Guillermo Cicileo
Roque Gagliano
Christian O´Flaherty
César Olvera Morales
Jordi Palet Martínez
Mariela Rocha
Álvaro Vives Martínez

IPv6 para Todos

Guía de uso y aplicación para diversos entornos

Internet Society™ | Capítulo Argentina

IPv6 para Todos

Guillermo Cicileo
Roque Gagliano
Christian O'Flaherty
César Olvera Morales
Jordi Palet Martínez
Mariela Rocha
Álvaro Vives Martínez

IPv6 para Todos

Guía de uso y aplicación para diversos entornos.

Internet Society™ | Capítulo Argentina

IPv6 para todos / Christian O'Flaherty ... [et.al.]. - 1a ed. - Buenos Aires : Asociacion Civil Argentinos en internet, 2009.
E-Book.

ISBN 978-987-25392-1-4

1. Informática. 2. Internet. I. O'Flaherty, Christian
CDD 004.678

Diseño de cubierta: DCV Anahí Maroñas
Diseño de interior: DCV Anahí Maroñas

1ª edición Octubre 2009

ISBN 978-987-25392-1-4

Queda hecho el depósito que establece la Ley 11.723

Agradecimientos

A **Internet Society** (www.isoc.org.) por haber donado los fondos que han permitido la realización de este Proyecto y su constante apoyo para estimular la continuidad y relevancia de los Capítulos.

A los miembros del **Proyecto 6DEPLOY** (www.6deploy.eu) por su colaboración en el contenido del presente libro y su constante trabajo brindando soporte en el despliegue de IPv6 mediante documentos, formación y mesa de ayuda virtual.

A **LACNIC** (www.lacnic.net) por sus aportes al contenido de este libro y, su colaboración en la traducción del mismo así como también por las tareas de capacitación orientadas a la toma de conciencia, que en torno a IPv6 vienen desarrollando en Latinoamérica y Caribe.

A todos los **autores**, **colaboradores** y **diseñadora** que han posibilitado con su dedicación y trabajo la concreción de este Proyecto, que tiene por objeto contribuir a la Comunidad de Internet en la adopción e implementación del nuevo Protocolo IPv6.

La Comisión Directiva
Capítulo Argentina de Internet Society – ISOC-Ar

Índice

1. Introducción 13

2. Usuario Final 19
Introducción 21
Instalación de IPv6 21
Comprobación de IPv6 28
Configuración avanzada de IPv6 35
Mecanismos de transición con IPv6 39
Desinstalación de IPv6 41

3. Home Office (redes residenciales) 43
Introducción 45
¿A qué se denomina "SOHO"? 45
Construyendo un SOHO con IPv6 45
Identificando las partes de un SOHO 46
Determinando los componentes que requieren configuración 47
Configurando los componentes del SOHO con IPv6 48
Referencias 48

4. Servicios 59
Introducción 61
Sobre servicios 61
Telnet 61
SSH 63
FTP 64
Mail 65
Transmisión Multimedia 67
Web 70
DNS 77
Clientes 93
Referencias 94

5. Empresas 95
Introducción a redes empresariales 97
Tareas previas para una implementación de IPv6 98
Planificando IPv6 en redes empresariales 100
Transición a IPv6 en una red empresarial y agotamiento de IPv4 107

6. Entorno académico y de investigación 109
Introducción 111
¿Por qué y para qué se utiliza IPv6 en educación e investigación? 111
Redes académicas en el mundo 114
Desplegando IPv6 en la universidad/centro de investigación 119
Consideraciones adicionales 128
Conclusiones 129

7. Proveedor de Servicio de Internet (ISP) 131
A quién está dirigido el Capítulo 133
Componentes del servicio 135
Implementación de IPv6 en la red 137
Como recibir bloques IPv6 del registro regional 138
Plan de numeración 139
Conclusiones 149

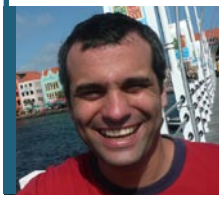
8. Epílogo 151

Autores

Guillermo Cicileo

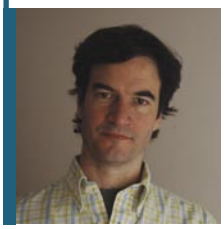
Se desempeña actualmente como Coordinador General de la RIU, red de las universidades nacionales de Argentina. Forma parte del comité de evaluación del FLIP6 - Foro Latinoamericano de IPv6 desde 2007 a la actualidad. Ha participado activamente de la creación de CLARA (Cooperación Latinoamericana en Redes Avanzadas), siendo miembro de la Comisión Técnica inicial del proyecto. Posteriormente tuvo a su cargo la coordinación del Grupo de Trabajo de Multicast de RedCLARA desde 2005 hasta 2008 y miembro de los grupos de trabajo de IPv6 y Ruteo Avanzado. A su vez ha sido instructor en los workshops de enrutamiento avanzado organizados por CLARA, dictando capacitaciones sobre multicast, IPv6 y BGP entre otros temas. Anteriormente fue vice-director de la red RETINA, teniendo a su cargo las áreas de Operaciones y Nuevas Tecnologías. Como parte de su actividad, llevó adelante la implementación de IPv6 en la red en forma nativa, tanto en su conectividad internacional como en su despliegue a nivel nacional. Su actividad laboral ha estado ligada a las redes científico y académicas a nivel nacional e internacional, desempeñándose en esas áreas durante mas de 15 años. Como parte de su trayectoria, dirigió la primera conexión de Argentina a Internet2 y Redes Avanzadas, así como la incorporación del país a la RedCLARA.

Roque Gagliano



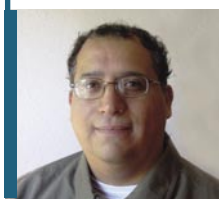
Con más de 10 años de experiencia en redes IP. Actualmente se desempeña como Ingeniero Senior de Proyectos y Responsable del área de política de LACNIC, el registro de Internet para América Latina y el Caribe. Sus responsabilidades incluyen la coordinación de proyectos técnicos y la gestión del proceso de desarrollo de políticas de asignación de recursos en la región de LACNIC. Participa también como instructor y expositor IPv6 de LACNIC para América Latina. Su experiencia en IPv6 abarca también el diseño de la solución para la red corporativa de LACNIC en Montevideo y de la red de servidores críticos en Brasil. Ha participado también en el lanzamiento de las primeras conexiones IPv6 en países o territorios como Haití, Saint Maarten, Curaçao y Trinidad y Tobago. Dentro de sus tareas también es activo dentro del IETF, particularmente en los grupos referidos a IPv6 e intercambio de tráfico. Anteriormente se desempeñó como Arquitecto de redes en ANTEL, Uruguay, diseñando la solución IPv6 para su red basada en tecnología MPLS. Previamente trabajó para Sprint Nextel Corp. en Estados Unidos. El Sr. Gagliano cuenta con una Maestría en Ingeniería Eléctrica de la Universidad de Kansas en EE. UU. y es Ingeniero Eléctrico de la UDELAR, Uruguay. Ha sido seleccionado como escolar Fulbright y de la OEA y es miembro de la IEEE.

Christian O'Flaherty



Licenciado en Ciencias de la Computación egresado de la Universidad Nacional del Sur, Bahía Blanca, Argentina. Su carrera profesional se inicia como docente en las materias Sistemas Operativos y Redes y Teleprocesamiento de Datos para luego dedicarse a la operación y planeamiento de red en la red Académica Nacional, Retina. Luego, como responsable de operaciones de Internet en Impsat Argentina, un proveedor de servicios Satelitales que evolucionó hasta convertirse en un proveedor regional de servicios IP. En el año 2006 la empresa fue adquirida por Global Crossing donde Christian se desempeñó como responsable de Producto Internet hasta el año 2009. Ese año, asume el cargo de Senior Education Manager en Internet Society, cargo que desempeña hasta la actualidad. Desde el año 2004 al 2008 se desempeñó como moderador de lista de políticas y Chair del foro público de políticas de Lacnic. En la actualidad, miembro de la comisión directiva en ISOC Argentina y en IPv6 Task Force Argentina.

César Olvera Morales

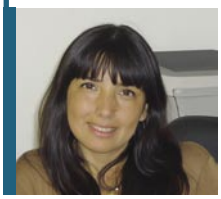


Físico por la Universidad Nacional Autónoma de México (UNAM), En 1998-2002 trabajó en DGSCA-UNAM, donde fue coordinador del Laboratorio de Interoperabilidad, realizando investigación y pruebas en IPv6, QoS, Multicast, MPLS, etc., organizando conferencias y seminarios sobre esas tecnologías, y ser conferencista en eventos nacionales e internacionales. En 2002 entró a Consulintel donde participa en varios proyectos IST y PROFIT, centrando sus tareas en investigación, pruebas, diseño e instalación de redes IPv6 en aspectos como encaminamiento, PLC, QoS, Multicast, MPLS, VPN, Seguridad, etc. Ha colaborado con ETSI, IPv6 Forum, Spirent, Agilent, Ixia, etc., en el diseño y conducción de pruebas de interoperabilidad, conformidad y prestaciones en dispositivos IPv6; y con grupos de trabajo de IPv6 de la IETF. También ha impartido formación en IPv6 en Latinoamérica y África.

Jordi Palet Martínez

Ha trabajado en computadores, redes y telecomunicaciones durante los últimos 25 años y en la actualidad es el CEO/CTO de Consulintel. Su experiencia. Su experiencia incluye programación en diferentes lenguajes, porting de Sistemas Operativos, diseño de circuitos electrónicos y microcomputadores, consultoría, implementación y diseño de redes. Implicado desde hace varios años en actividades de IETF, ISOC, ICANN, IPv6 Forum, IPv6 Cluster, IPv6 Task Forces y los RIRs, frecuentemente ofrece talleres de formación al respecto de IPv6 en todo el mundo y es autor de numerosos artículos, libros y documentos al respecto de IPv6. Ha dirigido y/o participado en numerosos proyectos de investigación, desarrollo e innovación, la mayoría de los cuales relacionados con IPv6 como 6SOS, Autotrans, Euro6IX, Eurov6, 6POWER, 6QM, 6LINK, ENABLE, RiNG and PlaNetS. Además de IPv6, ha trabajado en tecnologías relacionadas con PLC/BPL, movilidad IP, seguridad y routing, entre otras entre otras. Es ponente habitual en conferencias y eventos relacionados con IPv6, y forma parte de numerosos comités, incluyendo el de evaluación de FLIP6 (Foro Latinoamericano de IPv6) desde su inicio. Colabora estrechamente en tareas de divulgación y formación de IPv6 con AfriNIC, APNIC, ARIN y LACNIC.

Mariela Rocha



Se ha graduado como Ingeniera en Sistemas de Información en la Universidad Tecnológica Nacional de Argentina, y desde entonces se ha abocado a las nuevas tecnologías y a la ingeniería de redes, fundamentalmente en el ámbito académico. Comenzó a trabajar con IPv6 en el año 2003, participando en workshops y capacitaciones de Florida International University (FIU), cuando se desempeñaba en la Red Teleinformática Académica (RETINA), donde contribuyó a consolidar el despliegue de IPv6 en la red nacional.
Ha dictado numerosas capacitaciones sobre IPv6 para Universidades de Argentina, Proveedores de Servicios y otros organismos como NAP CABASE. También se ha desempeñado como expositora sobre el tema en la región de América Latina.
Desde el año 2006 es la coordinadora del Foro Latinoamericano de IPv6 y de la IPv6 Task Force de América Latina y el Caribe.
En la actualidad, es la coordinadora técnica en la Red de Interconexión Universitaria, donde dedica su experiencia al despliegue de nuevas tecnologías sobre la red de Universidades Nacionales de Argentina.

Álvaro Vives Martínez

Es ingeniero superior de telecomunicaciones en la especialidad de telemática por la Universidad de Vigo. Tras la participación en un proyecto de I+D europeo relacionado con la TV digital y el desarrollo de un Set-top Box DVB-MHP y de trabajar como profesor invitado en dicha Universidad paso a trabajar en Consulintel en 2002. En Consulintel ha participado en diversos proyectos de I+D a nivel español y europeo relacionados con IPv6: 6SOS, Euro6IX, 6POWER, 6QM, Eurov6, ENABLE, RiNG y 6DEPLOY. Ha estado al cargo de servicios de producción (DNS, http y FTP entre otros), gestión de redes, desarrollo de aplicaciones, impartido cursos y charlas, trabajado en proyectos de consultoría en Europa, Latinoamérica y África y realizado labores de estandarización en el IETF, todo ello relacionado con IPv6.

1. Introducción

1.1. La situación actual

Como es ya de amplio conocimiento, el conjunto de direcciones IPv4 que aún se encuentran bajo la administración de IANA (www.iana.net) y que no han sido asignadas a los Registros Regionales de Internet, se reduce a un ritmo significativo y su terminación se acerca rápidamente. En otras palabras, el sistema global de direcciones de Internet se está agotando.

El protocolo actual (Internet Protocol versión 4 o IPv4) dispone de aproximadamente 4 mil millones de direcciones y, debido al enorme éxito de Internet, se espera que se agote en los próximos años.

Es claro que muchas de las direcciones IPv4 que figuran como asignadas, no están siendo utilizadas por diversas razones. Durante algún tiempo, se pensó –y aún hay quienes lo sostienen- que mediante la optimización del uso de las direcciones IPv4, la recuperación de direcciones no utilizadas y el incremento de uso de tecnologías tipo NAT (del Inglés "Network Address Translation" o Traducción de Direcciones de Red), se podía resolver la demanda de direcciones IP, sin la necesidad de adoptar una nueva versión del Protocolo de Internet.

Gradualmente esta idea se ha ido desvaneciendo, en la medida que se ha ido viendo la enorme cantidad de dispositivos que necesitarán, en el mediano plazo, sus propias direcciones IP para conectarse a Internet, mucho de los cuales necesitarán, incluso, varias direcciones. Aún en el caso de una utilización más óptima de las direcciones IP, las más de 4 mil millones de direcciones que el protocolo IPv4 permite, no serán suficientes.

Es importante además destacar, que si bien NAT ha permitido, hasta el momento, el crecimiento de Internet, conlleva la pérdida de la conectividad extremo a extremo, y por tanto dificulta el despliegue de aplicaciones y servicios extremo a extremo (cliente a cliente), haciendo mas complejo y costoso el desarrollo de dichos servicios y aplicaciones y por tanto impidiendo la innovación en la Red.

El nuevo protocolo IPv6, dispone de 340 billones de billones de billones (sextillones) de direcciones, lo que hace que la cantidad de direcciones IPv4 parezca insignificante. Con este mayor espacio de direcciones, IPv6 ofrece una variedad de ventajas en términos de estabilidad, flexibilidad y simplicidad en la administración de las redes. También es probable que la *"Era IPv6"* genere una nueva ola de innovación en las aplicaciones y las ofertas de servicios ya que, termina con la necesidad de direcciones compartidas.

IPv6 se está implementando lentamente en redes y coexistirá con IPv4 por muchos años en esta transición. Si bien el trabajo técnico relacionado con el protocolo, en gran medida, se ha completado, lo que resta mayoritariamente es su despliegue en las redes de los proveedores de servicios de Internet.

1.2. En el camino correcto en Latinoamérica y Caribe

El camino de la adopción y promoción de IPv6 ha sido un camino lento, pero en ningún momento se ha dejado de avanzar.

En el año 2005 por ejemplo, LACNIC, el Registro de Direcciones de América Latina y Caribe, organizó por primera vez el *"IPv6 Tour"*, que consistió en 10 eventos realizados en igual cantidad de países de la región. En estos eventos participaron alrededor de 3.500 personas. Eran eventos de "evangelización" en los cuales se partía de la base de que los participantes no tenían ningún conocimiento. La situación, cuatro años después, es muy diferente.

LACNIC ha organizado con sus propios recursos y junto con otros socios del Proyecto 6DEPLOY -proyecto co-financiado por la Comisión Europea- actividades de entrenamiento en más de una decena de países donde han participado más de 800 personas. La diferencia sustancial es el tipo de actividades que se organizan. Ya no es necesario explicar que es IPv6, sino que se trabaja en talleres con aspectos prácticos de la implementación de IPv6. Muchas personas ya salen de estos talleres preparados para concretar los planes de adopción de la nueva versión del protocolo IP en sus organizaciones y a solicitar direcciones IPv6 a LACNIC. Esta es una maquinaria que ya está andando.

Hoy existen puntos de intercambio de tráfico (IXPs) en al menos 6 países de Latinoamérica y Caribe que brindan servicios sobre IPv6 en forma nativa en su infraestructura. El 75 % de los ccTLDs (country codes Top Level Domains) resuelven el DNS de los dominios de sus países sobre infraestructura IPv6 a través de, al menos, uno de sus servidores primarios y/o secundarios.

En los primeros 9 meses del 2009, más de 60 organizaciones y empresas de Latinoamérica y Caribe han recibido sus bloques de direcciones IPv6, lo cual supera ampliamente las 47 asignaciones hechas en todo el año 2008 por LACNIC y los registros nacionales de México y Brasil.

Hay operadores que ya brindan servicios bajo IPv6 a sus clientes y así podríamos continuar listando diversos hechos e indicadores que muestran el avance en la consolidación del camino de transición hacia IPv6.

A nivel de foros gubernamentales también ha habido progresos importantes. Temas relativos a IPv6 forman parte habitual de la agenda de organizaciones como CITEL (Comi-

sión Interamericana de Telecomunicaciones), de la CTU (Caribbean Telecommunication Union) y de otros foros gubernamentales destacándose incluso algunas resoluciones que muestran el compromiso de los gobiernos de participar en la promoción de IPv6 y comenzar con la adopción del nuevo protocolo en su propias infraestructuras.

¿Es esto suficiente? Claramente no, pero como se mencionaba anteriormente, estos elementos dan la sensación de estar en el camino correcto.

Nos encontramos en un momento en el que, al quedar solo un 10% de las direcciones IPv4 en el repositorio central que administra la IANA, es claro que hay que acelerar el paso y avanzar con más decisión en el camino iniciado, ya que todo lo que no se haga pronto, causará costos mayores más tarde.

El trabajo de organizaciones como LACNIC y la Internet Society (ISOC) contribuyen de manera fundamental a la mitigación de las posibles consecuencias negativas de la transición a IPv6. En última instancia, IPv6 es necesario para la continuidad, la estabilidad y la evolución de Internet.

"IPv6 para Todos" tiene como objetivo fomentar la utilización de IPv6 en los entornos más comunes aportando el conocimiento y la experiencia necesaria para que más gente y organizaciones obtengan logros, en el corto plazo, que los ayude a llevar adelante este proceso. **"IPv6 para Todos"** presenta ejemplos prácticos de configuración para que los lectores puedan experimentar la utilización del nuevo protocolo siguiendo las pautas de configuración planteadas.

1.3. ¿Qué es ISOC?

Internet Society (ISOC) es una organización internacional independiente sin fines de lucro que tiene sus oficinas centrales en Ginebra, Suiza y en Reston, Virginia, Estados Unidos. ISOC actúa como centro de intercambio de información global de información técnicamente confiable y objetiva acerca de Internet, como proveedor de educación y también como facilitador y coordinador de iniciativas relacionadas con Internet en todo el mundo. Aporta la base organizacional para el IETF (Internet Engineering Task Force), el IAB (Internet Architecture Board) y el IRTF (Internet Research Task Force).

La ISOC se fundó en 1992 para brindar liderazgo en estándares, educación y políticas relacionadas con Internet. Cuenta con el respaldo de una activa red mundial de miembros que ayudan a promover y lograr la misión de la ISOC por toda la comunidad de Internet y por todo el mundo. La Sociedad tiene más de 80 miembros institucionales y más de 28.000 miembros individuales en más de 80 Capítulos que contribuyen a regionalizar el alcance de las iniciativas en tecnología, educación y políticas de la ISOC.

El sitio web de Internet Society es: http://www.isoc.org.

1.4. El Capítulo Argentina de Internet Society

Los Capítulos de Internet Society son grupos conformados por personas que, residiendo en una región geográfica en particular (como por ejemplo una Ciudad o un País) o compartiendo un interés específico sobre temas relativos a Internet, se organizan voluntariamente y deciden llevar adelante distintas actividades, como miembros de ISOC, alineados con las metas y principios de la organización.

En Argentina, el Capítulo Argentina de ISOC (ISOC-Ar) es una organización civil sin fines de lucro, independiente y democrática, que funciona en el marco de la Asociación Civil de Argentinos en Internet. Fundada en el año 1999, ha obtenido su inscripción como persona jurídica mediante Resolución IGJ N° 297/2000, y tiene entre sus objetivos promover el desarrollo abierto y la evolución de la red Internet, sus servicios y contenidos para el beneficio de toda la gente, en particular de los habitantes de la República Argentina, mediante la promoción de actividades de la comunidad mundial de Internet propendiendo a la estrecha comunicación y acercamiento de los miembros de la Internet Society que residan en el país.

Alineados con la misión y objetivos de Internet Society, los miembros de ISOC-Ar hemos venido desarrollando en forma constante distintas actividades orientadas a afianzar los Principios Guía. Así, por ejemplo, desde el año 2007 llevamos a cabo las Jornadas de Accesibilidad: "Por una web sin barreras para personas con discapacidad", donde se exponen y debaten temas referidos a las dificultades que las personas con discapacidad, deben enfrentar para poder utilizar Internet y las buenas prácticas vigentes en la materia, tendientes a reducir esa brecha. También a través de la participación en diferentes eventos y seminarios o como co-organizador del Día de la Usabilidad realizado en Noviembre de 2008 o mediante la ejecución de proyectos financiados por la Internet Society.

1.4.1. Community Grants Programme (Programas de Subvenciones a la Comunidad)

Dentro de las actividades que la ISOC promueve para sus miembros y Capítulos, es el desarrollo del Programa de Subvenciones a la Comunidad.

Estos programas tienen como objetivo otorgar apoyo económico que permita el desarrollo de proyectos cuya propuesta sirva para:

- Mejorar la misión y las metas de ISOC, en especial aquellas alineadas con las Iniciativas Estratégicas y Principios de ISOC;
- Brindar servicios a las comunidades de los Capítulos;
- Fomentar el trabajo de colaboración entre los Capítulos o los miembros individuales;
- Mejorar y utilizar los conocimientos que se comparten en la comunidad global de Internet; y
- Estimular la continuidad y la relevancia de los Capítulos.

1.4.2 El Proyecto "IPv6 para Todos"

El presente libro, nació con el objeto de poder brindar a la comunidad de Internet, tanto local como global, un manual que facilite las herramientas necesarias para impulsar y fomentar la adopción del protocolo IPv6 en los diferentes entornos, motivados, además, por las preocupaciones que respecto a su adopción tardía, ciernen al tema.

Orientado en Capítulos para cada entorno específico, **"IPv6 para Todos"** explica de una manera clara y exenta de tecnicismos innecesarios, los pasos y requerimientos para configurar e implementar la nueva versión del Protocolo IP en ámbitos tan variados como son las Redes Residenciales, Redes Académicas, Empresas, Proveedores de Servicios de Internet (Internet Service Providers o "ISPs"), Usuarios Finales o Servicios.

El presente Proyecto ha sido posible gracias al apoyo financiero de la Internet Society, permitiéndonos materializar una idea sobre la cual ISOC-Ar venía trabajando hacía varios años. Por su parte, el contenido del libro ha contado con la colaboración de expertos tanto locales como internacionales en el tema, que han brindado sus conocimientos y experiencia para contribuir en este lento, pero inexorable camino hacia la adopción de IPv6.

Mónica Abalo Laforgia
Presidenta del Capítulo Argentina de Internet Society

Sebastián Bellagamba
Manager - Oficina Regional para América Latina
y el Caribe de Internet Society

Raúl Echeberría
Director Ejecutivo de LACNIC
Miembro de la Junta de Directores de Internet Society

2. Usuario final

1. Introducción

En este capítulo se realiza una introducción a la instalación y configuración básica de IPv6 en diferentes plataformas de usuario final (sistemas operativos).

Se contemplan los siguientes sistemas operativos:

- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008
- Windows 7
- Windows 2000
- Mac OS X
- Linux
- BSD

Obsérvese, que dado el gran número de versiones existentes en algunos casos, y especialmente en el de Linux y BSD, se presentan ejemplos genéricos, y por tanto, puede haber pequeñas diferencias dependiendo de la versión concreta, que habrán de ser dirimidas por el lector, con ayuda de documentación propia del sistema operativo que se trate.

2. Instalación de IPv6

La mayor parte de los sistemas operativos, desde el año 2001 aproximadamente, tienen algún tipo de soporte de IPv6.

Es cierto, que en algunos casos, inicialmente no se trataba de un soporte "comercial", sino versiones de prueba, aunque se incorporaban a sistemas operativos de "producción".

Tal es el caso del soporte de IPv6 en Windows 2000 (incluso en versiones anteriores de Windows NT, que por su antigüedad no describiremos en este documento), e incluso en la primera versión de Windows XP, antes del lanzamiento del denominado Service Pack 1 (SP1).

Cada vez es más frecuente que diversas plataformas o sistemas operativos, no solo incorporen IPv6, sino que además sea activado por defecto por el fabricante, sin requerir intervención alguna por parte del usuario.

Lo expuesto es válido no solo para sistemas operativos de computadores de sobremesa y portátiles, sino también para otros dispositivos que utilizan los mismos sistemas operativos, o versiones reducidas de los mismos, por ejemplo teléfonos celulares, agendas electrónicas, plataformas de juegos, etc. Es cierto, lógicamente, que en algunos casos, dichas versiones reducidas de los sistemas operativos, no incorporan todas las funcionalidades del sistema operativo original, y por tanto, se podría dar el caso de no poder acceder a todos las funciones que se mostrarán para la configuración y prueba de IPv6.

2.1 Instalación de IPv6 en Windows

Sin duda, una de las más completas pilas IPv6 es la existente en las plataformas Windows mas recientes:

- Windows XP SP1 y posteriores
- Windows Server 2003
- Windows Vista
- Windows Server 2008
- Windows 7

Como se ha indicado antes, algunas plataformas Windows, inicialmente sólo eran desarrollos "de prueba" (Technology Preview), por tanto tienen una funcionalidad mas limitada, y carecen de soporte por parte del fabricante:

- Windows XP sin SP
- Windows 2000 hasta SP1 (inclusive)

Existe también una versión para desarrolladores de Windows NT 4.0, en los detalles de la cual no entraremos en este documento.

Finalmente, existen productos de terceros, sin soporte por parte de Microsoft, para:

- Windows 95/98/ME
- Windows 2000 con SP2 y posteriores

En general, las características soportadas, algunas sólo en las últimas versiones, son:

- Autoconfiguración
- Túneles 6in4
- Túneles 6to4
- Relé 6to4
- Túneles TEREDO
- Túneles ISATAP
- IPsec (llaves manuales)

2.1.1 Instalación en XP/2003

En realidad podríamos decir que IPv6 ya esta instalado tanto en Windows XP como en Windows Server 2003, y por tanto, mas que instalación hablamos de activación.

Existen dos procedimientos para habilitar IPv6 en estas dos plataformas:

2.1.1.1 Línea de Comandos

En una ventana DOS ejecutar: **ipv6 install**

Tras unos segundos, un mensaje de confirmación nos indicara la correcta instalación.

También se podría utilizar, dependiendo de la versión**: netsh interface ipv6 install**

2.1.1.2 Interfaz gráfica

A través del entorno gráfico o panel de control, llegar hasta "Conexiones de red", seleccionar la "red de área local" o "red inalámbrica", "Propiedades" con el pulsador derecho del ratón y a continuación pulsar sobre "instalar", "protocolo" y seleccionar "Microsoft TCP/IP version 6".

El resultado será similar al mostrado en la siguiente captura de pantalla:

FIGURA 1: **CAPTURA DE PANTALLA DE INSTALACIÓN DE IPV6 EN XP/2003**

2.1.2. Instalación en Vista/2008

Desde el lanzamiento de Windows Vista, este sistema operativo incluye soporte de IPv6 instalado y habilitado por defecto.

Por lo tanto, no es necesario hacer ninguna configuración adicional. En caso de que se hubiera desactivado, se podría utilizar el procedimiento con netsh o entorno gráfico indicado para Windows XP/2003.

Téngase en cuenta que para usar netsh, se requiere una ventana de DOS explícitamente abierta con permisos de administración.

En comparación con XP/2003, IPv6 en Vista tiene funcionalidades adicionales, como por ejemplo:

- Soporte completo IPsec
- MLDv2
- Link-Local Multicast Name Resolution (LLMNR)
  - No requiere un servidor DNS. Los nodos IPv6 en un segmento piden el nombre a una dirección IPv6 multicast. Similar al funcionamiento de NetBIOS.
- Soporte de direcciones IPv6 en URLs
- IPv6 Control Protocol (IPV6CP - RFC5072)

- IPv6 sobre PPP
- DHCPv6, en el cliente y el servidor
- Identificador de Interfaz aleatorio por defecto (RFC3041)
- Teredo soporta NATs simétricos
  - Activo por defecto. Solo se utiliza si la aplicación requiere soporte IPv6 y no esta disponible de forma nativa.

Se puede comprobar que esta instalado, por medio de comandos o con el entorno gráfico, de forma similar a lo indicado para el caso de XP:

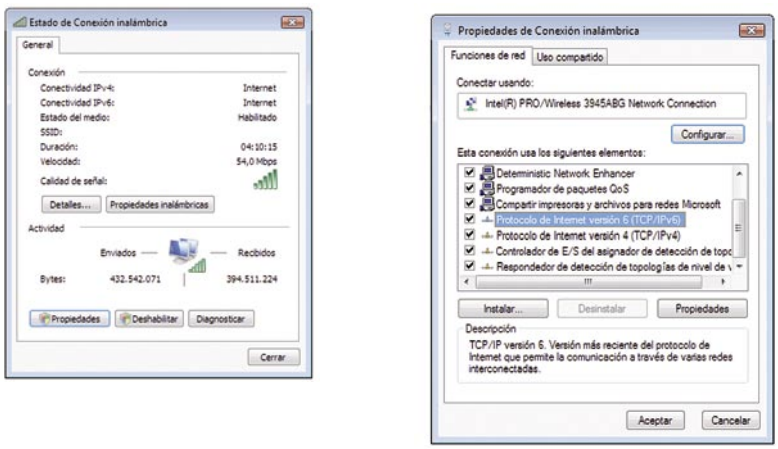


FIGURA 2: **PROPIEDADES DE CONEXIÓN DE RED E INSTALACIÓN DE IPV6 EN VISTA**

2.1.3. Instalación en Windows 7

Igual que en el caso de Vista/2008, Windows 7 incorpora IPv6 instalado y habilitado por defecto. Igualmente, en caso de que se hubiera desactivado, se podría utilizar el procedimiento con netsh o entorno gráfico indicado para Windows XP/2003.

Téngase en cuenta que para usar netsh, se requiere una ventana de DOS explícitamente abierta con permisos de administración.

Las características de esta versión se pueden resumir en:

- Soporte IPv6 similar al de Vista y Server 2008
  - IPsec, MLDv2, LLMNR, IPv6 en URLs, IPV6CP, IPv6 sobre PPP, DHCPv6, Teredo
  - Cambia: Identificador de Interfaz aleatorio por defecto (RFC3041)
    - No usa EUI-64 por defecto para el identificador de interfaz en las direcciones autoconfiguradas.

- Nuevas mejoras
  - IP-HTTPS (IP over Secure HTTP)
    - permite a los hosts atravesar un servidor proxy o firewall y conectarse a redes privadas por medio de IPv6 dentro de un túnel HTTPS. HTTPS no provee seguridad

a los datos, es necesario usar IPsec para dar seguridad a una conexión IP-HTTPS. Más información en *http://msdn.microsoft.com/en-us/library/dd358571.aspx*

- DirectAccess
  - Permite a los usuarios conectarse de manera transparente a la red corporativa sin establecer específicamente una conexión VPN. También permite al administrador de red seguir en contacto con los host móviles fuera de la oficina, y poder hacer actualizaciones y dar soporte a dichos equipos. Es una arquitectura donde un cliente IPv6 se comunica con un servidor IPv6 en la red corporativa. También se pueden usar conexiones desde Internet IPv4 empleando 6to4, Teredo e ISATAP. También se puede usar IP-HTTPS. DirectAccess usa túneles IPsec para proveer seguridad a la autenticación y al acceso de recursos.
  - El cliente puede ser un Windows 7 o Server 2008. El servidor puede ser un Server 2008

Igual que en el caso de Vista, se puede comprobar que esta instalado, mediante el entorno gráfico:

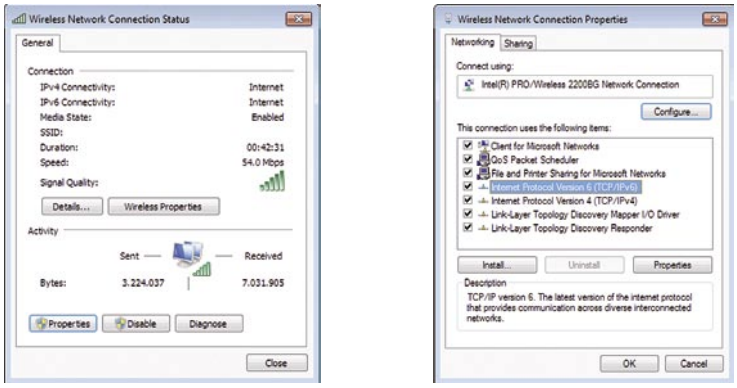


FIGURA 3: **PROPIEDADES DE CONEXIÓN DE RED E INSTALACIÓN DE IPV6 EN WINDOWS 7**

2.1.4. Instalación en Windows 2000

El método mas fiable para la instalación de la pila IPv6 para Windows 2000, requiere primero descargar el código correspondiente a la pila IPv6, dado que a diferencia de los sistemas operativos hasta ahora mencionados, no esta preinstalado por el fabricante.

Como hemos indicado antes, Windows 2000 IPv6 no está soportado por Microsoft, dado que se trataba de una versión de desarrollo.

Por lo tanto, en primer lugar, descargaremos "Microsoft IPv6 Technology Preview for Windows 2000":

- tpipv6-001205-SP2-IE6 para SP1 y SP2
- tpipv6-001205-SP3-IE6 para SP3

- tpipv6-001205-SP4-IE6 para SP4

Todos están disponibles en:
http://www.sixxs.net/faq/connectivity/?faq=ossetup&os=windows

Una vez descargado, el procedimiento de instalación es el siguiente:

- Entrar en el sistema como usuario con privilegios locales de administrador
- Extraer los ficheros de IPv6 Technology Preview, por ejemplo en C:\IPv6Kit
- Seguir el procedimiento de SPn & IE6 fixed.txt para cambiar el fichero/setup/hotfix.ini
- Ejecutar Setup.exe o hotfix.exe
- Desde el escritorio de Windows 2000, clic Inicio, luego Configuración, y luego Conexiones de Red. Alternativamente, hacer clic con el botón derecho en Mis Sitios de Red, luego clic en Propiedades
- Hacer clic con el botón derecho en conexiones basadas en Ethernet para las que se desea añadir el protocolo IPv6 y luego clic en Propiedades. Normalmente, esta conexión se denomina Conexión de Área Local
- Click Install
- En el cuadro de diálogo Seleccionar Tipo de Componente de Red, hacer clic en Protocolo, y luego clic Añadir
- En el cuadro de diálogo Seleccionar Protocolo de Red, hacer clic en Microsoft IPv6 Protocol y luego clic en Aceptar
- Click Cerrar para cerrar el cuadro de diálogo de las Propiedades de la Conexión de Área Local.

2.2. Instalación de IPv6 en Mac OS X

IPv6 esta soportado por Apple desde Mac OS X versión 10.2 (Jaguar) y se halla habilitado por defecto.

Por lo tanto, no es preciso hacer nada para instalarlo.

2.3. Instalación de IPv6 en Linux

IPv6 esta soportado a partir de versión del kernel 2.4.x.

Para comprobar si esta instalado:
#test -f /proc/net/if_inet6 && echo "Kernel actual soporta IPv6"

Para instalar el módulo IPv6:
#modprobe ipv6

Se puede comprobar el módulo con:
#lsmod |grep -w 'ipv6' && echo "modulo IPv6 cargado"

También se puede configurar la Carga/descarga automática del modulo (/etc/modu-

les.conf o /etc/conf.modules):

alias net-pf-10 ipv6 #habilita carga bajo demanda

alias net-pf-10 off #deshabilita carga bajo demanda

Se puede realizar la configuración permanente, en función de la versión de Linux.

2.3.1 Configuración permanente en Red Hat (desde v7.1) y similares

Añadir a /etc/sysconfig/network:
NETWORKING_IPV6=yes

Reiniciar la red:
service network restart
O
#/etc/init.d/network restart

2.3.2. Configuración permanente en SUSE

Añadir en /etc/sysconfig/network/ifcfg-<Interface-Name>:
SUSE 8.0: IP6ADDR="<ipv6-address>/<prefix>"
SUSE 8.1: IPADDR="<ipv6-address>/<prefix>"

2.3.3. Configuración permanente en DEBIAN

Con el módulo IPv6 cargado se edita /etc/network/interfaces, por ejemplo:

```
iface eth0 inet6 static
   pre-up modprobe ipv6
   address 2001:DB8:1234:5::1:1
   # Elimina completamente la autoconfiguración:
   # up echo 0 > /proc/sys/net/ipv6/conf/all/autoconf netmask 64
   # El encaminador esta autoconfigurado y no tiene dirección fija.
   # Se encuentra gracias a
   # (/proc/sys/net/ipv6/conf/all/accept_ra).
   # Si no habrá que configurar el GW:
   # gateway 2001:DB8:1234:5::1
```

Se reinicia o:

```
# ifup --force eth0
```

2.4. Instalación de IPv6 en BSD

El soporte de IPv6 en BSD esta disponible a partir de la versión 4.5.

Se trata de un soporte muy bueno y la pila se halla preinstalada, por lo que no se requiere ningún paso adicional.

3. Comprobación de IPv6

Una vez hemos instalado IPv6, en función de las diferentes plataformas, tenemos una o varias opciones para verificar que dicha instalación ha sido realizada correctamente e incluso si tenemos conectividad tanto en la red local, como con otras redes IPv6.

