Universal Plug and Play (UPnP)

Santiago Muñoz Castro

[1] Universidad de Granada, ETSIIT, ES
[2] Calle Periodista Daniel Saucedo Aranda, s/n, 18014 Granada
santiyagito22@correo.ugr.es

Abstract: En el transcurso de este documento vamos a relacionar los términos otorgados durante el desarrollo de la asignatura, es decir, conceptos y términos sobre sistemas distribuidos del tema 4 y 6, con la tecnología middleware Universal Plug and Play (UPnP) , donde abarcaremos profundamente en su funcionamiento, los protocolos que utiliza, los componentes que lo forman, características a tener en cuenta, algunos atributos de calidad y se acabara con un análisis crítico y conclusión sobre dicha tecnología. También se realizará un a introducción al concepto de middleware. La información ha sido obtenida de una mezcla de todas las referencias que aparecen a final del documento.

Keywords: UPnP, Middleware, cliente, router, red, dispositivo, servidor, malware, puerto, IP

1 Middleware

1.1 ¿Qué es?

Antes de indagar dentro de la tecnología middleware UPnP tenemos que conocer el término de middleware.

El término *middleware* se aplica al estrato software que provee una abstracción de programación, así como un enmascaramiento de la heterogeneidad subyacente de las redes, hardware, sistemas operativos y lenguajes de programación[1].

Algunos middlewares soportan un único lenguaje de programación como Java RMI, sin embargo, la mayoría se implementan sobre protocolos de internet como TCP/IP y tratan con las diferencias entre sistema operativo y hardware.

Dicho de una forma más simple, *middleware* es cualquier capa intermedia (software) de un sistema distribuido, es decir, se encuentra entre las aplicaciones y las plataformas. Aumentan también la productividad del programador utilizando abstracciones para acceder a los recursos y para las comunicaciones de las capas por encima del sistema operativo.

1.2 Clasificación

La clasificación puede ser descrita en dos grandes categorías[2]:

- **De integración:** Destinados a ser utilizados en sistemas heterogéneos.
  - Orientados a procesos (RPC).
  - Orientados a objetos.
  - Orientados a mensajes(MOM).
  - Orientados a componentes, del cual es

- **De aplicación:** Son los que se ajustan a aplicaciones específicas.

2 Universal Plug and Play

2.1 ¿En que consiste?

Mejor conocido como UpnP es un conjunto de protocolos de comunicación que permite a periféricos (dispositvos hardware externos con los que se comunica una computadora) en red, como impresoras, móviles, luces etc…, conocer con transparencia la presencia de otros dispositivos en la red y establecer servicios de red de comunicación, intercambio de datos y entretenimiento[3].

Es una extensión de Plug and play, aunque ambas no esten relacionadas directamente, son capaces de establecer comunicaciones automáticamente con otros dispositivos.

Una de sus funciones más destacadas está en abrir puertos de manera autónoma y automática, sin que el usuario tenga la necesidad de manejar y entender la configuración del router de forma manual y pada cada unos de los programas que quiere tratar, este middleare es muy utilizado en el mundo de los videojuegos[4] o para redes de hogar.

Permite a un dispositivo o programa, en una red privada, realizar una solicitud de abrir un puerto o varios temporalmente al router mientras este en funcionamiento.

2.2 Componentes

Los componentes más importantes que destacan el funcionamiento de un UPnP son los siguientes:

- **Servidor UPnP:** es el servidor (dispositivo maestro) que proporciona información específica almacenada en su biblioteca de datos y la transmite a los clientes UPnP de la red.

- **UPnP MediaServer ControlPoint:** es el cliente (dispositivo esclavo) que detecta de manera automática los servidores UPnP de una red, consulta su contenido y controla la transferencia de información.

- **Componentes de información:** su función es controlar parámetros de la información transmitida, por ejemplo en un UPnP AV (multimedia) existe el RenderingControl que controla parámetros multimedia como brillo, resolución, sonido etc…

- **Cliente/Servidor Remote User Interface(RUI)**: send/receive de los comandos de control entre servidores y clientes UPnP de la red.

- **QoS:** o calidad de servicio, es una funcionalidad no obligatoria pero muy importante. Se encarga de dar diferentes propiedades a los clientes y datos que se transmiten en la red.

- **Acceso Remoto:** establece los métodos necesarios para conectar dispositivos UPnP que tienen el mismo dominio multicast.

2.3 Características a tener en cuenta

Supongamos el caso de un ordenador conectado a un router que tiene activado UPnP, si este le pide al router que le abra un puerto para un servicio por ejemplo, el router recibirá la petición de abrir el puerto X para el dispositivo con IP Y, como el router ya conoce dicha IP debido a que el ordenador está conectado al dispositivo en la misma red, directamente le abre el puerto solicitado.

