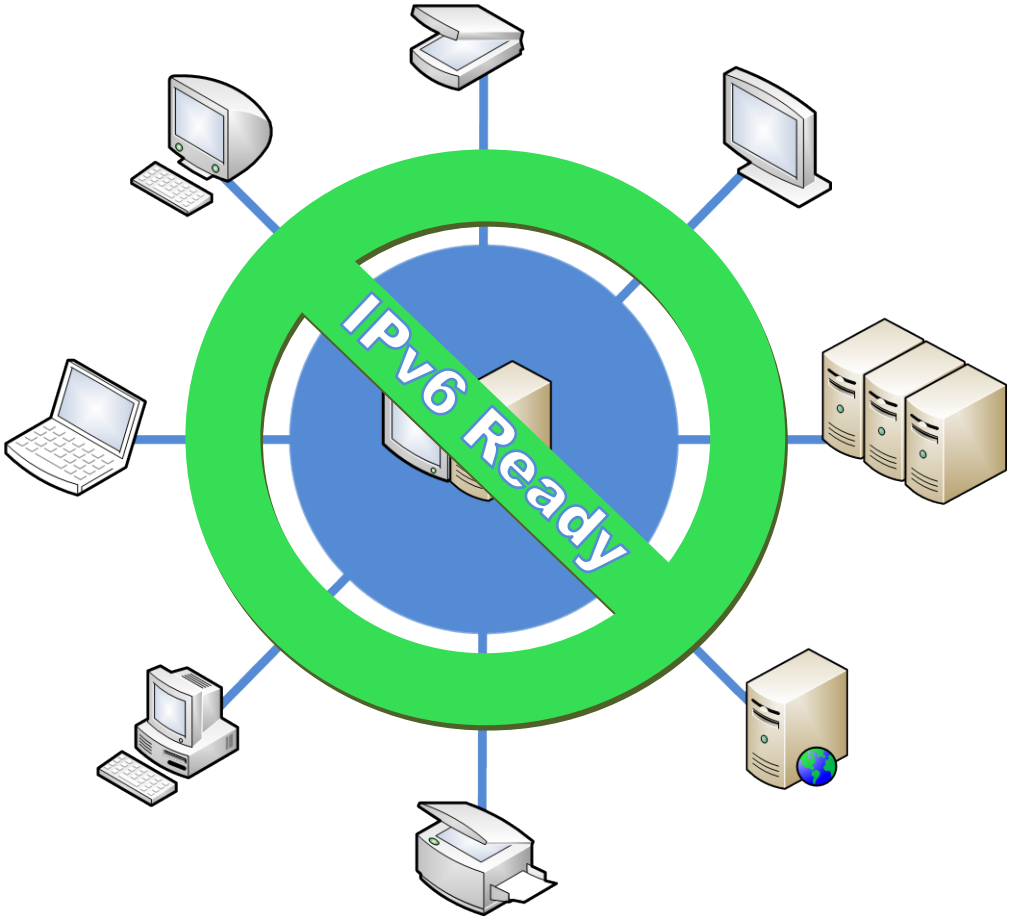


Supuesto practico de análisis para la transición de IPv4 a IPv6 en un entorno de redes empresariales WAN/LAN

Autor: Enrique Arias Martínez

Consultor: Miquel Font Rosselló

E.T.T. Telemática

10/01/2013

Dedicatoria y agradecimientos

Quiero dedicar este trabajo de fin de carrera a las personas que duran estos años, me han apoyado y ayudado en la ardua tarea de lograr llevar a cabo de mi deseo de realizar la carrera de Ingeniero técnico de Telecomunicaciones y cuyo resultado al fin, se plasma en este trabajo de fin de carrera..

En primer lugar se lo dedico a mi pareja Anabel, que me ha ayudado estos años a tener el máximo tiempo disponible para que pudiera dedicarme a mis estudios y que ha aguantado la soledad de mi compañía. A mi madre Gloria por enseñarme lo mejor de la vida, la fuerza de la convicción en mí mismo y a mis hermanas Yolanda y Rebeca por sus ánimos y apoyo.

También quiero agradarle muy sinceramente, toda la orientación y consejo recibido de Javier Fernández Álvarez, que desde las adversidades de la vida, me ha sabido transmitir lo mejor que una persona puede transmitir a otra, confianza y optimismo.

Agradecerles también a mis amigos May, Franfi, Magda, Juan Carlos, Miguel Serrano y Azucena Martin, todo el ánimo recibido.