3.1. Comprobación en Windows

Además de visualizar si la pila IPv6 ha sido instalada a través del entorno gráfico, como hemos indicado en la sección de instalación, podemos utilizar el comando ipconfig o ipv6 if (no disponible en las últimas versiones de Windows).

El comando ipconfig nos facilitará la información de configuración IPv6 de las diferentes interfaces, al igual que de IPv4, mientras que ipv6 if sólo muestra información relativa a IPv6.

Por ejemplo, si nuestra interfaz Ethernet fuese la número 5 (lo cual depende del hardware de cada equipo), el resultado de **ipv6 if 5**, sería similar a:

```
Interface 5: Ethernet: Local Area Connection
  Guid {F5149413-6E54-4FDA-87BD-24067735E363}
  uses Neighbor Discovery
  uses Router Discovery
  link-layer address: 00-01-4a-18-26-c7
  preferred global 2001:db8::fde7:a76f:62d5:3bb9, life 6d21h3m20s/21h33s (tem-
    porary)
  preferred global 2001:db8::201:4aff:fe18:26c7, life 29d23h51m39s/6d23h51m39s
    (public)
  preferred link-local fe80::201:4aff:fe18:26c7, life infinite
  multicast interface-local ff01::1, 1 refs, not reportable
  multicast link-local ff02::1, 1 refs, not reportable
  multicast link-local ff02::1:ff18:26c7, 2 refs, last reporter
  multicast link-local ff02::1:ffd5:3bb9, 1 refs, last reporter
  multicast link-local ff02::1:ff00:4, 1 refs, last reporter
  multicast link-local ff02::1:ff00:2, 1 refs, last reporter
  link MTU 1500 (true link MTU 1500)
  current hop limit 64
  reachable time 29000ms (base 30000ms)
  retransmission interval 1000ms
  DAD transmits 1
  default site prefix length 48
```

El resultado de ipconfig sería algo similar a:

Configuración IP de Windows

Adaptador **Ethernet** Publica:
Sufijo conexión específica DNS :
Dirección IP . . . . . : 10.10.10.250
Máscara de subred . . . . . : 255.255.255.0
Dirección IP . . . . . : 2a01:48:20:0:200:1cff:feb5:c535
Dirección IP . . . . . : fe80::200:1cff:feb5:c535%4
Puerta de enlace predet . . . . . : 10.10.10.1

Adaptador de túnel Consulintel:
Sufijo conexión específica DNS :
Dirección IP . . . . . : 2a01:48:20:0:200:1cff:feb5:c535
Dirección IP . . . . . : fe80::5:a0a:afa%5
Puerta de enlace predet . . . . . : 2a01:48:20::d5ac:227d

Adaptador de túnel Automatic Tunneling Pseudo-Interface:
Sufijo conexión específica DNS:
Dirección IP . . . . . : fe80::5efe:10.10.10.250%2
Puerta de enlace predet . . . . . :

Igualmente, si se utiliza **ipconfig /all**:

Configuración IP de Windows
Nombre del host . . . . . : dns1
Sufijo DNS principal . . . . . : consulintel.com
Tipo de nodo. . . . . : difusión
Enrutamiento IP habilitado . . . . . : S
Proxy de WINS habilitado . . . . . : S
Lista de búsqueda sufijo DNS . . . : consulintel.com

Adaptador Ethernet Publica:
Sufijo conexión específica DNS:
Descripción . . . . . : Adaptador Fast Ethernet PCI basado en Intel (Genérico)
Dirección física . . . . . : 00-00-1C-B5-C5-35
DHCP habilitado. . . . . : No
Dirección IP . . . . . : 10.10.10.250
Máscara de subred . . . . . : 255.255.255.0
Dirección IP . . . . . : 2a01:48:20:0:200:1cff:feb5:c535
Dirección IP . . . . . : fe80::200:1cff:feb5:c535%4
Puerta de enlace predet . . . . . : 10.10.10.1
Servidores DNS. . . . . : 80.58.0.33
80.58.32.97

```
                                    10.10.10.250
                                    fec0:0:0:ffff::1%1
                                    fec0:0:0:ffff::2%1
                                    fec0:0:0:ffff::3%1
```

Adaptador de túnel Consulintel:

```
   Sufijo conexión específica DNS:
   Descripción . . . . . . . . . . . . . . . : Configured Tunnel Interface
   Dirección física . . . . . . . . . . . . . : 0A-0A-0A-FA
   DHCP habilitado. . . . . . . . . . . . . . : No
   Dirección IP . . . . . . . . . . . . . . . : 2a01:48:20:0:200:1cff:feb5:c535
   Dirección IP . . . . . . . . . . . . . . . : fe80::5:a0a:afa%5
   Puerta de enlace predet . . . . . . . . . : 2a01:48:20::d5ac:227d
   Servidores DNS. . . . . . . . . . . . . . : fec0:0:0:ffff::1%2
                                    fec0:0:0:ffff::2%2
                                    fec0:0:0:ffff::3%2
   NetBios sobre TCPIP . . . . . . . . . . . : Deshabilitado
```

Adaptador de túnel Automatic Tunneling Pseudo-Interface:

```
   Sufijo conexión específica DNS:
   Descripción . . . . . . . . . . . . . . . : Automatic Tunneling Pseudo-Interface
   Dirección física . . . . . . . . . . . . . : 0A-0A-0A-FA
   DHCP habilitado. . . . . . . . . . . . . . : No
   Dirección IP . . . . . . . . . . . . . . . : fe80::5efe:10.10.10.250%2
   Puerta de enlace predet . . . . . . . . . :
   Servidores DNS. . . . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                    fec0:0:0:ffff::2%1
                                    fec0:0:0:ffff::3%1
   NetBios sobre TCPIP . . . . . . . . . . . : Deshabilitado
```


Una prueba adicional es comprobar que se puede "alcanzar" la propia interfaz, mediante el comando **ping/ping6** (uno, otro o ambos, pueden estar disponibles dependiendo de la versión específica de cada sistema operativo). Ejemplo utilizando la dirección de "loopback":

```
ping ::1
    Haciendo ping a ::1 desde ::1 con 32 bytes de datos:
    Respuesta desde ::1: tiempo<1m
    Respuesta desde ::1: tiempo<1m
    Respuesta desde ::1: tiempo<1m
    Respuesta desde ::1: tiempo<1m
    Estadísticas de ping para ::1:
      Paquetes: enviados = 4, recibidos = 4, perdidos = 0     (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
      Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

Si se desea intentar con la dirección "link-local" (enlace local, es decir válida solo en el segmento de red local en el que se conecta dicha interfaz) propia, de una determinada tarjeta de red (la cual se puede ver con ipv6 if o ipconfig):

ping6 fe80::e8a7:b568:a076:6ba3 (link-local propia)
Haciendo ping a fe80::e8a7:b568:a076:6ba3 desde fe80::e8a7:b568:a076:6ba3%5 con 32 bytes de datos:
Respuesta desde fe80::e8a7:b568:a076:6ba3: tiempo<1m
Respuesta desde fe80::e8a7:b568:a076:6ba3: tiempo<1m
Respuesta desde fe80::e8a7:b568:a076:6ba3: tiempo<1m
Respuesta desde fe80::e8a7:b568:a076:6ba3: tiempo<1m
Estadísticas de ping para fe80::e8a7:b568:a076:6ba3:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0 (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 0ms, Máximo = 0ms, Media = 0ms

El paso siguiente sería, comprobar que hay conectividad con la red local. Esto sólo es posible si hay otras máquinas con IPv6 correctamente configurada en dicha red local (y la configuración de los cortafuegos permite usar el comando ping). El uso sería equivalente al ejemplo anterior, pero utilizando la dirección de enlace local (o una dirección global, si existiera), de la máquina a la que se desea hacer ping.

ping fe80::200:87ff:fe28:a0e0%5 (link-local vecino en la interfaz 5)
Haciendo ping a fe80::200:87ff:fe28:a0e0%5 desde fe80::201:4aff:fe18:26c7%5 con 32 bytes de datos:
Respuesta desde fe80::200:87ff:fe28:a0e0%5: tiempo<1ms
Respuesta desde fe80::200:87ff:fe28:a0e0%5: tiempo<1ms
Respuesta desde fe80::200:87ff:fe28:a0e0%5: tiempo<1ms
Respuesta desde fe80::200:87ff:fe28:a0e0%5: tiempo<1ms
Estadísticas de ping para fe80::200:87ff:fe28:a0e0%5:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0 (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 0ms, Máximo = 0ms, Media = 0ms

Igualmente, si se tiene conectividad con el exterior de la red local, es decir, con otras máquinas IPv6 situadas en Internet, sería posible obtener un resultado similar a:

ping www.ipv6tf.org
Haciendo ping a www.ipv6tf.org [2a01:48:1:0:2e0:81ff:fe05:4658] desde 2001:db8:0:0:2c0:26ff:fea0:a341 con 32 bytes de datos:
Respuesta desde 2a01:48:1:0:2e0:81ff:fe05:4658: tiempo=99.661m
Respuesta desde 2a01:48:1:0:2e0:81ff:fe05:4658: tiempo<106.572m
Respuesta desde 2a01:48:1:0:2e0:81ff:fe05:4658: tiempo<88.624m
Respuesta desde 2a01:48:1:0:2e0:81ff:fe05:4658: tiempo<76.629m

```
Estadísticas de ping para 2a01:48:1:0:2e0:81ff:fe05:4658:
  Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
  Mínimo = 76.629ms, Máximo = 106.572ms, Media = 92.871ms
```

Un paso adicional, sería el uso de una herramienta que nos muestre los saltos entre los diferentes puntos de la red, desde nuestra propia máquina hasta la máquina destino, lo que se denomina un traceroute (traza de la ruta). Para ello se usa el comando tracert o tracert6 (según la versión/plataforma):

```
tracert www.lacnic.net
Traza a la dirección lacnic.net [2001:13c7:7002:4000::10]
sobre un máximo de 30 saltos:
1  <1 ms   <1 ms   <1 ms  2a01:48:1::ff0
2  29 ms   25 ms    7 ms  2a01:48::d5ac:227d
3  53 ms   60 ms   35 ms  tunnel105.tserv17.lon1.ipv6.he.net [2001:470:14:69::1]
4  75 ms  109 ms   34 ms  gige-g4-18.core1.lon1.he.net [2001:470:0:a3::1]
5  63 ms   43 ms   73 ms  10gigabitethernet1-1.core1.ams1.he.net [2001:470:0:3f::2]
6  447 ms  163 ms  112 ms  2001:7f8:1::a500:3549:2
7  297 ms  325 ms  319 ms  2001:450:2002:7f::2
8  303 ms  313 ms  656 ms  ar01.bb2.registro.br [2001:12ff:2:1::244]
9  297 ms  315 ms  313 ms  gw01.lacnic.registro.br [2001:12ff:1:3::212]
10 302 ms  320 ms  320 ms  www.lacnic.net [2001:13c7:7002:4000::10]
Traza completa.
```


3.2. Comprobación en Mac OS X

A través de Preferencias del Sistema/Red/Avanzado, se obtiene la pantalla siguiente, y en TCP/IP se puede verificar que esta automáticamente configurado.

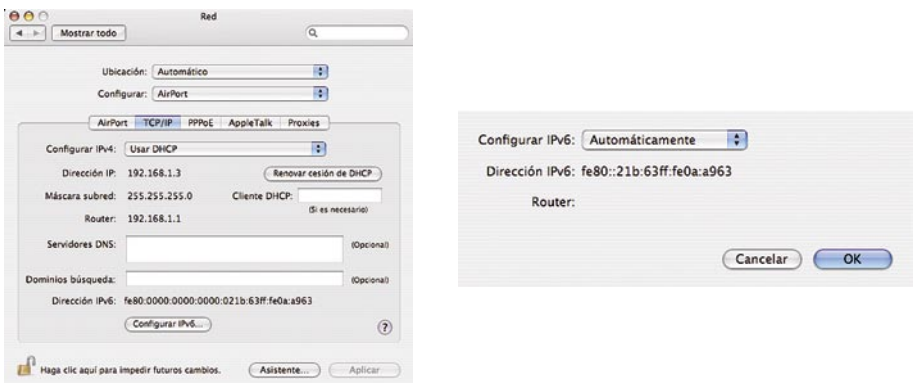


FIGURA 4: **COMPROBACIÓN DE CONFIGURACIÓN AUTOMÁTICA DE IPV6 EN MAC OS X**

Si se desea, se puede recurrir al terminal, para utilizar el comando ifconfig, por ejemplo:

```
$ ifconfig

lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=1<UP> mtu 1280
        inet6 2002:8281:57f9:1::1 prefixlen 16
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether 00:1b:63:bd:71:67
        media: autoselect status: inactive
        supported media: autoselect 10baseT/UTP <half-duplex> 10baseT/UTP <full-duplex> 10baseT/UTP <full-duplex,hw-loopback> 10baseT/UTP <full-duplex,flow-control> 100baseTX <half-duplex> 100baseTX <full-duplex> 100baseTX <full-duplex,hw-loopback> 100baseTX <full-duplex,flow-control> 1000baseT <full-duplex> 1000baseT <full-duplex,hw-loopback> 1000baseT <full-duplex,flow-control> none
fw0: flags=8802<BROADCAST,SIMPLEX,MULTICAST> mtu 4078
        lladdr 00:1e:52:ff:fe:46:46:0c
        media: autoselect <full-duplex> status: inactive
        supported media: autoselect <full-duplex>
en1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        inet6 fe80::21e:52ff:fe73:c2a6%en1 prefixlen 64 scopeid 0x6
        inet6 2001:df8::80:21e:52ff:fe73:c2a6 prefixlen 64 autoconf
        inet 130.129.87.249 netmask 0xfffff800 broadcast 130.129.87.255
        ether 00:1e:52:73:c2:a6
        media: autoselect status: active
        supported media: autoselect
en5: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether 00:1e:52:d7:90:f5
        media: autoselect status: inactive
        supported media: none autoselect 10baseT/UTP <half-duplex>
en2:   flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        inet6 fe80::21c:42ff:fe00:0%en2 prefixlen 64 scopeid 0x8
        inet 10.37.129.3 netmask 0xffffff00 broadcast 10.37.129.255
        ether 00:1c:42:00:00:00
        media: autoselect status: active
        supported media: autoselect
en3:   flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        inet6 fe80::21c:42ff:fe00:1%en3 prefixlen 64 scopeid 0x9
        inet 10.211.55.8 netmask 0xffffff00 broadcast 10.211.55.255
```

```
        ether 00:1c:42:00:00:01
        media: autoselect status: active
        supported media: autoselect
tun0: flags=88d1<UP,POINTOPOINT,RUNNING,NOARP,SIMPLEX,MULTICAST> mtu 1500
        open (pid 199)
```

De forma idéntica a como se ha hecho con Windows, se pueden usar los comandos ping6 y traceroute6 (obsérvese que en este caso el comando se escribe completo), desde una ventana de Terminal:

```
$ ping6 www.ipv6tf.org
PING6(56=40+8+8 bytes) 2001:df8::80:21e:52ff:fe73:c2a6 --> 2a01:48:1::2e0:81ff:
fe05:4658
16 bytes from 2a01:48:1::2e0:81ff:fe05:4658, icmp_seq=0 hlim=49 time=643.332 ms
16 bytes from 2a01:48:1::2e0:81ff:fe05:4658, icmp_seq=1 hlim=49 time=87.239 ms
16 bytes from 2a01:48:1::2e0:81ff:fe05:4658, icmp_seq=3 hlim=49 time=82.984 ms
16 bytes from 2a01:48:1::2e0:81ff:fe05:4658, icmp_seq=4 hlim=49 time=202.559 ms
^C
--- www.ipv6tf.org ping6 statistics ---
5 packets transmitted, 4 packets received, 20% packet loss
round-trip min/avg/max = 82.984/254.029/643.332 ms
```



```
$ ping6 fe80::21e:52ff:fe73:c2a6%en1
PING6(56=40+8+8 bytes) fe80::21e:52ff:fe73:c2a6%en1 --> fe80::21e:52ff:fe73:
c2a6%en1
16 bytes from fe80::21e:52ff:fe73:c2a6%en1, icmp_seq=0 hlim=64 time=0.089 ms
16 bytes from fe80::21e:52ff:fe73:c2a6%en1, icmp_seq=1 hlim=64 time=0.117 ms
16 bytes from fe80::21e:52ff:fe73:c2a6%en1, icmp_seq=2 hlim=64 time=0.118 ms
16 bytes from fe80::21e:52ff:fe73:c2a6%en1, icmp_seq=3 hlim=64 time=0.167 ms
^C
--- fe80::21e:52ff:fe73:c2a6%en1 ping6 statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.089/0.123/0.167 ms

$ ping6 www.ipv6tf.org
PING6(56=40+8+8 bytes) 2002:4e40:58c0:9:21e:52ff:fe73:c2a6 --> 2a01:48:1::2e0:81ff:
fe05:4658
16 bytes from 2a01:48:1::2e0:81ff:fe05:4658, icmp_seq=0 hlim=60 time=93.848 ms
16 bytes from 2a01:48:1::2e0:81ff:fe05:4658, icmp_seq=1 hlim=60 time=93.32 ms
16 bytes from 2a01:48:1::2e0:81ff:fe05:4658, icmp_seq=2 hlim=60 time=92.087 ms
16 bytes from 2a01:48:1::2e0:81ff:fe05:4658, icmp_seq=3 hlim=60 time=89.836 ms
^C
--- www.ipv6tf.org ping6 statistics ---
```

4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 89.836/92.273/93.848 ms

E igualmente con traceroute6:

$ traceroute6 www.ipv6tf.org
traceroute6 to www.ipv6tf.org (2a01:48:1::2e0:81ff:fe05:4658) from 2001:df8::80:21e:52ff:fe73:c2a6, 30 hops max, 12 byte packets
1 2001:df8:0:80::3 433.216 ms 0.813 ms 1.108 ms
2 htg0-ncore-2.gigabiteth5-2.swip.net 1.281 ms 1.141 ms 1.072 ms
3 avk-core-1.gigabiteth6-0-0.swip.net 1.514 ms 1.432 ms 2.269 ms
4 avk-core-2.tengigabiteth2-1.swip.net 1.444 ms 1.476 ms 1.275 ms
5 ibr01-tu15.stkh01.occaid.net 3.865 ms 2.842 ms 2.926 ms
6 bbr01-p2-0.lndn01.occaid.net 43.132 ms 42.645 ms 43.049 ms
7 neosky-ic-8241-lon.customer.occaid.net 66.522 ms 66.901 ms 67.478 ms
8 consulintel-neosky.consulintel.es 99.245 ms 106.983 ms 94.87 ms

3.3. Comprobación en otros sistemas operativos

En general en el resto de los sistemas operativos (Unix/similares/derivados, Linux, BSD, etc.), lo mas fácil es utilizar ifconfig, pero en ocasiones también existen entornos de interfaz gráfica de usuario (específicos de cada plataforma) para monitorizar el estado de las interfaces de red, y por tanto de IPv6. Por tanto, los ejemplos indicados para el caso de Mac OS X, son equivalentes.

Igualmente, se puede usar ping6 y traceroute6, por lo que todos los ejemplos indicados para Mac OS X en el apartado anterior, son igualmente válidos.

4. Configuración avanzada de IPv6

En algunas ocasiones, puede ser necesario realizar configuraciones avanzadas, por ejemplo configurar manualmente una dirección IPv6, modificar dicha configuración, o eliminarla.

Como en ocasiones anteriores, diversos sistemas operativos, realizan estas configuraciones de modos diferentes.

4.1. Configuración avanzada en Windows

Por diversos motivos, puede requerirse configurar manualmente una dirección IPv6. Para ello se usa el comando netsh con el formato siguiente:

netsh interface ipv6 add address [interface=]<cadena (nombre de interfaz o índice)> [address=]<dirección IPv6>[/<entero>] [[type=]unicast|anycast] [[validlifetime=]<entero>|infinite] [[preferredlifetime=]<entero>|infinite] [[store=]active|persistent]

Ejemplo:

netsh interface ipv6 add address 5 2001:db8::2 type=unicast validlifetime=infinite preferredlifetime=10m store=active

Igualmente, se puede revisar la configuración con netsh (asumiendo que es la interfaz numero 5):

netsh interface ipv6 show address 5

Una vez configurada una dirección manualmente, se puede modificar con:

netsh interface ipv6 set address [interface=]<cadena> [address=]<dirección IPv6> [[type=]unicast|anycast] [[validlifetime=]<entero>|infinite] [[preferredlifetime=]<entero>|infinite] [[store=]active|persistent]

Ejemplo:

netsh interface ipv6 set address 5 2001:db8::2 preferredlifetime=infinite

Y finalmente, dicha dirección puede ser eliminada con:

netsh interface ipv6 delete address [interface=]<cadena> [address=]<dirección IPv6> [[store=]active|persistent]

Ejemplo:

netsh interface ipv6 delete address 5 2001:db8::2 store=persistent

Igualmente, se puede dar el caso en que necesitemos agregar una ruta estática, y de forma similar, utilizaríamos:

netsh interface ipv6 add route add route [prefix=]<dirección IPv6>/<entero> [interface=]<cadena> [[nexthop=]<dirección IPv6>] [[siteprefixlength=]<entero>] [[metric=]<entero>] [[publish=]no|yes|immortal] [[validlifetime=]<entero>|infinite] [[preferredlifetime=]<entero>|infinite] [[store=]active|persistent]

Ejemplo:

netsh interface ipv6 add route 2002::/16 5 fe80::200:87ff:fe28:a0e0 store=persistent

Donde, fe80::200:87ff:fe28:a0e0 es la puerta de enlace que se desea configurar para la ruta 2002::/16.

Para borrar dicha ruta:

netsh interface ipv6 delete route [prefix=]<dirección IPv6>/<entero> [interface=]<cadena> [[nexthop=]<dirección IPv6>] [[store=]active|persistent]

Ejemplo:

netsh interface ipv6 delete route 2002::/16 5 fe80::200:87ff:fe28:a0e0 store=persistent

Y se pueden visualizar las rutas con:

netsh interface ipv6 show route [[level=]normal|verbose] [[store=]active|persistent]

Ejemplo:
netsh interface ipv6 show route

```
Publicar  Tipo          Mét  Prefijo          Índ  Puerta enl./Nombre int.
----------  ----------  ----  ----------------  ---  -----------------------------------
No        Manual      8   ::/0             13  Conexión de área local* 7
no        Manual      0  2002::/16         5  fe80::200:87ff:fe28:a0e0
no        Autoconf    8  2001:db8::/64     5  Local Area Connection
no        Autoconf    256  ::/0            5  fe80::200:87ff:fe28:a0e0
```

Finalmente, se puede agregar un servidor DNS con:

netsh interface ipv6 add dnsserver [name=]<cadena> [address=]<dirección IPv6> [[index=]<entero>]

En XP SP1/2003 SP1 se usa dns en lugar de dnsserver

Ejemplo:
netsh interface ipv6 add dnsserver "Local área network" 2001:7f9:1000:1::947c 1

El "index" representa la posición (preferencia) del servidor DNS que se configura en la lista de servidores DNS.

Y se pueden mostrar los servidores DNS configurados manualmente con:
netsh interface ipv6 show dnsservers [[name=]cadena]

Ejemplo:
netsh interface ipv6 show dnsservers