Algunos tienen la opcion de abrir y cerrar todos los puertos del router a la vez, aunque no siempre funciona ya que depende de las características de dicho router. Es la forma más sencilla y cómoda de abrir el puerto de un router, pero esta tecnología tiene un inconveniente.

El inconveniente es que el usuario no va a tener control sobre los puertos. Las aplicaciones pueden abrir el puerto que quieran, pudiendo pasar que abra un puerto

que no queremos que se abra, ya que al abrirlo es accesible desde el exterior y además es una vulnerabilidad.

Puede ocurrir que un malware acceda a nuestro ordenador, si el router tiene activado UPnP, el malware puede abrir el puerto que quiera para que el atacante (creador del virus) pueda acceder al ordenador desde fuera. Existen páginas o aplicaciones que te indican a partir de la IP pública del router, los puertos que tiene abiertos y cerrados para así controlar y evitar lo comentado anteriormente.

Esto ocurre debido a que UPnP no implementa una autenticación básica sino que confía plenamente en todos los dispotivos conectados en la red. Si queremos utilizar esta tencología y queremos evitar este problema debemos tener actualizado el firmware del router a la última versión, utilizar contraseñas fuertes para acceder al router y al Wi-Fi y mantener los equipos seguros (evitar instalar dispositivos poco fiables)[5].

2.4 Protoco de comunicación y funcionamiento

UPnP utiliza el puerto UDP 1900 y el puerto TCP 2869. Los puntos de control de UPnP son dispositivos que utilizan UPnP para controlar dispositvos UPnP [3]. UPnP soporta Zero Configuration Networking que es el conjunto de técnicas que permiten crear de forma automática una red IP sin configuración o servidores especiales[7].

El primer paso y base de UPnP es el direccionamiento IP, donde cada dispositivo es un cliente que debe implementar DHCP (protocolo de configuración dinámica del host) y que debe buscar un servidor que implemente también DHCP la primera vez que se conecte a la red. Si no hay servidor DCHP, el cliente se asignará una dirección a si mismo (AutoIP). Si el cliente recibe un nombre de dominio, este deberá emplear ese nombre para todas las operaciones de red, en caso contrario, lo hará con su dirección IP.

DHCP es un protocolo cliente/servidor donde el servidor asigna dinámicamente una dirección IP y otros parámetros a cada dispositivo de una red[6].

Una vez realizado el direccionamiento, es decir, que el dispositivo tenga establecido una dirección IP, se realizara el descubrimiento. El descubrimiento se realiza mediante el protocolo SSDP o Simple Service Discovery Protocol, este protocolo permite a los clientes que se acaban de añadir a la red por direccionamiento, anunciar sus servicios a los puntos de control presentes en la red. De esta forma siempre que se añada un punto de control, SSDP le ayudara a buscar a los dispositivos que le interesa controlar, esto se realiza mediante un mensaje de descubrimiento que contiene una URL que redirige a una página con información más detallada del dispositivo, datos básicos del dispositivo y algunos de sus servicios.

Cuando un punto de control descubra los servicios de un dispositivo, necesita más información sobre dicho dispositivo, para ello obtiene la descripción del dispositivo de la URL del mensaje de descubrimiento, esta descripción se codifica en XML (Lenguaje de marcas extensible) y contiene toda la información posible acerca del dispositivo como número de modelo, número de serie , parámetros y argumentos de cada acción, tipo de datos, rango etc…

Una vez obtenida la descripción total del dispositivo, el punto de control puede enviar acciones a los servicios de un dispositivo[3], para ello se enviá un mensaje de control (codificado en XML) mediante SOAP o Simple Object Access Protocol a la URL de control del servicio. Este servicio enviara una respuesta con otro mensaje de control con los resultados de dicha acción, similar al return de una función.

UPnP puede notificar eventos (eventing), el protocolo utilizado se conoce como General Event Notification Architecture (GENA). Se notificara al punto de control cuando se actualicen las variables de un servicio, para ello se envían también mensajes codificados en XML a todos los puntos de control que utilicen las acciones de dicho servicio. La primera vez que se suscribe un punto de control se le envía un mensaje especial sobre el estado de todos los servicios. El objetivo de estas notificaciones es conseguir escenarios con múltiples puntos de control. Dicho de una forma más simple, si un alumno habla con un profesor para cambiar una fecha de entrega y este accede, no bastara con notificar del cambio a ese alumno sino que se tendrá que enviar un mensaje de notificación a todos los alumnos para que sean conscientes del cambio. Lo mismo ocurre para los servicios y puntos de control.