INDICE DE CONTENIDOS

INDICE DE FIGURAS

INTRODUCCIÓN

Cuando surgió el protocolo IP[1], se pensó que el direccionamiento disponible era suficiente para todas las computadoras existentes y las que habría en cientos de años, pero esos cálculos no podían estar más lejos de la realidad. En vista que el planteamiento de direcciones IP inicial se agotarían sobre 1987, apenas la 10 años desde el comienzo de su implementación, IETF empezó a desarrollar mecanismos que permitieran disponer de más direcciones IP sin tener que reestructurar todas las redes existente que ya alcanzaba el millón en todo el mundo. Así aparecieron VLSM, CIDR, NAT y las direcciones privadas, que lo único que hicieron fue prolongar unos años más, apenas 20, las direcciones IP disponibles en Internet[2]. La explosión de Internet y el crecimiento de los países emergentes son algunas de las causas de este agotamiento. Pero a principio de la década de los noventa, viendo con las limitaciones que nació IP en su versión 4, los ingenieros empezaron a trabajar en una evolución de este protocolo. Esto promovió un grupo de trabajo que empezó a definir IP versión 6 o como se le nombra habitualmente IPv6.

IPv6 ha nacido y ahora solo hace falta llevarlo al mundo real. Desde el año 2002, que se habilitaron las primeras pilas de protocolo IPv6 en servidores y equipamiento de comunicaciones, su despliegue ha sido lento, solo ha habido unos pocos países que realmente han tomado conciencia de este problema, como Japón donde ya se dispone de servicios y redes puramente en IPv6.

Se tiene previsto que el despliegue de IPv6 dure más de 20 años, dado a que deberá coexistir como miles de millones de sistemas en IPv4 y no existe la premura de una fecha como la vivida con el famoso efecto 2000. Pero la realidad es que la implicación de IETF, gobiernos y empresas para que el despliegue de IPv6, se vaya acelerando, sea dado por el hecho de que este proceso a priori solo ofrece ventajas y ningún inconveniente.

Como dijo Albert Einstein, *no pienso nunca en el futuro porque llega muy pronto*, y el futuro en Internet es IPv6 y ya está aquí, por lo cual, empresas, gobiernos, organismos, universidades e Ingenieros debemos prepararnos para este salto tecnológico. Con este proyecto quiero mostrar el trabajo que deberemos realizar los Ingenieros de Telecomunicaciones en el ámbito de análisis, evaluación e implementación de redes IPv6.

[1] http://tools.ietf.org/html/rfc791
[2] https://www.ripe.net/internet-coordination/ipv4-exhaustion/faq

RESUMEN

JUSTIFICACIÓN DEL TFC

IPv6 está entre nosotros, puede ser que no lo veamos, pero está ahí, en servidores DNS y Web IPv6, en las redes de nuestros operadores de telecomunicaciones, dentro de nuestros ordenadores. Esto me lleva a plantear como nos debemos preparar los Ingenieros de Telecomunicaciones ante este nuevo reto. En este TFC abordaremos una problemática que se empezara a dar en nuestros trabajos cotidianos, la migración de entornos empresariales basados en IPv4 a las nuevas redes basadas en IPv6.

Debemos estar preparados para conocer este nuevo protocolo, dado que cambian radicalmente nuestra percepción de las redes de Internet. Dejaremos de hablar de difusión, ARP, etc., y empezaremos a usar nuevas terminologías como direcciones globales y locales, RA, ND, dejaremos de usar NAT, no habrá direcciones IP privadas al uso, etc., todo ello repartido en cientos de RFC que describen todo este nuevo mundo alrededor de IPv6.

ESCENARIO DEL TFC

El proyecto del TFC, se basa en el supuesto práctico de migración de unas infraestructuras de redes IPv4 de una empresa ficticia a IPv6. No solo será la migración, dado que en este supuesto realizaremos una labor profunda sobre los métodos de transición de IPv4 a IPv6 e intentaremos exponer en este supuesto los problemas que nos podríamos encontrar en el mundo real y como aplicar soluciones tecnológicas que sean viables y adecuadas en cada momento.

Antes de empezar definiremos el punto de partida del proyecto, dado que habrá que diseñar una red que se aproxime lo máximo a la realidad.

Partimos del supuesto que existe una empresa llamada *NetMania*, que se dedica al comercio de componentes informáticos, ordenadores y consumibles. Esta empresa comercializa sus productos tanto en tiendas como en venta on-line por Internet. Su sede central está en Madrid, donde se ubica sus departamentos de gestión y RRHH, gestión de ventas y un departamento de Informática, Sistemas y Telecomunicaciones que se encarga del CPD donde se aglutinan la granja de servidores y el núcleo de comunicaciones de la red de *NetMania*. Aparte, la empresa dispone de dos centros de distribución (CD) de productos para clientes de venta on-line y para su red de tiendas de venta presencial que se encuentran ubicadas en Madrid, Barcelona, Sevilla, Valencia y Bilbao.