```
DNS servers in LAN interface
Index      DNS server
-------   ------------------------------------------
1            2001:7f9:1000:1::947c
2            2001:7f9:1000:1::947c
```

Y por último, borrarlos con:
netsh interface ipv6 delete dnsserver [name=]<cadena> [[address=]<dirección IPv6>|all]

Ejemplo:
netsh interface ipv6 delete dnsserver "Local área network" all

4.2. Configuración avanzada en Linux

Añadir una dirección IPv6:

/sbin/ip -6 addr add <ipv6address>/<prefixlength> dev <interface>
/sbin/ifconfig <interface> inet6 add <ipv6address>/<prefixlength>
Eliminar una dirección IPv6:
/sbin/ip -6 addr del <ipv6address>/<prefixlength> dev <interface>
/sbin/ifconfig <interface> inet6 del <ipv6address>/<prefixlength>
Añadir ruta a través de una puerta de enlace:
/sbin/ip -6 route add <ipv6network>/<prefixlength> via <ipv6address> [dev <device>]
#/sbin/route -A inet6 add <ipv6network>/<prefixlength> gw <ipv6address> [dev <device>]

Ver rutas IPv6:
/sbin/ip -6 route show [dev <device>]
/sbin/route -A inet6
Eliminar ruta a través de una puerta de enlace:
/sbin/ip -6 route del <ipv6network>/<prefixlength> via <ipv6address> [dev <device>]
/sbin/route -A inet6 del <network>/<prefixlength> [dev <device>]

Añadir ruta a través de una interfaz:
/sbin/ip -6 route add <ipv6network>/<prefixlength> dev <device> metric 1
/sbin/route -A inet6 add <network>/<prefixlength> dev <device>

Eliminar ruta a través de una interfaz:
/sbin/ip -6 route del <ipv6network>/<prefixlength> dev <device>
/sbin/route -A inet6 del <network>/<prefixlength> dev <device>

4.3. Configuración avanzada en BSD

Añadir una dirección IPv6:
#>ifconfig <interface> inet6 add <dir. IPv6>

Eliminar una dirección IPv6:
#>ifconfig <interface> inet6 del <dir. IPv6>

Si se desea hacer la configuración de forma permanente, se emplea el fichero /etc/rc.conf:
ipv6_enable="YES"
ipv6_ifconfig_rl0="2001:618:10:4::4 prefixlen 64"

En /etc/defaults/rc.conf se pueden consultar las posibles opciones existentes y las que se usan por defecto.

Para aplicar cambios en rc.conf habrá que reiniciar.

Añadir ruta por defecto:

#>route –n add -inet6 default <dir. IPv6>

Eliminar ruta por defecto:
#>route –n del -inet6 default

4.4. Configuración avanzada en Mac OS X

Añadir una dirección IPv6:
ifconfig <interface> inet6 2001:db8:1:1::2/64

Eliminar una dirección IPv6:
ifconfig <interface> inet6 delete 2001:db8:1:1::2

Añadir ruta por defecto:
route add -inet6 default [2001:db8:1:1::1, -interface en1]

Eliminar ruta por defecto:
#>route del -inet6 default

Ver rutas IPv6:
netstat -r -f inet6

5. Mecanismos de transición con IPv6

Dado que no todos los ISPs, hoy en día, disponen de IPv6 en sus redes, es necesario utilizar lo que denominamos mecanismos de transición y coexistencia.

Básicamente, estos mecanismos, permiten que IPv4 e IPv6 coexistan, e incluso que cuando IPv6 no esta disponible de forma "nativa", se pueda utilizar IPv6 a través de la red IPv4, fundamentalmente mediante lo que denominamos "túneles".

Los mecanismos de túneles, se ocupan de que IPv6 sea "empaquetado" o "encapsulado", dentro de los paquetes IPv4, de tal forma que, como hemos indicado antes, IPv6 sea "transportado" en la red IPv4 existente.

Los siguientes gráficos permite visualizar como funcionan estos túneles y como se "empaqueta" IPv6 en IPv4.

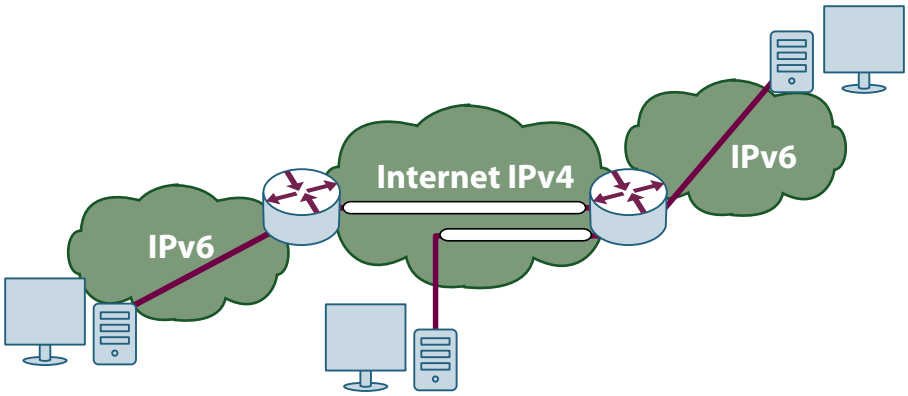


FIGURA 5: **TÚNELES IPV6 EN IPV4**

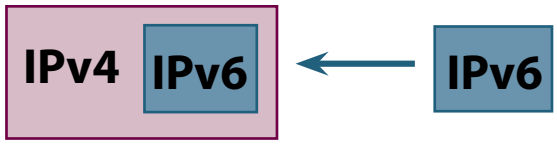


FIGURA 6: **ENCAPSULADO DE IPV6 EN IPV4**

Hay muchos mecanismos de transición y se trata de un tema sumamente complejo, por lo que este apartado, se centra sólo en aquellos mecanismos de túneles que consideramos más útiles, y que se denominan túneles automáticos y más concretamente en los denominados 6to4 y Teredo.

6to4 sólo funciona cuando se dispone de direcciones IPv4 públicas, por ejemplo, cuando un ordenador esta conectado a una red ADSL mediante un módem USB. En este caso, sin entrar en detalles técnicos, lo que ocurre es que se utiliza la dirección IPv4 para configurar automáticamente una dirección IPv6 y un túnel automático, que como decíamos anteriormente, permite utilizar IPv6 a través de la red IPv4.

Teredo (Miredo en sistemas Linux, BSD y Mac OS X) en cambio, funciona con direcciones IPv4 privadas, es decir detrás de los denominados "traductores de direcciones" o NAT, es decir, por ejemplo, cuando una conexión a una red ADSL se realiza mediante un encaminador en lugar de un módem. De forma parecida al caso de 6to4, se genera de forma automática una dirección IPv6 para cada ordenador conectado a dicho encaminador/NAT, y de igual modo, se utiliza IPv6 a través de la red IPv4.

Dado que estamos hablando de mecanismos de transición automáticos, generalmente no se requiere configuración alguna y el sistema operativo se ocupará automáticamente, de detectar si existe conectividad IPv6 en la red (por ejemplo proporcionada por el ISP), y en caso contrario de activar 6to4 o Teredo.

Si se necesita utilizar Miredo, solo será necesario descargar de la red el software correspondiente e instalarlo.

6. Desinstalación de IPv6

En general, no debiera de ser necesario desinstalar IPv6, pero si por algún se precisa hacerlo, facilitamos a continuación la información relativa a las plataformas mas relevantes.

6.1. Desinstalación en XP/2003/Vista/7

En algunas de estas plataformas, se puede usar:

ipv6 uninstall

En otros casos, dado que el comando ipv6.exe solo aparece hasta Windows XP, es necesario utilizar el comando netsh:

netsh interface ipv6 uninstall

Por supuesto que también es posible usar el entorno gráfico, de forma contraria a la indicada para la instalación.

En general se requiere reiniciar el sistema operativo para evitar efectos indeseados.

Como alternativa, si lo que se requiere es inicializar la pila a la situación por defecto de "fábrica", se puede usar (en la mayoría de las plataformas):

netsh interface ipv6 reset

Obsérvese que en Windows Vista, 2008 y 7, dado que la pila IPv6 esta totalmente integrada con la pila IPv4, no es posible desactivarlo por completo. En su lugar, se puede usar el entorno gráfico para desactivarlo en una interfaz de red concreta.

6.2. Desinstalación en Windows 2000

El procedimiento es el siguiente:

- Entrar en el sistema como usuario con privilegios locales de administrador
- Desde el escritorio de Windows 2000, clic Inicio, luego Configuración, y luego Conexiones de Red. Alternativamente, hacer clic con el botón derecho en Mis Sitios de Red, luego clic en Propiedades
- Hacer clic con el botón derecho en conexiones basadas en Ethernet para las que se desea añadir el protocolo IPv6 y luego clic en Propiedades. Normalmente, esta conexión se denomina Conexión de Área Local
- Seleccionar MSR IPv6 Protocol luego hacer Click en Desinstalar
- En el cuadro de diálogo Desinstalar MSR IPv6 Protocol, hacer clic en Sí
- En el cuadro de diálogo Red Local, hacer clic en Sí para reiniciar el PC

6.3. Desinstalación en Mac OS X

Podemos deshabilitar IPv6 en todas las interfaces con: **#ip6 –x**

Para habilitarlo de nuevo, basta con usar: **#ip6 –a**

Alternativamente, podemos usar el entorno gráfico.

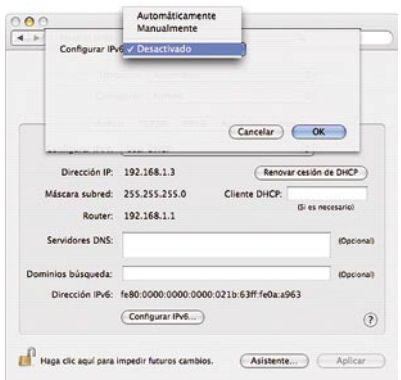


FIGURA 7: **DESHABILITAR IPV6 EN MAC OS X**

3. Home Office

1. Introducción

1.1. ¿A qué se denomina "SOHO"?

Se llama "SOHO" (Small Office Home Office) a una oficina pequeña o a una oficina montada en casa. En general, podría considerarse con esta denominación a cualquier conformación de oficina o grupo de profesionales independientes con una capacidad de hasta 10 trabajadores[1] *(Ver Figura 1 y Figura 2)*.

Basándonos en esta definición, cuando hablamos de Home Office en IPv6, nos referimos a la implementación de la red de un SOHO, de forma tal que cuente con la capacidad de operar con la nueva versión del protocolo IP: IPv6.

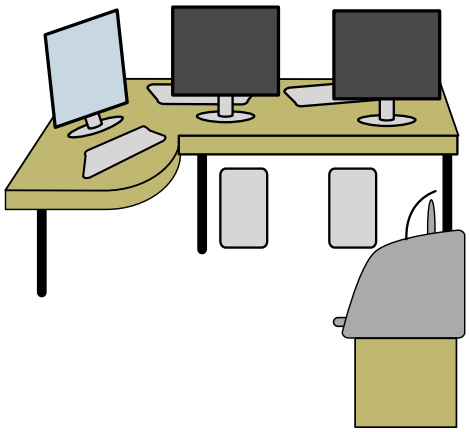


FIGURA1: **EJEMPLO DE NEGOCIO PEQUEÑO, CON MENOS DE 10 EMPLEADOS**

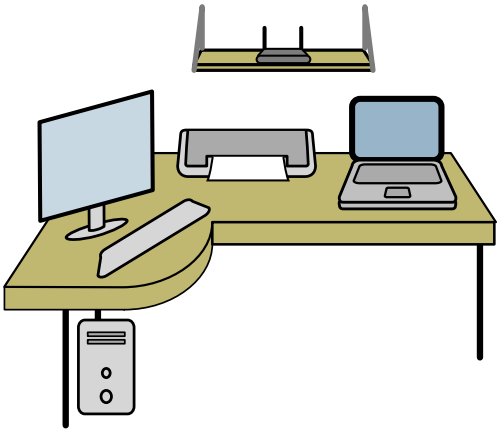


FIGURA 2: **EJEMPLO DE OFICINA EN CASA O RED RESIDENCIAL**

1.2. Construyendo un SOHO con IPv6

Antes de comenzar la construcción de un SOHO que implemente IPv6 en su red es importante tener claro las diferentes partes que lo componen. Una vez que éstas estén identificadas, podremos ver cuáles de ellas será necesario configurar para que funcionen con IPv6. A partir de ahí, será apropiado ver cómo hacerlo.

En resumen, las etapas que debemos cumplir serán:

1. Identificar las partes del SOHO
2. Determinar cuáles de ellas requieren configuración para trabajar con IPv6
3. Configurar el SOHO con IPv6

1 http://es.wikipedia.org/wiki/Small_Office,_Home_Office

2. Identificando las partes de un SOHO

Como hemos dicho en el párrafo anterior, este es el primer paso a la hora de pensar en la construcción de la red de un SOHO. Para llevar a cabo tal identificación, sugerimos hacerlo sobre tres aspectos bien delimitados:

2.1. Identificación del equipamiento que compone el SOHO, donde además habrá que distinguir entre:

2.1.1. Dispositivos de networking

2.1.2. Dispositivos terminales

2.2. Identificación de los sistemas operativos, en sus variantes:

1.2.1. Sistemas operativos de servidores

1.2. 2. Sistemas operativos de computadoras y laptops

2.3. Identificación de las aplicaciones

2.3.1. En servidores

2.3.2. En estaciones terminales

Comencemos por el punto **2.1.:**

- Dispositivos de Networking: deberemos identificar en nuestra red aquellos dispositivos que no constituyen nuestra interfaz de usuario, sino que son los que contribuyen a la comunicación de la red. En este conjunto podríamos incluir por ejemplo: el switch donde conectamos las terminales o computadoras, el router que el proveedor de Internet nos dejó instalado al contratar el servicio, el equipo que nos provee la conexión inalámbrica, entre otros.

- Dispositivos terminales: en este grupo encontramos aquellos dispositivos con los que interactuamos directamente, como por ejemplo: las computadoras de escritorio, las computadoras portátiles o laptops, PDAs, teléfonos IP, servidores de aplicaciones, entre otros.

En otra categoría podríamos identificar a las impresoras de red, que si bien no representan una interfaz directa con el usuario, tampoco es un dispositivo de networking, pero sin embargo vamos a querer su servicio dentro de la red y probablemente querramos tenerla en cuenta a la hora de trabajar con IPv6.

Siguiendo con el punto **2.2.**, deberemos identificar los sistemas operativos con los cuales trabajaremos, para ello tendremos en cuenta:

- Sistemas operativos de servidores: son los sistemas operativos que se ejecutan en aquellos dispositivos terminales que aportan servicios de red, como por ejemplo el servicio de e-mail. Podemos identificar entre ellos: sistemas operativos Linux, Windows, Unix, etc. Siendo los dos primeros los mas utilizados en redes SOHO.

- Sistemas operativos de computadoras y laptops: son aquellos que se ejecutan en los dispositivos terminales con los que trabajamos en forma directa. Los mas usados en estos casos pueden ser Windows, Linux y MAC OS.

Finalizando con la identificación de componentes de la red del SOHO, el punto 2.3. requiere que distingamos entre:

- Aplicaciones en servidores: llamamos así a aquellas que proveen servicios en forma centralizada para los distintos dispositivos de la red, como por ejemplo: servicio de DNS, e-mail, páginas web, entre otras.

- Aplicaciones en terminales: se trata de las aplicaciones que utilizamos para trabajar desde, por ejemplo, nuestra PDA, laptop o computadora de escritorio. Entre las mas conocidas están: editores de texto, planillas de cálculo, clientes de e-mail, navegador de páginas web, clientes de mensajería instantánea, clientes de servicio multimedia, aplicaciones hechas a medida, etc.

Cuando llegamos a esta instancia tenemos a todos nuestros componentes del SOHO claramente identificados, de forma tal que podremos determinar cuáles de ellos configurar para que funcionen con IPv6. Este es, entonces, el paso siguiente.

3. Determinando los componentes que requieren configuración

En general, en una red medianamente nueva, o sea, con equipos de networking cuya fecha de fabricación data de unos 3 o 4 años atrás, no deberíamos tener que hacer mas que actualizar los sistemas operativos si estos no soportaran IPv6.

Una buena práctica sería listar uno a uno los equipos de networking y buscar en la bibliografía o documentación de cada uno su compatibilidad con IPv6. Probablemente, y tal como dijimos anteriormente, nos encontremos con que debemos actualizar alguna versión de sistema operativo o instalar algún firmware para lograr el soporte IPv6, si es que nuestro equipamiento no está ya soportándolo en las condiciones en las que está.

Por ejemplo, para los routers Cisco, encontramos su soporte a partir de la versión de IOS 12.3T, en el caso de los Juniper todas las versiones de JunOS están soportando IPv6. Otro dato interesante son los equipos de conexión inalámbrica en los cuales la configuración del equipamiento para que soporte el protocolo IPv6 dependerá de la marca y modelo del router. A modo de ejemplo, los dispositivos AirPort de Apple[2], disponen de soporte IPv6, al igual que otros tales como los routers inalámbricos D-link[3].

2 http://www.apple.com/airportextreme/specs.html,
3 http://www.ipv6ready.org/logo_db/logo_search2.php?logoid_number=01-000322&btm=Search

En cuanto a los sistemas operativos, la mayoría de los linux, desde hace varios años, ya vienen con el stack de IPv6 cargado, así como las versiones de Unix (por ejemplo, en los sistemas operativos Solaris se consigue el soporte de IPv6 desde la versión 8). Respecto a los sistemas operativos MacOS, el soporte IPv6 está dado por defecto desde el año 2003 con las versiones de "Panther". En cuanto a los sistemas Windows XP y Windows Server 2003, estos tienen la posibilidad de cargar de forma muy simple la pila de IPv6. En cambio, en las versiones de Windows Vista esta característica está habilitada por defecto.

Ahora, refiriéndonos a las aplicaciones, muchas de ellas serán independientes de la versión protocolo IP a utilizar, pero otras no tanto. En este sentido se aplica el mismo criterio que para el equipamiento, habrá que tener en cuenta si se hace necesaria una actualización de la versión instalada. Probablemente encontremos mas inconvenientes en las aplicaciones hechas a medida, donde será necesario convocar a los programadores de las mismas para que modifiquen el código si éstas no han sido diseñadas para funcionar en forma independiente a la versión del protocolo IP utilizado.

Bajo este contexto, en el cual probablemente nos encontremos en una red que combina dispositivos factibles de realizar una transición a IPv6 y otros que no lo sean, debemos tener en cuenta la recomendación de mantener las dos versiones del protocolo IP ejecutándose al mismo tiempo, o sea, lo que suele llamarse "mecanismos de doble pila" o "Dual Stack".

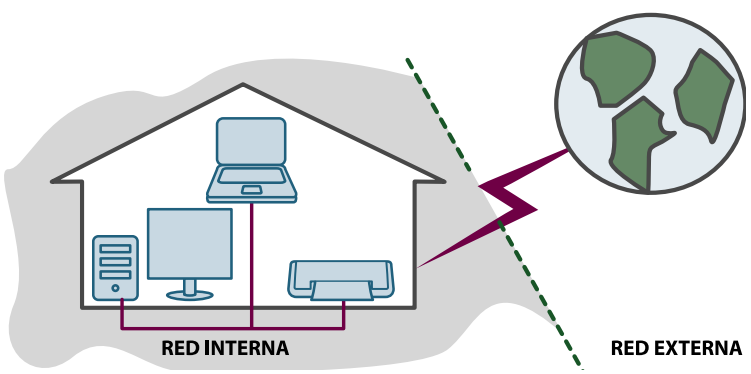
4. Configurando los componentes del SOHO con IPv6

Finalmente, con los dispositivos identificados, las versiones de software actualizadas para que soporten la nueva versión del protocolo IP y las modificaciones que hayan sido necesarias en las aplicaciones, estamos preparados para la etapa de la configuración.

Para ello, dividiremos la tarea en dos partes claramente separadas:

- Configuración de la red interna de nuestro SOHO (LAN)
- Configuración de la conexión con el exterior (Internet)

Las siguiente figura muestra el límite entre estas dos áreas:



Antes de comenzar con la descripción de estas dos tareas, trataremos el tema de cómo obtener las direcciones IPv6 con las que trabajaremos. Existen varias alternativas, algunas de ellas podrían ser:

- Disponer de direcciones propias, solicitadas al RIR correspondiente según la región donde nos encontremos.
- Que nuestro proveedor de Internet nos asigne un bloque de direcciones.
- Utilizar direcciones 6to4 (en este caso necesitaremos al menos una dirección IPv4 pública para hacerlo funcionar)
- Utilizar Túnel Brokers, de modo tal de establecer túneles automáticos con algún sitio capaz de proveer conectividad IPv6. Para esto solo es necesario disponer de un host dual-stack y un navegador para ver la web o interfaz del "broker" y configurar a partir de allí el túnel.

Con cualquiera de estas variantes u otras que no están descritas en este libro, lograremos disponer de direcciones IPv6, por lo que, ahora sí estamos listos para pensar en la configuración de la red.

4.1. Configuración de la red interna

A grandes rasgos, tenemos dos formas de realizar la configuración de la red interna de nuestro SOHO para que funcione también con IPv6: en forma manual y en forma automática (autoconfiguración).

Teniendo en cuenta que el objetivo de este libro es que el lector obtenga una forma práctica de llevar adelante su experiencia con IPv6, nos abocaremos a explicar cómo configurar nuestra red en forma automática.

Para que en una red pueda llevarse a cabo la autoconfiguración de interfaces con direcciones IPv6, será necesario que los dispositivos que deseen configurarlas soliciten los datos para hacerlo y además que algún otro dispositivo se encargue de anunciar dichos datos.

Estas solicitudes y anuncios forman parte del protocolo Neighbor Discovery[4], el cual a través de un conjunto de mensajes ICMPv6[5], se constituye en la base para que pueda llevarse a cabo el proceso de autoconfiguración.

En forma simplificada, los mensajes ICMPv6 que solicitan los datos se denominan "NS" (Neighbor Solicitation) y "RS" (Router Solicitation), y las respuestas vienen dadas

4 http://www.ietf.org/rfc/rfc2461.txt
5 http://www.ietf.org/rfc/rfc2463.txt

por otros mensajes ICPMv6 los llamados “NA” (Neighbor Advertisement) y “RA” (Router Advertisement).

Hecha esta introducción veamos cómo podemos realizar la autoconfiguración en la red del SOHO dependiendo de la topología de la misma.

Tomemos como ejemplo la red de la *figura 3*:

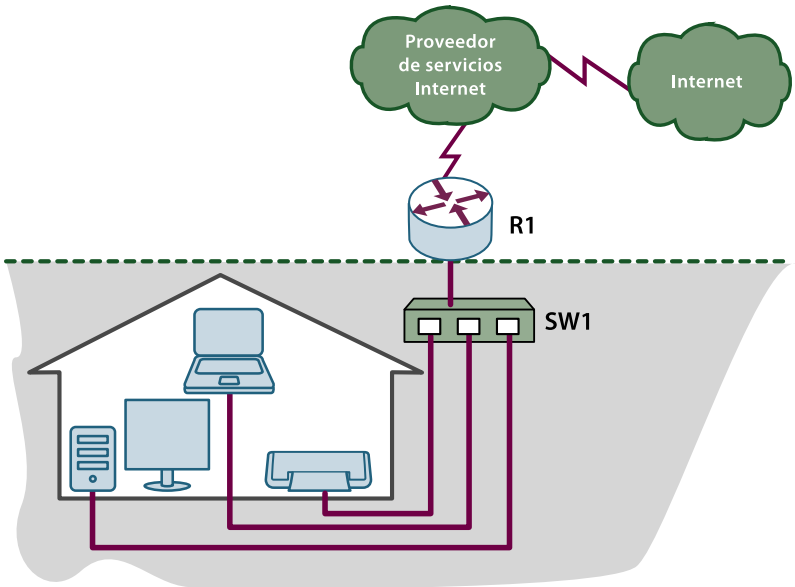


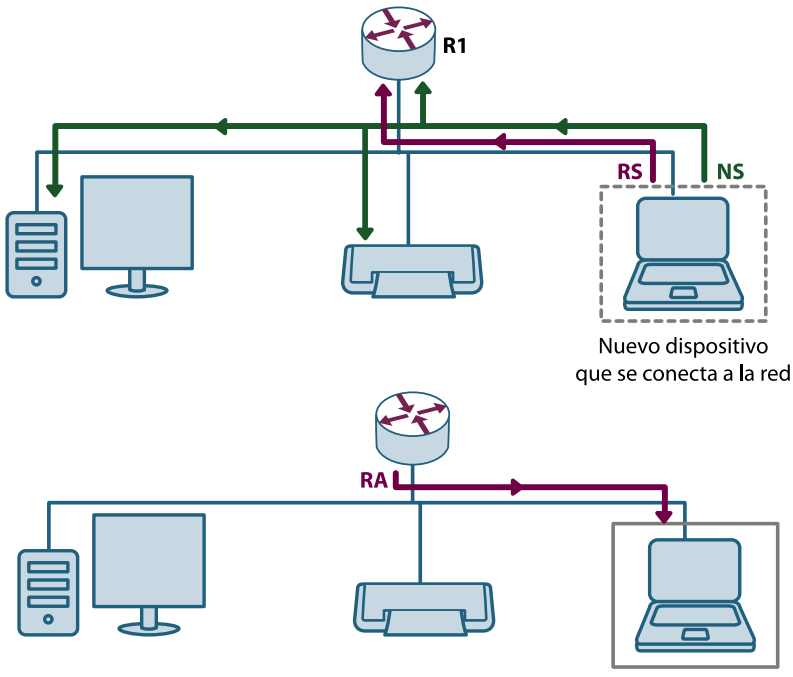
FIGURA 3: **RED CON UN ENLACE DEDICADO**

Como vemos, la red del SOHO posee un enlace a Internet “dedicado”, o sea, que el proveedor deja a disposición del cliente una conexión para que sea utilizada sólo por éste. En estos casos usualmente se dispone de un equipo router a donde llega el enlace de Internet (en la figura 3 está esquematizado con la sigla R1).

Una de las interfaces del router está conectada a la red interna del SOHO, a donde también conectan el resto de los dispositivos de la red. Todos lo hacen a través de un switch, al cual llamamos para nuestro ejemplo SW1.

En este caso, cuando un dispositivo (laptop, computadora de escritorio, etc) se conecta a la red, envía un mensaje NS para que puedan verlo todos los nodos de la red (Ver direcciones multicast – Ref), y generalmente un mensaje RS. Al recibir este último, el router R1 le envía como respuesta un mensaje RA conteniendo el prefijo IPv6 que el dispositivo debe utilizar para realizar el mecanismo de autoconfiguración.

Esta secuencia de mensajes se ve esquematizada en las siguientes figuras:



A modo de ejemplos, en los routers Juniper, para que el router sepa que debe anunciar el prefijo IPv6 para que el proceso de autoconfiguración de la red interna se lleve a cabo, debe hacerce[6]:

ipv6 nd prefix-advertisement <prefijoIPv6/longitud-prefijoIPv6>

En cuanto a los routers Cisco bastará con configurar la interfaz con una dirección IPv6 para que ésta sea anunciada hacia la red interna (solo habrá que indicar lo contrario en los casos en los que no se quiera llevar a cabo el anuncio del prefijo).

Obtenido el prefijo, el dispositivo está en condiciones de configurarse una dirección IPv6 basándose en el prefijo anunciado por el router y en su propia MAC Address (a través del método EUI-64[7]).

La *figura 4* es un modelo de la obtención de direcciones IPv6 en una red interna, luego de que se realice el proceso de autoconfiguración.

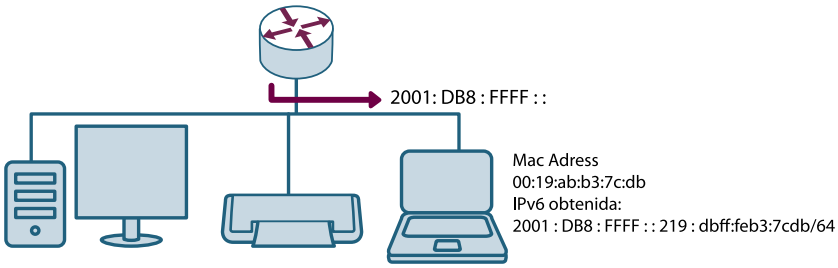


FIGURA 4: **AUTOCONFIGURACIÓN EN LA RED INTERNA**

6 http://www.juniper.net/techpubs/software/erx/junose700/swcmdref-a-m/html/i-commands318.html
7 http://standards.ieee.org/regauth/oui/tutorials/EUI64.htm

Supongamos ahora que no tenemos acceso al router que el proveedor de servicios de Internet dejó en el SOHO para nuestra conexión o, simplemente no existe tal equipo. Por lo tanto, debemos ver quién será el que enviará los mensajes RA.

Una alternativa podría ser una computadora conectada a la red interna, de forma tal que cumpla con la función de anunciar los RA y que con esto pueda llevar adelante la autoconfiguración. Hablamos por ejemplo de, un servidor con sistema operativo Linux corriendo el daemon radvd[8]. Otro método disponible sería usar un servidor de DHCPv6[9] *(ver figura 5)*:

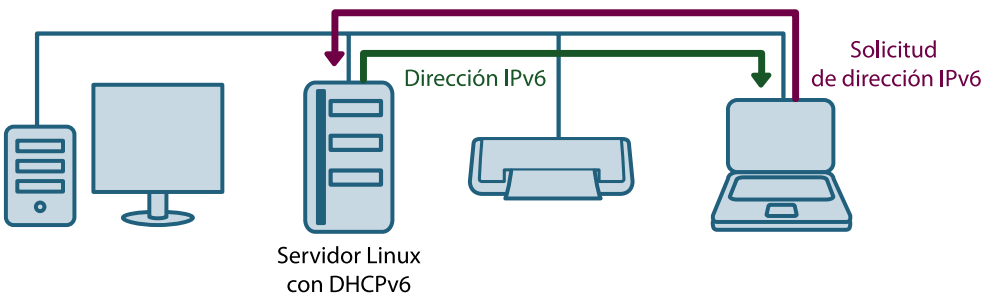


FIGURA 5: **EJEMPLO DE UTILIZACIÓN DE UN SERVIDOR PARA LLEVAR A CABO LA AUTOCONFIGURACIÓN.**

La diferencia entre utilizar el daemon o un servidor DHCPv6 radica en el mayor o menor grado al que queremos llegar con la autoconfiguración, ya que un servidor de DHCPv6 no solo lo podremos utilizar para anunciar los prefijos de la red sino además para comunicar otros datos como por ejemplo direcciones de los servidores de DNS, entre otros. En el caso de radvd solo nos permite anunciar los prefijos IPv6 para que las interfaces se autoconfiguren. Sin embargo, una buena práctica podría ser utilizar una combinación de ambos, de forma tal de facilitar el control de la administración sobre la red.

Para cualquiera de las variantes antes descritas, se sobreentiende que, tratándose de la red de un SOHO, el prefijo IPv6 es asignado por el proveedor de servicios de Internet o que se trata de direcciones propias.

4.2. Configuración de la conexión con el exterior (Internet)

Llegada esta instancia, es muy probable que ya tengamos decidido cómo resolver la configuración de la red del SOHO de forma tal que internamente pueda operar con IPv6, o lo que es lo mismo, hemos logrado que los dispositivos puedan comunicarse en la LAN a través de IPv6.

En esta sección veremos qué variantes hay a la hora de configurar una conexión IPv6 con el exterior de nuestra red.

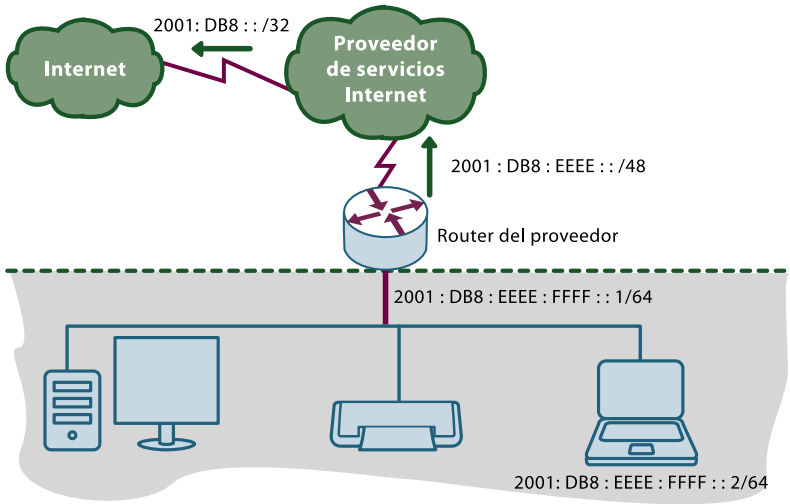
8 http://en.wikipedia.org/wiki/Radvd
9 http://www.ietf.org/rfc/rfc3736.txt

Tal como se trató anteriormente existe la posibilidad de que la red del SOHO tenga un enlace dedicado y que para ello el proveedor de servicios de Internet haya dispuesto un equipo router que lo conecta con el exterior.

Ahora bien, podemos considerar dos posibilidades:

A) Que el proveedor nos facilite, además del servicio de la conexión a través de IPv4, una conexión a Internet a través de IPv6.
B) Que el proveedor de servicios de Internet no pueda brindarnos una conexión a través de IPv6.

Si nuestro caso es el **A**, es muy posible que el proveedor ya esté anunciando a Internet su propio prefijo IPv6 y que, si da el servicio a los clientes, también les ofrezca un prefijo de su rango. Con esta situación, si el proveedor anuncia su prefijo, con seguridad también está anunciando el nuestro ya que es un subconjunto de su propio bloque de direcciones. Tal asignación y anuncio de prefijos se esquematiza en la siguiente figura:



Cuando se da esta situación, nada mas tenemos que hablar con nuestro proveedor para ver de qué forma prefiere implementar esto (a través de una sesión BGP con la red del SOHO, a través de rutas estáticas hacia nuestro router, etc). Pero en todo caso será solamente una cuestión de acuerdos. Tales acuerdos dependerán de las distintas alternativas de conectividad que tengamos, en todo caso, podría ser interesante consultar el RFC4779 y ver cuáles de ellas se ajustan mas a nuestra situación.

Ahora, si nuestro caso es el **B**, vamos a tener que encontrar la forma de atravesar la red IPv4 del proveedor para llegar a otra que pueda interpretar mis paquetes IPv6. Para ello debemos apelar a algún mecanismo de túneles.

Los túneles *(ver figura 7)*, son mecanismos que permiten que los paquetes puedan en-

capsularse de forma tal de atravesar redes con características diferentes. Pueden dividirse en dos grandes grupos:

- Túneles Manuales: tal como su nombre lo indica, se configuran en forma manual tanto en un extremo como en el otro del túnel. Esta solución, si bien funciona, impone establecer el túnel de forma estática con algún dispositivo remoto que pueda proveernos conexión hacia redes IPv6.

- Túneles Automáticos: al contrario de los manuales, no es necesario configurar en forma estática en ambos extremos sino que se establecen automáticamente con una configuración mínima.

4.2.1. Túneles Manuales

No entraremos en detalle respecto a este tipo de túneles, ya que, al igual que en el caso de la configuración de la red interna, nos abocaremos a lo que para el usuario podría ser mas práctico, los casos automáticos.

Tal como ya hemos mencionado, los túneles manuales deben ser configurados en ambos extremos del mismo. La siguiente figura esquematiza el funcionamiento

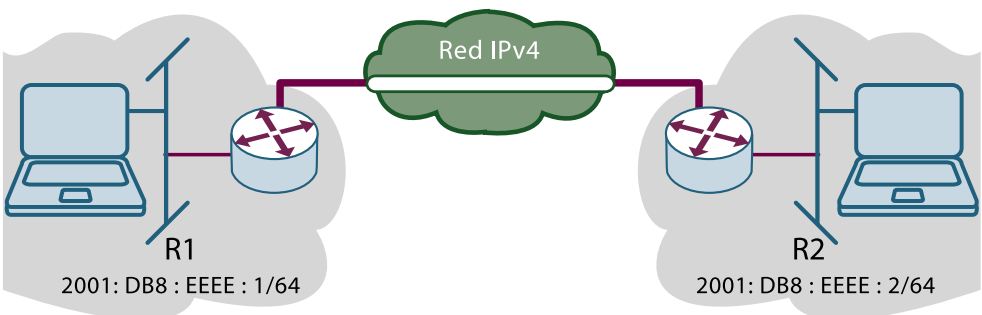


FIGURA 7: **ESQUEMA DEL FUNCIONAMIENTO DE UN TÚNEL MANUAL PARA ATRAVESAR REDES IPv6**

Una configuración típica y general para que se establezca el túnel de la figura, podría ser:

En R1

```
interface TunnelEjemploR1
no ip address
ipv6 address 2001:DB8:FFFF::1/64
tunnel source GigabitEthernet0/0
tunnel destination 1.1.1.1
tunnel mode ipv6ip
```

En R2:

```
interface TunnelEjemploR2
 no ip address
```

```
ipv6 address 2001:DB8:FFFF::2/64
tunnel source GigabitEthernet0/1
tunnel destination 2.2.2.2
tunnel mode ipv6ip
```

Estos comandos que aquí se expresan en forma general y solo a modo orientativo, variarán su sintaxis dependiendo del dispositivo que estemos configurando, su marca, sistema operativo, tipo, etc (puede ser desde un router hasta una computadora que funcione como tal).

4.2.2. Túneles Automáticos

Existe una gran variedad de este tipo de túneles, pero como es de lógica comprensión sólo podemos desarrollar algunos de ellos. Entre los que consideramos que pueden ajustarse a una red de un SOHO están los túneles 6to4 y Teredo.

4.2.2.1. 6to4

Los túneles 6to4 son un mecanismo que permite que dispositivos IPv6 que solo están conectados a redes IPv4, puedan alcanzar otras redes IPv6. Para lograr esto, trabaja con un grupo de direcciones preestablecidos por la IANA[10] para túneles 6to4: el bloque 2002::/16.

Así, el mecanismo de túneles 6to4 trabaja de la siguiente manera: un dispositivo, que dispone de una dirección IPv6, quiere comunicarse con otra dirección IPv6 que está por fuera de su red. Para ello, debe disponer de un router que soporte pseudo-interfaces 6to4 y que sea capaz de rutear el prefijo 2002::/16.

Además, necesitará también de al menos una dirección IPv4 pública de forma tal de calcular la dirección 6to4 para el router a partir de ésta. Este cálculo se realiza de la siguiente manera:

1- Se descompone la dirección IPv4 en notación nibble, por ejemplo:

Si disponemos de la dirección IPv4 192.0.2.1, su descomposición en nibbles sería:

192 ----> C0
0 ---> 00
2 ---> 02
1 ---> 01

2- Construimos la primer parte de la dirección del router utilizando el prefijo que antes mencionamos para las direcciones 6to4, de la siguiente manera:

2002:C000:0201::/48

10 http://www.iana.org/

3- Ya tenemos el prefijo para nuestro router, ahora elegimos cualquier identificador de interfaz[11], por ejemplo:

2002:C000:0201::1/128

Siguiendo con el desarrollo del funcionamiento de los túneles 6to4, además del dispositivo que intenta comunicarse con una red IPv6 y del router (generalmente de borde) con la pseudo-interfaz 6to4, necesitaremos un router en Internet contra el cual levantar el túnel. Ahora bien, ¿cuál es ese router? Existen en la red de redes varios de estos dispositivos con una dirección de tipo anycast, mas exactamente con la dirección: 192.88.99.1[12]. Asimismo, utilizando el mecanismo de la notación en nibble, esta dirección será: 2002:c058:6301::/128.

Así, el túnel estará construído entre la direcciones IPv4 de nuestro router y la dirección anycast 192.88.99.1. En virtud de ello tendremos un prefijo IPv6 6to4 2002:C000:0201::/48 para utilizar en nuestra LAN y la dirección 2002:c058:6301::/128 alcanzable a través del túnel. El prefijo 2002::/16 lo deberemos rutear por esa interfaz.

Este es un ejemplo de la creación de un túnel 6to4 en un router Cisco:

```
interface Tunnel2002
description Tunnel 6to4 a Internet
no ip address
no ip redirects
ipv6 address 2002:C000:0201::/48
tunnel source GigabitEthernet0/0
tunnel mode ipv6ip 6to4

interface GigabitEthernet0/0
description interfaz para 6to4
ip address 192.0.2.1 255.255.255.0

ipv6 route 2002::/16 Tunnel2002
```

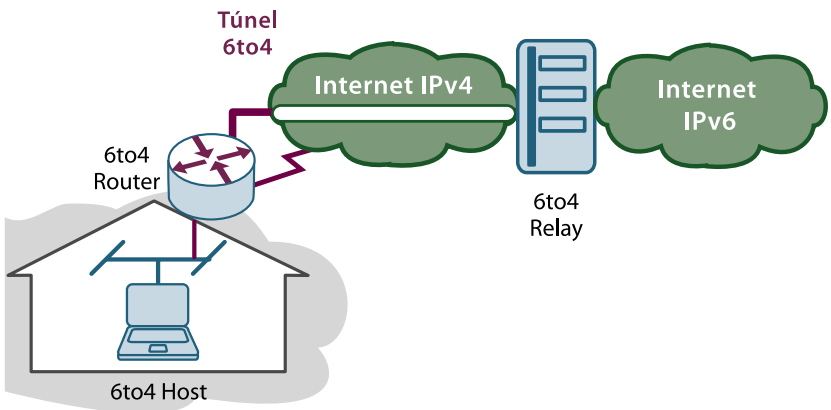



FIGURA 8: ESTABLECIMIENTO DE UN TÚNEL 6TO4

11 http://www.ietf.org/rfc/rfc3513.txt
12 http://www.ietf.org/rfc/rfc3068.txt

4.2.2.2. Teredo[13]

Teredo (o Miredo para los casos de software open-source) es un mecanismo que permite que un dispositivo pueda acceder a redes IPv6 aun estando detrás de un NAT IPv4.

Para lograrlo debe disponer de un servidor (por ejemplo, un servidor linux o BSD), de forma tal que éste sea el que provea las direcciones IPv6 con las cuales podremos atravesar el NAT. El servidor debe contar con una dirección IPv4 pública y alcanzable desde Internet.

Quien intenta acceder a Internet con los servicios de este Servidor Teredo, y conectarse con alguna dirección IPv6, es lo que denominamos Cliente Teredo.

Un servidor Teredo escucha las peticiones de un Cliente Teredo en el puerto 3544 de UDP[14] y le devuelve una dirección IPv6 para que éste la utilice y llegue a su destino.

Para que el tráfico pueda ir y venir entre las direcciones IPv6 de Internet y nuestro Cliente Teredo, vamos a comunicarnos con un Relay Teredo. Éste es el encargado de recibir el tráfico IPv6 del Cliente Teredo y reenviarlo.

También hay que tener en cuenta que el servidor Teredo, será quien anuncie hacia Internet el prefijo Teredo 2001:0000::/32.

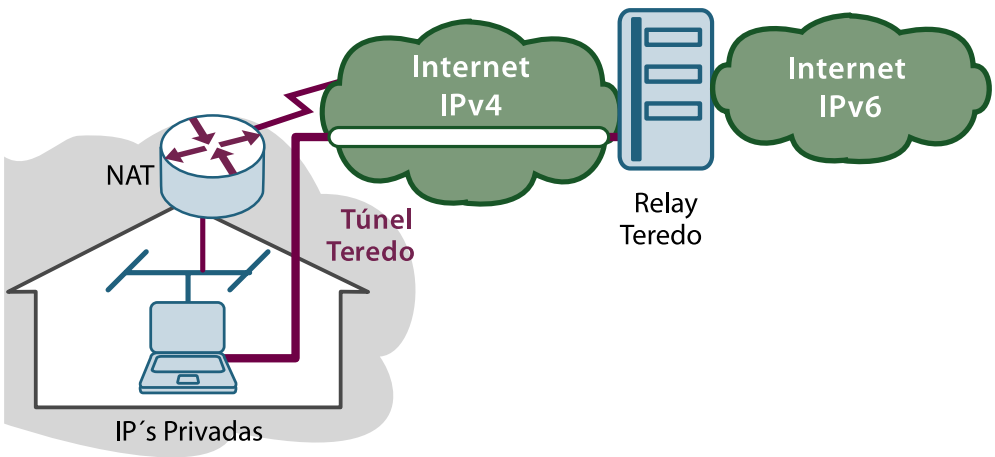


Figura 9: Esquema del funcionamiento de los túneles Teredo/Miredo

Si llegamos hasta aquí e hicimos todos los pasos descriptos, estamos conectados a IPv6 tanto internamente como con el exterior. Por lo que podríamos decir que nuestra tarea esta cumplida.

13 http://www.ietf.org/rfc/rfc4380.txt
14 http://www.ietf.org/rfc/rfc0768.txt

Asimismo, recordamos al lector que la misión del capítulo es dar una guía orientativa de las herramientas y pasos que pueden ayudarnos a la hora de querer armar nuestra red de la pequeña oficina o red residencial de forma tal que opere con IPv6, pero que no se constituye en la única forma de hacerlo, por el contrario, sólo mostramos un pequeño subconjunto dentro de las cuestiones prácticas que ofrece el mundo de la transición hacia IPv6.

5. Referencias

http://portalipv6.lacnic.net/

http://www.ipv6tf.org

4. Servicios con IPv6

1. Introducción

Este capítulo describe como instalar y configurar varios servicios básicos con IPv6 en algunos de los sistemas operativos más comunes. Prácticamente todos los servicios, aplicaciones y dispositivos de uso mayoritario soportan IPv6 (una lista detallada puede encontrarse en *http://www.ipv6-to-standard.org*).

Debe tenerse claro que la aplicación o programa del servicio se ejecuta sobre una plataforma, el servidor, con su sistema operativo y su hardware. De esta forma, el primer paso es habilitar IPv6 en la plataforma del servidor posibilitando así el transporte de datos sobre el protocolo IPv6 hacia/desde el servidor. Los pasos para habilitar IPv6 en diferentes sistemas operativos están descriptos en el capítulo dedicado a Usuario Final. Después para desplegar servicios con IPv6 basta con instalar y configurar las programas que soporten IPv6 y que en general son versiones extendidas de los que soportan IPv4

2. Sobre Servicios

Los servicios ofrecidos en Internet se conciben para que sean accedidos por cualquier cliente. Es decir el modelo cliente-servidor se basa en un servidor que es accedido por muchos clientes, iniciando siempre la comunicación el cliente.

Para facilitar el acceso a los servicios hay que conocer la dirección de red o IP (Internet Protocol) del servidor. De cara a hacer este proceso más amigable para el usuario final se creó el DNS (Domain Name System o Sistema de Nombre de Dominio) que traduce un nombre de dominio de un servidor en la dirección IP de dicho servidor, y por tanto es lo recomendado siempre en lugar de la direccion IP.

Por ejemplo, cuando accedemos a www.google.com desde un cliente web, de forma transparente al usuario, se resuelve este nombre de dominio a la dirección IP de un servidor web que ofrece al cliente la página de Google.

La dirección IP que se obtiene mediante el DNS puede ser IPv4, IPv6 o ambas. De esta forma se pueden hacer accesibles los servicios por IPv6 de forma amigable y transparente para el usuario final.

A continuación se aborda la instalación y configuración de distintos servicios sobre varias plataformas.

3. Telnet

3.1. Descripción del servicio:

Telnet es una aplicación muy conocida para comunicarse con otro equipo por medio de una interface de comandos usando el protocolo TELNET y el puerto TCP 23. Se basa

en el modelo cliente-servidor por lo que se requieren ambos para establecer la comunicación. El servidor telnet se instala por medio del programa “telnetd”.

3.2. Pasos de instalación y configuración:

Existen versiones para las distintas distribuciones de Linux. Las más comunes se instalan de la manera siguiente.

3.2.1. Debian:

Para instalar usar:
 # sudo apt-get install telnetd

El fichero de configuración es /etc/inetd.conf.

Para reiniciar el servicio usar:
 # sudo /etc/init.d/inetd restart

3.2.2. Fedora:

Para instalar usar:
 # yum install telnet-server telnet

Telnet se instala como un servicio llamado por el proceso xinetd. Para habilitar o deshabilitar telnet, se debe modificar el fichero /etc/xinetd.d/telnet, y donde se habilitaría telnet con: disable = no.

Por otro lado, se puede usar lo siguiente para reiniciar telnet:
 # /etc/init.d/xinetd restart

3.2.3. Red Hat Enterprise:

Para instalar usar:
 # up2date telnet-server telnet

Telnet se instala como un servicio llamado por el proceso xinetd. Para habilitar o deshabilitar telnet, se debe modificar el fichero /etc/xinetd.d/telnet, y donde se habilitaría telnet con: disable = no.

Por otro lado, se puede usar lo siguiente para reiniciar telnet:
 # /etc/init.d/xinetd restart

3.2.4. Ubuntu:

Para instalar usar:

 # sudo apt-get install telnetd

El fichero de configuración es /etc/inetd.conf.
Para reiniciar el servicio usar:
 # sudo /etc/init.d/openbsd-inetd restart

3.2.5. FreeBSD:

En FreeBSD el paquete del servidor telnet ya está instalado por defecto en /usr/libexec/telnetd

El fichero de configuración es /etc/inetd.conf. En este fichero habría que quitar el comentario (es decir borrar el #) en la siguiente línea para habilitar el servidor telnet:
#telnet stream tcp nowait root /usr/libexec/telnetd telnetd

Después habría que habilitar el servicio inetd para cargar telnet. En el fichero /etc/rc.conf, agregar la línea:
inetd_enable= "YES"

Para finalmente reiniciar el servidor telnet a través del servicio inetd usar el comando:
 # /etc/rc.d/inetd restart

4. SSH

4.1. Descripción del servicio:

SSH permite la comunicación con otro equipo por medio de una interface de comandos pero usando un canal seguro con encriptación y el puerto TCP 22. SSH generalmente sustituye a telnet cuando es necesaria la comunicación segura. SSH se basa también en el modelo cliente-servidor por lo que se requieren ambos para establecer la comunicación. El servidor SSH se instala por medio del programa "sshd".

4.2. Pasos de instalación y configuración:

Existen varias aplicaciones para servidores SSH. Para Linux destaca el Portable OpenSSH y para BSD el OpenSSH.

4.2.1. Debian/Ubuntu:

Para instalar usar:
 # sudo apt-get install openssh-server

Por defecto el servidor SSH queda habilitado después de instalarlo. Para detener, iniciar o reiniciar el servidor SSH usar:

 # sudo /etc/init.d/ssh stop
 # sudo /etc/init.d/ssh start
 # sudo /etc/init.d/ssh restart

4.2.2. Red Hat Enterprise:

El paquete openssh-server-4.3p2-29.el5.i386.rpm o superior incluye un servidor de SSH (http://rpmfind.net). Para ejecutar usar:

 # rpm -ihv openssh-server-4.3p2-29.el5.i386.rpm

El servidor tiene dos ficheros de configuración: /etc/ssh/sshd_config y /etc/ssh/ssh_host_key. El primer fichero se usa para la configuración de los aspectos generales, y aunque se puede modificar para adaptarlo al sistema particular, los valores por defecto de instalación son generalmente suficientes para usar el servidor SSH. El segundo fichero se usa para guardar las claves usadas en la comunicación con otros hosts.

Alternativamente para instalar podría usarse para buscar un sshd e instalarlo si es el caso:

 # up2date --showall | grep sshd

4.2.3. FreeBSD:

OpenSSH es parte del núcleo del sistema operativo, no son necesarios más pasos para instalarlo. El servicio se habilita en /etc/rc.conf

5. FTP

5.1. Descripción del servicio:

El protocolo FTP se usa para obtener o transferir ficheros desde/hasta un host remoto. FTP generalmente usa los puertos 20 y 21. Se basa en el modelo cliente-servidor por lo que se requieren ambos para establecer la comunicación. El servidor SSH se instala por medio del programa “ftpd”.

5.2. Pasos de instalación y configuración:

Existen varios programas de servidor FTP que soportan IPv6 (http://linuxmafia.com/faq/Network_Other/ftp-daemons.html). Algunos de los más comunes se instalan de la manera siguiente.

5.2.1 Red Hat:

El programa de Pure-FTPd se puede instalar desde pure-ftpd-1.0.22.tar.gz o superior

(http://www.pureftpd.org). Para instalar usar

 # tar xzvf pure-ftpd-1.0.22.tar.gz

Cambiarse a la carpeta resultante y ejecutar los comandos típicos para instalación:

./configure
make
make install

5.2.2. Ubuntu:

Para instalar el programa proftpd usar:

 # sudo apt-get install proftpd

6. Mail

6.1. Descripción del servicio:

El servicio de email o correo electrónico es uno de los más utilizados. Generalmente se usan los protocolos SMTP (puerto 25) para enviar los mensajes de correo, y POP3 (puerto 110) o IMAP4 (puerto143) para obtener los mensajes. El servicio se basa en el modelo cliente-servidor por lo que se requieren ambos para establecer la comunicación. Los principales servidores y clientes de correo soportan IPv6.

6.2. Pasos de instalación y configuración:

Existen varios programas servidores de SMTP, POP3 y IMAP4 que soportan IPv6. Sendmail (http://www.sendmail.org) es un servidor SMTP muy popular para ambientes Unix. El programa de la Universidad de Washington WU-IMAP (http://www.washington.edu/imap) para servidores IMAP4 y POP3 es muy usado. A continuación se describe como se instalan y configuran estos programas en algunos sistemas operativos.

6.2.1. Linux:

Descargar e instalar el programa Sendmail.

Sendmail no viene habilitado con IPv6 por defecto (por lo menos hasta la versión 8.12.X). Para habilitar el soporte IPv6, en el fichero de configuración: devtools/Site/site.config.m4, escribir la línea:

APPENDDEF(`confENVDEF', `-DNETINET6')

Y reconstruir (rebuild) Sendmail.

Después, en el fichero: sendmail.mc, escribir la línea:

DAEMON_OPTIONS(`Port=smtp, Name=MTA-v6, Family=inet6')dnl

Hacer un nuevo sendmail.cf, y reiniciar Sendmail.

Si se recibe algún mensaje de error, revisar que las librerías asociadas tengan soporte IPv6, reconstruyéndolas (rebuild) con soporte IPv6.

Por otro lado si se quiere un servidor POP3/IMAP4, descargar e instalar el programa UW-IMAP.

Para habilitar el soporte IPv6, en el fichero de configuración: /etc/inetd.conf, escribir las líneas:

 # Servidor IMAP con soporte IPv6
imap stream tcp6 nowait root /usr/sbin/tcpd imapd
 # Servidor POP3 con soporte IPv6
pop-3 stream tcp6 nowait root /usr/sbin/tcpd ipop3d

También es posible usar el programa Courier-IMAP en lugar del UW-IMAP. Descargar e instalar el programa Courier-IMAP (http://www.courier-mta.org/imap).

Al compilar el Courier-IMAP, automáticamente se habilitará IPv6 si se detecta el soporte IPv6 en el sistema operativo. Con esto no son necesarios pasos adicionales.

6.2.2. FreeBSD:

Descargar e instalar Sendmail.

Para habilitar el soporte IPv6, en el fichero de configuración: etc/sendmail.ipv6.cf, escribir la línea:

 # Opciones del SMTP daemon
O DaemonPortOptions= Port=smtp, Name=MTA-v6, Family=inet6, Addr=[dirección IPv6 del servidor mail]

Para iniciar el servicio de Sendmail, en el fichero: /etc/rc.local, escribir la línea
 # Servidor SMTP Sendmail con soporte IPv6
/usr/sbin/sendmail -C/etc/sendmail.ipv6.cf -bd -q30m

Por otro lado, Popper es un servidor POP3. Para instalarlo en BSD usar:
 # cd /usr/ports/mail/popper
 # make install

Para habilitarlo y configurarlo con IPv6, en el fichero: /etc/inetd.conf, escribir la línea:
 # Servidor POP3 Popper con soporte IPv6
pop3 stream tcp6 nowait root /usr/local/libexec/popper popper

6.2.3. Windows Server 2008:

El Windows Server 2008 tiene soporte completo con IPv6 en todas las aplicaciones de red y servicios principales, excepto para los servidores SMTP del Internet Information Services (IIS). Pero en cambio, el servidor de SMTP si tiene soporte IPv6 en el Microsoft Exchange Server 2007 con Service Pack 1. La instalación y configuración para IPv6 de este Exchange Server es en líneas generales igual que en el caso de IPv4.

7. Transmisión multimedia

7.1 Descripción del servicio:

Cada día es más común la necesidad de enviar o transmitir audio y video por medio de Internet y/o Intranets. La transmisión multimedia se basa en el modelo cliente-servidor por lo que se requieren ambos para establecer la comunicación.

7.2. Pasos de instalación y configuración:

Existen varios programas para transmisión de contenidos multimedia que soportan IPv6. El Windows Media Services es el más común en plataformas Windows, y se instala y configura de la manera siguiente.

7.2.1. Windows Servers

Para los servidores Windows 2000, 2003 y 2008 se puede usar la aplicación Windows Media Services (WMS) para la transmisión en vivo o bajo demanda de audio y video. El Windows Media Services actúa como servidor de streaming de fuentes codificadas (encoded). Las tareas que realiza el Windows Media Services incluyen: la espera de las peticiones de los clientes, revisar que la conexión de un usuario específico está permitida, controlar las conexiones de red, construir los paquetes de streaming usando como carga útil las fuentes codificadas, la entrega con IPv4 e IPv6 de los paquetes de streaming a destinos Unicast, Anycast, Multicast, etc.

- El Windows Media Services es un componente que viene integrado con los sistemas operativos Windows Servers.
- En Windows 2003 Server es posible actualizarlo si es necesario con: *http://download.microsoft.com/download/1/2/e/12e25064-8b99-4229-a554-acb67493742d/UpgradeWMS9S.exe*
- En Windows 2008 Server también viene integrado el Windows Media Services 2008 en el núcleo del sistema, o es posible instalarlo con: *http://www.microsoft.com/windows/windowsmedia/forpros/serve/prodinfo2008.aspx*

Otro aplicación que puede ser necesaria, para codificar (encoded) las fuentes multimedia, es el Windows Media Encoder (WME). Esta aplicación codifica las fuentes multime-

dia como DVD, entradas analógicas de audio/video, etc. a formatos que pueden usarse para la transmisión, tales como mp3 para audio and AVI para video. El Windows Media Encoder también puede usarse como transmisor multimedia pero solo cuando haya pocos clientes (5 o menos). Para instalar esta aplicación usar: *http://download.microsoft.com/download/8/1/f/81f9402f-efdd-439d-b2a4-089563199d47/WMEncoder.exe*

Para acceder a la interface de configuración del Windows Media Services: Programas > Herramientas Administrativas > Servicios de Windows Media

La base para la para transmisión de contenidos multimedia son los puntos de publicación.

7.2.1.1. Creación de un punto de publicación nuevo

Existen dos modelos diferentes **Push** y **Pull**.

Push

El encoder inicia la transmisión del streaming multimedia. Se configura en el enconder cual es el servidor de streaming, y cada vez que se inicia la codificación, se envía a ese servidor de streaming el flujo multimedia. Es la forma más sencilla de gestionar todo, aunque se consume ancho de banda, entre el encoder y el servidor de streaming, incluso si no hay usuarios conectados al servidor.

La configuración es como sigue:

- En el encoder, en Propiedades > Salida, seleccionar "Push to server (the connection is initiated by the encoder)"
  - Nombre del servidor: streaming.ejemplo.com:8100 (este es el servidor de streaming en el puerto 8100 ya que es posible que el puerto 80 este ocupado por un servidor de Web)
  - Punto de publicación: Publishing point: nombre_del_evento_a_transmitir (este será el punto de publicación de la conexión de los usuarios)
  - Copiar setting: push_test (esta es una configuracion en el servidor de streaming que se copia para crear el punto de publicación "nombre_del_evento_a_transmitir". Esta configuración extrae el streaming del codificador y pone push:* en el tipo de streaming)

- Se puede ajustar la compresión en Propiedades > Compresión. Para realizar pruebas se recomienda que el total del streaming no supere los 150 kbps. Anchos de banda mayores pueden usarse dependiendo del disponible en las redes donde se vaya a hacer la transmisión.

- Una vez realizado esto se inicia la codificación con "Start Encoding" y el encoder envía el flujo al servidor de streaming. Es posible que salga un aviso acerca de los pasos que hay que hacer si el punto de publicación es multicast. Se puede ignorar.

- Llegará un punto que el enconder pida un usuario y password para publicar en nuestro servidor de streaming y debes usar el siguiente usu/pass: prueba/4321.

- El usuario que se pone tiene que tener permisos de escritura en el WMS, para ello se configura en propiedades (del servidor de streaming) > autorización > autorización ACL de puntos de publicación de WMS.

- También hay que habilitar propiedades (del servidor de streaming) > autenticación -> autenticación de negociación WMS.

- Así, el servidor creará automáticamente el punto de publicación y los usuarios podrán conectarse a él por medio de las siguientes URLs :
  - *http://streaming.ejemplo.com:8100/nombre_del_evento_a_transmitir*
  - *mms://streaming.ejemplo.com/nombre_del_evento_a_transmitir*

- El punto de publicación es de distribución (no bajo demanda) y aparece en la interfaz gráfica de color azul en vez de verde.

Pull

La configuración es como sigue:

- En el encoder, en Propiedades > Salida, seleccionar "Pull"

- En el WM Server se configura un punto de publicación de tipo "extraer" con una URL como
  - *http://nombre_servidor:puerto_servidor*

- Cuando se recibe una petición de conexión en el WM Server, desde un usuario, el server se conecta al enconder y hace el streaming.

7.2.1.1. Transmisión/grabación de un evento

Usualmente hay que tener una máquina (Windows 2003) dedicada, por razones de prestaciones, e instalarle el Windows Media Encoder (WME).

Si se usa una cámara de video externa, además hay que instalar a ese servidor una tarjeta capturadora de video a la que se conecta la cámara. Alternativamente se puede usar una cámara USB sin necesidad de tarjeta capturadora.

El WME se puede configurar para codificar el audio/video de la cámara, hacer la transmisión del streaming y además de grabarlo en el disco duro local. Si se esperan más de cinco conexiones de streaming entonces no se puede usar una sola máquina, y lo que hay que hacer es usar un computador para el WMS y otra para el WME. Esto depende de la capacidad de CPU del servidor que grabe la sesión. Para usar un servidor de streaming + encoder hay que seguir las instrucciones del modelo Pull mencionado arriba.

8. Web

8.1. Descripción del servicio:

La navegación web utiliza el protocolo HTTP para transferir hipertextos, páginas web o páginas HTML, y para la navegación web generalmente se usa el puerto 80. Se basa en el modelo cliente-servidor por lo que se requieren ambos para establecer la comunicación. El servidor web o HTTP se instala por medio del programa "httpd".

8.2. Pasos de instalación y configuración:

Es el más utilizado de los servicios y los programas que se utilizan para ofrecer este servicio son muchas, pero las más extendidas son Apache e IIS. Veremos cómo instalar y configurar ambas aplicaciones para que respondan a peticiones sobre IPv6.

8.2.1. Apache

Apache es el más extendido de los servidores web actualmente y su entorno natural de ejecución son las plataformas Linux. Para tener soporte IPv6 hay que utilizar versiones 2.x. Lo ejemplos aquí mostrados se basan en la versión 2.0.63.

Para la instalación se pueden utilizar los sistemas habituales de cada distribución (apt-get install apache2, yum, up2date, rpm, etc.) o descargarse los ficheros fuentes desde http://httpd.apache.org y compilarlo:

