Redes Activas con IPv6

D. Larrabeiti, M. Calderón, A. Azcorra, A. García
Universidad Carlos III de Madrid

J. E. Kristensen
Ericsson Telebit A/S

Las redes activas proponen un nuevo paradigma de arquitectura de red en la que los nodos se definen como entornos de ejecución abiertos en la que determinados usuarios pueden cargar y ejecutar código con el fin de efectuar un procesamiento específico sobre flujos de datos – generalmente a nivel superior al de red. De muy distintas maneras, IPv6 ha tratado varios problemas de IPv4 que facilitan la implantación real de esta interesante tecnología, todavía circunscrita al ámbito académico.

Las Redes Activas

En los últimos años, la tecnología de redes activas [1] ha sido objeto de intensa investigación, como respuesta a las críticas vertidas sobre el modelo actual de protocolos en el que se fundamenta Internet. Dichas críticas, originadas en trabajos de DARPA en 1995, se centran en la gran dificultad de implantar nuevos servicios y protocolos sobre la arquitectura de protocolos existente en la que los nodos de la red tienen su función limitada al encaminamiento de paquetes. Así como el ciclo de maduración e implantación de una tecnología de nivel de aplicación implementable extremo a extremo es muy rápido -usualmente estimado en seis meses-, el ciclo de implantación de protocolos de red es lento -entre cinco y diez años- y depende fuertemente de acuerdos entre fabricantes de dispositivos de red para su normalización e implementación. Ejemplos de este fenómeno son la lentitud de implantación actual de IP versión 6, a pesar de que su diseño incluyó diversos mecanismos de transición e interfuncionamiento con la actual IP versión 4, o el caso del servicio multidestino en IPv4 con mucha mayor demanda potencial del mercado de servicios multimedia en internet.

Como evolución de los modelos de red tradicionales se ha propuesto un nuevo modelo identificado por el término redes activas. La idea fundamental es añadir programabilidad a las redes. Las redes activas constituyen una arquitectura de red en la que los nodos de la misma pueden realizar procesamiento "a medida" sobre los paquetes que los atraviesan. Las redes activas producen un cambio en el paradigma de red: de nodos capaces exclusivamente de transportar octetos de forma pasiva, a nodos capaces de procesar los paquetes a cualquier nivel de la pila de protocolos.

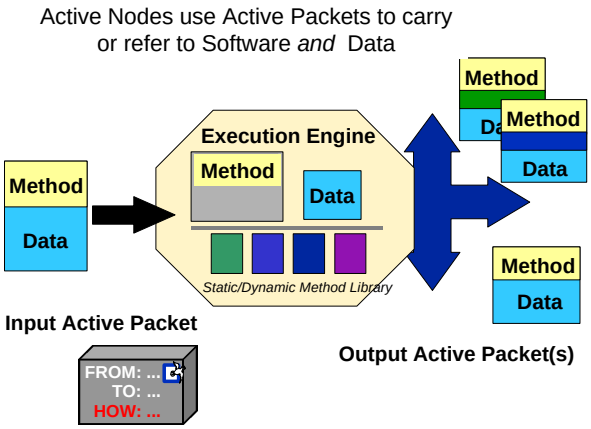


Figura 1. Un paquete activo atravesando un nodo activo

De esta definición se deduce fácilmente que la principal ventaja de la tecnología de redes activas es una importante reducción en el tiempo necesario para implantar nuevos protocolos y servicios. Esta característica ha atraido cierto interés de la industria, adoptando tímidamente algunas ideas de redes activas para facilitar el diseño por parte del cliente de aquellos servicios para los que la programabilidad de la red es imprescindible. El objetivo básico es definir una plataforma que permita desplegar rápidamente nuevas funcionalidades de red sobre arquitecturas de diferentes fabricantes, supuesto ésta ampliamente difundida, y siempre que no se degraden apreciablemente las prestaciones del resto de funciones del nodo, fundamentalmente las de encaminamiento.