Por su comienzo modesto, *NetMania* nunca ha realizado un *hosting* de sus servicios de Internet, debido al costes que suponía estos servicios años atrás, sino que han ido creciendo poco a poco según crecía la compañía, con lo cual ahora dispone de un departamento propio para la gestión de todos sus servicios TIC.

Debido a este crecimiento, el departamento de Informática, Sistemas y Telecomunicaciones, ha plantado a la dirección de la empresa, ampliar los servicios que ofrecen por Internet y crear una plataforma independiente de comercio electrónico.

Esto obligara a solicitar a TeleNet, el ISP que provee el acceso de Internet a la empresa, un nuevo rango de direcciones IP públicas, pero nos encontraremos la problemática del agotamiento de direcciones IPv4.

Aparte de este problema, hay que tener en cuenta que en un futuro no muy lejano, cada vez habrá más redes de IPv6 y se cuando estas redes se desconecten de redes antiguas de IPv4 , se podrán dar casos de pérdidas de servicios con la consiguiente perdidas de clientes.

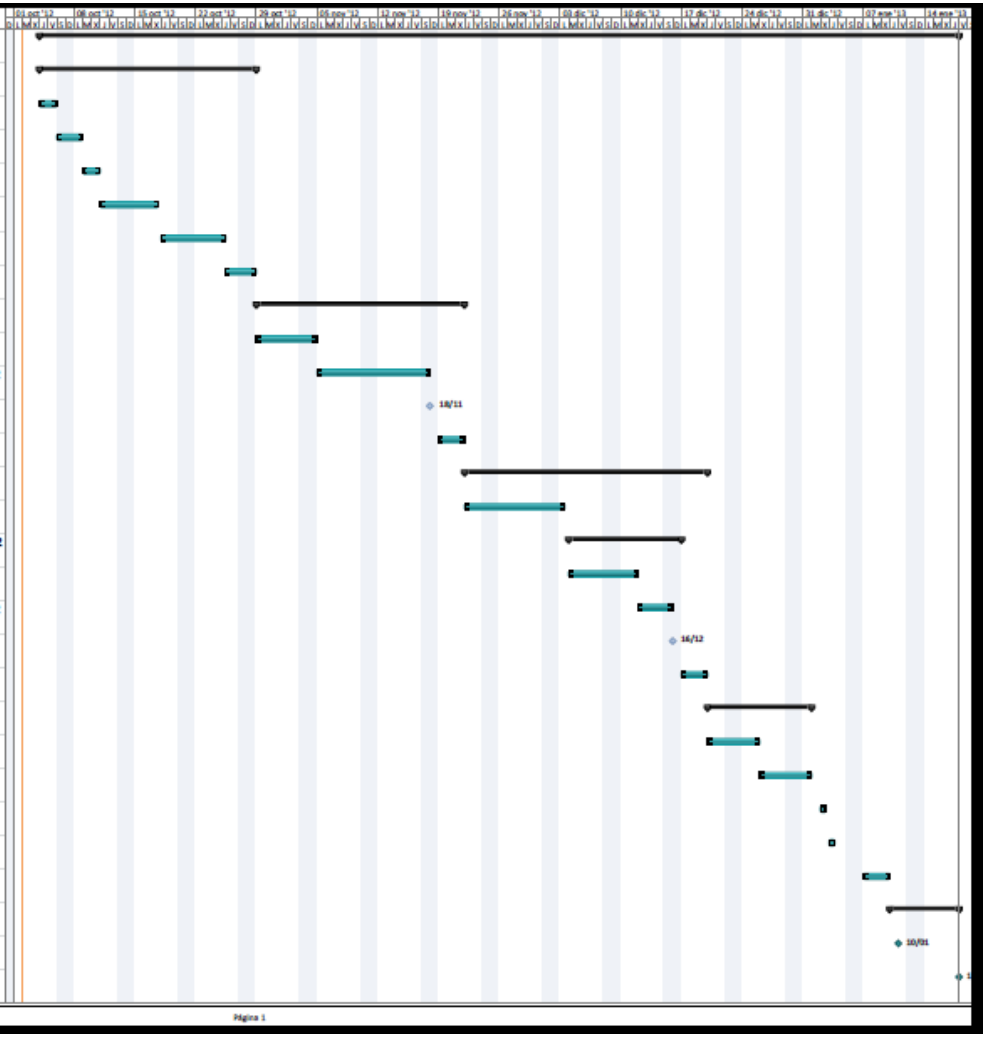
OBJETIVOS DEL TFC

Los objetivos que nos planteamos en la realización de este TFC son:

- Analizar las ventajas de IPv6 frente IPv4 frente al despliegue de nuevos servicios por Internet.
- Adquirir competencia en el conocimiento de redes en IPv6 y servicios asociados a esto, tales como DNS y DHCP6.
- Conocer y aplicar todos los métodos de transición de IPv4 a IPv6.
- Evaluar el impacto económico de dicha transición.
- Realizar un estudio de las buenas prácticas en la implementación de Ipv6.