```
#>cd /usr/local/src
#>tar -xzvf httpd-2.0.63.tar.gz
#>cd httpd-2.0.63
#>./configure --prefix=/usr/local/apache2 --enable-module=so
#>make
#>make install
```

El parámetro --prefix indica la carpeta en la que se hará la instalación. El parámetro --enable-module=so habilita el soporte de Dynamic Shared Object (DSO) para poder cargar dinámicamente módulos, por ejemplo PHP.

8.2.2.1. Escuchar IPv6

A partir de Apache 2.0.x el soporte IPv6 viene habilitado por defecto, así que después de instalarlo solo hay que iniciarlo para que escuche por IPv6. Recordar que primero el soporte IPv6 debe estar configurado en el servidor Linux.

La directiva que controla las IPs y puertos por los que escucha el servidor web es Listen y se encuentra en el fichero de configuración principal httpd.conf. Por defecto escucha por todas las IPs y el puerto 80 (http):

Listen 80

Para comprobar que está escuchando por IPv6 el servidor en el puerto 80 se puede utilizar el comando netstat:

```
[root]# netstat -tan
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address  Foreign Address     State
...
tcp  0     0    :::80        :::*            LISTEN
...
```

Lo que indica que está escuchando (LISTEN) en cualquier dirección (::) del servidor, ya sea IPv4 o IPv6, por el puerto 80 (:80).

8.2.1.2. Virtual Hosts

Para configurar hosts virtuales IPv6 hay que utilizar corchetes [] para "encerrar" la dirección IPv6, por ejemplo:

```
NameVirtualHost [2001:db8:1::1000:1234]
NameVirtualHost 10.0.0.3

<VirtualHost [2001:db8:1::1000:1234]>
 DocumentRoot /example/htdocs/web-v4-v6
 ServerName www.example.com
</VirtualHost>

<VirtualHost 10.0.0.3>
 DocumentRoot /example/htdocs/web-v4-v6
 ServerName www.example.com
</VirtualHost>

<VirtualHost [2001:db8:1::1000:1234]>
 DocumentRoot /example/htdocs/web-solo-v6
 ServerName ipv6.example.com
</VirtualHost>
```

La anterior configuración permite al servidor:

- Atender peticiones sobre IPv4 a la dirección 10.0.0.3 y sobre IPv6 a la dirección 2001:db8:1::1000:1234
- Las peticiones recibidas a esas direcciones se distinguen por la URL a la que van dirigida, por eso
- Las peticiones a *www.example.com* se atienden por IPv4 e IPv6, sirviendo el contenido de la carpeta /example/htdocs/web-v4-v6
- Las peticiones a ipv6.example.com se atienden por IPv6 solamente, sirviendo el contenido de la carpeta /example/htdocs/web-solo-v6

NOTA: Lo normal, en el ejemplo anterior, es que www.example.com resuelva por DNS a las dos direcciones IPv4 e IPv6. Igualmente ipv6.example.com debería resolver solamente a la dirección IPv6. Para más información ver sección sobre DNS más adelante.

6.1.3. Truco: Mostrar dirección IPv6/IPv4 del cliente

Puede resultar de interés mostrar en la página web de nuestro servidor la dirección IP que utiliza el cliente para acceder. Para ello, aunque existan otras formas de hacerlo, mostraremos un ejemplo de cómo hacerlo utilizando el lenguaje de programación PHP, que es el más común en entornos Linux/Apache.

Solo habría que introducir en la página inicial, por ejemplo index.php, el siguiente código:

```
<?php if(strpos($_SERVER['REMOTE_ADDR'],".")===false)
 {
  echo "<font color='#FF0000' size=2 face='verdana'>Esta usando IPv6 (".$_
SERVER['REMOTE_ADDR']).</font><br><br>";
  }else{
  $DIRv4=str_replace("::ffff:","",$REMOTE_ADDR);
   echo "<font color='#FF0000' size=2 face='verdana'>Esta usando IPv4 (".$_
SERVER['REMOTE_ADDR']).</font><br><br>";
  }
?>
```


8.2.1.3. Truco: Deshabilitar sendfile

Apache 2 soporta un método llamado sendfile ofrecido por el sistema operativo que aumenta la velocidad a la que sirve datos. Algunos controladores de tarjetas de red también soportan hacer TCP-checksums offline. En algunos casos, esto puede llevar a problemas de conexión y checksums TCP inválidos para tráfico IPv6.

En estos casos, hay que deshabilitar sendfile o bien recompilando el servidor utilizando la opción de configuración **--without-sendfile** o bien utilizando la directiva **EnableSendfile off** en el fichero de configuración de Apache (httpd.conf).

La directiva EnableSendfile off solo se soporta en versiones posteriores a la 2.0.44.

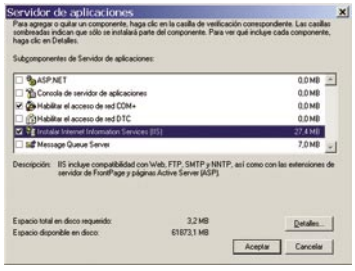
8.2.1.5. Comprobar que funciona

Utilizando el truco de mostrar la dirección con la que accedemos, se puede probar desde un navegador en el propio servidor que se puede acceder por IPv4 e IPv6, para ello se pueden utilizar las direcciones de localhost IPv4 (127.0.0.1) e IPv6 (::1):

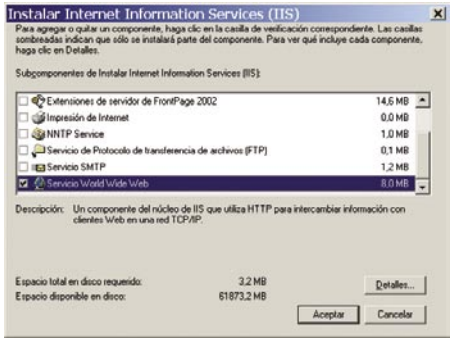
8.2.2. IIS

IIS (Internet Information Services) de Microsoft tiene su entorno natural en los servidores Windows, por lo que aquí se explicará utilizando como plataforma Windows Server 2003 R2 SP2 Standard Edition actualizado, que viene con IIS v6.0.

Su instalación/desinstalación se hace desde **Agregar o quitar programas** en el Panel de Control. Entrando en **Quitar o Agregar Componentes de Windows** se accede al Asistente para componentes de Windows.



En el Asistente para componentes de Windows, seleccionar **Servidor de Aplicaciones** y hacer clic en Detalles… Seleccionar **Instalar Internet Information Services (IIS)** y hacer clic en **Detalles…**

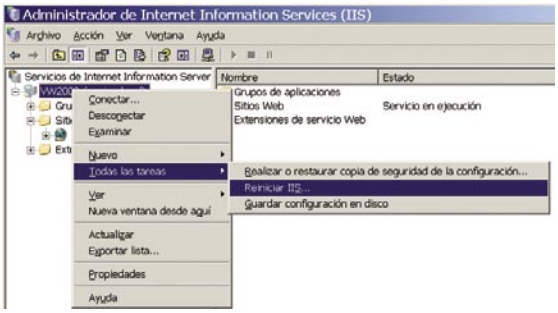


Para instalar correctamente el servidor web hay que activar **Administrador de Servicios de Internet Information Services, Archivos Comunes y Servicio World Wide Web.**

NOTA: Será necesario disponer del CD de instalación de Windows Server 2003.

8.2.2.1. Escuchar IPv6

Una vez instalados el servidor IIS e IPv6 *(C:\>netsh interface ipv6 install)* en el servidor conviene reiniciar el servicio de IIS para hacer que escuche por IPv6. Para ello se utiliza el **Administrador de IIS** que se encuentra en las Herramientas administrativas. Seleccionando el servidor sobre el que se ejecuta el IIS y haciendo clic con el botón derecho, aparece la opción **Reiniciar IIS…** dentro de Todas las Tareas:



Podemos comprobar que se está escuchando por el puerto 80 (http) sobre IPv6:

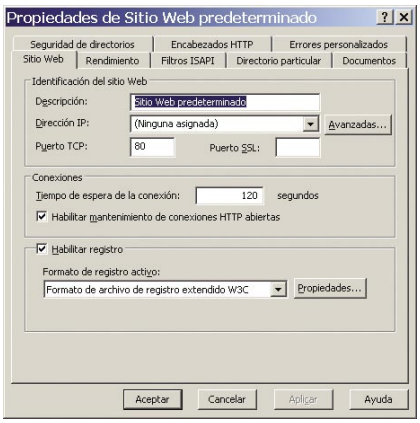
C:\>netstat -an -p tcpv6
Conexiones activas

Proto Dirección local Dirección remota Estado
TCP [::]:80 [::]:0 LISTENING 0
...

8.2.2.2. Configurar IIS

La configuración de IIS para que devuelva páginas web sobre IPv6 se hace para cada web. Para ello hay que usar el **Administrador de IIS** que se encuentra en las Herramientas Administrativas.

Haciendo clic con el botón derecho sobre la web a configurar y seleccionando Propiedades se entra a configurar las características de la web:



En la solapa Sitio Web debe configurarse en Dirección IP el valor Ninguna Asignada. De esta forma se escucha por el puerto 80 y por todas las direcciones IPv4 e IPv6. Se pueden añadir detalles entrando en Avanzadas…

En la siguiente figura se ve un ejemplo donde se puede acceder a la web mediante:

- **Solo IPv4:** *ipv4.example.com*, que resuelve a la IPv4 192.168.1.101
- **IPv4 e IPv6:** *www.example.com* que resuelve a las direcciones IPv4 e IPv6 del servidor
- **Solo IPv6:** ipv6.example.com que resuelve a la dirección IPv6 del servidor

Otro ejemplo más sencillo que permitiría el acceso usando cualquier IP y cualquier nombre de dominio sería:

8.2.2.3. Truco: Mostrar dirección IPv6/IPv4 del cliente

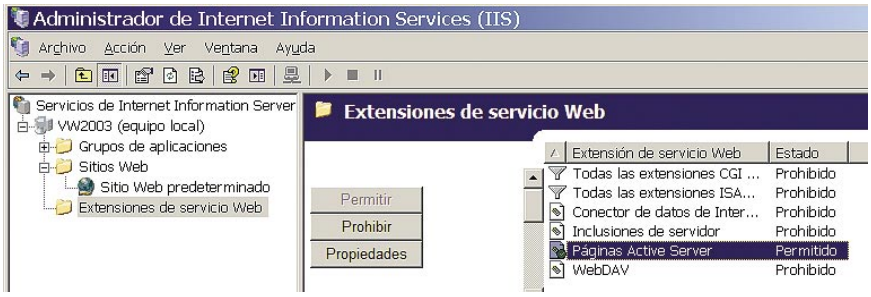
Puede resultar de interés mostrar en la página web de nuestro servidor la dirección IP que utiliza el cliente para acceder. Para ello mostraremos un ejemplo de cómo hacerlo utilizando el lenguaje de programación ASP, que es el más común en entornos Windows/IIS.

Solo habría que introducir en la página inicial, por ejemplo default.asp, el siguiente código:

```
<%
  if InStr(Request.ServerVariables("REMOTE_ADDR"),".") = 0 then
    response.Write( "<font color='#154983' size=2 face='verdana'> Esta usando
IPv6.<br><br>")
  else
    response.Write ("<font color='#FF0000' size=2 face='verdana'> Esta usando
IPv4.<br><br>")
  end if

    response.Write ("(" &Request.ServerVariables("REMOTE_ADDR") & ")</
font><br><br>")
  %>
```

NOTA: Para que funcionen las páginas ASP, estas debe permitirse en las Extensiones de servicio Web en el Administrador de IIS. Tal como se muestra en la siguiente figura.



8.2.2.4. Comprobar que funciona

Utilizando el truco de mostrar la dirección con la que accedemos, se puede probar desde un navegador en el propio servidor que se puede acceder por IPv4 e IPv6, para ello se pueden utilizar las direcciones de localhost IPv4 (127.0.0.1) e IPv6 (::1):

9. DNS

9.1. Descripción del servicio:

El servicio de DNS traduce nombres de dominio a direcciones de red tanto IPv4 como IPv6, y su función es fundamental en la Internet actual.

Sin entrar en mucho detalle sobre cómo funciona el DNS, debe tenerse claro que son cosas diferentes el transporte de tráfico DNS (a través de una red IPv4 y/o IPv6) y los datos contenidos en los servidores DNS (registros A para IPv4 y AAAA para IPv6). Ambas cosas con independientes del protocolo IP utilizado. En la siguiente figura puede verse como para resolver una dirección IPv6 (AAAA) se utiliza transporte IPv4 e IPv6 de manera indiferente.

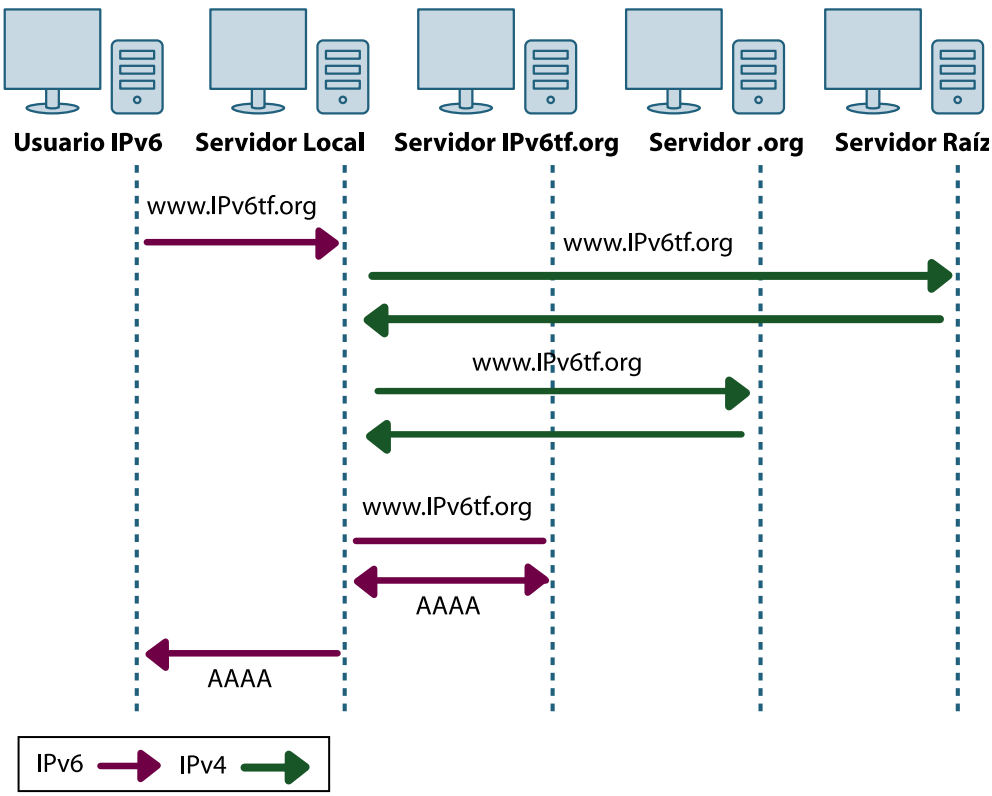


FIGURA 1: **DIFERENCIA ENTRE TRANSPORTE Y CONTENIDO EN DNS**

Por esto veremos como por un lado se configura la aplicación servidor para que atienda peticiones IPv6 (transporte) y por otro lado cómo se incluyen datos relacionados con IPv6 en los contenidos servidos (datos).

Actualmente es recomendable que todos los servidores DNS sean de doble-pila, es decir, que sean capaces de hacer peticiones DNS sobre IPv4 e IPv6 debido a que no toda

la infraestructura de DNS soporta IPv6. Además así se asegura la compatibilidad con los servidores ya existentes.

Otro concepto importante es el de servidor maestro o primario y el de servidor secundario o esclavo para un dominio. En pocas palabras, el servidor maestro es donde se crean y actualizan los datos del DNS, que luego se propagan a los servidores esclavos automáticamente.

9.2. Pasos de instalación y configuración:

Existen varios programas de servidor DNS que soportan IPv6, los más usados, tanto en IPv4 como en IPv6, son BIND para plataformas tipo UNIX y Windows DNS Server para plataformas Windows, los cuales se instalan y configuran de la siguiente manera.

9.2.1 BIND

BIND (Berkeley Internet Name Domain) es el más extendido de los servidores DNS actualmente y su entorno natural de ejecución son las plataformas Linux. Para su configuración habrá que editar ficheros de texto.

Para la instalación se pueden utilizar los sistemas habituales de cada distribución (apt-get, yum, up2date, rpm, etc.) o descargarse los ficheros fuente desde *https://www.isc.org/software/bind* y compilarlo:

```
# tar -xzvf bind-9.4.2-P2.tar.gz
# cd bind-9.4.2-P2
# ./configure
# make
# make install
```

Partiendo de una instalación ya existente como ejemplo (BIND 9.4.2-P2) se mostrará como:

- Habilitar el atender peticiones sobre IPv6 (Escuchar IPv6)
- Asociar direcciones IPv6 a nombres de dominio (Registros AAAA)
- Resolución inversa de direcciones IPv6 a nombres de dominio (Registro PTR)

9.2.1.1. Escuchar IPv6

El fichero principal que contiene la configuración del servidor DNS se encuentra en nuestro caso en /etc/named.conf, y es donde hay que cambiar cosas.

Para habilitar la escucha por IPv6 del servidor debe añadirse a la sección options la directiva listen-on-v6 {};, de forma que quede el inicio de named.conf de forma parecida a:

```
options {
    directory "/var/named/";
    listen-on-v6 { any; };
```

```
};
```

De esta forma el servidor DNS escuchara en todas las direcciones IPv6 que posea el servidor.

9.2.1.2. Registros AAAA

Las direcciones IPv6 se almacenan en registros de tipo AAAA en el DNS. Todo servidor DNS tiene lo que se llaman ficheros de zona que contienen la información del DNS relacionada con un subdominio. Utilizaremos el subdominio example.com.

En BIND se configura en /etc/named.conf las zonas de las que se encarga el servidor, por ejemplo, se declara que la zona que se encuentra en el fichero /var/named/example.com.zone se cargue al iniciar el servidor que será el maestro o primario[1] para el subdominio example.com:

```
zone "example.com" {
    type master;
    file "example.com.zone";
};
```

Los ficheros de zona para resolución directa pueden contener registros con direcciones IPv4 e IPv6 a la vez. Siguiendo con el ejemplo, editamos /var/named/example.com.zone y añadimos lo siguiente:

```
ipv4-ipv6   IN    A     10.0.0.3
    IN    AAAA   2001:db8:1:0:0:0:1234:5678

ipv6      IN    AAAA   2001:db8:1:0:0:0:1234:5678

ipv4            IN    A     10.0.0.3
```

Hemos configurado que:

- ipv4.example.com resuelva solamente a una dirección ipv4 (10.0.0.3).
- ipv6.example.com resuelva solamente a una dirección IPv6 (2001:db8:1:0:0:0:1234:5678).
- ipv4-ipv6.example.com resuelva a una dirección IPv4 y a una dirección IPv6 a la vez (será decisión del sistema operativo y/o aplicación utilizar una u otra dirección).

9.2.1.3. Registros PTR

Este tipo de registros PTR no es nuevo y es el mismo que se utiliza para la resolución inversa de direcciones IPv4 a nombres de dominio. La diferencia con IPv6 viene en la notación utilizada para representar las direcciones IPv6 (notación usando nibbles[2]) y en el

1 Para hacer que sea secundario o esclavo usar type slave;
2 Un nibble son cuatro bits, por lo que se suele representar en formato hexadecimal.

nombre de dominio usado para ello (IP6.ARPA). Los ficheros de zona para resolución inversa de direcciones IPv6 contendrán solamente direcciones IPv6.

Ahora veamos un ejemplo con IPv6:

En /etc/named.conf se declara la zona de resolución inversa correspondiente al prefijo 2001:db8:1::/48 que nos han delegado para nuestras redes:

```
zone "1.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa" {
type master;
file "2001_0db8_0001.zone";
};
```

Como se observa se divide el prefijo en nibbles y se concatenan en orden inverso al dominio ip6.arpa.

El fichero 2001_0db8_0001.zone contendrá:

```
$TTL 86400
@ IN SOA ns1.example.com. dnsadmin.example.com (
  2002071901 ; serial
  28800 ; refresh
  7200 ; retry
  604800 ; expire
  86400 ; ttk
  )
IN NS ns1.example.com.

4.3.2.1.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0 IN PTR www.example.com.
8.7.6.5.4.3.2.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0 IN PTR ipv6.example.com.
```

Lo que significa que:

- La dirección 2001:db8:1::1000:1234 resolverá al nombre de dominio *www.example.com*
- La dirección 2001:db8:1::1234:5678 resolverá al nombre de dominio *ipv6.example.com*

Hay que tener en cuenta que el número total de nibbles de una dirección IPv6 es de 32, por lo que los nibbles declarados en named.conf (12 en nuestro ejemplo) y los nibbles de cada dirección en el fichero de zona (20 en nuestro ejemplo) deben sumar 32.

9.2.1. 4. Probando la configuración

Para comprobar que los cambios se han aplicado, primero reiniciamos el servidor DNS (en nuestro sistema de ejemplo se utiliza /etc/init.d/named restart).

Se puede ver como el servidor está escuchando en las direcciones IPv6 e IPv4 en el puerto del DNS (puerto 53):

```
# netstat -tan
Proto Recv-Q Send-Q Local Address        Foreign Address   State
...
tcp    0    0  ::1:53                  :::*        LISTEN
tcp    0    0  2001:db8:1:0:0:0:1234:5678:53  :::*       LISTEN
tcp    0    0  10.0.0.3:53              0.0.0.0:*   LISTEN
tcp    0    0  127.0.0.1:53             0.0.0.0:*   LISTEN
...
```

Desde el mismo servidor se puede utilizar la aplicación cliente dig que permite hacer consultas a nuestro servidor.

Para resolver *ipv6.example.com*:

```
# dig any ipv6.example.com

; <<>> DiG 9.4.2-P2 <<>> any ipv6.example.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48527
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 6

;; QUESTION SECTION:
; ipv6.example.com.                IN     ANY

;; ANSWER SECTION:
ipv6.example.com.    172800  IN   AAAA   2001:db8:1:0:0:0:1234:5678
...
;; Query time: 4 msec
;; SERVER: ::1#53(::1)
;; WHEN: Wed Jun 17 17:23:48 2009
;; MSG SIZE  rcvd: 296
```

Para resolver *ipv4-ipv6.example.com*:

```
# dig any ipv4-ipv6.example.com

...
;; QUESTION SECTION:
; ipv4-ipv6.example.com.                IN     ANY

;; ANSWER SECTION:
ipv4-ipv6.example.com.  172800  IN   A    10.0.0.3
ipv4-ipv6.example.com.  172800  IN   AAAA  2001:db8:1:0:0:0:1234:5678
```

...

Para la resolución inversa de 2001:db8::1000:1234

 # dig -x 2001:db8::1000:1234

; <<>> DiG 9.4.2-P2 <<>> -x 2001:db8::1000:1234
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1333
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 4

;; QUESTION SECTION:
;4.3.2.1.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa. IN PTR

;; ANSWER SECTION:
4.3.2.1.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa. 172800 IN PTR www.example.com.

;; Query time: 1 msec
;; SERVER: ::1#53(::1)
;; WHEN: Wed Jun 17 17:37:02 2009
;; MSG SIZE rcvd: 270

9.2.1.5. Fichero de Pistas (Sección Extra)

En /etc/named.conf se configura el uso de un fichero de pistas ("hints") que contiene las direcciones IP de los servidores raíz del DNS.

