tecnimap 2002
www.tecnimap.com
VII JORNADAS SOBRE TECNOLOGÍAS DE LA INFORMACIÓN PARA LA MODERNIZACIÓN DE LAS ADMINISTRACIONES PÚBLICAS
A CORUÑA
15, 16, 17 y 18 de octubre de 2002
Palacio de Congresos y de la Ópera
Ponencias

Repercusión de IPv6 en la Administración General del Estado

Maria José Lucas Vegas
Ingeniera Superior de Telecomunicaciones
Jefa de Proyecto de Sistemas Informáticos
Subdirección General de Planificación y Coordinación Informática
Ministerio de Trabajo y Asuntos Sociales

IP es un protocolo de paquetes utilizado para intercambiar tráfico de voz, datos, y video sobre redes de comunicaciones. Proporciona servicios de direccionamiento, fragmentación, recomposición y demultiplexado de protocolos. Es la base de los demás protocolos IP (tcp, udp, telnet, etc). Como protocolo de nivel de red contiene información de direccionamiento y control que permite encaminar paquetes, siendo su última versión IPv6.

La versión IP anterior, IPv4, tiene limitaciones importantes:

- Crecimiento excesivo en las tablas de direccionamiento de los routers
- Las clases de servicio están vagamente definidas y poco utilizadas. Las aplicaciones en tiempo real requieren de ciertas prestaciones de la red que hoy día no son factibles con la aplicación de IPv4.
- Agotamiento de las direcciones IPv4. Se espera que con la aparición de los dispositivos móviles, usuarios, etc, se produzca una demanda de direcciones que IPv4 no puede asumir.

- Complejidad en el tratamiento de las cabeceras del protocolo IPv4 dentro de los routers
- El soporte de seguridad dentro del propio protocolo es opcional

Nuevas funcionalidades de IPv6

Las nuevas funcionalidades que aparecen con la nueva versión del protocolo IP son:

- Autoconfiguración de las interfaces de red
- Soporte para encapsular protocolos.
- Clases de servicio que distinguen tipos de datos
- Autentificación y encriptación.
- Mecanismos de transición para la migración desde IPv4 a IPv6
- Simplificación de las cabeceras para una mayor eficiencia y rendimiento en el proceso de enrutamiento.
- Incremento en el espacio de direccionamiento.
- Etc.

A continuación vemos algunas de las nuevas funcionalidades:

1.- Direccionamiento: Se ha incrementado el espacio de direccionamiento para que sea suficiente para los próximos 30 años, de tal modo que se de soporte a dispositivos móviles (pda´s, teléfonos, coches, etc.) redes residenciales (HAN Home Area Networks) y servicios de datos inalámbricos, entre otros.

Se utilizan 128 bits en lugar de los 32 bits que se utilizaban en ipv4, siendo los tipos de direcciones los siguientes:

- Direcciones unicast. Son direcciones asignadas a un único interfaz. Se han definido direcciones especiales como son:

  - Dirección loopback (::1): se asigna a una dirección virtual a la que el host puede enviarse paquetes. La dirección equivalente de IPv4 es 127.0.01
  - Dirección inespecífica: esta dirección se utiliza como dirección de fuente durante el proceso de autoconfiguración. Equivale a la dirección 0.0.0.0 de IPv4
  - Direcciones compatibles(::<dirección IPv4>):se utilizan cuando se necesita enviar tráfico IPv6 a través de redes IPv4 mediante túneles. Los puntos finales de estos túneles pueden ser host o routers. Las direcciones de este tipo se forman añadiendo 96 bits a ´0´ delante de una dirección válida IPv4
  - Direcciones mapeadas a IPv4 (::FFFF:<dirección IPv4>): estas direcciones se utilizan cuando un host IPv6 quiere comunicar con un host IPv4. Esto requiere una pila doble de protocolos en el host o en el router para la traducción de cabeceras.
  - Direcciones de ámbito local: pueden utilizarse únicamente dentro de la red física a la que la interfaz del host está conectada.
  - Direcciones de ámbito privado: estas direcciones no pueden ser enrutadas a través de internet. Las direcciones equivalentes en IPv4 son: 10.0.0.0, 176.16.0.0-176.31.0.0,192.168.0.0-192.168.255.0.