PLANIFICACIÓN DEL TFC

	Nombre de tarea	Duración	Comienzo	Fin
1	**Trabajo de fin de Carrera**	**76 días?**	**jue 04/10/12**	**jue 17/01/13**
2	**Introducion**	**17 días**	**jue 04/10/12**	**lun 29/10/12**
3	Justificación del TFC	2 días	jue 04/10/12	vie 05/10/12
4	Punto de partida	3 días	sáb 06/10/12	mar 09/10/12
5	Estudio de necesidades de la compañía	2 días	lun 08/10/12	mié 10/10/12
6	Entorno actual de red IPv4	5 días	jue 11/10/12	mié 17/10/12
7	Analisis de la arquitectura de red	6 días	jue 18/10/12	jue 25/10/12
8	Evaluación de impacto economico	2,88 días	jue 25/10/12	lun 29/10/12
9	**Diseño de la migración a IPv6**	**17,88 días**	**lun 29/10/12**	**mié 21/11/12**
10	Direccionamiento	6,13 días	lun 29/10/12	lun 05/11/12
11	Metodos de transición	11 días	lun 05/11/12	dom 18/11/12
12	Primera entrega		dom 18/11/12	
13	Servicios de red	4 días	lun 19/11/12	mié 21/11/12
14	**Fase de implementación**	**19,88 días**	**jue 22/11/12**	**mié 19/12/12**
15	Electronica y servcios de red	8 días	jue 22/11/12	lun 03/12/12
16	**Servidores**	**9 días?**	**mar 04/12/12**	**dom 16/12/12**
17	Servidores basados Linux	7 días	mar 04/12/12	mar 11/12/12
18	Servidores basados en Windows	3,75 días	mié 12/12/12	dom 16/12/12
19	Segunda entrega		dom 16/12/12	
20	PC y Terminales	4 días	lun 17/12/12	mié 19/12/12
21	**Fase de operación**	**7,88 días**	**jue 20/12/12**	**lun 31/12/12**
22	Manual de buenas practicas	5 días	jue 20/12/12	mar 25/12/12
23	Analisis final del proyecto	3,88 días	mié 26/12/12	lun 31/12/12
24	Glosario	1 día	mié 02/01/13	mié 02/01/13
25	Bibliografía	1 día	jue 03/01/13	jue 03/01/13
26	Anexos	4 días	lun 07/01/13	mié 09/01/13
27	**Entrega de proyecto**	**6 días**	**jue 10/01/13**	**jue 17/01/13**
28	Entrega de memoria	1 día	jue 10/01/13	jue 10/01/13
29	Entrega de presentación	1 día	jue 17/01/13	jue 17/01/13



UNA VISIÓN DE IPV6

La nueva versión del protocolo IP, está pensada para nuestro mundo actual y el de mañana. Una de sus mayores premisas es romper la barrera de las limitaciones de direcciones IP que tenía en su versión 4 e ir mucho más allá.

En IPv6 tenemos 2^{128} direcciones IP o lo que es lo mismo, 340 sextillones de direcciones disponibles, aunque realmente las direcciones disponibles serán, 2^{64} direcciones para identificar las redes de 2^{64} nodos cada una, para toda una nueva generación de dispositivos IP conectados a Internet, como vehículos, sistemas domóticos, redes de sensores, etc.

Con esta ventaja, en IPv6 se han eliminado la necesidad de las direcciones privadas, aunque en principio se introdujeron de una manera un poco ambigua y se definieron como direcciones de sitio local (site local), pero estas fueren desechadas en el RFC 3879.

DENTRO DE IPV6

En IPv6 cambia casi todo, hasta la notación de las direcciones. Antes con IPv4 era muy sencillo referirnos a la direcciones IP mediante una notación de 4 bloques de números decimales que indicaban 8 bits cada bloque, para especificar una dirección IP de 32 bits. Pero ahora surge el problema de tener que indicar direcciones de 128 bits, y si utilizásemos la notación de IPv4 para indicar una dirección IP tendríamos que hacerlo así, 192.201.56.102.216.5.158.130.221.76.25.185.236.125.54.67, que resultaría realmente muy complicado a la par de los posibles errores que se comentarían al tener una serie tan larga de número. Así que se ideo un nuevo método de notación, en el cual consistió en dividir el bloque de 128 bits de las direcciones IP en trozos de 16 bits, dando lugar a 8 bloques de 16 bits cada uno y en vez de utilizar la base decimal para indicar los dígitos de cada bloque sea optado por la base hexadecimal, con lo que una dirección IPv6 vendría a indicarse de la siguiente manera, 2001:0DB8:14A0:AF56:0024:0EF8:0000:56BB, siendo más pequeñas y por lo tanto más manejable.