```
zone "." {
    type hint;
    file "named.root";
};
```

Sin necesidad de entrar en detalles, estos servidores han empezado a ser accesibles por IPv6 desde hace poco (4 de Febrero de 2008) y el fichero de pistas se ha actualizado convenientemente.

Por esto, de cara a completar la configuración de IPv6 en su servidor DNS deberá actualizar el fichero de pistas utilizado para que incluya las direcciones IPv6 de los servidores raíz que las posean. El último disponible en http://www.internic.net/zones/named.root es del 12 de Diciembre de 2008 donde siete de los trece servidores raíz ya tienen una dirección IPv6 asociada.

Como ejemplo del contenido del fichero named.root:

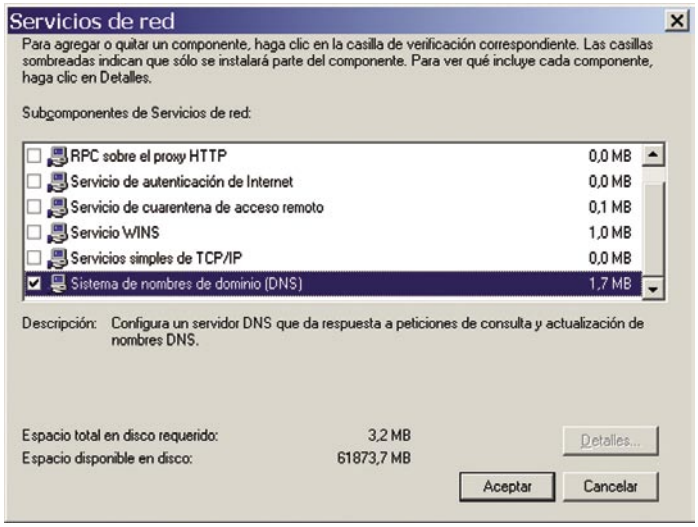
```
.                    3600000 IN NS   A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.  3600000    A    198.41.0.4
A.ROOT-SERVERS.NET.  3600000    AAAA 2001:503:BA3E::2:30
```

9.2.2. Windows DNS Server

Windows DNS Server de Microsoft tiene su entorno natural en los servidores Windows, por lo que aquí se explicará utilizando como plataforma Windows Server 2003 R2 SP2 Standard Edition actualizado.

Su instalación/desinstalación se hace desde Agregar o quitar programas en el Panel de Control. Entrando en Quitar o Agregar Componentes de Windows se accede al Asistente para componentes de Windows:

En el Asistente para componentes de Windows, seleccionar Servicios de red y hacer clic en Detalles… El servidor DNS se denomina Sistema de nombres de dominio (DNS):



NOTA: Será necesario disponer del CD de instalación de Windows Server 2003.

9.2.2.1. Escuchar IPv6

Una vez instalado el servidor DNS e IPv6 en el servidor (C:\>netsh interface ipv6 install) hay que hacer que el servidor DNS escuche sobre IPv6. Para ello hay que utilizar:

```
C:\>dnscmd /config /EnableIPv6 1
Registry property EnableIPv6 successfully reset.
Command completed successfully.
```

NOTA: dnscmd.exe es parte de las Windows Server 2003 Support Tools, que pueden encontrarse en la carpeta Support\Tools del CD de Windows Server 2003 y se instalan ejecutando suptools.msi en esa carpeta.

Es necesario reiniciar el servidor DNS o el servidor para que empiece a escuchar por IPv6. Esto se hace entrando en Herramientas Administrativas y ejecutando la aplicación de gestión Servicios. Localizar Servidor DNS y reiniciarlo.

Para comprobar que el servidor DNS (puerto 53) está escuchando por IPv6 se puede utilizar el comando netstat:

```
C:\>netstat -a -n -p udpv6
Conexiones activas
  Proto  Dirección local          Dirección remota    Estado
  UDP    [::]:53                  [::]:0              LISTENING   0
  ...
  UDP    [2001:db8:1::1000:1234]:53  [::]:0          LISTENING   0
  UDP    [fe80::1%1]:53           [::]:0             LISTENING   0
  UDP    [fe80::ffff:ffff:fffd%6]:53 [::]:0          LISTENING   0
  UDP    [fe80::200:1cff:feb5:5a88%5]:53  [::]:0     LISTENING   0
```

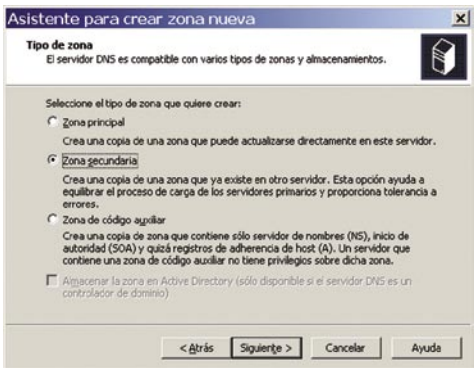

9.2.2.2. Registros AAAA

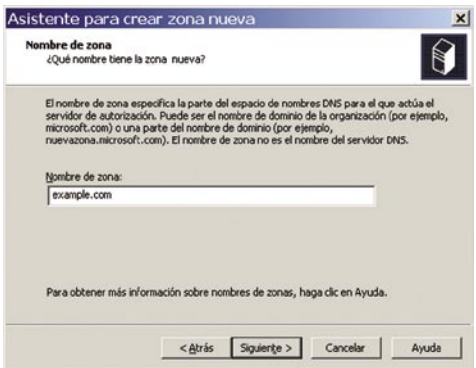
Si el servidor es esclavo o secundario para una zona que contiene registros AAAA con direcciones IPv6, entonces se puede usar la interfaz gráfica para configurarlo. Esto, siempre y cuando el servidor maestro para la zona y los demás esclavos tengan una dirección IPv4 accesible, ya que la interfaz gráfica no permite introducir direcciones IPv6 para ellos.

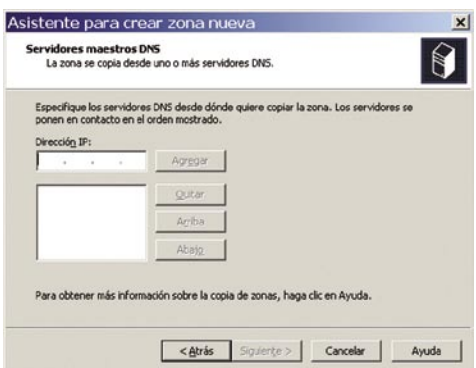
Para configurar un nuevo dominio con el servidor como esclavo o secundario, hay que utilizar la interfaz gráfica de configuración, que es la herramienta DNS dentro de las Herramientas Administrativas.

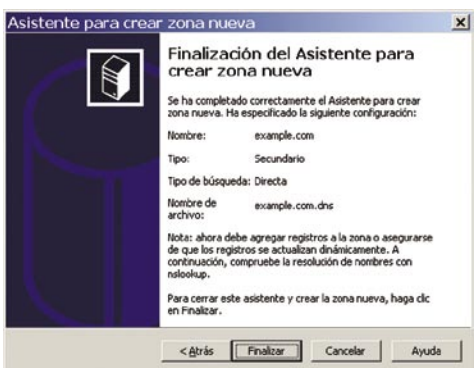
Para ello se hace clic con el botón derecho del ratón sobre Zonas de búsqueda directa para una zona de resolución de nombres de dominio a IP. Se selecciona Zona nueva, lo que abrirá el asistente para crear una nueva zona:

Seleccionar Zona secundaria como tipo de zona, poner el nombre de la zona (por ejemplo example.com) y configurar las direcciones IPv4 de los servidores maestros (el primario y otros secundarios si los hubiese).









Si el servidor es maestro o primario para una zona con registros AAAA con direcciones IPv6 entonces hay que utilizar la interfaz de comandos para configurarlo[3], concretamente dnscmd. Algunos de los comandos disponibles son son[4]:

- **Añadir una zona**: dnscmd serverName /ZoneAdd zoneName zoneType [options]

3 También se usarían comandos en caso de ser un servidor secundario o esclavo pero no haber ningún otro servidor accesible por IPv4.

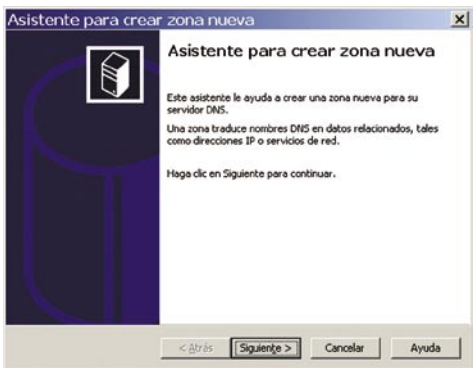
4 Usar dnscmd /? para obtener ayuda sobre los comandos disponibles. Usar dnscmd <comando> /? para obtener ayuda sobre un comando específico.

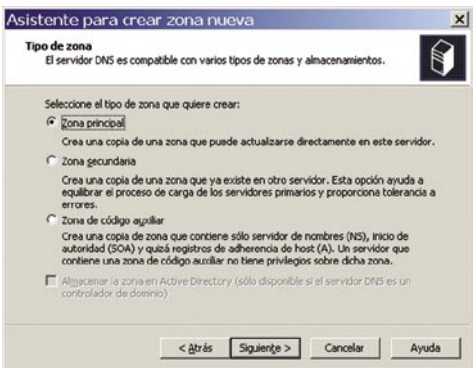
- **Borrar una zona:** dnsdmd serverName /ZoneDelete zoneName [/DsDel] [/f]
- **Añadir un registro:** dnscmd serverName /RecordAdd zoneName nodeName [/Aging] [/OpenAcl] [Ttl] typeRR dataRR
- **Borrar un registro:** dnscmd serverName /RecordDelete zoneName nodeName typeRR dataRR [/f]
- **Ver zonas del servidor:** dnscmd serverName /Enumzones
- **Ver contenido de una zona:** dnscmd serverName /ZonePrint zoneName
- **Ver registros asociados a un nombre de dominio:** dnscmd serverName> /EnumRecords <ZoneName> <NodeName>

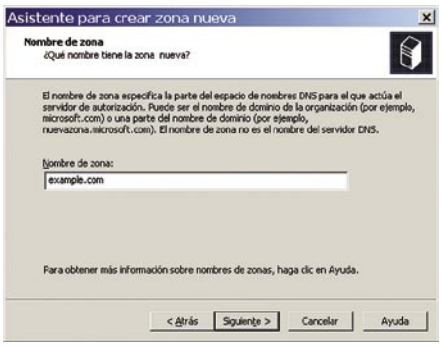
Veamos un ejemplo en el que se va a crear una zona example.com de la que el servidor es primario y en la que:

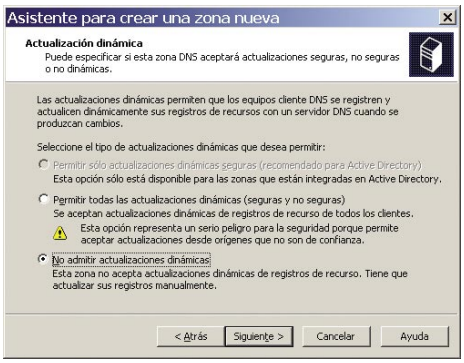
- *ipv4.example.com* resuelva solamente a una dirección IPv4 (10.0.0.3).
- *ipv6.example.com* resuelva solamente a una dirección IPv6 (2001:db8:1:0:0:0:1234:5678).
- *ipv4-ipv6.example.com* resuelva a una dirección IPv4 y a una dirección IPv6 a la vez (será cosa de la aplicación usar una u otra dirección).

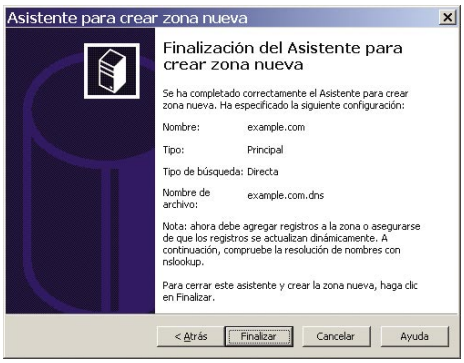
Primero creamos la zona desde la interfaz gráfica. Para ello se hace clic con el botón derecho del ratón sobre Zonas de búsqueda directa para una zona de resolución de nombres de dominio a IP. Se selecciona Zona nueva, lo que abrirá el asistente para crear una nueva zona:











Ahora introducimos los registros utilizando la línea de comandos:

C:\>**dnscmd ::1 /RecordAdd example.com ipv4 A** 10.0.0.3
Add A Record for ipv4.example.com at example.com
Command completed successfully.

C:\>**dnscmd ::1 /RecordAdd example.com ipv6 AAAA 2001: db8:1:0:0:0:1234:5678**
Add AAAA Record for ipv6.example.com at example.com
Command completed successfully.

C:\>dnscmd ::**1 /RecordAdd example.com ipv4-ipv6 A 10.0.0.3**
Add A Record for ipv4-ipv6.example.com at example.com
Command completed successfully.

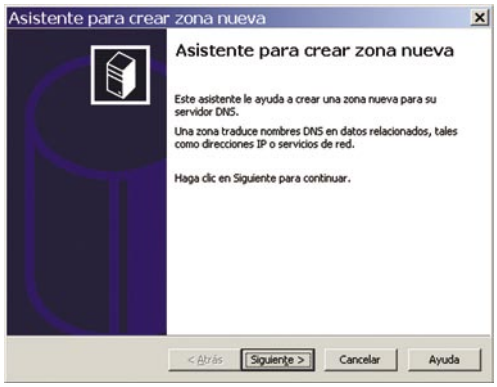
C:\>**dnscmd ::1 /RecordAdd example.com ipv4-ipv6 AAAA 2001: db8:1:0:0:0:1234:5678**
Add AAAA Record for ipv4-ipv6.example.com at example.com
Command completed successfully.

9.2.2.3. Registros PTR

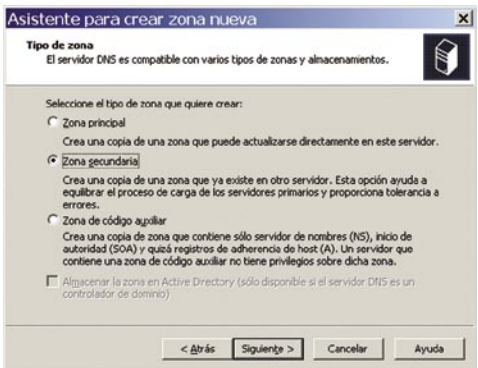
Si el servidor es esclavo o secundario para una zona que contiene registros PTR con nombres de dominio, entonces se puede usar la interfaz gráfica para configurarlo. Esto, siempre y cuando el servidor maestro para la zona y los demás esclavos tengan una dirección IPv4 accesible, ya que la interfaz gráfica no permite introducir direcciones IPv6 para ellos.

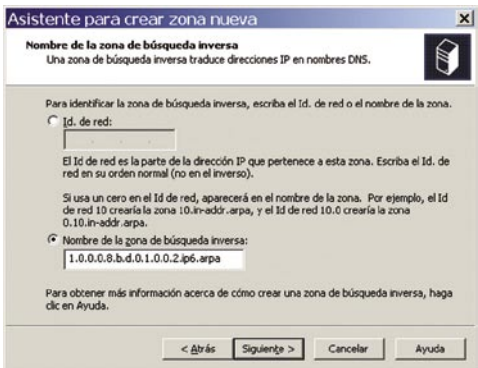
Para configurar un nuevo dominio con el servidor como esclavo o secundario, hay que utilizar la interfaz gráfica de configuración, que es la herramienta DNS dentro de las Herramientas Administrativas.

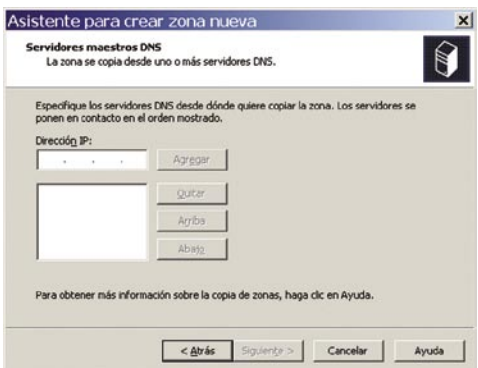
Para ello se hace clic con el botón derecho del ratón sobre Zonas de búsqueda inversa para una zona de resolución de direcciones IPv6 a nombres de dominio Se selecciona Zona nueva, lo que abrirá el asistente para crear una nueva zona:

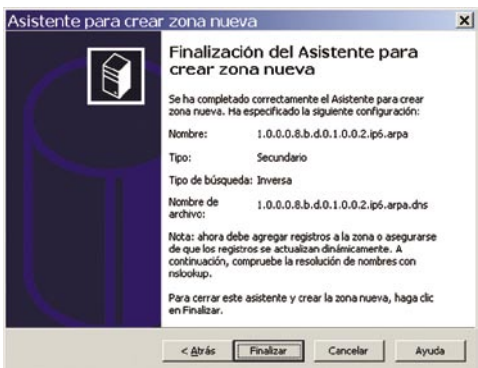


Seleccionar Zona secundaria como tipo de zona, poner el nombre de la zona (por ejemplo 1.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa para el caso de encargarse de la resolución inversa del prefijo 2001:db8:1::/48) y configurar las direcciones IPv4 de los servidores maestros (el primario y otros secundarios si los hubiese).









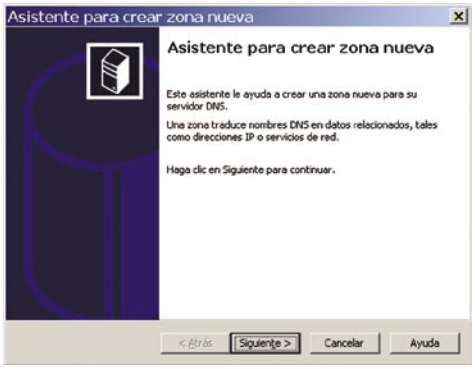
Si el servidor es maestro o primario para una zona con registros PTR que resuelven a direcciones IPv6 entonces hay que utilizar la interfaz de comandos para configurarlo[5], concretamente dnscmd. En el apartado anterior se dan más detalles sobre los comandos más comunes.

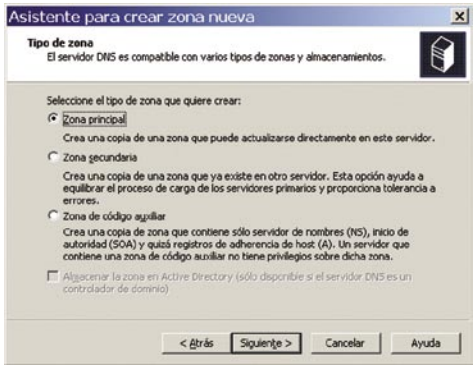
5 También se usarían comandos en caso de ser un servidor secundario o esclavo y no haber ningún otro servidor accesible por IPv4.

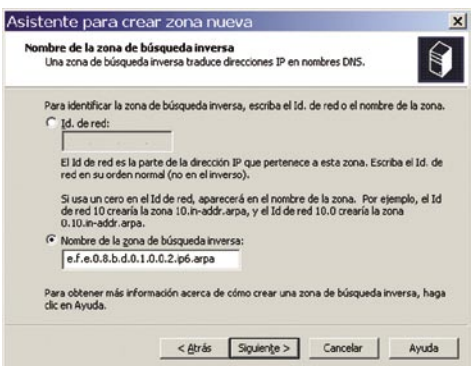
Veamos un ejemplo en el que se va a crear una zona e.f.e.0.8.b.d.0.1.0.0.2.ip6.arpa de la que el servidor es primario, correspondiente al prefijo 2001:db8:efe::/48, y en la que:

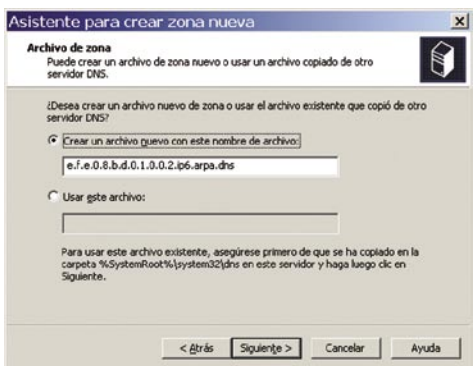
- 2001:db8:efe::1000:1234 resuelva a www.example.com.
- 2001:db8:efe::1234:5678 resuelva a ipv6.example.com.

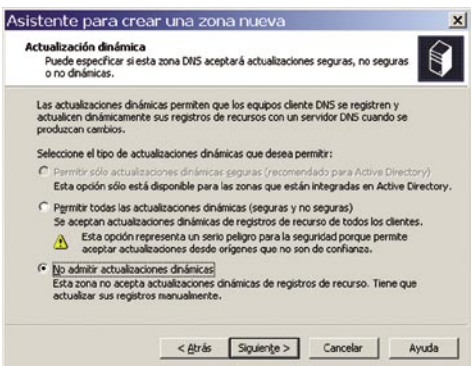
Primero creamos la zona desde la interfaz gráfica. Para ello se hace clic con el botón derecho del ratón sobre Zonas de búsqueda inversa para una zona de resolución de direcciones IPv6 a nombres de dominio. Se selecciona Zona nueva, lo que abrirá el asistente para crear una nueva zona:











Ahora introducimos los registros utilizando la línea de comandos:

C:\>**dnscmd ::1 /RecordAdd e.f.e.0.8.b.d.0.1.0.0.2.ip6.arpa 4.3.2.1.0.0.0.1.0.0.0.0**
.0.0.0.0.0.0.0 PTR www.example.com.
Add PTR Record for 4.3.2.1.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.e.f.e.0.8.b.d.0.1.0.0
.2.ip6.arpa at e.f.e.0.8.b.d.0.1.0.0.2.ip6.arpa
Command completed successfully.

C:\>**dnscmd ::1 /RecordAdd e.f.e.0.8.b.d.0.1.0.0.2.ip6.arpa 8.7.6.5.4.3.2.1.0.0.0.0**
.0.0.0.0.0.0.0 PTR ipv6.example.com.
Add PTR Record for 8.7.6.5.4.3.2.1.0.0.0.0.0.0.0.0.0.0.0.0.e.f.e.0.8.b.d.0.1.0.0
.2.ip6.arpa at e.f.e.0.8.b.d.0.1.0.0.2.ip6.arpa
Command completed successfully.

9.2.2.4. Probando la configuración

Aparte de la interfaz gráfica en la que resulta más sencillo ver la información se dispone de varios comandos muy útiles. A continuación se dan ejemplos de estos comandos para los ejemplos realizados anteriormente.

Para ver los registros AAAA y A de resolución directa que se han creado se utilizan los siguientes comandos:

C:\>**dnscmd ::1 /Enumrecords example.com ipv4**
Returned records:
@ 3600 A 10.0.0.3
Command completed successfully.

C:\>**dnscmd ::1 /Enumrecords example.com ipv4-ipv6**
Returned records:
@ 3600 A 10.0.0.3
3600 AAAA 2001:db8:1::1234:5678
Command completed successfully.

C:\>**dnscmd ::1 /Enumrecords example.com ipv6**
Returned records:
@ 3600 AAAA 2001:db8:1::1234:5678
Command completed successfully.

O para ver todo el contenido de la zona example.com:

C:\>**dnscmd ::1 /zonePrint example.com**
;
; Zone: example.com
; Server: ::1
; Time: Thu Jun 18 16:48:45 2009 UTC

;
@ 3600 NS vw2003.
3600 SOA vw2003. hostmaster. 5 900 600 86400 3600
ipv4 3600 A 10.0.0.3
ipv4-ipv6 3600 A 10.0.0.3
3600 AAAA 2001:db8:1::1234:5678
ipv6 3600 AAAA 2001:db8:1::1234:5678
;
; Finished zone: 4 nodes and 6 records in 0 seconds
;

Para ver que hemos configurado correctamente una zona secundaria de resolución inversa y ver su contenido:

C:\>dnscmd ::1 /Enumzones

Enumerated zone list:
Zone count = 5

Zone name Type Storage Properties
...
1.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa Secondary File Rev
...

C:\>dnscmd ::1 /Zoneprint 1.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa

;
; Zone: 1.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa
; Server: ::1
; Time: Thu Jun 18 16:20:30 2009 UTC
;
@ 172800 NS dns1.novagnet.com.
172800 SOA ns1.example.com. dnsadmin.example.com. 200906 1802 36000 7200 1814400 7200
4.3.2.1.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0 172800 PTR www.example.com.
8.7.6.5.4.3.2.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0 172800 PTR ipv6.example.com.

Para ver que hemos configurado correctamente una zona primaria de resolución inversa y ver su contenido:

C:\>dnscmd ::1 /Enumzones

Enumerated zone list:
Zone count = 3

Zone name Type Storage Properties
...
e.f.e.0.8.b.d.0.1.0.0.2.ip6.arpa Primary File Rev
...

C:\>dnscmd ::1 /Zoneprint e.f.e.0.8.b.d.0.1.0.0.2.ip6.arpa

```
;
; Zone:   e.f.e.0.8.b.d.0.1.0.0.2.ip6.arpa
; Server: ::1
; Time:   Thu Jun 18 17:09:41 2009 UTC
;
@ 3600 NS      vw2003.
            3600 SOA      vw2003. hostmaster. 3 900 600 86400 3600
4.3.2.1.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0 3600 PTR      www.example.com.
8.7.6.5.4.3.2.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0 3600 PTR      ipv6.example.com.
```

La herramienta más común como cliente DNS en entornos Windows es nslookup, que sería el equivalente al dig utilizado en Linux. Veamos algunos ejemplos de uso para probar lo configurado en los ejemplos. Para resolución directa:

```
C:\>nslookup
> server 127.0.0.1
Servidor predeterminado:  localhost
Address:  127.0.0.1

> set type=ANY

> ipv4.example.com
ipv4.example.com      Internet address = 10.0.0.3

> ipv6.example.com
ipv6.example.com      AAAA IPv6 address = 2001:db8:1::1234:5678

> ipv4-ipv6.example.com
ipv4-ipv6.example.com   Internet address = 10.0.0.3
ipv4-ipv6.example.com   AAAA IPv6 address = 2001:db8:1::1234:5678
```

Para resolución inversa:

```
C:\>nslookup
> server 127.0.0.1
Servidor predeterminado:  localhost
Address:  127.0.0.1

> set type=PTR

>4.3.2.1.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.e.f.e.0.8.b.d.0.1.0.0.2.ip6.arpa

4.3.2.1.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.e.f.e.0.8.b.d.0.1.0.0.2.ip6.arpa
name = www.example.com
```

>8.7.6.5.4.3.2.1.0.0.0.0.0.0.0.0.0.0.0.0.e.f.e.0.8.b.d.0.1.0.0.2.ip6.arpa

8.7.6.5.4.3.2.1.0.0.0.0.0.0.0.0.0.0.0.0.e.f.e.0.8.b.d.0.1.0.0.2.ip6.arpa
name = ipv6.example.com

10. Clientes

Prácticamente todos los sistemas operativos actuales (concretamente de sus últimas versiones) tienen clientes de los servicios descritos arriba ya instalados por defecto o fáciles de conseguir e instalar.

Sistema Operativo / Servicio	BSD	Linux	Mac OS X	Windows XP SP1 y posterior, Vista, 7, 2003, 2008
Telnet	Línea de comandos	Línea de comandos	Línea de comandos	Línea de comandos, PuTTY
SSH	Línea de comandos, OpenSSH	Línea de comandos, OpenSSH	Línea de comandos	PuTTY, SecureCRT SSH
FTP	Línea de comandos	Línea de comandos	Línea de comandos	SmartFTP
E-mail	Thunderbird	Thunderbird	Apple Mail, Thunderbird	Outlook
Reproductor Multimedia	VLC	VLC	VLC, iTunes	Windows Media Player, VLC, Winamp
Navegador Web	Firefox, Opera, Chrome, etc.	Firefox, Opera, Chrome, etc.	Safari, Firefox, Opera, Chrome, etc.	Internet Explorer, Firefox, Opera, Chrome, etc.
DNS	Soportado	Soportado	Soportado	Soportado

11. Referencias

DAVIES, J. (2008). **Understanding IPv6, Second Edition**, Estados Unidos: Microsoft Press.

MALONE, D., MURPHY, N. (2005). **IPv6 Network Administration**, Estados Unidos: O'Reilly

VAN BEIJNUM, I. (2006). **Running IPv6,** Estados Unidos: Apress.

Apache HTTP Server Project. Consultado en < **http://httpd.apache.org**> el 15 de Junio de 2009

Comparison of IPv6 application support. Consultado en <**http://en.wikipedia.org/wiki/Comparison_of_IPv6_application_support**> el 15 de junio de 2009

Internet Information Services. Consultado en <**http://www.microsoft.com/windowsserver2003/iis/default.mspx**> el 15 de Junio de 2009

IPv6 to Standard. Consultado en <**http://www.ipv6-to-standard.org**> el 15 de junio de 2009

ISC BIND. Consultado en <**https://www.isc.org/software/bind**> el 15 de Junio de 2009

5. Empresa

1. Introducción a redes empresariales

Definir dónde está la frontera entre una red empresarial y una red doméstica no es trivial; muchas veces los dos conceptos se confunden particularmente dado que muchas redes empresariales hacen uso de servicios de acceso a Internet residenciales. En este capítulo entenderemos que una red empresarial es aquella que cuenta con una clara interfaz con su proveedor de servicio, generalmente un cortafuegos, y brinda servicios internos y externos.

Cuando se habla de direccionamiento dentro de una red empresarial, siempre se piensa en NAT (Network Address Translation). Casi 100% de las redes empresariales implementan NAT para su direccionamiento IPv4, colocando una clara frontera entre la red interna de la empresa y el exterior. A diferencia de lo que sucede en un proveedor de servicios, en la empresa, NAT IPv4 escala dado que brinda suficiente direcciones para prácticamente cualquier implementación conocida. Pero, ¿qué se pierde con el uso de NATv4 (NAT para IPv4)? Hemos escuchado hablar del principio de extremo a extremo y de cómo es quebrado con NAT, también sobre el problema del NAT para aplicaciones como Voz sobre IP. Sin embargo, en muchas empresas el único servicio externo que la gran mayoría de sus usuarios utilizan es el servicio web, el resto se soluciona con servicios internos propios de la empresa. Un caso particular son las empresas con necesidades de alta interactividad entre sus usuarios y usuarios externos, donde el uso de NATv4 puede traer inconvenientes.

El agotamiento de las direcciones IPv4 ha sido descrito en la introducción, y es evidente por tanto que las redes empresariales necesitan prepararse para la implementación de IPv6. Pero, si tengo suficientes direcciones IPv4 dentro de mi empresa para hacer NAT, ¿por qué necesitaría IPv6?

Como generalización podemos encontrar las siguientes razones:

- Los usuarios dentro de una red empresarial necesitarán acceder a contenido que sólo estará disponible en IPv6.
- Los servicios que la red empresarial brinda al exterior deberán ser alcanzables sobre IPv6, dado que posiblemente existirán clientes externos que sólo contarán con direcciones IPv6.

Las nuevas redes empresariales pueden tener un desafío mayor dado que pueden no contar con ni siquiera una dirección IPv4 para poder realizar NATv4. Para estas redes el IETF está trabajando en definir los mecanismos de traducción que van a ayudar a enfrentar la transición a IPv6 parar estas empresas, en particular desde que NAT-PT ha sido catalogado como "histórico" por el documento RFC4966.

Toda implementación de una nueva tecnología comienza con un pre-proyecto, cuyo tiempo de desarrollo e implementación dependerá por ejemplo del tamaño de la red. Quizás uno de los desafíos más grandes de IPv6 es que para conocer su verdadero impacto es necesario conocer detalladamente los equipos y aplicaciones con que cuenta

la empresa. Lamentablemente muchas veces este conocimiento no existe, dificultando la evaluación del impacto de IPv6 en una instalación en plena operación.

Las etapas en que está organizado este capítulo abarcan las tareas previas a comenzar a planificar una implementación de IPv6 en la empresa, para pasar luego a los diferentes aspectos que forman un plan de implementación.

2. Tareas previas para una implementación de IPv6

Dentro de las tareas previas (o tareas de pre-proyecto) que debemos realizar para lograr una implementación exitosa de IPv6 en la empresa se incluyen: Información, relevamiento del impacto, realización de una primera experiencia y elaboración de un pre-proyecto.

La información es esencial para poder realizar un estudio adecuado de cualquier nueva tecnología e IPv6 no es la excepción. Cuando pensamos en informarnos existen diferente fuentes de información como pueden ser libros, manuales de aplicaciones y equipos, normas o estándares, conferencias y cursos en general. Luego de informarse un administrador de una red debería reconocer si IPv6 le afecta (donde seguramente la respuesta sea que sí) y si tiene las habilidades para estudiar el impacto de IPv6 en su infraestructura o necesita buscar ayuda adicional.

Luego de llegar a la conclusión que IPv6 afecta a mi infraestructura, es necesario estudiar adónde IPv6 impacta en mi infraestructura y no sólo equipamientos sino que posiblemente incluso mi negocio, sea cual fuese este.

La mejor forma de comenzar a trabajar en estos proyectos complejos es comenzar iterando a partir de algún objetivo específico. Entonces tomemos dos ejemplos concretos, por un lado una empresa que brinda servicios de alojamiento de Internet (hosting) y por el otro una pequeña empresa con terminales para la navegación.

Para el caso de la empresa de hosting *(ver Figura 1)*, el objetivo que puede tener para IPv6 es asegurarse que todo su contenido sea accesible sobre IPv6. Para alcanzar este objetivo, el análisis del impacto de IPv6 puede concluir que sus comunicaciones internas como conexiones SQL, accesos a servidores de aplicación, etc. no necesitan soportar IPv6. Este simple análisis terminó con una implementación de IPv6 que sólo abarca el acceso de la red y el front-end web, simplificando la tarea a realizar y disminuyendo sus costos.

En el segundo caso, en una empresa con terminales *(ver Figura 2)*, se evalúa que va a ser necesario que los terminales implementen doble pila para poder acceder a contenido en IPv6. Por otro lado los servidores que tienen contacto con el exterior también necesitan implementar doble pila para, por ejemplo, poder enviar emails a servidores SMTP que sólo implementen IPv6.

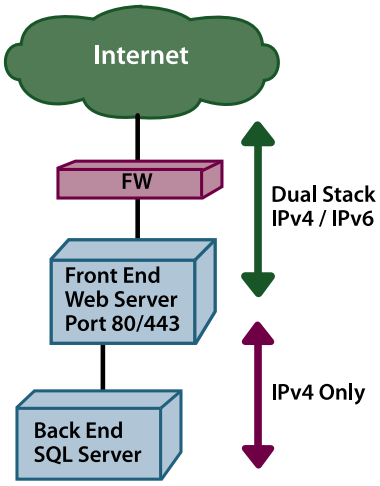


FIGURA 1: **EMPRESA DE HOSTING**

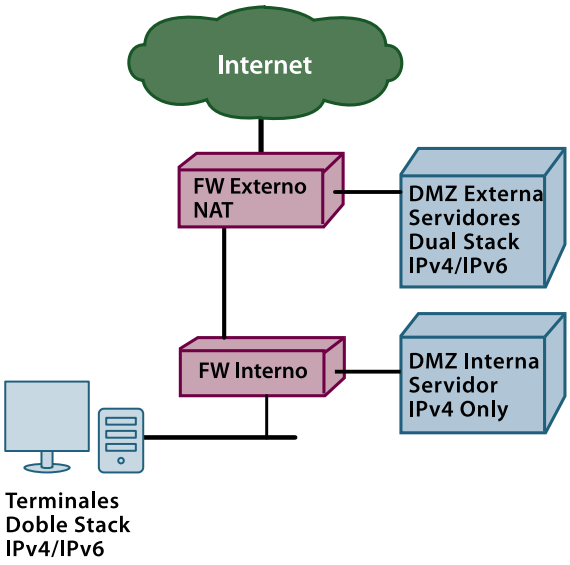


FIGURA 2: **EMPRESA CON TERMINALES PARA NAVEGACIÓN**

¡Cuidado! Es perfectamente correcto intentar llevar IPv6 a cada rincón de la red, pero simplemente ésta debe ser una decisión consciente por parte del administrador.

En la *figura 3* se muestran algunos de los elementos que se podrían ver impactados por la implementación de IPv6 y que deberían ser analizadas por el administrador.

Una vez trazado un objetivo de trabajo y hecho el relevamiento para evaluar el impacto de IPv6, es posible hacer una estimación de los costos involucrados y pasar a la etapa de planificación.

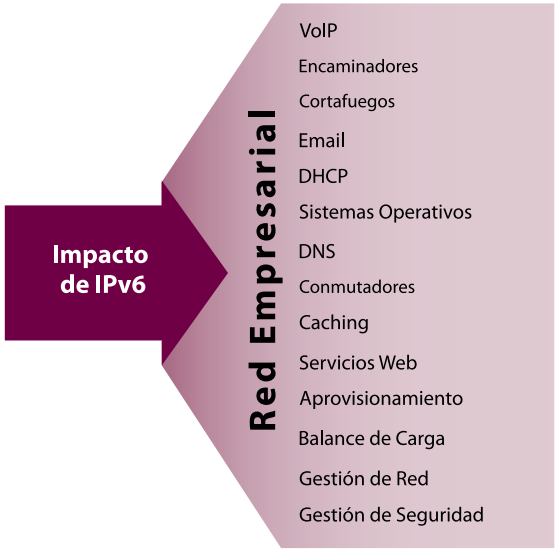


FIGURA 3: **DISTINTOS ELEMENTOS QUE DEBER SER EVALUADOS PARA ESTUDIAR EL IMPACTO DE IPV6.**

Para poder analizar el impacto de IPv6 en una empresa es necesario analizar elementos tan dispersos como el direccionamiento de la red, el encaminamiento, las aplicaciones o procesos de seguridad. En la figura 3 se muestran diferentes elementos que impactan el estudio del impacto de IPv6 en una red empresarial.

3. Planificando IPv6 en redes empresariales

La planificación de IPv6 involucra diferentes aspectos como ser:

- Direccionamiento.
- Encaminamiento.
- Seguridad.
- Servicios

En general la planificación de IPv6 resulta en imitar lo que ya se ha realizado para IPv4.

La gran mayoría de las redes empresariales serán doble pila (seguramente con direcciones IPv4 privadas) por lo que ambos IPv4 e IPv6 coexistirán. Sin embargo, la implementación de IPv6 también le da a los administradores la oportunidad de realizar un nuevo comienzo y realizar los cambios que estaban pendientes en su infraestructura.

3.1. Plan de Direccionamiento

El plan de direccionamiento dentro de una empresa es bastante sencillo. En general se utilizará como unidad un bloque /64 para todo dominio de difusión. Entonces, en general se utilizan /64 para las redes locales (LAN), las redes de área extensa (WAN) y las loopbacks. En general una empresa recibirá de su proveedor un bloque /48 sin discriminación de tamaño que equivale a 65.535 redes /64. Sin embargo, si una empresa sumando su cantidad de redes (LAN, WAN y loopbacks) y pensado en un crecimiento del 300% necesita más que un /48, deberá solicitar un bloque mas grande a su proveedor o al registro de direcciones si utiliza direcciones independientes del proveedor.

En IPv6 existen suficientes direcciones Globales Unicast para cualquier empresa, por lo que surge la pregunta de que aún teniendo suficiente cantidad de direcciones, tiene sentido utilizar NAT? La respuesta queda a cargo del lector, pero seguiremos el estudio utilizando únicamente direcciones Globales Unicast.

Para estudiar cómo direccionar una empresa, vamos a tomar un ejemplo. En la figura 4 se muestra una empresa típica con una DMZ en su sede central (o Sucursal 1) y dos sucursales llamadas 2 y 3.

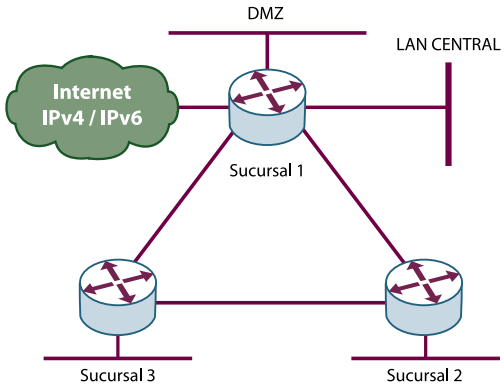


FIGURA 4: **EJEMPLO DE RED EMPRESARIAL CON SEDE CENTRAL Y DOS SUCURSALES**

Sea que la empresa obtiene direcciones de parte de su proveedor de conectividad o sea que las obtiene de su registro nacional o regional (por ejemplo LACNIC), la empresa normalmente recibirá un bloque /48 para su numeración interna. Supongamos entonces que se recibe el bloque de documentación: 2001:DB8::/48 el cual debe ser dividido de tal forma que se pueda abarcar todas las redes de la empresa. En IPv6 ya no se cuentan las terminales en una LAN pues se va a asignar a cada una un /64 que va a poder numerar todas los terminales que se deseen. En su lugar, lo que sí se cuentan son las cantidades de redes y subredes a numerar.

Toda dirección IPv6 cuenta con tres campos: el prefijo globalmente encaminado, el identificador de subred y el identificador de interfaz según se indica en la siguiente *figura 5*.

n bits	m bits	128 n-m bits
Prefijo Global Unicast	**Identificador de subred**	**Identificador de interfaz**

FIGURA 5: **CONSTRUCCIÓN DE UNA DIRECCIÓN IPV6 EN SUS TRES ELEMENTOS**

Para una red empresarial, en general, el largo del Prefijo Global Unicast es dado por el proveedor (en nuestro caso n=48). También en general vamos a escoger un identificador de interfaz igual a un /64 por dos motivos: facilitar la autoconfiguración en las redes locales y respetar que muchas veces el equipo ha sido especializado para trabajar con direcciones IPv6 con esta longitud. Con esto queda entonces definido que el identificador de subred tendrá una longitud m=16. Si uno desea realizar agregación geográfica dentro de la red (recomendado para evitar la aparición de múltiples redes en el encaminado interno), en los 16 bits correspondiente al identificador de subred se deberán identificar dos elementos, a la sucursal dentro de la empresa y a la red dentro de cada sucursal.

En la *tabla 1* se muestran algunas posibilidad de divisiones del bloque /48 recibido partiendo **m** en diferentes múltiplos de 2. La primer columna indica la separación del identificador de subred, comenzando por el bit más significativo (a la izquierda).

División	Cantidad de Sucursales	Cantidad de redes por sucursal
/50	4	16.384
/52	16	4.096
/56	256	256
/58	1.024	64
/60	4.096	16
/62	16.384	4

Tabla 1: **Algunas opciones para dividir un /48 en una empresa**

Supongamos que en nuestro ejemplo tomamos /56 como frontera de división interna pues es el mejor compromiso entre el crecimiento esperado dentro de cada sucursal y el crecimiento del número de sucursales. De los 256 bloques /56 existentes deberemos elegir: uno para cada sucursal, uno para la red externa (la asumimos separada de la sucursal 1), uno para la WAN de la empresa y uno para las loopbacks de los equipos. Para facilitar la agregación en caso de crecimiento en el futuro, lo mejor es no utilizar numeración secuencial, sino posibilitar el crecimiento de cada sucursal. La forma más eficiente de realizar esta asignación es la forma binomial, realizando asignaciones del primer bloque, luego del último y luego siempre asignar un bloque entre medio de los dos bloques más separados. En este caso se asigna en el siguiente orden:

1- 2001:DB8::/56
2- 2001:DB8:0:FF::/56
3- 2001:DB8:0:7F::/56
4- 2001:DB8:0:3F::/56
5- 2001:DB8:0:B0::/56
6- ...

El problema con este método es que el resultado son bloques cuya idenficación no tiene un significado singular y por ende son difíciles de recordar. Otra posibilidad menos eficiente para la asignación de direcciones es realizarlo de forma inteligente, como en el siguiente ejemplo, donde se intenta colocar el número de sucursal dentro del bloque de direcciones correspondiente. En la siguiente tabla 2 se muestra la distribución de direcciones propuesta para facilitar la operación.

Bloqueo direcciones /56	Destino
2001:DB8::/56	**Redes Externas (DMZ)**
2001:DB8:0:1000::/56	**Sucursal 1.**
2001:DB8:0:2000::/56	**Sucursal 2.**
2001:DB8:0:3000::/56	**Sucursal 3.**
2001:DB8:0:AA00::/56	**Donde se escogen las redes WAN 2001:DB8:0:AAXY::/64 para las conexiones desde la sucursal X a la Y.**
2001:DB8:0:BB00::/56	**Donde se escogen las Loopbacks 2001:DB8:0:BBXX::1/64 para el router de la sucursal X.**

Tabla 2: **Propuesta de numeración para red ejemplo**

El resultado del plan de numeración para esta red se muestra en la figura 6 donde se detallan todas las redes a utilizar.

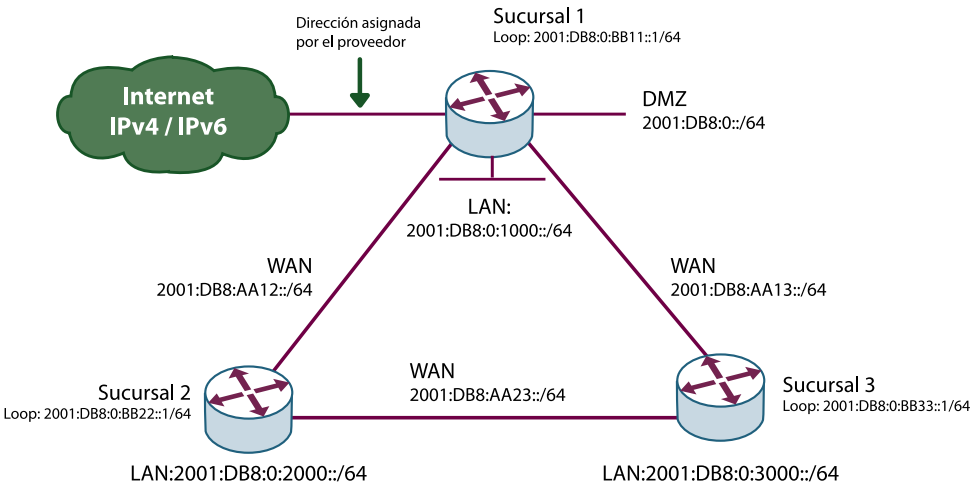


FIGURA 6: **RED EMPRESARIAL DE EJEMPLO**

Un concepto que es importante asimilar es que hay desperdicios de direcciones en IPv6, pero esto no debe preocupar de sobremanera a quien diseña redes empresariales pues esta normalmente recibe de su proveedor muchas más direcciones de las que necesita sin que se le realice ninguna pregunta.

3.1.1. Numeración de servidores

Para escoger el identificador de interfaz dentro de cada LAN que le corresponde a cada servidor se realizará generalmente numeración estática. La razón es apuntar a la máxima disponibilidad y el evitar tener que realizar cambios ante problemas con la dirección de red. En el momento de escoger la dirección IPv6 estática a utilizar para un servidor se debe elegir entre:

- escoger una dirección fácil de recordar, como por ejemplo 2001:DB8::1. Esta opción facilita la operación pues hace más fácil el análisis de problemas.
- escoger una dirección aleatoria como por ejemplo: 2001:DB8::ACF:2311:FFED:CAFE. Esta dirección si bien complica el análisis en el problema de detectar problemas, se cree que debe ser más difícil de rastrear por parte de posibles ataques por fuerza bruta (“port scanning”).

A la hora de analizar cual de las dos opciones utilizar, piénsese que el espacio IPv6 es muy extenso y realizar barridos para buscar direcciones válidas en forma bruta o secuencial puede llevar un tiempo muy largo a menos que se cuente con registros de DNS. Por lo tanto, si un servidor tiene su registro en el DNS accesible públicamente, es menos importante utilizar direcciones aleatorias.

Ejemplo de numeración estática *(ifconfing en FreeBSD):*