Buscando servicios de red

El mecanismo clásico empleado para acceder a la mayoría de servicios de una red distintos del simple transporte de paquetes está basado en entidades del plano de control que entran en contacto con agentes del servicio requerido. Este procedimiento es predominante tanto en IPv4 como en IPv6. En este caso, es el terminal el responsable de localizar los agentes más cercanos (servidores reales o sus representantes (*proxies)*) que proveen el servicio. Uno de los métodos más sencillos y utilizados de gestionar la localización de los servicios dentro de un dominio administrativo de manera centralizada es mediante DHCP. DHCP permite asignar recursos compartidos con cualquier tipo de política programada. Así por ejemplo, un agente DHCP puede pasar a una máquina no sólo la dirección IPv6 al arrancar, sino los parámetros de configuración

de cualquier otro servicio de red: localización de agentes NTP, proxies HTTP, servidores DNS, guardián de puerta H.323, etc.

Un método complementario de buscar los agentes más próximos es mediante búsquedas multidestino en anillo mediante el envio de peticiones sucesivas con un alcance creciente. Este mecanismo es especialmente adecuado para IPv6, puesto que el soporte de multicast es un requisito de conformidad en la nueva versión de IP.

Finalmente existe un tercer método más adecuado a servicios transparentes de su ubicación y de implementación distribuida, consistente en lanzar el código servidor en ciertos puntos de un camino hacia un destino dado. Este es el caso de las redes activas transparentes al plano de usuario. Esto quiere decir que los emisores esperando un procesamiento especial por parte de la red direccionan sus paquetes hacia su destino final, los routers los reconocen como paquetes especiales y los procesan con un código programado e implantado por ciertos usuarios autorizados.

Un ejemplo claro es un servicio de flujo multimedia *n* a *n* multicalidad de servicio sobre una internet a gran escala. Este servicio se requiere en aplicaciones de videoconferencia con terminales de capacidades o velocidades de acceso heterogéneas. Una opción válida es emplear codificación por capas y el servicio multidestino, dejando a IP la tarea de reducir ciegamente la tasa en enlaces congestionados. Esta solución impide prever con una cierta certeza la composición del contenido resultante y la tasa agregada de todas las *n* fuentes de tráfico. Una segunda solución complementaria más compleja, pero también más efectiva en términos de aprovechamiento del ancho de banda es realizar descarte inteligente de paquetes, transcodificación o selección de capas etc en los propios nodos de la red con receptores alcanzables en distintos enlaces. Esto permite adaptar el flujo agregado a las necesidades de un subárbol de receptores, controla la tasa utilizada e incluso evitar el reenvio de paquetes que no alcanzarán su destino debido a cuellos de botella posteriores. En este caso de aplicación activa con ubicación transparente, cada terminal puede enviar su flujo sin importarle qué nodos de la red procesarán su flujo.

Un segundo ejemplo es el servicio multidestino fiable, que puede llegar a ser escalable gracias a la retransmisión y agregación distribuida (evitando el conocido problema de la implosión de naks). Y lo mismo es aplicable a múltiples procesadores de paquetes disponibles en el mercado hoy: TCP spoofing, conmutación de capa 4, NAT, enmascaramiento de puertos, filtros de contenidos, etc, que constituyen de hecho, formas preconfiguradas estáticamente de procesadores activos transparentes.

IPv6 y las Redes Activas

Hay un obstáculo práctico importante a la implementación de transparencia de ubicación de nodos activos: la eficiencia global resultante en el router. ¿ cómo mantener las prestaciones de un router -optimizado para encaminar paquetes comprobando simplemente la dirección destino- si se requiere un tratamiento especial para los paquetes no direccionados explícitamente a él ?

Este problema no es nuevo. Una solución desarrollada para algunos protocolos de señalización que precisan la propiedad señalada es la opción Router Alert (RFC-2113) [2]. Como se describe en este documento, la opción router alert tiene la semántica: "los routers deben examinar este paquete con más atención (comprobar el campo de protocolo de la cabecera IP, por ejemplo) para determinar si es preciso o no procesamiento adicional ". Sólo las opciones no optimizadas en el *fast path* deben implicar el desvio del paquete al *slow path* y por consiguiente, en principio, no se deberían degradar las prestaciones sobre el resto de paquetes.