También sean especificados métodos para que sea más fácil aun el manejo de unas direcciones IP tan grande. Uno de ellos consiste en la eliminación de los ceros a la izquierda, esto hace que un bloque que contenga por ejemplo 0A65 , se pueda escribir como A65. Además, en el caso de que dicho bloque sea 0000, este se escribirá como 0. Así si nos fijamos en el ejemplo anterior , podríamos escribir la dirección de la siguiente manera, 2001:DB8:14A0:AF56:24:0EF8:0:56BB. También hay un caso muy singular que hay que tener la cuenta, que es en caso de una secuencia contigua de ceros, en este caso, se puede sustituir esta secuencia de ceros, por una pareja de dos puntos "::", que viene a indicar un bloque de ceros consecutivos en la dirección IP. Así la dirección FFE0:000:0000:0000:0000:0000:0000:0001, se puede indicar como FFE0::1. Hay que tener en cuenta que esto solo se puede aplicar una única vez, esto es, si una dirección IP dispone de dos bloques de ceros consecutivos no contiguo, solo se podrá aplicar esta regla a uno de estos bloques, que por lógica será el que contenga más ceros, de esta manera la dirección IP

2001:0DB8:0000:0000:0000:1A76:000:0001, se representara de la siguiente manera, 2001:DB8::1A76:0:1 siendo más sencilla su comprensión.[3]

LA NUEVA CABECERA IPV6

En la nueva cabecera de IPv6, hay variaciones sustanciales en cuanto al formato y contenido con respecto a la cabecera de IPv4. Se pasa de una cabecera de 20 octetos en 14 campos (2 de ellos opcionales, los campos de opciones y relleno) a una cabecera de 40 octetos en 8 campos de longitud fija.

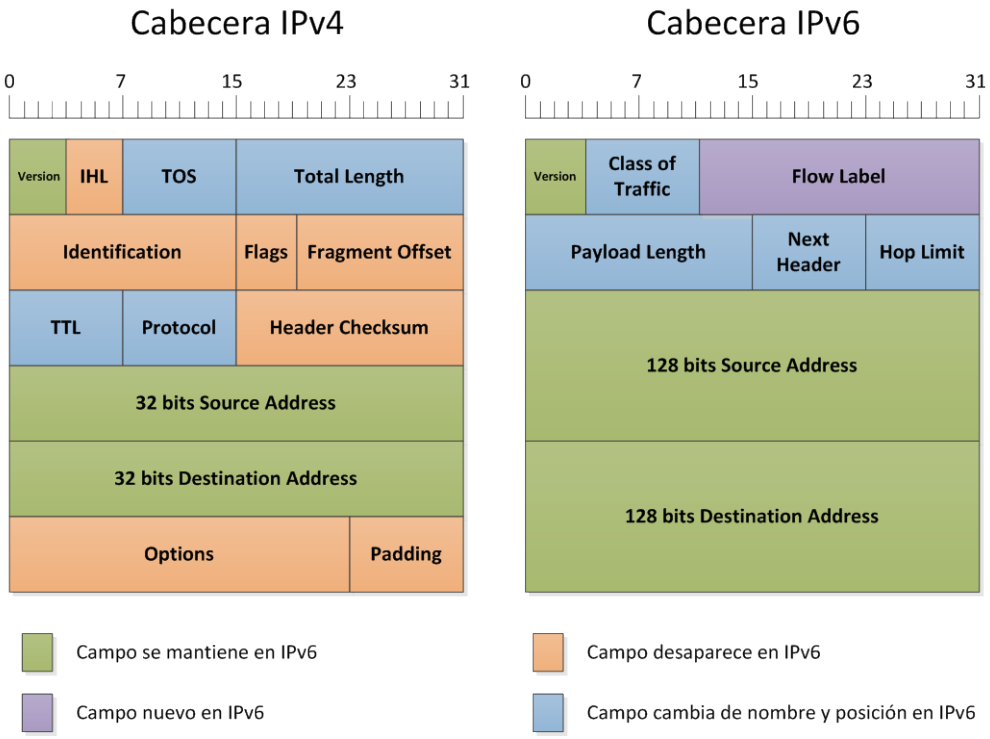


Figura 1 Diferencias entre cabeceras IP

Ciertos campos sean mantenido con función similares, como el campo *TOS* que ha pasado a llamarse *Class of Service* , *TTL* pasa a ser *Hop Limit* pero su uso es similar, mientras que otros han desaparecido en IPv6 debido a que estas funcionalidades no se implementan en IPv6 como la fragmentación de la cabecera IP o *Header Checksum* que era un campo redundante (la comprobación de la integridad del datagrama ya lo hace el protocolo superior).