```
bge0: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        options=1b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING>
        inet6 fe80::21a:64ff:fe6d:367e%bge0 prefixlen 64 scopeid 0x3
        inet 192.0.2.2 netmask 0xffffff00 broadcast 192.0.2.255
        inet6 2001:DB8::2 prefixlen 64
        ether 00:1a:64:6d:36:7e
        media: Ethernet autoselect (100baseTX <full-duplex>)
        status: active
```

3.1.2. Numeración de terminales

Para la numeración de terminales existen tres opciones que un administrador de red debe analizar:

- numeración manual. En este caso se deberá numerar manualmente cada una de las terminales.
- numeración automática sin estado o sin servidor ("stateless" o "serverless") utilizando el mecanismo "anuncios de encaminadores" (o "route advertisements"). Este mecanismo utiliza paquetes ICMPv6 y grupos de multicast locales a la interfaz. A través de este mecanismo se puede configurar la dirección IPv6, la longitud del prefijo y la ruta por defecto. Sin embargo no es posible configurar elementos adicionales como pueden ser servidores de DNS, de WINS o incluso gateway SIP para la auto-configuración de un teléfono sobre IP. Estas configuraciones se implementan en DHCPv6, particularmente a través de la opción sin estado ("stateless configuration"). Al no mantener estados, el administrador de la red no tendrá control sobre cuales son las terminales que se conectan a la red IPv6. Cualquiera con acceso al medio común tendrá acceso.
- numeración automática con estados ("stateful") . En este caso la configuración de la dirección IPv6 se hace a través de DHCPv6 igualmente que con IPv4. De esta forma es posible definir un pool de direcciones o incluso asignar direcciones particulares para cada terminal. Utilizando DHCPv6 en su configuración con estados es posible realizar un control de acceso más estricto. Un parámetro que no se obtiene aún (aunque hay trabajos en este sentido) por parte de DHCPv6 es la ruta por defecto. Por esto, aún cuando se utilizar DHCPv6 en modo con estados, es necesario utilizar el mecanismo de anuncio de encaminadores para obtener la ruta por defecto.

Cualquiera que sea el mecanismo de direccionamiento que se escoja, es recomendado contar con un aplicaciones que permita la gestión de las direcciones IPv6. En la fecha de esta publicación, algunas de las opciones existentes eran: Haci (aplicaciones libre), IP Address Management Module (Men & Mice), Address Commander (Incognito Aplicaciones) y VitalQIP (Alcatel Lucent).

3.2. Plan de encaminamiento

El plan de encaminamiento para IPv6 no debe variar en demasía sobre lo que ya se hace en IPv4. En general para una empresa tiene sentido que en IPv6 se mantenga la mis-

ma topología que en IPv4. El mantener dos topologías significaría incrementar el costo de operación del encaminamiento de la red y el aumento de incidentes.

Las opciones para el encaminamiento en IPv6 son:

- encaminamiento estático.
- encaminamiento dinámico.

En particular dentro del encaminamiento dinámico en IPv6 existen las siguientes categorías:

- protocolos vector distancia: RIPNG (RIP Next Generation).
- protocolos vector camino (o "path vector"): BGPv4.
- protocolos estado de enlaces: ISIS o u OSPFv3.

Con todas estas opciones, se debe considerar especialmente las capacitación ya existente en la compañía. En caso de estar utilizando OSPFv2 para la red IPv4, tiene sentido utilizar OSPFv3 en IPv6, al igual que utilizar BGPv4 para el encaminamiento externo. En caso de utilizar direccionamiento estático para IPv4, se puede utilizar las mismas configuraciones para IPv6.

Si es posible evitar el uso de RIPNG, se evitarían tiempos de convergencia largos y problemas de conocimiento parcial de topología. También el uso de RIPNG imposibilita el uso de técnicas modernas de ingeniería de tráfico.

3.3. Plan de seguridad en IPv6

Cuando se configura IPv6 en una red, estamos habilitando el acceso a través de una nueva capa de red. Esto hace que las reglas de seguridad perimetral existentes para IPv4, ya no serían válidas para IPv6. Pero la seguridad no es solamente la configuración del cortafuegos u otro equipamiento, también son procesos y procedimientos que han sido elaborados a través de los años (incluso muchas veces siguiendo recomendaciones internacionales como la ISO 27000) que deben ser revisadas y analizadas. Lo importante es considerar que IP es la denominación del Protocolo Internet que involucra a los dos IPv4 e IPv6. Esta distinción debe realizarse en los procedimientos correspondientes.

Para la configuración perimetral es necesario configurar reglas IPv6 que imitan a las reglas IPv4. Tomemos el siguiente ejemplo para la configuración de reglas para un servidor web utilizando IPFW en un equipo FreeBSD:

ipfw add 1020 permit log tcp from any to "$ip4" dst-port 80 setup keep-state in via bge0
ipfw add 2020 permit log tcp from any to "$ip6" dst-port 80 setup keep-state in via bge0

En este ejemplo la variable $ip4 representa la dirección IPv4 del servidor web y la variable $ip6 su dirección IPv6. En el caso de IPFW, se detecta si la regla debe aplicarse a IPv4 o IPv6 dependiendo del formato de la direcciones en la regla. Esto debe verificarse en el momento de analizar el cortafuegos a utilizar, al igual que su habilidad para mantener estados en IPv6.

Existen dos puntos que necesitan especial atención en la configuración de cortafuegos en IPv6 con respecto de IPv4: ICMPv6 y multicast.

En el caso de ICMPv6, nuevos tipos deben ser considerados, particularmente el tipo 128 es ahora "echo request" y el tipo 129 "echo reply". Más importante aún es entender que IPv6 no realiza fragmentación en los encaminadores, sino que sólo de extremo a extremo. Para poder tener una comunicación exitosa a través de un ambiente con MTUs variados se implementa el proceso de descubrimiento de MTU del camino (o PMTUD). El proceso PMTUD se explica en la Figura 7, donde el cortafuegos debe permitir el paso de paquetes ICMPv6 del tipo 2 al servidor. El documento RFC4890 detalla recomendaciones para el filtrado de paquetes ICMPv6.

El otro caso de interés es sobre el filtrado de multicast y en particular de multicast local al enlace (direcciones ff02::/16). En IPv6 no existe dirección de difusión (o "broadcast"), y elementos como la autoconfiguración de direcciones, la detección de direcciones duplicadas y el descubrimiento de vecinos dependen del uso de multicast. El filtrado de multicast local al enlace por parte de un cortafuegos impide su funcionamiento en IPv6.

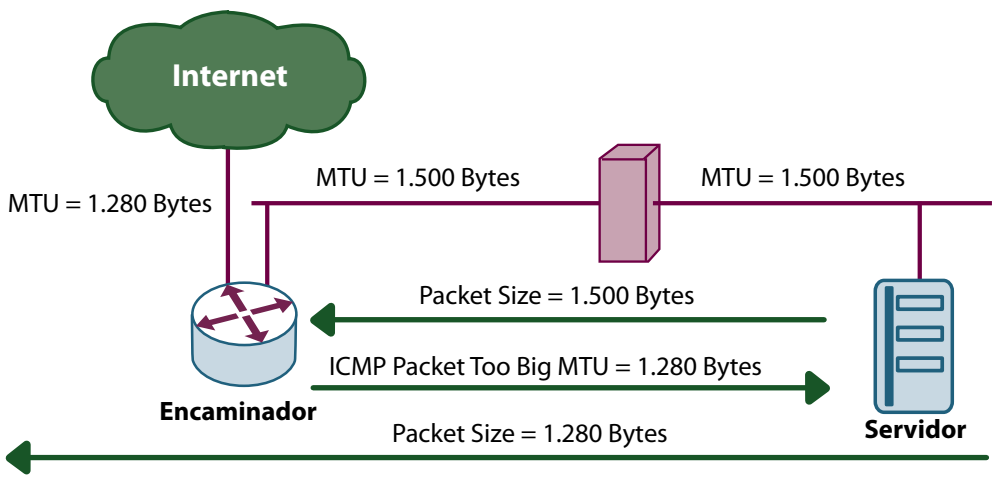


FIGURA 7: **DESCUBRIMIENTO DEL MTU**

Para el descubrimiento del MTU, como se indica en la *figura 7*, el servidor envía un paquete de tamaño 1.500 Bytes que es descartado por algún encaminador en algún punto del camino pues es mayor que el MTU del siguiente enlace. El encaminador devuelve al servidor un paquete de control ICMPv6 "Packet too Big" (tipo=2) con la información del MTU del enlace que ocasionó el problema. Al recibir este mensaje el servidor acomoda el paquete para el nuevo MTU de la comunicación. Si el cortafuegos en el camino llegara a bloquear los paquetes ICMPv6 del tipo=2 al servidor, la comunicación no ocurriría.

Además de la configuración del cortafuegos el resto de los equipos que tienen en cuenta la seguridad perimetral como IDS, herramientas de análisis de logs, etc. deben ser actualizadas para soportar IPv6.

3.4. Plan de Servicios e IPv6

Las empresas deberán adaptar sus servicios para poder soportar IPv6. Estos servicios son a veces externos o internos. Involucran aplicaciones comerciales, de código abierto o generadas localmente. Como regla práctica, cualquier aplicación o equipo que manipula paquetes IP o direcciones IP, deben ser evaluados para entender su soporte de IPv6.

En particular podemos nombrar el: mail, web, chat, dns, sistemas de gestión (en particular de direcciones).

En el capítulo **"Servicios con IPv6"** se dan ejemplos de configuraciones de diferentes servicios para su soporte de IPv6.

4. Transición a IPv6 en una red empresarial y agotamiento IPv4.

La transición desde una red dónde sólo se utiliza IPv4 a una red donde aparece IPv6 no es un proceso que se vaya a realizar en un sólo día como fue el caso del cambio a la televisión digital, o el cambio de NCP a TCP/IP en Internet el 1° de Enero de 1983. En su lugar, el proceso será paulatino, donde a medida que las fuentes y/o los receptores de tráfico que hagan la transición a IPv6, la mayoría del tráfico se irá volcando al nuevo protocolo. Como conclusión IPv4 e IPv6 van a convivir en los mismos medios físicos por muchos años y no es claro incluso que IPv4 desaparezca completamente. Para los administradores de redes empresariales, esto no es algo extraño pues existe mucha experiencia en la convivencia de IPv4 con otros protocolos como son IPX, AppleTalk o DECnet en los mismos medios físicos.

Como la transición se hace en forma paulatina, se hace también en forma desacoplada entre el cliente y el servidor. En un momento dado, el cliente puede tener soporte para IPv6, mientras que el servidor no lo tiene o viceversa. A esta característica le debemos sumar que es posible que los sistemas operativos de los clientes incluyan mecanismos de túneles automáticos como son 6to4 o Teredo que hacen que la conectividad IPv6 de los clientes puede no ser óptima. En sistemas operativos como Vista, el usuario muchas veces desconoce que posea esta funcionalidad activada.

Cuando se realiza el plan de implementación de IPv6 para una empresa, existen claramente dos elementos a considerar: la infraestructura y los servicios. En ambos casos el principal cuidado es siempre el considerar la degradación del servicio por parte de los clientes.

En el caso de la infraestructura (configuración de encaminadores, cortafuegos, bases de datos, aplicaciones de gestión), la degradación podría darse por escoger una conexión con un retardo en IPv6 excesivo. Cuando un cliente comienza a utilizar IPv6, al encontrar un servicio en IPv6 va a preferir esta conexión por sobre IPv4. Si la conexión IPv6 posee un retardo muy superior a la conexión IPv4, el cliente va a sentir el impacto. Para solucionar

este problema, siempre se deberán preferir conexiones nativas o túneles a puntos cercanos. Si la empresa tiene su propia política de encaminado, debería intentar configurar todas sus conexiones con IPv6.

En el caso de la configuración de los servicios, el punto crucial es el momento en que se publican las direcciones IPv6 a través de los registro AAAA en los servidores de DNS. A partir de ese momento los clientes externos e internos que tengan acceso IPv6 de alguna forma (nativa o tunelizada) comenzarán a preferirlo sobre el acceso IPv4. Para esto es importante considerar que: no se deben configurar registros AAAA para servicios que no tienen acceso IPv6 y que puede ser una buena práctica realizar inicialmente experimentos con dominios del tipo *ipv6.miempresa.midominio*.

Como hemos visto previamente, existe la posibilidad muy cierta que en un futuro cercano ya no se puedan asignar direcciones IPv4 públicas en Internet. En este escenario de escasez de direcciones IPv4, las empresas deberán enfrentar dos desafíos:

- la posibilidad de no contar con suficientes direcciones IPv4 para sus servicios.
- tener que brindar servicios a clientes que sólo cuentan con direcciones IPv6.

Respecto al primer escenario, el caso extremo se daría para una empresa que no tiene ninguna dirección IPv4, pero debe acceder tanto al contenido en IPv6 como en IPv4, así como brindar servicios a clientes externos IPv6 e IPv4. Para esto existió una solución llamada NAT-PT que fue catalogado como "histórico" por el documento RFC4966. La solución NAT64/NAT46 es la reemplazante que está a estudio de la IETF y deberá ser adoptada por empresas en esta situación. En caso de tener alguna dirección IPv4 pública o privada traducida por el proveedor (escenario llamado Carrier Grade NAT o CGN), el acceso al contenido IPv4 se haría en la mayoría de los casos utilizando traducción NAT usual.

El segundo escenario es que una empresa cuyos clientes sólo tienen acceso IPv6 debe asegurarse que todos sus servicios sean accesibles para estos.

Sin duda existen muchas incertidumbres sobre cómo acontecerán los cambios que con seguridad llegarán en los próximos años y cuál de las diferentes opciones tecnológicas sobresaldrá, pero en todos los escenarios IPv6 estará presente en las redes de las empresas y estas deben prepararse para este futuro con incógnitas aún, pero claramente con muchas oportunidades.

6. Entorno académico y de investigación

1. Introducción

En este capítulo mostraremos las características que tiene el despliegue de IPv6 en el ámbito de las redes de investigación y educación. Estas redes están compuestas en general por universidades y centros de investigación, pudiendo en algunos casos incluir escuelas y otros organismos relacionados. Es importante destacar la experiencia de este sector ya que ha sido el que ha liderado el desarrollo de la nueva versión del protocolo IP y donde mayor experiencia en el despliegue se cuenta.

A lo largo del capítulo veremos algunas de las ventajas que IPv6 presenta para este entorno y mostraremos también las principales redes en el mundo que hoy cuentan con esta tecnología. Además, desde un punto de vista práctico, se proporcionará la información necesaria para que una universidad o centro de investigación pueda desplegar IPv6 en su red fácilmente.

2. ¿Por qué y para qué se utiliza IPv6 en educación e investigación?

Hemos mencionado que el sector académico/científico ha sido el que lideró la incorporación del protocolo IPv6 y uno de los sectores que al día de hoy cuenta con más experiencia en este tema. Debemos preguntarnos entonces ¿por qué esto es así? Trataremos de responder a esta pregunta en esta sección.

2.1. Un poco de historia

Si nos remontamos a los orígenes de Internet, podemos ver que la tecnología subyacente a esta red está estrechamente ligada a los ambientes de investigación y educación. Recordemos por ejemplo que los protocolos que hoy componen la base de la Internet actual, es decir, el TCP/IP, se originaron en proyectos de investigación en EE.UU. dentro del área de defensa, pero en los que fueron parte esencial las Universidades de Stanford y el University College of London.

Posteriormente, podemos citar entre otras experiencias que contribuyeron al desarrollo y evolución de la Internet como hoy la concebimos, a los protocolos que hicieron posible la World Wide Web – WWW y el protocolo HTTP[1], todo ello desarrollado a partir de necesidades propias de la investigación en el CERN[2]. A su vez, el primer navegador gráfico, algo que hoy nos parece tan natural, fue desarrollado en el año 1992 por el National Center for Supercomputing Applications - NCSA[3]. Y así sucesivamente, podríamos citar la mayoría de las tecnologías, protocolos, software y aplicaciones que se utilizan actualmente en Internet.

1 http://www.w3.org/Protocols/HTTP/AsImplemented.html
2 http://public.web.cern.ch/public/
3 http://www.ncsa.uiuc.edu/

Pues bien, algo similar sucede con IPv6. Cuando la IETF se propuso investigar y promover la creación de una nueva versión del protocolo IP que superara las limitaciones inherentes a la versión 4, nuevamente el proceso estuvo liderado por grupos basados en universidades y centros de investigación, como el MIT, Universidad de Harvard, CERN, entre otros, junto a las empresas principales en el área de Internet (véase por ejemplo el RFC1752[4]).

2.2. Experiencias previas

Una de las primeras experiencias en la utilización de IPv6 estuvo originada en el proyecto 6bone, un intento de establecer una red "virtual" como campo de pruebas de la nueva versión del protocolo. Hablamos de una red virtual, porque muchas de las conexiones estaban inicialmente basadas en túneles encapsulados en los enlaces de Internet IPv4, si bien posteriormente se realizó la transición a conexiones nativas. Este experimento finalizó en el año 2006.

Los primeros despliegues de IPv6 en gran escala se dan en el marco de redes académicas o de investigación, como Abilene (Internet2) en EE.UU., Geant en Europa, CERNET2 y CSTNET2 en China o WIDE y JGN2 en Japón.

Europa a través de varios proyectos de investigación ha impulsado el avance de IPv6, siendo importante mencionar por ejemplo las iniciativas como 6NET[5], Euro6IX[6] o GEANT[7].

Sumando a estas iniciativas, una mención especial merece el desarrollo de las versiones de IPv6 para sistemas operativos BSD y Linux a través de los proyectos KAME y USAGI respectivamente, en los cuales las Universidades han sido parte activa del proyecto.

Todas estas referencias que hemos mencionado sirven para mostrar la estrecha ligazón que existe entre el ámbito académico/científico y el desarrollo y utilización de la nueva versión del protocolo IP. Esto da lugar a que sea en estos sectores donde mas rápidamente se diseminó su uso y se vieron las posibilidades que brindan las nuevas características. En el próximo punto citaremos algunos ejemplos de ello.

2. 3. Servicios y aplicaciones de las redes académicas de hoy

Una particularidad de las redes académico/científicas actuales es que cuentan con servicios que no son habituales en otro tipo de redes. Citaremos algunos de ellos y veremos de qué forma IPv6 puede ayudar a su aprovechamiento.

- Actualmente existe en este tipo de redes lo que se denomina "grids", algunas veces

4 http://www.ietf.org/rfc/rfc1752.txt
5 http://www.6net.org/
6 http://www.euro6ix.org/
7 http://www.geant.net

traducido como “mallas”, que son sistemas que se encuentran en una capa entre las aplicaciones y los servicios de red y en los cuales la idea es compartir recursos que pueden estar distribuídos globalmente, accediéndolos desde sitios remotos. Puede tratarse de capacidad de cómputo, almacenamiento de datos, la utilización de algún instrumental costoso como microscopios de alta tecnología o de difícil acceso como telescopios ubicados en lugares alejados.

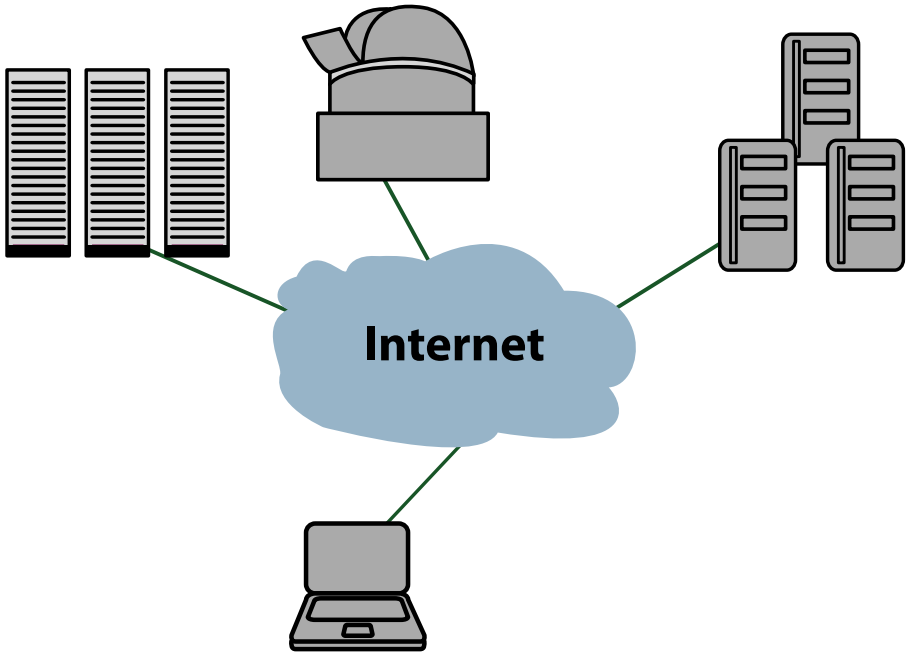


Figura 1: **Recursos compartidos a través de un grid.**

Mediante este tipo de sistemas, es posible la utilización del equipamiento por un conjunto de personas que excede a la organización dueña del mismo y por esto se habla de “organizaciones virtuales”. No es la idea de este capítulo entrar en detalles sobre los sistemas grids, pero sí mencionar el beneficio que para tal servicio puede prestar la incorporación de IPv6. Por un lado, las capacidades de seguridad que brinda IPSec, tales como autenticación y cifrado de los datos de extremo a extremo, facilitan la privacidad y el control necesarios. La posibilidad de tener direcciones IP globales, públicamente alcanzables, permite el despliegue en gran escala de los servicios grids, tanto desde el punto de vista de los recursos como de los dispositivos en condiciones de utilizarlos.

- Otro tipo de tecnología habitual en este tipo de redes es multicast. Esto permite una utilización óptima del ancho de banda cuando se hacen transmisiones de datos a muchos destinatarios, ya que no es necesario replicar esa transmisión para cada receptor. Es posible entonces emitir contenidos con una señal con mejor calidad, ya que el ancho de banda a utilizar no se multiplica en función de los receptores. Multicast se utiliza para hacer streaming de video y audio, para contenidos bajo demanda, videoconferencia multipunto, etc. Si bien en IPv4 esta tecnología está disponible, en

IPv6 es parte del protocolo desde su diseño y su utilización es mucho más sencilla.

- Las videoconferencias son un elemento del trabajo diario de los docentes e investigadores, muchas veces limitadas por la utilización de NAT. La posibilidad de tener una IP pública permite establecer comunicaciones extremo a extremo sin problemas.

- Como se mencionó antes para los grids, la movilidad incluída en el protocolo IPv6, facilita el acceso a los recursos desde cualquier organización. Esta es una característica muy deseable, ya que es habitual el traslado de investigadores entre grupos de trabajo.

- Por último, el crecimiento que han tenido los anchos de banda y las transferencias de datos que se realizan, han hecho necesario utilizar los llamados jumbo-frames (9000 bytes o más) para mejorar la eficiencia de la utilización de ancho de banda. IPv6 permitirá mejorar aún más estas tasas de transferencia mediante la utilización de "jumbogramas", en la medida que las redes estén preparadas para el uso de esta tecnología.

3. Redes Académicas en el mundo

Antes de pasar a hablar del despliegue de IPv6 en una universidad o centro de investigación, es conveniente situarnos en el contexto de las redes académicas o de investigación que existen, para poder tener una perspectiva de los servicios que podemos tener disponibles.

Actualmente los sectores científicos y de educación poseen redes físicas que los vinculan, la mayoría de ellas con características avanzadas tales como calidad de servicio, multicast y, como ya hemos mencionado, IPv6 en forma nativa.

Podemos ver en la *figura 2*: Mapa mundial de las NRENs un mapa de las redes académicas existentes en el mundo. Estas redes llevan el nombre genérico de REN por su sigla en inglés: "Research and Education Network" al que generalmente se agrega la característica de ser de cobertura nacional, por lo que se habla de NRENs.

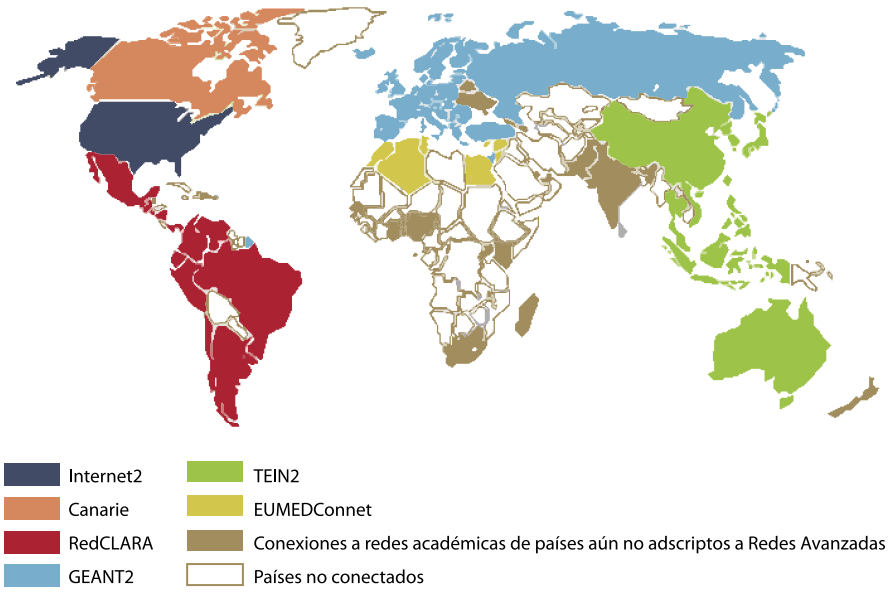


FIGURA 2: **MAPA MUNDIAL DE LAS NRENS**[8]

La mayoría de estas redes tiene soporte de IPv6 desde hace años, por lo que, dependiendo de la región del mundo donde nos encontremos, vamos a poder aprovechar esa disponibilidad para lograr la conectividad nativa de la institución a la que pertenecemos.

Citamos a continuación las principales redes regionales. Cabe mencionar que muchas de esas redes están compuestas por otras de características nacionales (NRENs), que son las que en última instancia llevarán la conectividad al sitio final (universidad, centro de investigación, instituto, escuela, etc). Como veremos más adelante, es de estas redes nacionales de donde vamos a poder obtener los recursos necesarios para implementar IPv6 en nuestra institución.

En EE.UU. las Universidades están conectadas a la red Abilene, a través del proyecto Internet2 como se muestra en la *figura 3:* Abilene (Internet2) - EE.UU.

En América Latina, es RedCLARA la red que vincula todas las redes nacionales de investigación y educación (NRENs), *ver figura 4:* RedCLARA - América Latina.

En Europa, la red GEANT ha ido evolucionando hasta alcanzar la totalidad de los países y en su nueva versión lleva el nombre de GEANT3. Conecta mas de 3.500 universidades y centros de investigación. *Ver figura 5*: GEANT2 - Europa.

Finalmente, en la región denominada Asia-Pacífico, la red TEIN2 tiene características similares, interconectando las principales redes nacionales de esa zona y con Europa. *Ver Figura 6:* TEIN2 - Región de Asia Pacífico.

8 http://www.redclara.net/index.php?option=com_wrapper&Itemid=293&lang=es

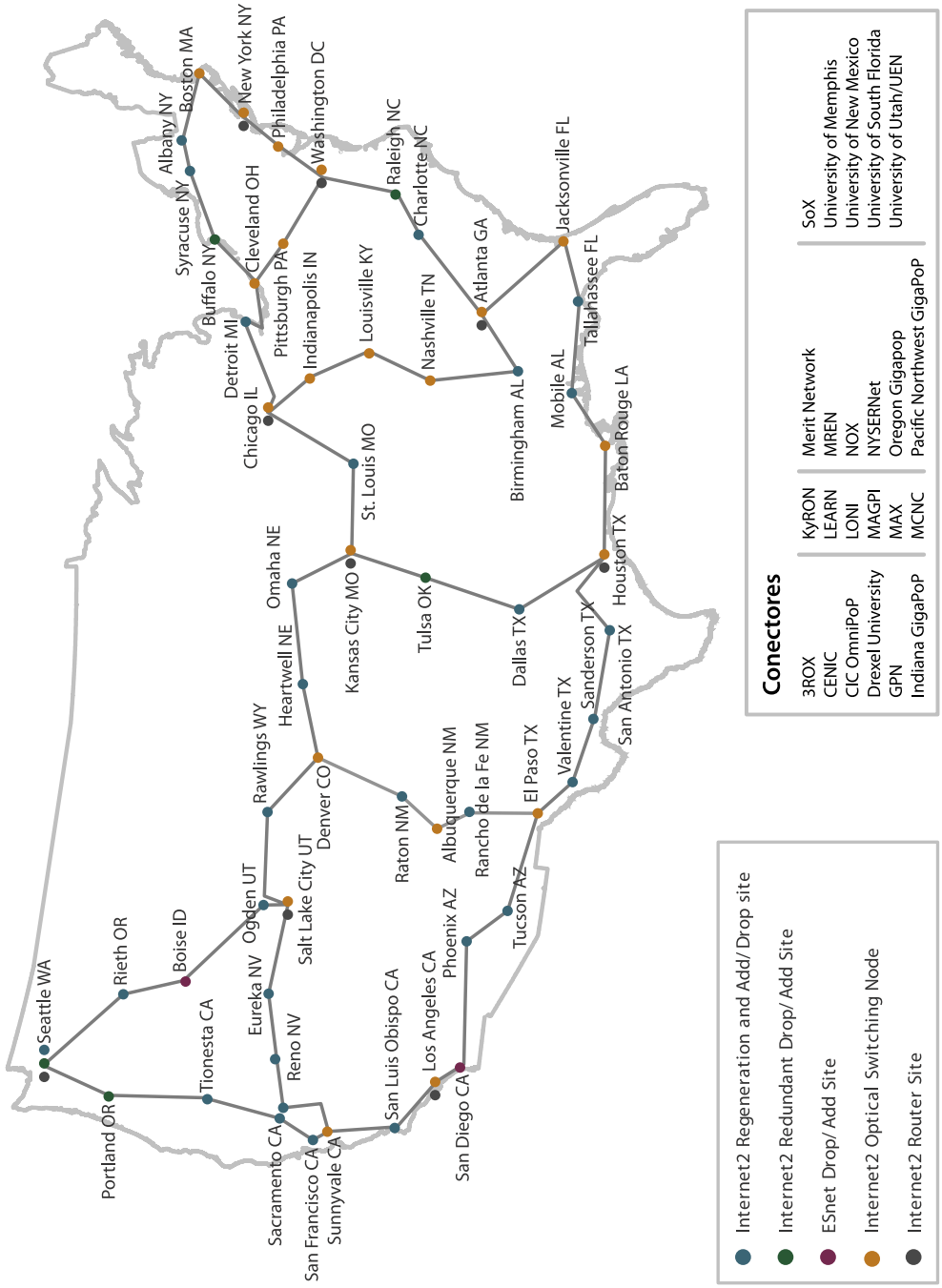


FIGURA 3: **ABILENE (INTERNET2) – EEUU**[9]

9 http://www.internet2.edu/pubs/200904-Internet2CombinedInfrastructureTopology.pdf

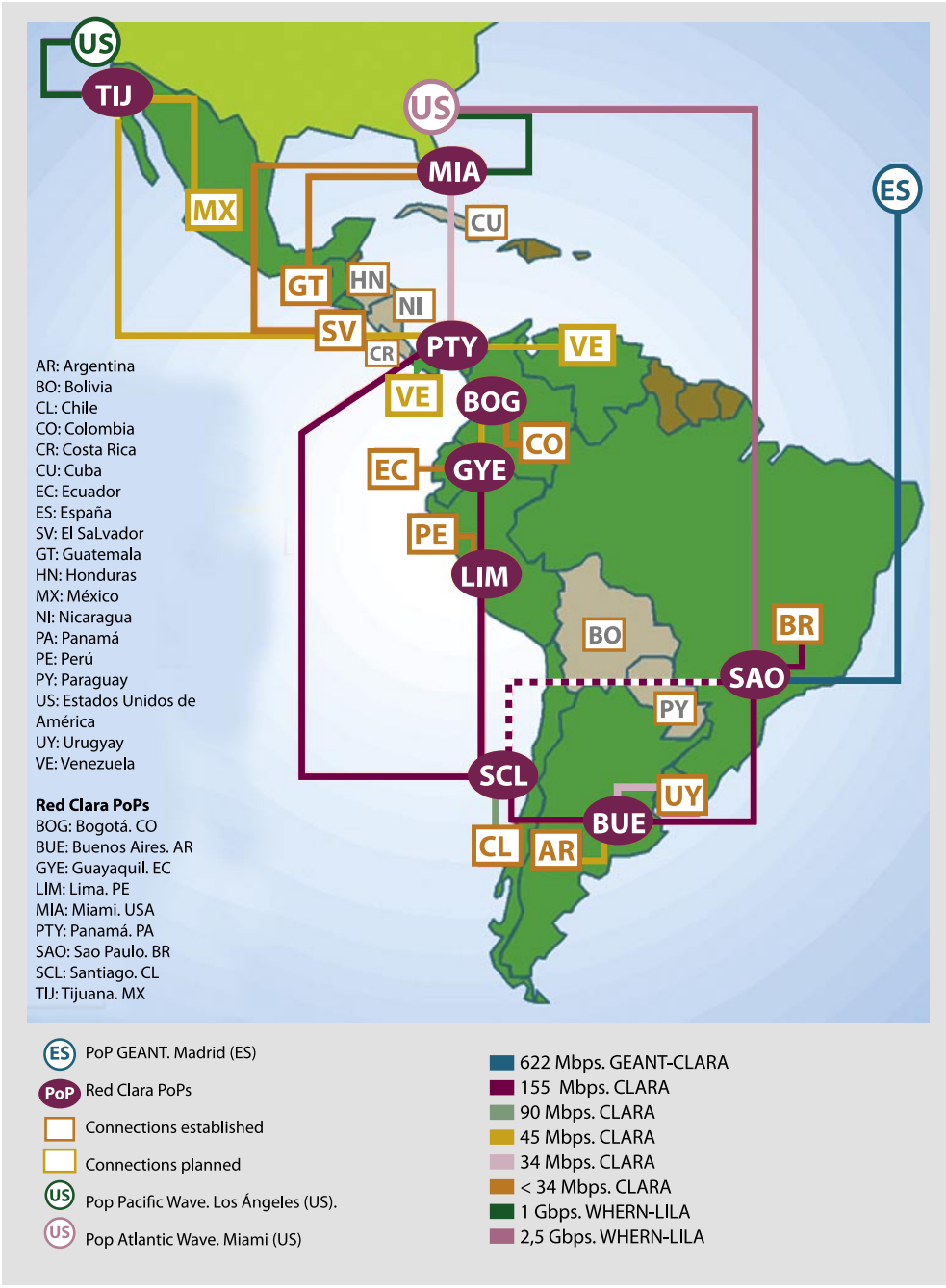


FIGURA 4: **REDCLARA - AMÉRICA LATINA**[10]

10 http://www.redclara.net/index.php?option=com_content&task=view&id=51&Itemid=236

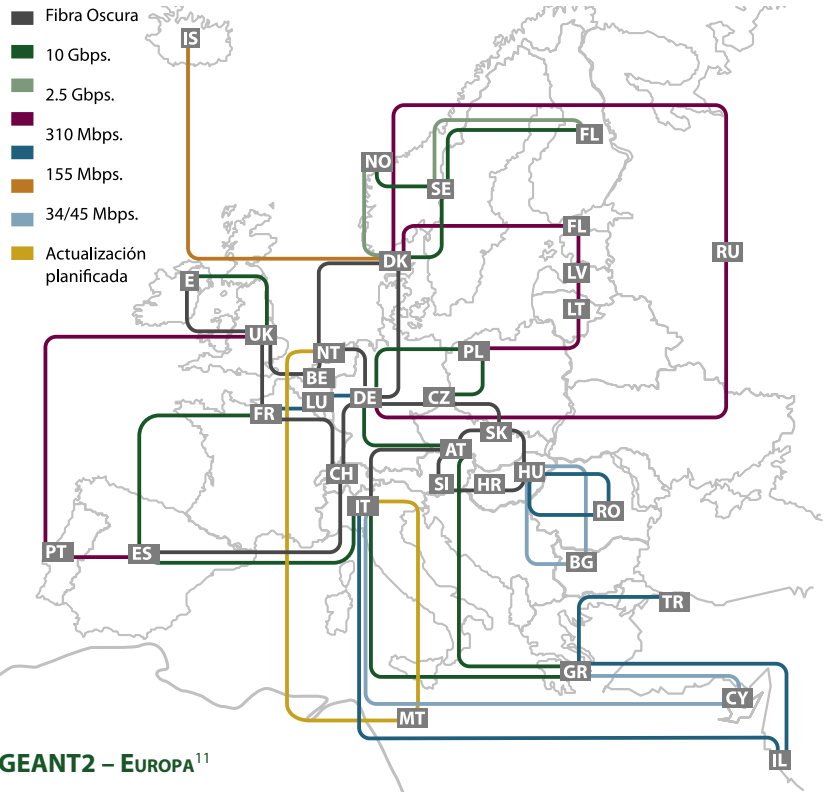


FIGURA 5: **GEANT2 – EUROPA**[11]

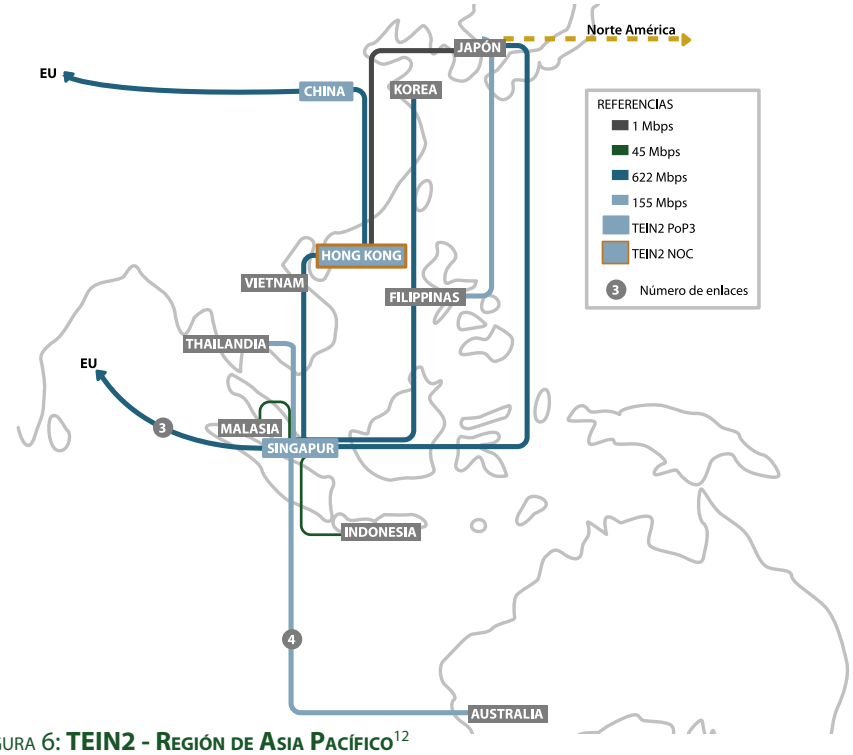


FIGURA 6: **TEIN2 - REGIÓN DE ASIA PACÍFICO**[12]

11 http://www.geant2.net/upload/img/jan08map.jpg
12 http://www.tein2.net/upload/img/TEIN2-web.gif

4. Desplegando IPv6 en la universidad/centro de investigación

En esta sección nos ocupamos de los pasos necesarios para poder hacer un despliegue de IPv6 en una red de una universidad o, más generalmente, en una institución de características educativas o científicas.

Si bien puede pensarse que no hay diferencias entre este tipo de institución y una red de una empresa o una oficina pequeña, hay algunas particularidades por las que veremos que vale la pena hacer una sección separada. Hacemos la salvedad de que estaremos hablando de las redes que están al servicio del investigador o del docente y no haremos mención a redes de administración, ya que esos casos son similares a los tratados en otros capítulos de este libro.

4.1 Equipamiento, aplicaciones y servicios a tener en cuenta

En una red como la que estamos tratando, podemos destacar los siguientes equipos a grandes rasgos:

- Routers
- Servidores
- Estaciones de trabajo (PC, portátiles, otros dispositivos)
- Equipos de videoconferencia
- Conmutadores (cableados o inalámbricos)
- Firewall

En cuanto a los servicios que se encuentran normalmente disponibles, podemos citar:

- DNS
- Servicio de mail entrante, saliente y casillas de correo
- HTTP/HTTPS
- Directorios y servicios de autenticación
- Grids
- Monitoreo

En función de esto podemos identificar las aplicaciones que son más comúnmente utilizadas. Nos centraremos en las soluciones de código abierto ya que constituyen la elección mas habitual en el ámbito que estamos describiendo.

- Bind
- Sendmail o Postfix
- Apache
- OpenLDAP
- Radius
- Globus
- Diversos paquetes de aplicaciones libres para monitoreo

Todos los paquetes de aplicaciones previamente mencionados soportan IPv6 en sus últimas versiones, por lo que solamente deberemos tener en cuenta las opciones de configuración que correspondan. Antes de dedicarnos a ello, trataremos el tema de los rangos de direcciones que pueden utilizarse.

4.2. Cómo asignar direcciones IPv6 en una Universidad

Al momento de definir un rango IPv6 para una institución de este tipo, debemos tener en cuenta que, como ya se explicó, la mayoría de los centros de investigación o universidades se encuentran conectados a una red nacional o regional de educación e investigación (NREN).

La NREN, que por lo general ya poseerá una conectividad nativa a IPv6, podrá suministrar un rango de direcciones a nuestra institución.

En estos casos, el rango que se obtendrá será un /48, pudiendo disponer de 256 subredes /56 para asignar internamente en la institución, de acuerdo a las prácticas habituales.

También es importante mencionar que muchas veces las instituciones académico/científicas están conectadas a una NREN pero también obtienen el servicio de Internet de un proveedor.

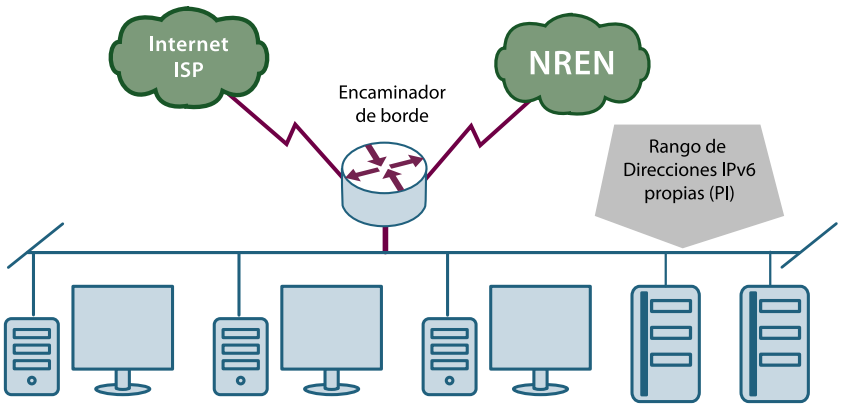


FIGURA 7: **ESQUEMA DE CONECTIVIDAD DE UNA INSTITUCIÓN FINAL EN UNA NREN**

En esos casos cumplen las condiciones para poder solicitar su propio rango IPv6 directamente a alguno de los Registros Regionales de Internet (RIRs). También, en algunos de los RIRs, existen políticas especiales que pueden ser aprovechadas por organizaciones como universidades o centros de investigación, aun no teniendo la característica de multiproveedor.

Un párrafo especial merece la conexión que obtiene la institución de parte de la NREN. En la mayoría de los casos, esto será a través de un enlace transparente, punto a

punto, que llega a algún punto de presencia de la NREN. En estos casos configurar IPv6 en modo nativo no será un problema. Sin embargo, existen casos en que la conectividad interna de la NREN es hecha a través de alguna tecnología de VPN, por lo general MPLS, ofrecida por un proveedor.

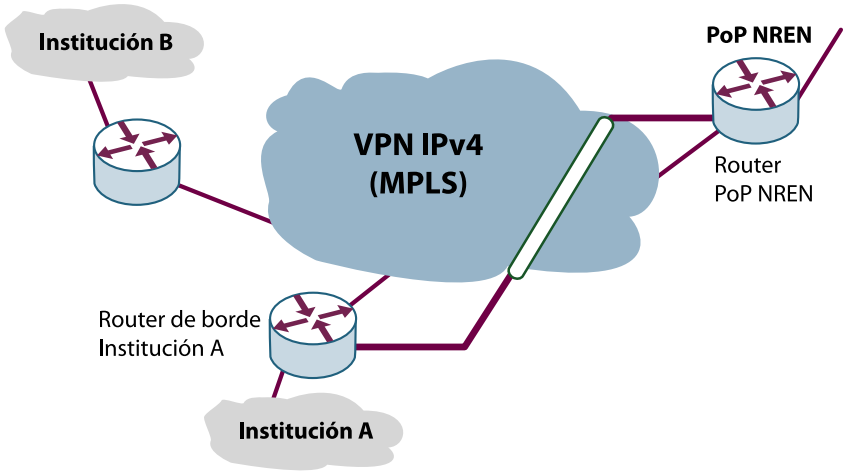


FIGURA 8: **CONECTIVIDAD INTERNA DE UNA NREN A TRAVÉS DE UNA VPN**

¿Qué se puede hacer en estos casos? La solución es utilizar alguna técnica de encapsulado del tráfico IPv6 en IPv4. Esto puede ser algo tan simple como un túnel configurado entre el punto de presencia de la NREN y el router de borde de la institución. También podría utilizarse alguna técnica como 6PE, "carrier de carrier", etc.

4.3. Configuración de equipos

A continuación daremos una breve descripción de la configuración en los distintos equipos que mencionamos antes, necesaria para implementar IPv6 en una red de una institución académica.

4.3.1. Routers

Los equipos de encaminado deberán tener configurados los prefijos IPv6 que correspondan a la institución en las interfaces que van a tener IPv6 habilitado. Es conveniente permitir que los prefijos de red sean anunciados en cada LAN, para permitir la autoconfiguración de dispositivos.

Una mención especial merece el protocolo de encaminado interno que utiliza la institución: dado que ahora será necesario incluir el intercambio de información de IPv6 además de IPv4, se deberá utilizar algún sistema de encaminado interno que soporte IPv6. La recomendación es entonces utilizar OSPFv3 o IS-IS, que permiten manejar diferentes topologías en cada versión de IP. Esto último es importante cuando se hace un despliegue

de IPv6 por etapas en la red interna, ya que de lo contrario se crearían problemas de encaminado al existir equipos intermedios que pueden no funcionar con IPv6.

Ejemplo de configuración (Cisco):