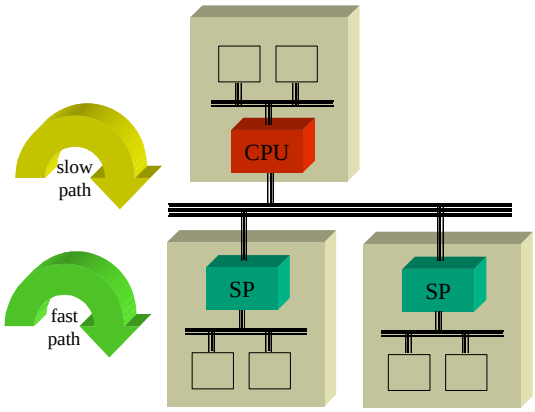
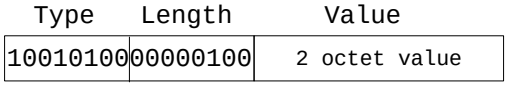


Figura 2. Flujo de datos optimizado y lento en una arquitectura multiprocesador

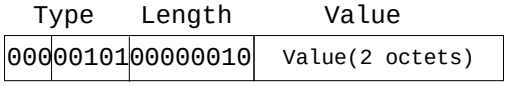
Entre los protocolos que utilizan actualmente esta opción se encuentran IGMPv2 (RFC-2236) [3] y RSVP (RFC-2205) [4]. En el primero, todos los mensajes deben incluir esta opción y la optimización se limita al router local. En el último, los mensajes de PATH, dirigidos a su destino final, son modificados en tránsito para capturar las características del camino origen-destino.

a) IPv4




```
Value:
     0 - Router shall examine packet
     1-65535 – Reserved
```

b) IPv6




```
Value:  A 2 octet code in network byte order with the following
      values:

         0        Datagram contains a Multicast Listener Discovery
                  message [RFC-2710].
         1        Datagram contains RSVP message.
         2        Datagram contains an Active Networks message.
         3-65535  Reserved to IANA for future use.
```

Figura 3. Formato de la opción Router Alert a) en IPv4 (RFC-2113) b) en IPv6 (RFC-2711)

En IPv6, Router Alert (RFC-2711) [5] es una opción salto a salto (*Hop-by-Hop*) con el mismo significado general que en IPv4. Sin embargo, a diferencia de IPv4, donde sólo se define el valor 0 (Figura 3.a), en IPv6 existen tres valores reservados, uno de ellos (valor 2) para mensajes de redes activas. Los otros están asignados a RSVP y a los mensajes de descubrimiento de receptores multidestino (MLD) [6] incluido en ICMPv6 (Figura 3.b).

Otra importante característica de IPv6 muy útil en redes activas es la etiqueta de flujo en la cabecera base. Su objetivo es evitar el análisis de campos de protocolos de capas superiores para realizar clasificación de paquetes en la red. Efectivamente, los paquetes de alerta son extremadamente útiles para programar el comportamiento de nodos a lo largo de un trayecto o dominio. La cabecera base de IPv6 es un lugar privilegiado para dicha etiqueta asignada por IPv6 en la máquina origen para los paquetes pertenecientes a un mismo flujo y preservada en su viaje por la red. Una vez identificado un par <dirección origen, etiqueta de flujo> por un paquete con router alert el nodo queda programado para proveer procesamiento ad-hoc para dicho flujo con las máximas prestaciones. En este sentido, las redes activas pueden emplearse como medio de implantación de protocolos de ingeniería de tráfico.

Para el caso de no desearse transparencia de ubicación, IPv6 también posee una interesante herramienta: la cabecera de ruta (*routing header*). Gracias al soporte ubicuo de este tipo de especificación de ruta desde fuente - además de los imprescindibles mécanismos de seguridad habilitándolo en la práctica – como un requisito de conformidad para todas las implementaciones de IPv6, es posible especificar qué nodos

activos implementarán el servicio. El requisito de que las respuestas de la máquina destino llevarán la misma cabecera de ruta es también importante para asegurar que las peticiones y respuestas de señalización de los protocolos activos seguirán una secuencia coherente de nodos