La característica más novedosa de la cabecera de IPv6 es la llamada *Next Header* (Extensión de cabecera), que es una capacidad expansiva de la cabecera y sirve para incluir ciertas funcionalidades nuevas y otras que antes teníamos embebidas dentro de la cabecera de IPv4, ocupando un espacio y tiempo de proceso por solo tenerla en la cabecera. Lo que sea realizado en IPv6 es crear unas extensiones, de tal manera que estas se incluirán solo y cuando sean necesarias. Así el campo de *Next Header* normalmente realizará la misma función del campo *Protocol* de la cabecera de IPv4,

[3] RFC 4291, 2.3 Text Representation of Address Prefixes

esto es, informa del protocolo superior del datagrama. Pero en IPv6. si en lugar de tipo de protocolo, que sería la siguiente cabecera en el datagrama, indicamos otra valor, como por ejemplo *Routing Header* (0x43), esto hará que se incluya la final de los 40 octetos de la cabecera IP (dado que esta tiene una longitud fija) una extensión de datos, donde se incluirá la información concreta del tipo de cabecera. Esto permite realizar un encadenamientos de cabeceras de extensión para poder enviar más información de una solo vez. Aquí ponemos un ejemplo de cómo podemos enviar varias cabeceras de extensión encadenadas dentro de una cabecera IPv6.

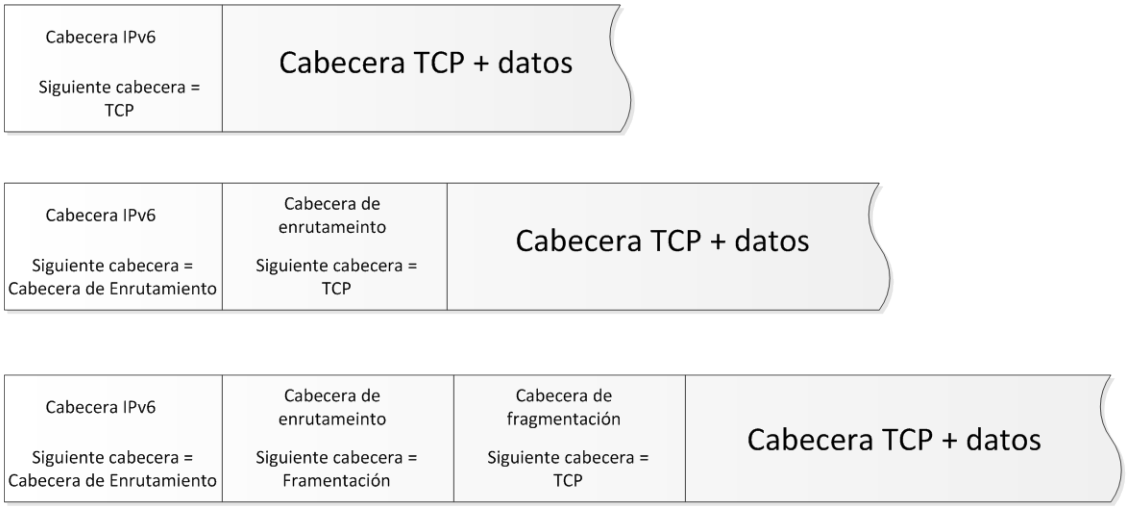


Figura 2 Cabeceras de extensión

Estas cabeceras de extensión solo son procesadas por los nodos destinos excepto *Hop-by-Hop Options Header.*

PREFIJO DE RED (AGRUPAMIENTO DE DIRECCIONES)

En IPv4 se implemento VLSM como medida para ampliar el número de direcciones disponibles . Ahora esto ya no es necesario en IPv6, pero otras de las medidas de IPv4 para la conservación de direcciones que fue CIDR ha sido tomado por IPv6 como modo de diferenciar entre las direcciones de red y la dirección del nodo en la red. CIDR proveía en IPv4, una maneja muy sencilla de reducir el tamaño de las tablas de enrutamiento de los encaminadores. Esta característica ha hecho que en IPv6 se adopte la notación CIDR para indicar la parte de red de una dirección IPv6. Esto hace que las direcciones IPv6 se dividan en prefijo de red y dirección de host o Identificador de interface. La sintaxis es ***dirección_ipv6/longuitud_prefijo***, donde ***dirección_ipv6*** son los 128 bits de la dirección IPv6 y ***longuitud_prefijo*** es un valor en decimal que indica cuantos bits continuos forman la dirección de red. De esta manera, la dirección IPv6 **2001:DB8:14A0:0:5AA5::56BB/64** indica:

- 2001:DB8:14A0:: es la dirección de red, indicado por el prefijo 64.
- 5AA5::56BB es ID del interface o identificador local del nodo, indicado por los restantes bits del prefijo.