```
interface GigabitEthernet0/1
ipv6 address 2001:0db8:1009:101::1/64
ipv6 nd prefix 2001:0db8:1009:101::1/64
ipv6 ospf 1 área 0

ipv6 router ospf 1
router-id 1.1.1.1
área 0 range 2001:db8:1009::/48
```

En la configuración con la NREN, la institución muy probablemente deberá establecer una sesión BGP para publicar su prefijo de red y también aprender todos los prefijos externos a la institución. Alternativamente, si es el único enlace hacia afuera, se podrá utilizar una ruta por defecto y la NREN tendrá una ruta estática a nuestro prefijo por dicho enlace.

Ejemplo:

```
router bgp 64500
address-family ipv6 unicast
neighbor 2001:0db8:ffff::2/64 remote-as xxx
network 2001:0db8:1009::/48
```


Tal como se mencionó anteriormente, es posible que la conexión a la NREN o bien alguna parte de la red interna de la universidad pase por una red sólo IPv4. En esos casos será necesario establecer un túnel manual entre los extremos que soporten IPv6.

Ejemplo:

```
interface tunnel 1000
ipv6 address 2001:db8:FFFF:FFFF::1/64
tunnel source GigabitEthernet 0/1
tunnel destination 10.1.1.1
tunnel mode ipv6ip
```

4.3.2. Servidores

Los sistemas operativos que se utilizan para brindar servicios en este tipo de instituciones generalmente son sistemas Linux o Unix. Estos sistemas tienen soporte de IPv6 desde hace muchos años, con versiones muy estables, por lo cual no representa un problema configurarlos.

En general no haremos autoconfiguración en los servidores, sino que vamos a querer especificar direcciones estáticas y hacerlo manualmente. En los sistemas Li-

nux se puede deshabilitar la autoconfiguración mediante un parámetro del kernel: "net.ipv6.conf.*.autoconf=0".

La configuración de direcciones IP en las interfaces varía según la variante de sistema operativo que se utilice, por ejemplo en Solaris se realiza definiendo un archivo /etc/hostname6.xxx, donde xxx es el nombre de la interfaz de red, mientras que en los sistemas como Ubuntu/Debian, se utiliza el archivo /etc/network/interfaces.

Normalmente vamos a querer que los servidores estén registrados en el DNS, tanto las zonas directas como inversas. Veremos esto más adelante, en la sección donde se explica cómo configurar DNS.

4.3.3. Estaciones de trabajo (PC, portátiles, otros dispositivos)

Tanto las PC de escritorio como las portátiles tendrán sistemas operativos que soportan IPv6, ya sea Linux o Windows. En algunos casos, puede haber estaciones de trabajo con sistemas Unix, que también, como ya mencionamos, simplifican el despliegue de IPv6.

Es conveniente que este tipo de dispositivos se configure de forma automática, preferiblemente con un servidor DHCPv6, que permite tener un control mayor sobre la asignación de direcciones y suministrar otra información como por ejemplo cuáles son los servidores de DNS. También facilitará la actualización automática de los registros en el DNS de la institución si se utiliza esa facilidad.

En general, las aplicaciones de uso diario, no tendrán problemas en lo que a la nueva versión del protocolo IP se refiere. Entre esas aplicaciones podemos citar los clientes de correo, navegadores de Internet, sistemas de colaboración, etc.

Dentro de los equipos conectados a la red en una institución universitaria podemos encontrar diverso tipo de instrumental preparado para adquisición de datos y que proveen una interfaz de red, tales como microscopios, analizadores, controladores, sensores en general. En esos casos, es muy probable que no estén preparados para soportar IPv6. También podemos encontrar limitaciones en impresoras de red y escáneres, por lo que habrá que contemplar la necesidad de mantener la compatibilidad con IPv4. Por esa razón, la recomendación es que los equipos terminales de usuario mantengan el sistema de doble pila o "dual stack".

4.3.4. Equipos de videoconferencia

Más allá de los sistemas por software es común encontrar en este tipo de instituciones equipos especializados para realizar videoconferencias. Estos pueden ser de sala o de escritorio, consisten normalmente de hardware especializado con versiones de software propietarias. Entre los equipos mas conocidos que existen en el mercado, tenemos por

ejemplo, Polycom, Tandberg, Aethra, Sony, LifeSize, con una gran variedad de modelos dentro de estas marcas.

El nivel de soporte de IPv6 varía en función del modelo y marca que se esté utilizando, por lo cual queda fuera del alcance de este capítulo poder brindar recomendaciones de configuración. Sin embargo, vale la pena mencionar que al momento de evaluar la adquisición de un equipo de videoconferencias, se debe evaluar qué grado de adopción del protocolo IPv6 posee. En algunos casos es posible utilizar sólo el protocolo SIP en IPv6, no estando soportadas las comunicaciones en H323. También es posible que el equipo tenga una configuración manual limitada y sólo permita mecanismos de autoconfiguración. Estas mismas consideraciones valen para los equipos denominados MCU – Unidad de Control Multipunto.

4.3.5. Conmutadores (switches) cableados o inalámbricos

Desde el punto de vista de IPv6, los dispositivos de capa 2 no deberían representar un problema ya que no necesitan interpretar el tráfico de capas superiores. Sin embargo, en el caso de los conmutadores, es conveniente que puedan soportar características como "MLD snooping", que permite determinar a qué puertos enviar el tráfico multicast en función de los grupos multicast a los cuales se han suscripto dispositivos conectados a esos puertos.

En cuanto a los puntos de acceso inalámbricos, en general en las universidades se utilizan en modo transparente, cumpliendo sólo una misión de punto de acceso, por lo que tampoco representan un inconveniente. Sólo en el caso en que estos equipos actúen como routers, será necesario tener en cuenta el soporte de IPv6 y de las opciones de configuración que permite. No obstante, este no suele ser el modo que se utiliza en este tipo de instituciones, ya que no permite una administración centralizada.

4.3.6. Cortafuegos (firewalls)

Los firewall son un punto crítico en la infraestructura de red disponible. Se debe verificar que el soporte de IPv6 exista y que permita configurar reglas de filtrado en forma similar que con IPv4. No analizaremos aquí las distintas marcas existentes, ya que hay una variedad muy amplia de soluciones. Sólo mencionaremos que existen soluciones de código abierto como ip6tables para Linux o ip6fw para BSD que pueden utilizarse.

Es importante tener en cuenta que deben reproducirse las mismas reglas en IPv6 que en IPv4, porque de lo contrario se estarían teniendo políticas diferentes para una versión del protocolo que para otra.

4.4. Implementación de servicios con IPv6

Para finalizar esta sección, examinaremos algunos de los servicios que una institución de estas características debe definir. Veremos a continuación cómo configurar algunos

de ellos y las consideraciones a tener en cuenta en cada caso. Además para los servicios más comunes puede verse más información de configuración en el capítulo dedicado a Servicios y Servidores.

4.4.1. DNS

Las universidades o centros de investigación suelen tener sus propios rangos de direcciones IPv4 y administran sus propios servidores de nombres, tanto de los dominios directos como inversos. En el caso de IPv6 esto será similar, por lo que veremos cómo configurar este servicio.

La aplicación más utilizada para DNS es BIND, que como ya mencionamos, soporta IPv6. Una primera consideración será que el servidor de nombres tenga direcciones IPv6 configuradas y sea alcanzable dentro de la red interna tanto por IPv4 como IPv6. Esto permitirá que el DNS responda en forma nativa en IPv6.

Así como en IPv4 tenemos los registros "A" para definir direcciones IP asociadas a un nombre, en IPv6 utilizaremos los registros "AAAA", que funcionan de una manera análoga. En general definiremos los dos tipos de registro dentro de la misma zona.

Ejemplo:

```
ns1   IN      A       192.0.2.18
      IN      AAAA    2001:0db8::18
ns2   IN      A       192.0.2.12
      IN      AAAA    2001:0db8::12
```


Por otro lado, también será necesario definir los inversos en la zona correspondiente, que para IPv6 es ip6.arpa. Los registros que se utilizan son los mismos registros PTR que en IPv4. Es importante tener en cuenta que se deben completar todos los grupos de ceros que se omiten habitualmente en la escritura de una dirección IPv6 y además, cada dígito hexadecimal de la dirección debe incluirse en la representación reversa, separado por puntos. Esto hace más compleja la edición manual de las zonas reversas.

Ejemplo:

```
$ORIGIN 0.0.0.0.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa.