  - Direcciones unicast globales. Se espera que lleguen a ser el formato de dirección predominante para la conexión de los nodos a internet

• Direcciones multicast: son identificadores asignados a un conjunto de interfaces en múltiples hosts. Los paquetes que se envían a una de estas direcciones se hacen llegar a todos los interfaces que tienen asignada esta dirección. No hay direcciones de broadcast en IPv6, ya que su funcionalidad queda asumida por las direcciones multicast. Algunas direcciones de propósito especifico son:

- FF01::1: todas las interfaces del host
- FF02::1 : todos los sistemas del ámbito local
- FF01::2 : todos los routers locales a un host dado
- FF02::2 todos los routers que pertenecen a la misma red de área local
- FF05::2: todos los routers dentro de un mismo ámbito privado
- FF02::B: agentes móviles dentro de la misma red de área local
- FF02::1:2: todos los agentes DHCP dentro de una misma red de área local.
- FF05::1:3 todos los servidores DHCP dentro de un mismo ámbito privado.

• Direcciones anycast: son un tipo especial de direcciones unicast que se asignan a interfaces en múltiples hosts. Los paquetes que se envían a esta dirección se hacen llegar a la interfaz más cercana que tenga esta dirección. Son direcciones experimentales.

Las direcciones IPv6 se representan como series de campos hexadecimales de16 bits separados por ":", con un formato x:x:x:x:x:x:x:x.

2.- Clases de tráfico

Se ha añadido un nuevo campo de 8 bits (clase de tráfico) que permite a las aplicaciones la especificación de una prioridad en el tráfico que generan.

3.- Etiquetas de flujo

IPv6 introduce el concepto de flujo, una serie de paquetes relacionados que van desde una fuente a un destino y requiriendo un procesamiento especial en los routers.

3.- Mecanismos de transición de IPv4 a IPv6: existirá un período de migración de Ipv4 a IPv6 donde coexistirán redes y hosts que funcionen con uno u otro protocolo. Al conjunto de modos de migración de IPv4 a IPv6 se le suele denominar SIT (Simple Internet Transition). La transición emplea los siguientes mecanismos:

- Implementación de un pila dual de IPv4 e IPv6 para los host y routers que deban de interoperar.
- Encapsulamiento de las direcciones IPv4 en IPv6. Los hosts serán asignados a direcciones IPv6 interoperables con IPv4 y los hosts con direcciones IPv4 serán mapeados a direcciones IPv6.
- Mecanismos de tunelación para transportar paquetes IPv6 sobre redes IPv4. Estos túneles pueden ser automáticos (con direcciones IPv6 compatibles con IPv4) o manuales.
- Traducción de cabeceras IPv4/IPv6 realizada por los routers. Se pretende que esta técnica se utilice cuando la implementación de IPv6 este muy avanzada y queden pocos sistemas IPv4.

Impacto de la nueva versión en las aplicaciones de la pila tcp/ip

Como ejemplos de aplicaciones tcp/ip que se verán afectadas por la nueva versión de IP podemos citar: ICMP, DNS y DHCP

1.- ICMPv6: Este protocolo realiza las mismas funciones que en IPv4: generación de errores de rutas, diagnósticos, etc. Con la versión 6 de IP, va a encargarse ademas de:

- Descubrimientos de vecinos: premite conocer las direcciones de ámbito local dentro de la misma subred, verificando ademas que los hosts o los routers de la misma siguen activos. Substituye al protocolo ARP (Address Resolution Protocol) de IPv4.
- Autoconfiguración de direcciones: dado que el campo de 128 bits de direcciones de IPv6 resuelve muchos problemas de IPv4, el tamaño en sí mismo de las direcciones puede representar un problema para el administrador de red. Por ello IPv6 ha sido diseñado con la capacidad de asignar automáticamente una dirección a una interfaz en tiempo de arranque, con la intención de que la red funcione con un mínimo de intervención por parte del administrador. Los nodos IPv6 normalmente utilizarán este procedimiento para obtener su dirección IPv6. El proceso funciona como sigue: durante el arranque del sistema, el nodo comienza la autoconfiguración obteniendo un token de su interfaz hardware, por ejemplo los 48 bits de la dirección MAC. El nodo crea una dirección unicast tentativa con ámbito de red de área local con el token obtenido. El nodo comprueba entonces que no existe en su red ningún nodo utilizando esta dirección, si fuese así el proceso se pararía y se configuraría manualmente. Si no hay ningún host en su red el nodo asigna la dirección tentativa a su interfaz. El host enviará ahora mensajes a la dirección multicast que designa todos los routers. Si existe algún router responderá con un mensaje de anuncio. Si no recibe ninguna respuesta intentará comunicarse con algún servidor DHCP para que le proporcione mas información de configuración. Si no obtuviera respuesta, el nodo continuaría con la dirección obtenida y comunicándose solo con aquellos nodos con los que comparte la misma red de área local.

- Descubrimiento de oyentes multicast (MLD Multicast Listener Discovery): es el proceso utilizado por un router para descubrir los miembros de un grupo multicast particular. Proporciona la funcionalidad que daba IGMPv2 en IPv4.