Sea establece como una buena práctica en el despliegue de IPv6, que el prefijo /64 siempre indique el *ID Interface*.[4]

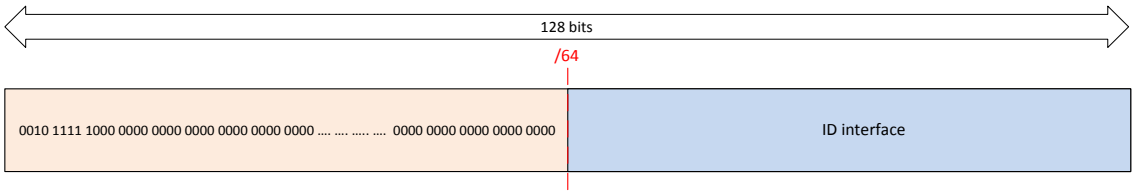


Figura 3 Dirección y prefijo en IPv6

Pero el prefijo de red, a su vez se ha dividido para tener una organización más detallada y exhaustiva del direccionamiento asignado. El RFC 3578, divide el prefijo de red en dos bloques, uno que indica la topología pública o *global routing prefix* formado por los primeros 48 bits y otro bloque asignado a la topología del sitio o *subnet ID* que está formado por los 16 bits restante. El bloque de la topología publica sirve para la organización jerárquica del direccionamiento en Internet. IANA se encarga de la asignación *global routing prefix*, en este caso define solo los 3 primeros bits del prefijo, el resto de bits están delegados en los RIR que asignan hasta los 23 bits (/23) del prefijo de red siguientes. A su vez, cada LIR o ISP reciben por defecto hasta los 32 bits (/32) y los sitios o clientes finales recibirán hasta los 48 bits (/48). Esto significa que un usuario final recibe 65.536 redes de 2^{64} direcciones cada una. Esto hace que muchos operados de telecomunicaciones, estén valorando en dar un prefijo más cortos a sus usuarios finales domésticos, con la premisa de que ningún usuario normal necesitara tantas redes ni tantas direcciones en su domicilio particular.

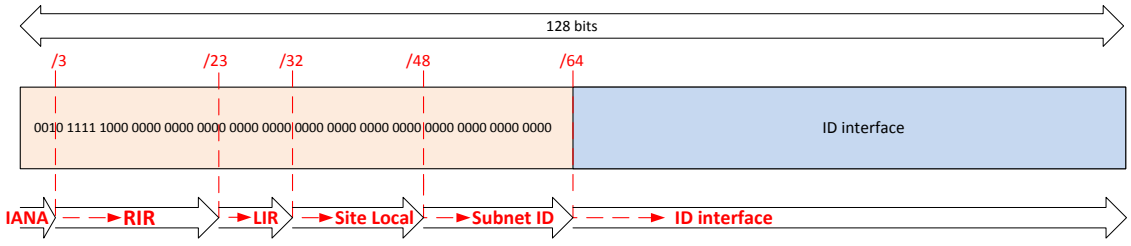


Figura 4 División del *global routing prefix*

De esta manera, la dirección IPv6 **2001:DB8:14A0:A8:5AA5::56BB** indica:

- 2001:DB8:14A0:: es la dirección de red del sitio local, indicado por el prefijo 48.
- A8 sería el número de la subred del sitio local, indicado por los 16 bits siguientes.
- 5AA5::56BB es ID del interface o identificador local del nodo, indicado por los restantes 64 bits.

Para ciertas direcciones especiales utilizaremos otros criterios que explicaremos más adelante.

[4] RFC 3177, IAB/IESG Recommendations on IPv6 Address Alocations to Sites

TIPOS DE DIRECCIONES EN IPV6

IPv6 también cambia nuestra concepción de los diferentes tipos de direcciones IP que conocíamos en IPv4, así las direcciones de difusión o *broadcast* desaparecen y aparecen un nuevo tipo de dirección llamadas *anycast*[5], que indican el host más cercano dentro de un grupo de host. Se siguen manteniendo las direcciones del tipo *unicast* y potenciando el uso de las direcciones de tipo *multicast* para múltiples servicios como por ejemplo, el descubrimiento de vecinos (ND, *Neigborth Discovery*).