8.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0   IN PTR ns1.example.org.
2.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0   IN PTR ns2.example.org.
```

De esta forma podemos definir toda la información correspondiente a los servidores y equipos que tengan una IP asignada en forma estática.

Ahora bien, una de las herramientas mas poderosas que nos brinda IPv6 es la autoconfiguración de dispositivos. ¿Cómo podemos reflejar esta información en el DNS sin perder la dinámica que nos brinda esta opción? Para esto, se utiliza la opción de actualización

dinámica que proveen las versiones actuales de BIND. Mediante esta técnica, es posible que un nodo o el servidor DHCPv6 sean quienes agregan los registros correspondientes en las zonas directa e inversa. En estos casos se suele utilizar una clave compartida entre el servidor DNS y el cliente como forma de autorizar los cambios. Por esa razón mencionamos anteriormente que es más fácil que este proceso se lleve a cabo desde el servidor DHCPv6, que será el agente autorizado a modificar en forma dinámica las zonas del DNS. La correcta configuración de esta facilidad excede el objetivo de este capítulo, por lo que no entraremos en detalles sobre ello, pero se puede obtener buena información en los manuales de referencia de BIND o en documentación sobre DNS.

4.4.2. Servicio de mail entrante, saliente y casillas de correo

Para implementar un servicio SMTP tanto entrante como saliente con IPv6, simplemente es necesario que el servidor cuente con direcciones IPv6, ya que el software para este servicio está preparado para utilizar la nueva versión del protocolo.

Respecto de las casillas de correo, es necesario utilizar un software POP3 o IMAP que funcione sobre IPv6. Hay versiones de código abierto disponibles como por ejemplo la de la Universidad de Washington[13] que lo soportan.

4.4.3. Servidores web

Uno de los servicios fundamentales en este tipo de redes es el servidor web, ya que suelen existir páginas institucionales, tanto centrales, como descentralizadas pertenecientes a las facultades, departamentos, direcciones, etc. También puede haber páginas por proyectos, grupos de alumnos, cátedras y en general una gran variedad de servidores que conviven dentro de la misma red.

Afortunadamente el servidor más utilizado en los sistemas de código abierto es Apache, que está preparado para manejar IPv6 sin problemas.

Un punto a tener en cuenta aquí es que el servidor debería estar configurado para responder requerimientos tanto en IPv4 como en IPv6. Muchas veces esto es hecho simplemente utilizando un único socket IPv6 y utilizando para ello las direcciones IPv4-mapeadas (direcciones del tipo ::ffff:a.b.c.d).

Para un buen funcionamiento de este servicio, es necesario definir los registros correspondientes en el DNS para cada uno de los servidores web instalados en la institución. Como vimos, esto consiste en definir los registros AAAA y también los reversos dentro de la jerarquía ip6.arpa.

13 http://www.washington.edu/imap/

4.4.4. Directorios y servicios de autenticación

Un servicio comúnmente utilizado en las instituciones académicas es el de directorios, por medio del cual se accede a diversa información de las personas que forman parte de la institución y que permite ser compartida con otras instituciones similares. De esta manera, se tiene una única visión de los datos sobre cada persona, tanto personales como de acceso a diversos recursos (estaciones de trabajo, red, autenticación para el correo, etc).

La implementación más utilizada para este tipo de directorios es LDAP y un software de código abierto ampliamente difundido es openLDAP, que soporta IPv6 en modo nativo. Al igual que se mencionó para los servidores web, se debería permitir el acceso en doble pila bajo cualquiera de las dos versiones del protocolo IP.

Un servicio relacionado al de directorios y que suele estar ligado es el de radius. Mediante este protocolo se puede autenticar y autorizar el acceso a los recursos en forma distribuida, dirigiendo las consultas al servidor de la institución que corresponda. De esa forma se implementan dentro de la comunidad académica servicios como el "roaming" de investigadores o docentes entre las instituciones, conservando los mismos accesos a los recursos desde distintos sitios, como si se estuviera en la organización de origen.

Se deberá revisar que el software que implementa radius en nuestra institución soporte IPv6. Una de las versiones de software de código abierto existentes, freeradius, está preparada para ello. Es importante controlar que los equipos puedan conectarse tanto en IPv4 como en IPv6 a dicho servidor, ya que éste será un servicio básico de la infraestructura de nuestra red.

4.4.5. Grids

Ya mencionamos anteriormente las ventajas que IPv6 puede presentar para sistemas grid. El software sobre el cual están basados estos sistemas, Globus Toolkit, soporta IPv6 en sus últimas versiones, por lo cual los desarrollos que se hagan sobre el mismo estarán preparados para utilizar la nueva versión de IP. La condición para esto es que, el servidor sobre el cual corre el sistema y las aplicaciones sobre las cuales se definen los servicios grids estén preparadas para ello. Como ya vimos, por lo general será así.

4.4.6. Monitoreo

Normalmente las redes universitarias ponen al servicio de sus usuarios diversos sistemas de información sobre el tráfico que pasa por la red, pudiendo medirse características tales como los servicios utilizados, IPs de origen y destino del tráfico e incluso sistemas autónomos entre los cuales se realiza mayor intercambio de información. A su vez, los administradores de la red, tanto de la institución como los de las diversas partes que la componen (facultades, departamentos), necesitan tener control sobre los enlaces que forman la infraestructura de la red.

Existen muchos paquetes de software que se utilizan habitualmente. Sólo mencionaremos algunos de ellos que soportan IPv6: MRTG, Cacti, Nagios, Ntop, Ethereal.

5. Consideraciones adicionales

Para finalizar vamos a remarcar algunas de las características de IPv6 que benefician o pueden ser de utilidad para las redes universitarias y para los administradores de esas redes.

5.1. Direcciones disponibles

Las universidades se caracterizan por tener grandes cantidades de equipos, con muchas subredes bajo diferente administración (facultades, departamentos). Como vimos, muchas de las aplicaciones que utilizan los investigadores y docentes requieren direcciones IP públicas, globalmente alcanzables. Las posibilidades que brinda IPv6 en ese sentido facilitan poder cumplir con este requerimiento.

5.2. Autoconfiguración

Las redes con gran cantidad de equipos terminales, con administración descentralizada, como es el caso de este tipo de instituciones, se ven favorecidas por las posibilidades de configuración automática de equipos, fundamentalmente con DHCPv6. Esto permite mantener un control adicional sobre la asignación de IP a los equipos terminales, tanto cableados como inalámbricos.

5.3. Renumeración

La posibilidad de poder renumerar fácilmente las redes, con sólo programar cambios en los equipos routers, es fundamental para redes de gran tamaño como las que estamos analizando. Esto da una gran flexibilidad a la hora de contratar proveedores de Internet, ya que el cambio de uno a otro no presupone un gran esfuerzo para los administradores de la red.

5.4. Movilidad

Como ya se ha mencionado, la movilidad es una característica muy común entre los investigadores y docentes, por lo que el acceso a los recursos desde distintas redes, con las mismas características que en el propio lugar de trabajo, facilitan la colaboración entre los grupos de trabajo inter-institucionales.

5.5. Otras cuestiones prácticas

Terminaremos esta sección mencionando algunas aplicaciones más tradicionales que sin embargo son muy utilizadas en los ambientes de investigación.

Es común realizar transferencias de datos utilizando ftp o ejecutar procesos en una máquina remota, mediante una sesión ssh. Estas dos aplicaciones permiten por ejemplo utilizar capacidad de cómputo de otros sitios, transfiriendo los datos y los resultados de la ejecución de un programa. Ambas aplicaciones tienen soporte de IPv6, por lo cual se podrán utilizar sin necesidad de configuración previa.

Otro tipo de actividad que suele utilizarse en estos entornos es la visualización remota, ya sea a través de sistemas X-windows como también mediante interfaces más simples como por ejemplo VNC. Tampoco tendremos problema en estos casos en utilizar IPv6, ya que X-windows lo soporta y en el caso de VNC hay versiones que lo contemplan.

También son habituales dentro de los sistemas de educación a distancia los paquetes de software llamados de "campus virtual" o "entornos de enseñanza virtual". Una de las aplicaciones más utilizada es moodle, que ya ha incorporado el soporte de IPv6.

Por último, muchas veces es importante poder saber si contamos con conectividad IPv6 extremo a extremo con algún sitio, para lo cual podemos utilizar herramientas como traceroute6 o mtr, que nos reportarán el camino que hace nuestro tráfico para llegar a destino. De esta forma, si todo el camino funciona con IPv6, podremos obtener ventajas de esta disponibilidad. También podemos chequear con ping6 si un host o server responde los paquetes IPv6.

6. Conclusiones

A lo largo de este capítulo hemos visto las condiciones particulares que tienen las redes de instituciones científicas o académicas. Esto queda reflejado tanto desde el punto de vista de la historia y la investigación en las tecnologías que constituyen la base de Internet, como también en la experimentación con nuevas aplicaciones y protocolos.

Vimos también que muchos de los servicios que son necesarios para la educación o la ciencia actuales difieren de lo utilizado en otro tipo de redes como las empresarias o de proveedores de Internet, por lo que merecen un análisis especial.

Como queda puesto de manifiesto, la mayoría de estos servicios y aplicaciones están listos para funcionar sobre IPv6 y, sumado a que existe una vasta experiencia en la utilización de la nueva versión del protocolo, estamos en condiciones de incorporar nuestras instituciones a las redes que ya tienen soporte nativo de IPv6.

7. Proveedor de Servicios de Internet (ISPs)

1. A quién está dirigido el capítulo

Esta sección del libro está dedicada a las personas responsables de la planificación y/o operación de un Backbone IP que actualmente brinda solo servicios IPv4. Este es el caso típico de proveedores de servicios de Internet en diferentes modalidades (accesos dedicados, proveedores de banda ancha, proveedores regionales, etc.). Para simplificar las configuraciones se mostrarán ejemplos que servirán como referencia.

Se detallarán los temas que enfrentará el administrador al momento de encarar el proyecto. Tendrá que hacer un plan de numeración, tendrá que asignar direcciones a interfaces (existen algunas consideraciones al utilizar IPv6) tendrá que tener en cuenta los servicios que utiliza para la operación del Backbone IP, habrá consideraciones de routing al implementar pares (peers) IPv6, etc.

El siguiente diagrama muestra la topología típica de un proveedor de servicios y el área sobre la que describiremos la implementación de IPv6.

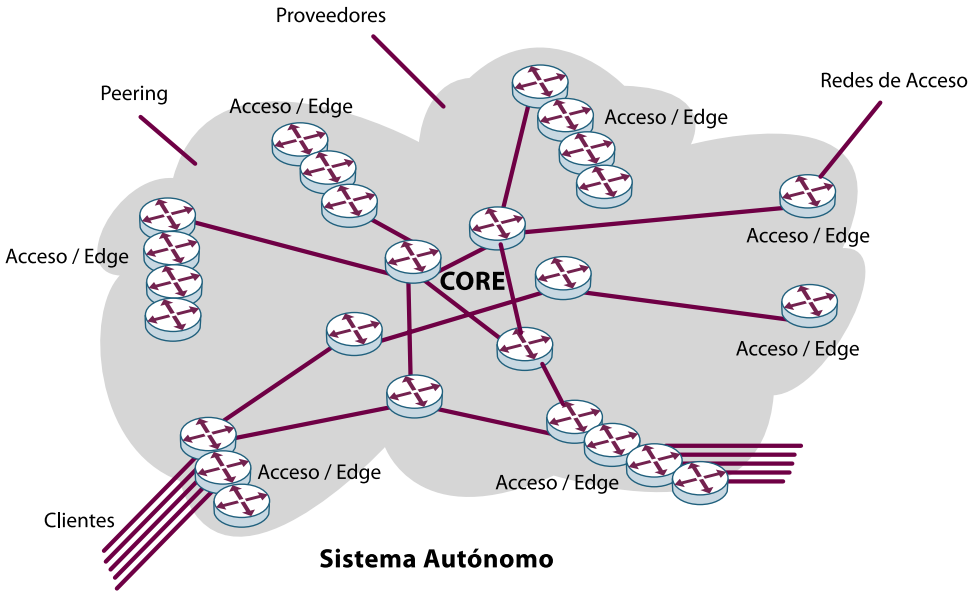


FIGURA 1: **TRONCAL ("BACKBONE") EJEMPLO**

Cuando la red del proveedor tiene gran cantidad de routers en el troncal ("backbone"), se utiliza un esquema de Reflectores de Rutas (Route Reflectors). Ello es necesario para hacer escalable la implementación de BGP. En estos casos la configuración descrita servirá como ejemplo para complementar las configuraciones BGP que utilizan actualmente.

Describiremos los cambios necesarios en los equipos dentro de la zona resaltada. Este capítulo no describe lo que ocurre en otros equipos ya que fue cubierto en otras secciones de este libro. No detallaremos configuraciones en equipos de cliente (CPEs), ni en redes

LAN, en Hosts clientes o servidores, ni en las redes de acceso utilizadas por los proveedores de banda ancha.

1.1. Tecnologías y proveedores incluídos en el texto

Para los ejemplos de configuración presentados se consideró tanto el caso de Cisco IOS como el de Juniper JunOS. Existen otros proveedores de routers no contemplados, sin embargo es menos frecuente su uso en el backbone y el CLI (Command Line Interface) en otros equipos suele ser similar al de Cisco IOS.

En caso de estar utilizando ambos proveedores en el backbone, también pueden utilizar estas configuraciones como ejemplo. Son pocos los casos en los que deben considerarse configuraciones particulares para la compatibilidad entre Cisco y Juniper.

1.2. Descripción de los servicios a habilitar

Para desplegar IPv6 en un backbone IP existen diferentes alternativas. Según los servicios del proveedor, el tamaño de la red y la capacidad del equipamiento instalado cada administrador debe elegir la solución que mejor se ajuste.

Como ocurre en otros entornos la solución de doble pila o dual stack es la mas recomendable. Sin embargo, en el core de la red podemos utilizar métodos mas simples y rápidos de implementar que el doble pila y que no son tan ineficientes como los túneles. Es el caso del MPLS utilizando 6PE.

Para simplificar el texto solo presentaremos estos dos casos, la implementación con doble pila y el caso de un backbone MPLS. Haremos una referencia a la utilización de túneles y sus configuraciones aunque no es una solución recomendada. La utilización de 6PE no solo aplica a los proveedores que ya tengan implementado MPLS para ofrecer otros servicios sino también en caso que el core de la red no pueda soportar doble pila.

1.3. Clientes utilizando IPv6 sin que el proveedor lo haya habilitado

Antes de comenzar con los ejemplos de configuraciones y las recomendaciones de implementación es conveniente tener en cuenta que muchos de sus clientes pueden estar haciendo uso de IPv6 sin que el proveedor lo haya habilitado. En capítulos anteriores se presentaron mecanismos de transición que sirven para utilizar IPv6 cuando el proveedor no lo soporta. Esto parece una gran ventaja y un proveedor de servicios podría considerar que puede postergar la implementación ya que sus clientes actuales no lo presionarán, sin embargo, esos mecanismos no cubren todas las necesidades y en muchos casos pueden complicar los diagnósticos cuando hay problemas.

Puede ser muy útil conocer como los clientes actuales hacen uso de esos mecanismos

de transición. Para eso, deberá analizar que relé Teredo o 6to4 están utilizando actualmente sus clientes. Es posible que la prestación actual de los servicios IPv6 utilizados con mecanismos de transición automáticos no sea buena. Por otro lado, los mecanismos de transición siempre tienen alguna ineficiencia no solo por el encapsulamiento (overhead) que agregan a cada paquete sino por los recorridos adicionales que hacen los paquetes entre ambos extremos y los relés.

Una vez implementado IPv6 en el backbone es aconsejable habilitar también alguno de estos relés para que los clientes que no se conectan en forma nativa en IPv6, puedan tener un servicio con mejores prestaciones utilizando el relé 6to4 o Teredo instalado en la propia red del proveedor.

2. Componentes del servicio

2.1. Red de un proveedor de servicios de Internet

Las configuraciones que describiremos mostrarán la implementación del IGP y del BGP para habilitar IPv6 en el backbone. Asumimos que el IGP es utilizado solo para mantener la información de routing de interfaces del backbone y que el BGP contiene la tabla completa y todas las redes/rutas propias del proveedor. Mostraremos solo las configuraciones necesarias en OSPF e ISIS que son los protocolos de encaminamiento (routing) interno más utilizados actualmente.

Asumiremos que actualmente el backbone tiene una correcta configuración de encaminamiento (routing) para IPv4 tanto a nivel BGP como IGP y describiremos solo los agregados para habilitar IPv6 sin detenernos en las clásicas configuraciones y explicaciones de estos protocolos de encaminamiento (routing) ya conocidos y utilizados.

En el caso de BGP veremos las configuraciones necesarias en caso de hacer "full mesh" de vecinos BGP y que también servirán como referencia para el caso mas general utilizando route reflectors. Esta última solución es la recomendada cuando se tienen más de cuatro routers en el backbone.

2.1.1. Equipos centrales (core) y equipos de acceso (edge)

Siguiendo las mejores prácticas para el diseño del backbone IP, tendremos encaminadores (routers) centrales que normalmente se denominan encaminadores (routers) de core y equipos de borde o acceso que son llamados encaminadores (routers) de edge. Para simplificar el texto no se incluirán todas las configuraciones de encaminamiento (routing) IGP y BGP para ambos casos, ya que serán muy similares. Sin embargo, en casos como MPLS esta distinción es importante ya que los cambios solo afectarán a los equipos de acceso.

El tamaño de la red tampoco influye mucho en las configuraciones necesarias. Como veremos mas adelante, para habilitar IPv6 solo tendremos que hacer agregados a las con-

figuraciones actuales en interfaces, en BGP y en algunos casos en el IGP. El objetivo es seguir los mismos estándares que tiene el backbone actual. Es posible que utilice configuraciones diferentes como una jerarquía de route reflectors, ajustes en los timers del IGP o del BGP, etc. Todas esas características estarán disponibles también para IPv6.

2.1.2. Proveedores superiores (upstream providers)

Antes de comenzar con las configuraciones en la red propia es conveniente contactar a los actuales proveedores. Actualmente muchos ofrecen IPv6 nativo a sus clientes, otros solo lo hacen configurando túneles y otros no lo soportan todavía. En caso que su proveedor no disponga de servicio IPv6 o que no pueda/quiera incluir servicio IPv4 e IPv6 sobre el mismo puerto, tendrán que utilizar un túnel. Inicialmente le conviene contactar al proveedor superior de su actual proveedor o consultar en el NAP local si existe algún servicio de túnel IPv6 gratuito en su país o región.

Si no existe un servicio local, y los proveedores superiores no lo soportan, tendrá que utilizar uno público. Es importante verificar la calidad de la conexión IPv4 entre su red y la del otro extremo del túnel eligiendo una en la que no exista perdida de paquetes o mucho retardo.

Un ejemplo de servicio público de túneles IPv6 es OCCAID[1], una red con recursos voluntarios que ofrece tránsito IPv6. Este servicio solo estará disponible para aquellos casos de instituciones que pueden demostrar que han solicitado tránsito IPv6 a sus proveedores y estos confirman que no pueden darlo.

2.1.3. Servidores y Servicios

Inicialmente los servicios y servidores no requieren actualizaciones. Al habilitar el encaminamiento (routing) IPv6 en el backbone toda la funcionalidad IPv4 se mantiene y ningún servicio será afectado. Solo hay que verificar que los sistemas operativos que poseen IPv6 habilitado no utilicen autoconfiguración y comiencen a utilizarlo. Es conveniente dejar correctamente configurado el encaminamiento (routing) antes de comenzar a trabajar en servicios, servidores y cortafuegos (firewalls).

También es importante notar que aunque los servicios no se verán afectados, es recomendable habilitar IPv6 en los servidores públicos para que la implementación tenga sentido. No habrá mucho tráfico IPv6 si nuestros DNS solo responden consultas IPv4. Los detalles sobre las configuraciones necesarias en servidores y servicios las encontrará en el capítulo correspondiente.

2.1.4. Peerings

Actualmente gran parte del tráfico IPv6 puede conseguirse vía peerings e interconexiones gratuitas. Es habitual que los proveedores sean mas flexibles al momento de

1 http://www.occaid.org/initiatives.php?node=gips

aceptar una interconexión de tráfico gratuito utilizando IPv6 que con IPv4. La recomendación es contactar primero a los peerings actuales IPv4 para verificar si soportan interconexiones IPv6 y bajo que modalidad.

Es común que los NAPs locales posean algún proyecto IPv6 que en algunos casos es solo de peering entre miembros y en otros casos incluyen servicios como tránsito. Recomendamos contactar al NAP/IXP cercano para conocer mejor el estado de implementación en su ciudad o país.

3. Implementación de IPv6 en la red

3.1. Plan y etapas recomendadas

Como en otros proyectos de red será necesario realizar un cuidadoso planeamiento antes de comenzar con los cambios en los equipos. Todas las configuraciones descritas tendrán impacto en el backbone IP y pueden afectar el servicio.

En general la primer etapa para el despliegue de IPv6 en el backbone es la capacitación del personal que liderará el proyecto. Es importante conocer y entender en detalle los servicios, equipos y configuraciones de la red actual para tomar las decisiones correctas durante la planificación. También es conveniente estar en contacto con el proveedor actual de equipos de red para conocer las limitaciones y tener el soporte adecuado desde el comienzo.

En paralelo se puede hacer el pedido de direcciones IPv6 al registro regional. Los detalles sobre las políticas actuales y los procedimientos están descritos mas adelante. El plan de numeración puede realizarse asumiendo que recibirá un /32 y sin tener que esperar el bloque definitivo. Una vez que el registro haya informado cual es el bloque, será simple actualizar la planilla utilizada. Solo cambiarán los primeros 8 dígitos hexadecimales de los bloques.

Luego conviene analizar las alternativas de implementación (doble pila, 6PE, túneles, etc.) y decidir cual será la mas conveniente considerando los servicios ya configurados en la red. Este capítulo le servirá para conocer las alternativas, las configuraciones involucradas y decidir cual será la mas adecuada.

Una vez identificados los equipos sobre los que habrá que trabajar (según el tipo de implementación y las configuraciones actuales de encaminamiento (routing)) será necesario un relevamiento de recursos (memoria disponible en cada uno, utilización de procesador, etc.) para asegurarse que las configuraciones no comprometerán el correcto funcionamiento de los equipos. Es bueno tener en cuenta que la topología IPv4 no necesariamente debe ser igual a la topología IPv6. En caso que algún enlace o equipo no soporte IPv6 y teniendo otros caminos disponibles, será posible hacer que el IGP solo vea aquellos caminos válidos. Si el IGP utilizado es IS-IS esta posibilidad será un poco mas compleja de implementar.

Luego se puede armar el plan de configuraciones comenzando por la habilitación de IPv6 en los routers, siguiendo con la configuración del IGP si fuera necesaria y terminando por la habilitación de IPv6 en las sesiones BGP.

4. Como recibir bloques IPv6 del registro regional

Considerando que este capítulo está dedicado a proveedores de servicio Internet, la recomendación es utilizar bloques IPv6 propios, recibidos directamente del RIR (Regional Internet Registry). Es posible que para las direcciones IPv4 no haya podido calificar para recibir los bloques directamente. En el caso de las direcciones IPv6 conviene revisar nuevamente las políticas del registro. Por ejemplo, en el caso de un proveedor de banda ancha que está utilizando direcciones IPv4 privadas (RFC1918) para sus clientes y desea reemplazar ese direccionamiento privado por direcciones IPv6 públicas (denominadas IPv6 globales en este caso), podrá hacer un requerimiento al registro pidiendo las direcciones IPv6 necesarias para ese cambio.

Describiremos algunas de las políticas que aplican a los proveedores de Internet que deseen recibir direcciones IP del registro:

Distribución mínima:

Los RIRs aplicarán un tamaño mínimo para distribuciones de IPv6 para facilitar el filtro basado en el prefijo. El tamaño mínimo de distribución para un espacio de direcciones IPv6 es /32 (obviamente, se puede solicitar un bloque más grande si se requiere).

Consideraciones de la infraestructura IPv4:

Cuando un proveedor de servicios IPv4 pide espacio IPv6 para una transición final de servicios existentes a IPv6, el número de clientes actuales de IPv4 podría ser usado para justificar un pedido más grande del que estaría justificado si el mismo estuviera basado solamente en la infraestructura IPv6.

En algunos casos los proveedores no hacen asignaciones IP a clientes pero acceden a bloques propios asignados por el registro utilizando las políticas de Usuarios Finales. En caso de poseer direcciones IPv4 portables, se puede acceder a direcciones IPv6 portables. En el caso de LACNIC la política actual dice:

> *LACNIC asignará bloques de direcciones IPv6 portables directamente a Usuarios Finales si cuentan con asignaciones de direcciones IPv4 portables previamente realizadas por LACNIC.*

Las asignaciones se realizarán en bloques menores o iguales a un /32 pero siempre mayores o iguales a un /48.

En algunos casos, es posible acceder a direcciones IPv6 portables sin tener asignaciones IPv4 portables previas. La política que permite recibir direcciones IPv6 del registro en

el caso de LACNIC establece los siguientes requisitos:

- En caso de anunciar la asignación en el sistema de rutas inter-dominio de Internet, la organización receptora deberá anunciar un único bloque, que agregue toda la asignación de direcciones IPv6 recibida.

- Proveer información detallada mostrando como el bloque solicitado será utilizado dentro de tres, seis y doce meses.

- Entregar planes de direccionamiento por al menos un año, y números de terminales sobre cada subred.

- Entregar una descripción detallada de la topología de la red.

- Realizar una descripción detallada de los planes de encaminamiento de la red, incluyendo los protocolos de encaminamiento a ser usados, así también como cualquier limitación existente.

- Las asignaciones se realizarán en bloques menores o igual a un /32 pero siempre mayores o iguales a un /48.

5. Plan de Numeración

Antes de comenzar con las recomendaciones para el plan de numeración, tengamos en cuenta las siguientes reglas:

En ningún caso el segmento o bloque debe ser menor a un /64. La única excepción a esta regla puede ser el caso de las interfaces, sin embargo, veremos mas adelante que también en las punto a punto conviene utilizar /64.

Para las asignaciones a clientes el criterio recomendado por el RFC3177 y los RIRs es:

- /48 en el caso general, excepto para suscriptores muy grandes. Es decir, hasta los usuarios residenciales deberían recibir /48.

- /64 cuando se conoce por diseño que una y sólo una subred es necesaria. Solo en los casos de conexiones individuales (un buen ejemplo podría ser conexiones dial-up).

A los clientes se recomienda asignar bloques /48 o mayores. Si tenemos en cuenta que el cliente no podrá partirlo en bloques menores a /64 estaremos dejando a disposición de los clientes 2^{16} (65.535) segmentos o bloques para su red interna y cada uno de esos segmentos puede tener 2^{64} dispositivos. En caso de asignar bloques mas grandes a /48 será necesario documentarlo correctamente para poder justificarlo al momento de pedir nuevos bloques IPv6 al registro. Un cliente podría recibir un bloque mayor a /48 si tiene

múltiples sitios u oficinas y cada una recibirá un /48.

Una buena referencia mantenida por la comunidad sobre el plan de numeración en IPv6 puede encontrarse en el Wiki de ARIN[2].

También será una buena referencia el RFC 4291 que describe los diferentes tipos de direcciones, la representación y las recomendaciones en routers y en hosts.

Cada segmento de LAN (Ethernet) utilizará un /64.

Es conveniente reservar para la infraestructura de red un /48 por PoP. Seguramente la utilización de este bloque será muy baja para muchos PoPs, sin embargo, siempre es mejor tener en un bloque totalmente independiente (no utilizado para clientes) y con direcciones IP disponibles para el PoP en el futuro.

Es conveniente utilizar un /64 dedicado a loopbacks. Considerando que cada una será un /128 la cantidad de direcciones disponibles en un solo /64 será suficiente.

Para cada interfaz punto a punto se recomienda utilizar un /64. Esto parece un gran desperdicio de direcciones IP ya que un /127 puede ser suficiente (así como en IPv4 podemos utilizar /31), sin embargo puede tener inconvenientes operativos tal como se describe en el RFC3627.

5.1. Políticas relacionadas con las asignaciones IPv6 (a clientes e internas)

A diferencia de IPv4 no existe un tamaño máximo de asignación a clientes. Cada proveedor puede tener su propia política de asignaciones para alentar una utilización óptima del bloque de direcciones total. Sin embargo, todas las asignaciones /48 a usuarios finales deben ser registradas en el RIR/NIR para poder evaluar apropiadamente la utilización cuando es necesaria una distribución subsiguiente.

A los RIRs/NIRs no les concierne el tamaño de direcciones que los LIRs/ISPs realmente asignan. Por lo tanto, los RIRs/NIRs normalmente no pedirán información detallada sobre redes de usuarios IPv6 como lo hicieron en IPv4. Solo en algunos casos podrían requerir esta información.

5.1.1. Asignación a la infraestructura del operador

Cada PoP de la red puede tener un /48 dedicado. Aquí también parece ineficiente la utilización de las direcciones IPv6, sin embargo estará cumpliendo con las políticas actuales. En el caso de LACNIC la política dice:

Una organización (ISP/LIR) puede asignar un /48 por PoP como un servicio de infraes-

2 http://www.getipv6.info/index.php/IPv6_Addressing_Plans.

tructura de un operador de servicio IPv6. Cada asignación a un PoP es considerada como una asignación sin tener en cuenta el número de usuarios que usen el PoP. Puede obtenerse una asignación separada para operaciones propias del operador.

5.2. NAT y Protección de la RED

En muchos casos el plan de numeración IPv4 utilizado en la red incluye segmentos con direcciones privadas (RCF1918) con el objetivo de ocultar esos dispositivos. En esos casos, para acceder a Internet desde esos segmentos se utiliza NAT (Network Address Translation). Es conveniente evaluar la utilización de IPs privados y NAT desde dos aspectos:

- Como "habilitador" de gran cantidad de direcciones IP
- Como recurso de seguridad para evitar el acceso a segmentos protegidos

Lamentablemente la utilización de NAT complica mucho a las aplicaciones y en algunos casos hace imposible su utilización. Realizar diagnósticos por problemas de conectividad se hace muy complejo y normalmente los desarrolladores de software deben tener en cuenta el soporte de NAT cuando requieren conexiones entre aplicaciones pasando por una red pública.

Cuando se utiliza IPv6, no hay necesidad de utilizar NAT, y de hecho no esta estandarizado. Existirán suficientes direcciones IPv6 para todos los dispositivos que se necesiten. Todos podrán tener direcciones IPv6 únicas.

Con respecto a las ventajas de seguridad o la utilización de NAT como protección, se recomienda leer el RFC4864, específicamente las políticas de protección (Local Network Protection) que lograrán niveles similares o superiores sin utilizar NAT.

En caso de necesitar direcciones IPv6 no accesibles globalmente, pero únicas (ULA[3]: Unique Local Addresses), se puede utilizar una herramienta[4].

Es posible que la falta de planificación y correcto asesoramiento al momento de implementar IPv6, resulte en serios problemas de seguridad. Lamentablemente muchas personas y proveedores han escuchado desde finales de la década del 90 que las direcciones IPv4 se estaban acabando. Como el problema no llegó hasta ahora muchos creen que nunca ocurrirá y por eso corren el riesgo de hacer una implementación desesperada cuando les llegue el momento. Existen características muy convenientes en IPv6 relacionadas con seguridad (como IPSec mandatorio, eliminación de NAT, etc.) pero también un impacto grande en aplicaciones y firewalls que debe ser tenido en cuenta (como la necesidad de permitir algunos paquetes ICMP). En el RFC4942 podremos encontrar un análisis del impacto en la seguridad al implementar IPv6.

3 RFC4193: http://www.ietf.org/rfc/rfc4193.txt
4 http://www.sixxs.net/tools/grh/ula/

5.3. Configuraciones

5.3.1. Habilitando IPv6 en los routers

Los routers Juniper ya vienen con routing IPv6 habilitado. En el caso de Cisco IOS debemos utilizar los comandos globales:

```
ipv6 unicast-routing
ipv6 multicast-routing
ipv6 cef
!
```

Para habilitar IPv6 en una interfaz para un router Juniper:

```
interfaces fe-0/0/1 {
  unit 0 {
    family inet6 {
      address 2001:DB8:C003:1001::1/64;
    }
  }
}
```

Para asignar una dirección IPv6 a una interfaz en Cisco IOS:

```
interface GigabitEthernet1/1
description Interface de Backbone
ipv6 address 2001:DB8:C003:1001::1/64
```


5.3.2. Configurando el IGP

En caso de implementar doble pila en todo el backbone será conveniente utilizar el mismo IGP para IPv6 e IPv4. En caso de tener habilitado MPLS en el backbone, no será necesario configurar el IGP con soporte IPv6 en el core ya que la información de reenvío (forwarding) estará a cargo del LDP o RSVP-TE.

Si actualmente está utilizando OSPF para IPv4 o si hay planes futuros de cambiar el IGP es posible tener procesos IGP diferentes para IPv4 e IPv6. Las alternativas están detalladas en el RFC4029 y son:

- OSPFv2 para IPv4, IS-IS para IPv6
- OSPFv2 para IPv4 y OSPFv3 para IPv6

También es posible utilizar IS-IS para IPv4 y OSPFv3 para IPv6, sin embargo requerirá conocimientos y experiencia en ambos protocolos. No tiene mucho sentido complicar la operación de la red innecesariamente.

En caso de estar utilizando IS-IS como IGP para IPv4 podrá habilitar IPv6 utilizando el mismo proceso.

En el caso de OSPF será necesario un proceso nuevo.

La configuración de OSPF para una interfaz de Backbone en un Cisco IOS será similar a:

```
interface Nombre-Interface
description Interface de Backbone
ipv6 address 2001:DB8:C003:1001::1/64
ipv6 ospf network point-to-point
ipv6 ospf 1 área 0
```

y la configuración del proceso será similar a:

```
ipv6 router ospf 1
auto-cost reference-bandwidth 10000
router-id Direccion-IP
área 0 range 2001:db8:C003::/48
```

5.4. Sesiones BGP

5.4.1. Consideraciones importantes

Las configuraciones BGP incluídas a continuación son solo ejemplos que servirán para conocer los comandos mínimos necesarios o los mas comunes para la implementación de IPv6. Estos comandos se agregarán a las configuraciones BGP existentes y no deberían afectar en nada a las sesiones actuales. Es muy probable que las configuraciones actuales de BGP para IPv4 incluyan otros ajustes que también pueden aplicarse a las sesiones BGP para IPv6 (por ejemplo modificaciones en los timers, límites en la cantidad de prefijos, etc.).

Si para asegurar el anuncio de los prefijos en IPv4 se utilizan rutas estáticas a null para el bloque grande agregado (Hold Down routes), lo mismo conviene hacer para el bloque IPv6.

Por ejemplo:

En Cisco IOS:

```
ipv6 route 2001:DB8::0/32 Null0 254
```

En Juniper:

```
routing-options {
 rib inet6.0 {
  static {
    route 2001:DB8::0/32 {
    discard;
    install;
    readvertise;
    }
```

```
    }
  }
}
```

En general las necesidades y el funcionamiento de BGP para IPv4 será igual que para IPv6. Por eso, conviene seguir las mismas prácticas que se utilizaron para la configuración actual de BGP. Esto permitirá que los diagnósticos sean mas simples ya que las áreas de operación comprenderán mas fácilmente las nuevas configuraciones.

Configuración de BGP en Cisco IOS

```
router bgp NumeroASN
 address-family ipv6
 redistribute commands

 neighbor direccion-IP-RR activate
 neighbor direccion-IP-RR send-community
 neighbor direccion-IP-RR peer-group nombre-grupo

exit-address-family
```


Configuración con Route Reflector en Junipter:

```
protocols {
   bgp {
      group nombre {
         family inet6 {
            labeled-unicast {
               explicit-null;
            }
         }
      }
   }
}
```

Configuración de Route Reflector en Cisco IOS:

```
router bgp NumeroASN
 address-family ipv6
 neighbor direccion-IP activate
 neighbor direccion-IP route-reflector-client
 neighbor direccion-IP send-community
 neighbor direccion-IP peer-group grupo
exit-address-family
```

5.4.2. Filtros

Es muy probable que actualmente las sesiones BGP tengan configurados filtros para evitar el intercambio de prefijos de direccionamiento privado (RFC1918) o de direccionamiento inválido. El equivalente de esos filtros para las sesiones BGP IPv6 serían:

En Juniper:

```
policy-options {
 policy-statement direcciones-ipv6-invalidas {
   term deny-IPv6 {
    from {
     route-filter 0000::/3 orlonger
     route-filter 4000::/2 orlonger
     route-filter 8000::/1 orlonger
     route-filter 2001:DB8::/32 orlonger
    }
    then {
     reject;
    }
   }
 }
}
```


En Cisco IOS:

```
ipv6 prefix-list ipv6-invalidas seq 20 permit ::/3 le 128
ipv6 prefix-list ipv6-invalidas seq 30 permit 4000::/2 le 128
ipv6 prefix-list ipv6-invalidas seq 40 permit 8000::/1 le 128
ipv6 prefix-list ipv6-invalidas seq 50 permit 2001:DB8::/32 le 128
```

5.4.3. Proveedores utilizando MPLS

Los proveedores que ya tienen configurado MPLS en el backbone, pueden utilizar la técnica conocida como 6PE, que permite habilitar IPv6 solo en los equipos de borde o acceso (PE: Provider Edge). El funcionamiento de 6PE es similar al que actualmente utiliza para el servicio VPN en MPLS. En el backbone MPLS habrá información de prefijos intercambiada por BGPv4 e información de re-envio o "forwarding" conocida por LDP o RSVP-TE para saber como hacer llegar los paquetes hasta el otro extremo del sistema autónomo. La información de forwarding para los equipos intermedios ya será conocida, por eso solo habrá que configurar IPv6 doble pila en los equipos de borde.

Para conocer en detalle el funcionamiento de 6PE puede consultarse el RFC4798. En ese RFC no solo se describe esta técnica sino que también se explica como utilizarla para casos mas complejos como la interconexión de sistemas autónomos diferentes (haciendo una analogía con la técnica de interconexión de ASNs utilizada para VPNs).

La ventaja de 6PE es la simplicidad de configuración. Teniendo ya implementado MPLS la parte mas compleja está resuelta y la habilitación de IPv6 es mas simple que la utilización de VPNs. La desventaja es que el routing del tráfico depende de los LSPs y no de la dirección IP que lleva cada paquete. Si bien lo mismo ocurre para el tráfico IPv4, en caso que un LSP no pueda establecerse y por error algún paquete IPv4 (de Internet) llegue sin etiqueta a cualquiera de los routers del backbone (incluyendo los del core), este lo podrá encaminar correctamente. Para el tráfico IPv6 este problema provocará el descarte de esos paquetes.

En este capítulo no describiremos la utilización de IPv6 en VPNs sobre MPLS ya que el libro está enfocado en el servicio de Internet, sin embargo es algo posible. El RFC4364, que reemplazó al RFC2547 (comúnmente referenciado para las VPNs MPLS) contempla tanto IPv4 como IPv6.

La configuración incluída en el ejemplo, describe el caso de 6PE utilizando BGP con route reflectors ya que será la situación mas común para los proveedores que desplegaron MPLS.

Configuraciones 6PE para Cisco IOS

```
mpls ipv6 source-interface Loopback0

router bgp NumeroASN
 address-family ipv6
 redistribute connected route-map accion-conectadas
 redistribute static route-map accion-estaticas
 neighbor direccion-IP-RR activate
 neighbor direccion-IP-RR send-community
 neighbor direccion-IP-RR send-label
 neighbor direccion-IP-RR peer-group nombre-grupo

exit-address-family
```

Configuraciones 6PE en Juniper

```
protocols {
   bgp {
      group Nombre {
         family inet6 {
            labeled-unicast {
               explicit-null;
            }
         }
      }
   }
}
```

5.4.4. Utilización de túneles

La utilización de túneles en el backbone es la solución menos eficiente y permite una solución en el corto plazo que no escala. Ofrecer servicios IPv6 con túneles dentro de la red del proveedor hace complejos los diagnósticos, afecta la disponibilidad de los servicios IPv6 y dificulta la adecuada utilización de los recursos (enlaces y routers). Los túneles en estos casos son configurados manualmente. Esta solución debe ser considerada como transitoria y no la implementación definitiva en la red.

En caso que en alguna porción de la red no pueda implementarse IPv6, la configuración de un túnel permitirá ocultar o crear un puente entre ambos extremos IPv6 sin modificar los equipos intermedios. El resultado será una topología diferente de red para el tráfico IPv4 e IPv6. En el siguiente diagrama, vemos como la topología de red anterior es modificada por los túneles. Si bien el tráfico IPv4 puede tener dos caminos disponibles para llegar de un extremo a otro, la configuración del túnel para el tráfico IPv6 tiene el efecto de unirlos utilizando un único camino, el túnel, que require que los routers en ambos extremos estén disponibles para que el tráfico pueda atravesarlo.

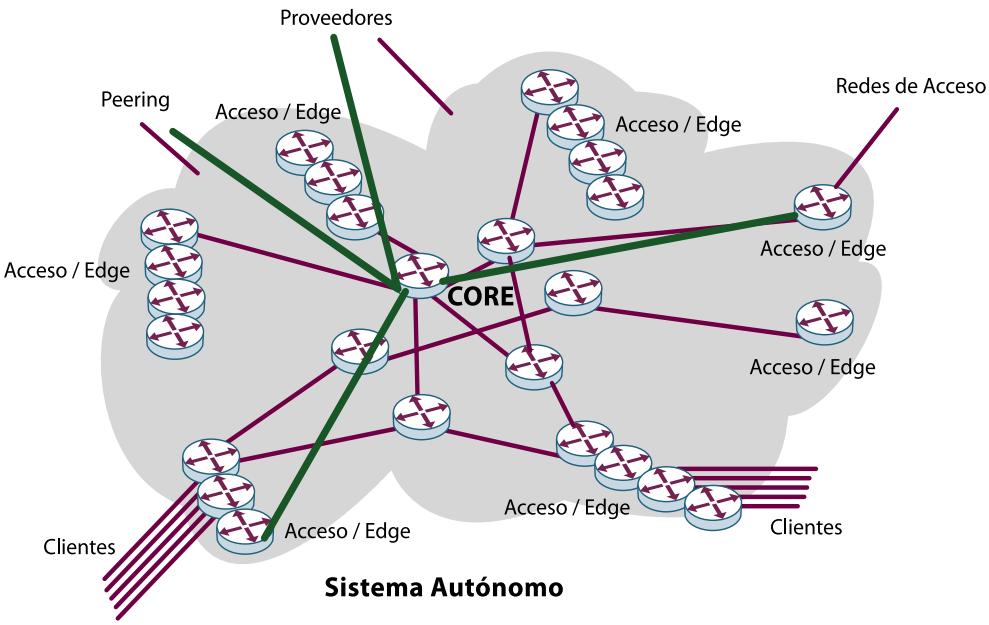


FIGURA 2: **EJEMPLO DE UTILIZACIÓN DE TÚNELES**

Una consideración importante al momento de implementar túneles (no solo para transportar tráfico IPv6 sino con cualquier tipo de túneles) es el del MTU máximo soportado entre los extremos y el configurado en la interfaz túnel. Una vez configurado cada túnel, es conveniente verificar con diferentes tamaños de paquete el correcto routing del tráfico. En el RFC4213 sección 3.2 podremos encontrar una explicación detallada de este problema y las recomendaciones.

5.4.5. Opciones de Túneles

La utilización de túneles manuales descrita en el RFC4213 sección 3 es denominada "configured tunneling" para diferenciarla de otras técnicas de túneles automáticos. En ese mismo RFC se describen mecanismos automáticos que se usan como transición pero que no son útiles para estos casos. En el backbone de un proveedor, utilizamos túneles para encapsular cualquier paquete IPv6 entre dos extremos que solo pueden verse a nivel IPv4. Una vez que el paquete llega al extremo final del túnel usando IPv4, ese router recupera el paquete IPv6 que estaba encapsulado y continua con el encaminamiento (routing) IPv6 normal.

El mecanismo mas simple y comúnmente utilizado por los proveedores de servicio es el de túneles GRE (RFC2893). Estos túneles han sido usados desde hace muchos años para encapsular diferentes protocolos y tienen una probada interoperabilidad. Otra posibilidad es utilizar túneles L2TPv3 (RFC3931).

5.4.6. Conexiones de clientes utilizando túneles

Será muy común durante los próximos años que los clientes prefieran comenzar con pruebas de servicios IPv6 antes de habilitar el doble pila en el servicio de Internet que le contratan al proveedor. También puede ocurrir que sus clientes necesiten llegar con IPv6 a un router diferente del que tienen actualmente conectado para el servicio de Internet. En esos casos es conveniente tener disponible como parte de los servicios del proveedor, la terminación de túneles GRE encapsulando IPv6. De esta manera el cliente podrá hacer un despliegue inicial utilizando solo «el» o «los» routers que desea involucrar al comienzo.

En todos los casos la configuración de los túneles será similar. Se incluyen a continuación unos ejemplos como referencia.

Configuración para Cisco IOS

```
interface TunnelEjemploR1
 no ip address
 ipv6 address 2001:DB8:FFFF::17/64
 tunnel Interface-Origen
 tunnel destination Direccion-IPv4-Destino
 tunnel mode ipv6ip
```

Configuración para Juniper

```
interfaces {
   Interface-origen {
      unit UNIT {
         tunnel {
            source Direccion-IPv4-Origen ;
            destination Direccion-IPv4-Destino ;
```

```
            }
            family inet6 {
               address 2001:DB8::17/64 ;
            }
         }
      }
   }
```

6. Conclusiones

Habilitar IPv6 en el backbone del proveedor no es una tarea compleja y muy probablemente no sea necesario hacer inversión alguna en equipos. Es un trabajo que requiere planificación y mucho cuidado al momento de hacer los cambios en la red por el impacto que tienen las configuraciones de routing en los equipos de Core. Por suerte todavía hay tiempo para hacer un despliegue ordenado y sin apresuramientos.

En este capítulo solo se describió como habilitar el routing IPv6. Ofrecer servicios IPv6 puede ser una tarea mas compleja para los proveedores ya que impacta en muchas áreas no cubiertas en este libro como monitoreo de red, sistemas de provisionamiento de servicios, herramientas de gestión, etc. Con respecto a los servidores y servicios, se puede consultar el capítulo correspondiente y suele ser la siguiente etapa para un proveedor de Internet.

8. Epílogo

Visión global del despliegue de IPv6 en el mundo

A lo largo de los capítulos anteriores, hemos aprendido cual es la situación actual de las direcciones IPv4, que es IPv6, porqué IPv6 es necesario, así como que pasos se han dado en Latinoamérica y Caribe, donde se ha originado esta publicación.

Igualmente hemos explicado diferentes aspectos técnicos relacionados con el despliegue de IPv6 en diferentes sistemas operativos y entornos de redes, desde usuarios residenciales hasta redes de proveedores de servicios de Internet.

Pero, ***¿cuál es la situación actual de despliegue de IPv6 en el mundo?***

De una forma muy genérica, se podría decir que el despliegue de IPv6 en el mundo, esta teniendo lugar, aunque a pasos desiguales, sin cambios drásticos. Pero debemos concretar, dependiendo del punto de vista de la red desde el que se observe dicho despliegue.

Así, desde el punto de vista de las redes académicas, en Japón, Europa y Norteamérica se ha producido un despliegue muy importante, en gran medida debido a las grandes inversiones públicas para fomentar el mismo. Además, y especialmente en el caso Europeo, la Comisión Europea ha co-financiado, junto con el sector privado, gran número de proyectos de Investigación y Desarrollo, que a su vez han posibilitado a la industria y otros actores, la adquisición de los conocimientos y sin duda la culminación del desarrollo y la estandarización de IPv6, para alcanzar un grado de madurez que permita dicho despliegue.

Como resultado directo, muchos países y regiones han adoptado políticas públicas, tendentes a recalcar que el despliegue de IPv6 no es caro si se planifica adecuadamente, es decir, con cierta anticipación, la cual depende del caso específico de cada red, y por tanto asegurándose que las adquisiciones de equipamiento, aplicaciones y servicios, tengan soporte de IPv6, de tal modo que no sea necesario realizar nuevas adquisiciones cuando se desee "activar" IPv6.

De hecho, como consecuencia de este tipo de políticas públicas, en varios países y regiones, de todo el mundo, hay fechas concretas para la obligatoriedad de la activación de IPv6 en las redes de la administración pública y otras redes relacionadas (educación, defensa, etc.).

Desde el punto de vista de las grandes redes, las que podríamos denominar de grandes operadores ("carriers"), y fundamentalmente en aquellos casos de operadores inter-

nacionales, que en su mayoría tiene redes intercontinentales, hace ya varios años que en un alto porcentaje, han dado grandes pasos y en muchos casos, tienen un soporte muy completo de IPv6.

Sin embargo, la situación es muy diferente en la última milla, e incluso en muchas de las redes de los proveedores de servicios de Internet nacionales/regionales. En estos casos, salvo excepciones notables sobre todo en Japón, algunas en otros países asiáticos, y un reducido número de casos en Europa y Norteamérica.

¿Y desde el punto de vista de los sistemas operativos, aplicaciones y servicios?

En realidad, como se ha podido descubrir en los capítulos anteriores, los sistemas operativos de computadores, teléfonos celulares y otros muchos dispositivos, comenzaron a tener soporte de IPv6 desde el año 2001, y hoy en día es relativamente difícil encontrar una plataforma que adolezca del mismo. Es más, por la forma en la que IPv6 ha sido diseñado, y la visión técnica de un despliegue en paralelo con IPv4, lo que denominamos co-existencia, los llamados mecanismos de transición, que también hemos descrito anteriormente, permiten incluso de forma automática, que dichos dispositivos puedan utilizar IPv6, extremo a extremo, aun cuando los proveedores de servicios de Internet no lo faciliten.

Lógicamente, el uso de estos mecanismos de transición automáticos, no es una forma óptima, y la situación ideal es precisamente que los proveedores de servicios de Internet, despliegen IPv6 en la última milla, que precisamente, como acabamos de indicar, es el paso en el que en general, en todo el mundo, hay una carencia mas importante y por tanto donde es necesario incidir con mas fuerza.

Desde el punto de vista de las aplicaciones, dado que los sistemas operativos tienen en general un soporte adecuado de IPv6, es cada vez mas frecuente que éstas, las aplicaciones, sean agnósticas y funcionen indistintamente con IPv4 e IPv6.

Respecto de los servicios, por ejemplo servidores web, en general la adopción de IPv6 esta siendo lenta, dado que los centros de datos ("data centers") y los propios proveedores de servicios de Internet, no han visto aún la necesidad de dicho despliegue, por ejemplo, incentivos económicos inmediatos. Obviamente, siempre hay excepciones, y podemos mencionar el caso concreto de Google, que ya está dando grandes pasos desde hace apenas un par de años, lo que sin duda, empujará a otros competidores para que tomen decisiones similares.

Por último, desde el punto de vista del tráfico, cabe destacar una situación muy diferente a lo que se puede esperar del bajo nivel de despliegue en la última milla. Debido a la activación de IPv6 en casi todas las plataformas de usuario (y como hemos visto, con gran número de sistemas operativos que incluso lo habilitan por defecto), y gracias a los mecanismos de transición automáticos, y a algunas aplicaciones, fundamentalmente cliente-a-cliente (peer-to-peer), el tráfico IPv6 a través de dichos mecanismos de transición esta cre-

ciendo desde hace mas de dos años de una forma muy significativa. Podemos mencionar, destacados ejemplos como BitTorrent, aplicaciones de mensajería, e incluso aplicaciones de redes privadas virtuales automáticas.

Este último aspecto, el incremento del trafico de forma automática, sin duda alguna, constituirá un importante aliciente y motivación económica, especialmente en aquellas regiones del mundo donde el ancho de banda es más caro, para que los proveedores de servicios de Internet, apuesten por desplegar IPv6 en la última milla lo antes posible, o bien utilizar mecanismos de transición ubicados en sus propias redes (como pueden ser relés 6to4 y Teredo), como medida provisional, hasta que puedan realizar un despliegue de doble pila completo. Ello les permitirá tener ahorros de dichos anchos de banda e indirectamente mejorar la calidad de servicio a los usuarios.

Las direcciones IPv4 que utilizan los dispositivos para conectarse a Internet se están agotando.

El éxito de Internet y el surgimiento de más y nuevos servicios, así como los constantes desarrollos tecnológicos han traído como resultado la necesidad de desarrollar una nueva versión del protocolo IP (IPv6) que permita utilizar tanta cantidad de direcciones IP como sean necesarias (340 sextillones de direcciones).

Sin embargo, la implementación de este nuevo protocolo y su adopción definitiva es un proceso lento, pero constante.

Organizaciones internacionales como la Internet Society, LACNIC, el Proyecto 6DEPLOY -que cuenta con la co-financiación de la Comisión Europea- han venido trabajando y trabajan comprometidamente en las diferentes regiones a través de tutoriales, conferencias, capacitaciones, talleres, etc.

"**IPv6 para Todos**" –un proyecto liderado por el Capítulo Argentina de ISOC- es un libro pensado para brindar las herramientas necesarias que permitan a los usuarios, a través de un leguaje claro, sencillo y exento de tecnicismos, comprender, desplegar e implementar IPv6 en los distintos entornos.

Dra. Mónica Abalo Laforgia
Presidenta
Capítulo Argentina de Internet Society – ISOC-Ar

Con la colaboración de:

Financiado por: