT Management and Control Device Control Protocols (DCPs)
- UPnP: The Discovery & Service Layer For The Internet of Things (April 2015)
  Full Whitepaper | Short Marketing Brief
- Why You Should Upgrade to UPnP+ (February 17, 2015)
  YouTube recording | Presentation slides only
- UPnP+ demo at IBC (September 2014) - YouTube video
- UPnP Internet of Things Overview December 2014
- UPnP Internet of Things Overview (July 2014)
- Bringing UPnP to the Cloud and IOT (May 2014)
- UPnP+ Cloud demo video
- UDA V2.0 with Cloud Annex

Your Company

OPEN CONNECTIVITY FOUNDATION™

3855 SW 153rd Drive, Beaverton, Oregon 97003, Phone: 1.503.619.0673