El último paso de UPnP es la presentación. Si un dispositivo tiene una URL de presentación, el punto de control accederá a la página desde un navegador y según el tipo de página, se permitirá al usuario controlar el dispositivo y/o consultar su estado.

2.5 Algunos atributos de calidad

Algunos atributos de calidad y características de UPnP que hay que mencionar son:

- **Independencia de formato y dispositivos**: UPnP puede ejecutarse en muchos medios que soportan IP como Ethernet, IrDA, FireWire, Bluetooth y Wi-fi, donde no son necesarios controladores especiales, basta con los protocolos comunes de red.

- **Control mediante IU (Interfaz de usuario):** con UPnP los dispositivos presentan una interfaz de usuario mediante un navegador web.

- **Independencia de lenguaje de programación y SO (Sistema Operativo):** se puede utilizar cualquier lenguaje de programación y sistema operativo para la creación de productos UPnP, tampoco se restringe el diseño de una API para las aplicaciones que se ejecutan en los puntos de control.

- **Extensibilidad:** UPnP pueden tener servicios específicos para un producto en capas superiores a la arquitectura básica, los fabricantes de productos pueden definir dispositivos y tipos de servicios propios, extender dispositivos y servicios ya definidos.

3 Análisis crítico y conclusión

UPnP es una tecnología middleware que no puede utilizar cualquiera, por defecto muchos routers la desactivan, ya que los usuarios no son conscientes de su existencia, en ese caso es mejor tenerla desactivada.

UPnP puede hacer que aplicaciones consigan acceso directo a internet a través de un puerto específico que ha sido abierto automáticamente para dicha aplicación, evitando tener que hacerlo de forma manual, cosa que resulta muy tediosa y complicada.

Un ejemplo, es que podemos conectar una impresora, un termómetro domático, un detector de luminosidad (sensores como el de la práctica 4) a la red/ordenador de nuestro hogar de forma automática, sin necesidad de ajustar manualmente la configuración del router.

Otro ejemplo, en el mundo de los videojuegos, hace que el cortafuegos permita la conexión de todos los juegos que necesitan conexión a internet, evitando problemas de comunicación online sin necesidad de ajustar cada acceso.

La desventaja de esta tecnología es lo vulnerable que deja a nuestro router, ya que puede pasar el cortafuegos o firewall, como ya hemos dicho antes, una aplicación o dispositivo malicioso podría abrir un puerto del router sin ningún problema para que el atacante puede accede a nuestro router desde un sistema externo de forma muy fácil, como si le abriésemos la puerta al enemigo.

Existen algunas alternativas que pueden llegar a realizar algunas de las funciones de UPnP, como chromecast, DLNA, SAMBA, Ushare entre otras más, que por cada una se podría realizar otro trabajo. Aun así UPnP es la tecnología para este ámbito más utilizada, documentada y soportada actualmente.

En resumen, el uso adecuado de esta tecnología nos ayudará a reducir en gran cantidad el trabajo y complejidad que conlleva abrir puertos para que se conecten aplicaciones o dispositivos de nuestra red. Sin embargo, hay que tener sumo cuidado con dichas aplicaciones o dispositivos que instalemos ya que pueden arruinar por completo toda la red de nuestro hogar.

En mi opinión, esta tecnología si se sabe utilizar puede que me sea muy útil ya que mejorara mi conexión a la hora de jugar a videojuegos o para facilitarme el trabajo si quiero conectar por ejemplo la impresora al router de la casa. Sobre el desarrollo del trabajo, me ha gustado indagar sobre esta tecnología y expandir mi habilidad para buscar información en internet acerca de un tema, cosa que llevaba mucho tiempo sin realizar.

References

1. *G. Coulouris,2012,Distributed Systems: Concepts and Design (5th Edition).*
2. Transparencias del profesor Russo.
3. Wikipedia UpnP, https://es.wikipedia.org/wiki/Universal_Plug_and_Play, último acceso 12/06/21.
4. AdslZone, https://www.adslzone.net/2018/05/03/upnp-que-es/, último acceso 12/06/21 .
5. RedesZone, https://www.redeszone.net/tutoriales/internet/upnp-problema-seguridad-red/, último acceso 13/06/21.
6. DHCP,https://es.wikipedia.org/wiki/Protocolo_de_configuraciónn_dinámica_de_host, último acceso 14/06/21.
7. Zeroconf, https://es.wikipedia.org/wiki/Zeroconf , últimoa acceso 14/06/21