- Cálculo de la unidad de transferencia máxima: esta funcionalidad permite a un host ajustar el tamaño máximo del paquete a lo largo del camino a recorrer por el mismo.

2.- DNSv6

Con la introducción de las direcciones de 128 bits, IPv6 hace aún más difícil, para el usuario de red reconocer a otro usuario a través de su dirección IP.Se han definido una serie de extensiones a DNS para soportar el almacenamiento y la recuperación de las direcciones de Ipv6:

o un nuevo recurso de registro, AAAA, que mapea el nombre de dominio con la dirección de IPv6.

o Un nuevo dominio (IP6.int), que se utiliza para dar soporte a la búsqueda dirección-dominio.

o Un cambio en la definición de las consultas, de tal modo que sepan procesar de una manera adecuada los registros de tipo A (IPv4) y de tipo AAAA (IPv6).

3.- DHCPv6

Las diferencias con DHCPv4 son las siguientes:

- tan pronto como el cliente arranca, ya tiene una dirección ip disponible, que puede utilizar para comunicarse con un servidor DHCP.
- El cliente utiliza una dirección multicast para conectarse con el servidor en lugar de una dirección de broadcast.

- IPv6 permite el uso de más de una dirección ip por interfaz y DHCPv6 puede proporcionar más de una dirección ip cuando le es solicitado.
- No es necesaria la compatibilidad con BOOTP
- Aparece un nuevo mensaje de reconfiguración, que permite cambiar la parametrización de los hosts.

Impacto en las aplicaciones, hardware y software.

Aquellas unidades dentro de la Administración que quieran migrar de protocolo de nivel de red, deben de tener en cuenta que este cambio afectará tanto a las aplicaciones, como al hardware, al software, etc.

Más en concreto:

- Aplicaciones: se debería realizar un inventario de todas aquellas aplicaciones que presentan interfaces con el nivel de red e interaccionan con el mismo haciendo uso de las funcionalidades que proporciona, de tal modo que se verifique el impacto del cambio de direccionamiento, cabeceras de protocolo, impacto en los protocolos de transporte (udp, tcp), posibles cambios en los rendimientos de las aplicaciones, uso del cifrado por parte de las aplicaciones (IPv6 incorpora servicios de seguridad, por lo que no sería necesario implantar estos servicios en las aplicaciones), verificar el uso de aplicaciones tcp/ip como tcp, udp, dns; que funcionan basándose en ip, etc. Podemos entender como aplicaciones, tanto las desarrolladas por las propias unidades, como todas aquellas relacionadas con la gestión de red, gestión de almacenamiento, correo electrónico, VoIP, gestión de equipos, etc.

- Hardware: dado que las máquinas trabajarán con un nuevo protocolo puede ser necesario hacer un upgrade por razones de rendimiento de aplicaciones, incremento en el tráfico cursado durante la época de transición de IPv4 a IPv6, soporte de nuevos protocolos, etc. Este upgrade podría consistir en un incremento,

dentro de los equipos, de la cpu, la memoria, los adaptadores de red, los tipos y la velocidad de líneas a la que se conectan (fibra, ethernet, cable, cobre, etc), etc.

- Software: al incluir un nuevo protocolo puede ser necesario hacer un upgrade de las máquinas a nivel de software de base, con el impacto que esto puede suponer en las aplicaciones que funcionan sobre este software. Además de esto, habría que planificar los cambios de direcciones ip de las máquinas, revisar el diseño de las redes (routers con doble pila de protocolos, firewall, NAT, DNS, etc), planificar los cambios, plantear la posibilidad de que convivan sistemas con IPv4 e IPv6 así como la resolución de los problemas que esto pudiera plantear, etc.

- Ficheros de carácter personal: en la normativa asociada (Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal y el Reglamento de medidas aprobado por el Real Decreto 994/1999, etc) se describen qué son los datos de carácter personal, su tipología, su registro en la Agencia de Protección de Datos, la cesión o comunicación de datos, etc. Si nos centramos en el soporte tecnológico que hace posible la implementación de las medidas de seguridad mínimas establecidas en el Reglamento, se deberían revisar todos los procedimientos relacionados con el control de accesos, gestión de soportes, copias de respaldo y recuperación, auditorías, identificación y autentificación, cifrados de datos en las redes de comunicaciones, etc, de tal modo que quede garantizada la protección de los datos personales. Además, IPv6 permite que un usuario puede tener asignada una dirección ip fija, con lo cual habría que tratar esta dirección ip como un dato de carácter personal (con sus medidas de seguridad asociadas) dado que identifica de manera unívoca a una persona en concreto

Por último, si varias unidades administrativas quisieran comunicarse a través de ip, habría que tener en cuenta el nivel de implantación de IPv6 que tengan en sí mismas así como los servicios que quisieran compartir, prestar, etc.