Arquitectura Router-Asistente

Hasta la fecha, la mayor parte del trabajo en redes activas ha sido bastante teórico y por consiguiente, sólo unas pocas ideas han derivado en productos industriales. Con el fin de dotar esta tecnología de un punto de vista más realista en un contexto industrial, se está desarrollando una plataforma experimental en el contexto del proyecto IST GCAP [7]. En este sistema, el código de usuario se carga dinámicamente en los nodos de la red mediante paquetes activos y soporte de transparencia usando la opción salto a salto de router alert de IPv6 ya mencionada. El entorno presupone que el código de usuario se ha validado antes de su habilitación y es almacenado en servidores accesibles mediante mecanismos de seguridad convencionales. El código se comparte por un flujo de paquetes dado y tiene un tiempo de vida dado, retemporizable por paquetes subsiguientes. Un concepto importante en esta arquitectura es el elemento *Router Assistant*, desarrollado en la universidad Carlos III de Madrid, conectado a un router IPv6 Ericsson Telebit AXI462. En este sistema, el router delega las funciones de procesado activo en un asistente presente en una red local de alta velocidad como si de un coprocesador externo se tratara.

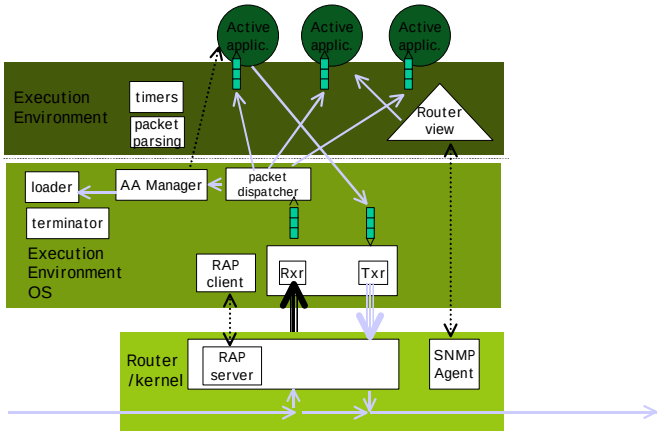


Fig. 4. Arquitectura Router-Asistente en un nodo activo

La Figura 4 muestra cómo las aplicaciones activas se cargan dinámicamente por los usuarios en un entorno de ejecución de un nodo de la red. Este nodo se compone de un motor de encaminamiento (un router) y una unidad de procesamiento de alto

nivel (un asistente). El sistema se controla por un módulo que realiza el papel de sistema operativo para las aplicaciones activas, filtrando y entregando paquetes al entorno. La principal ventaja de este sistema es un claro aislamiento entre las funciones normales del router y las activas.

Conclusiones

Las redes activas tienen un fuerte potencial en la próxima generación de redes comunicaciones, en la que la programabilidad de la red es fundamental. Y sus servicios nos son más cercanos de lo que parece: en la actualidad existen en el mercado diversos dispositivos de red con algunas funcionalidades de una red activa transparente, en el sentido amplio de su definición: conmutadores de capa 4-7, NAT, filtros, condicionadores de tráfico, etc, dispositivos, típicamente ubicados en la frontera de la red de acceso de una organización, pero con una flexibilidad menor de la provista por la tecnología de redes activas. Para llevar esto a la práctica es necesario la aplicación de mecanismos que preserven las prestaciones de los nodos de red, como la presentada en la sección anterior, y facilitada por las funcionalidades ofrecidas por IPv6 aquí detalladas.

Referencias

[1] D.L. Tennenhouse, J.M. Smith, W.D. Sincoskie, D.J. Wetherall and G.J. Minden. A Survey of Active Network Research. *IEEE Comunications Magazine*, pp. 80-86, January 1997.

[2] RFC-2113. IP Router Alert Option. D. Katz. February 1997.(Status: PROPOSED STANDARD)

[3] RFC-2236. Internet Group Management Protocol, Version 2. W. Fenner. November 1997. (Updates RFC1112) (Status: PROPOSED STANDARD)

[4] RFC-2205. Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification. R. Braden, Ed., L. Zhang, S. Berson, S. Herzog, S. Jamin. September 1997. (Updated by RFC2750) (Status: PROPOSED STANDARD)

[5] RFC-2711. IPv6 Router Alert Option. C. Partridge, A. Jackson. October 1999. (Status: PROPOSED STANDARD)

[6] RFC-2710. Multicast Listener Discovery (MLD) for IPv6. S. Deering, W. Fenner, B. Haberman. October 1999. (Status: PROPOSED STANDARD)

[7] Proyecto IST GCAP (Global Communication Architecture and Protocols for new QoS services over IPv6 networks) IST-1999-10 504.