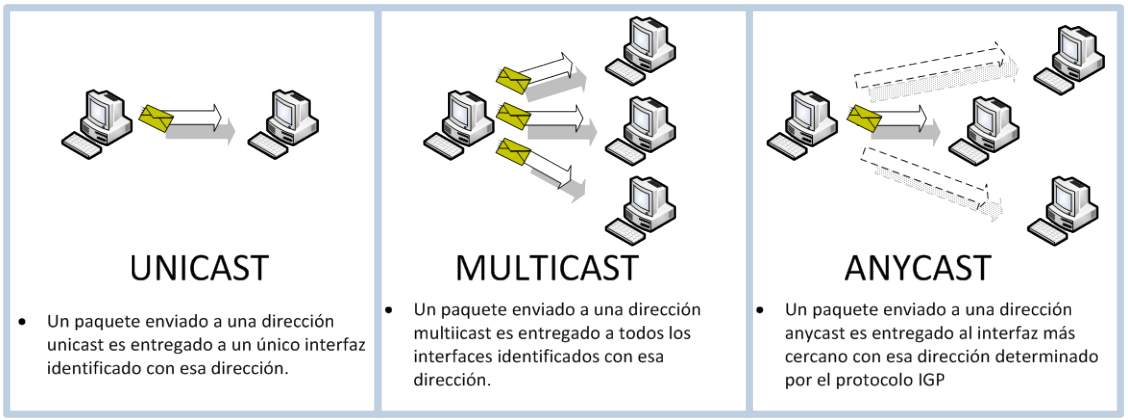


Figura 5 Tipo de direcciones

DIRECCIONES *UNICAST*

Dentro de las direcciones *unicast* en IPv6, podemos diferenciarlas por el tipo de uso que hacemos de ellas, así tenemos:

- Globales: Son las direcciones que proceden del prefijo (2000::/16) asignado por la IANA para el grupo de direcciones publicas globales. Son las direcciones que serán visibles en Internet.

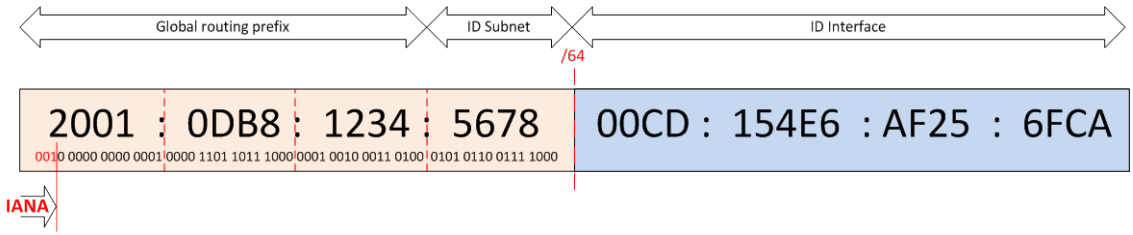


Figura 6 Tipo de dirección global

[5] RFC 4786, Operation of Anycast Services

- Enlace local (*Local link*): Estas direcciones se configuran automáticamente y se usan para descubrir vecinos (en el mismo enlace), descubrimiento de rutas y por distintos protocolos de enrutamiento. El prefijo asignado para este tipo de direcciones es FE80::/10 más el identificador del interface. Su alcance solo llega al segmento local de red.

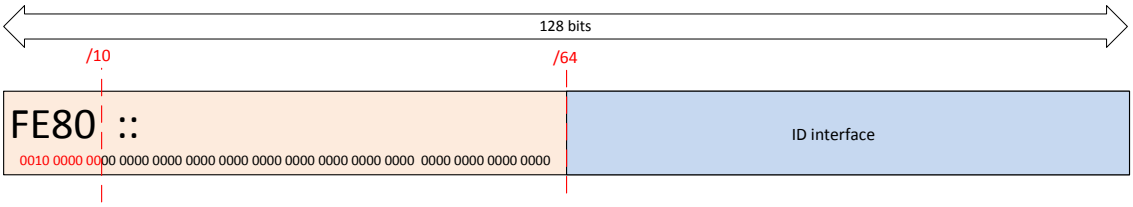


Figura 7 Tipo de dirección de enlace local (Link-Local)

- Mapeado a IPv4(*IPv4-mapped*): Con esta dirección se puede representa una dirección de IPv4 en IPv6. Consiste en 80 bits a 0 y 16 bits a 1, para indicar después los 32 bits de la dirección de IPv4

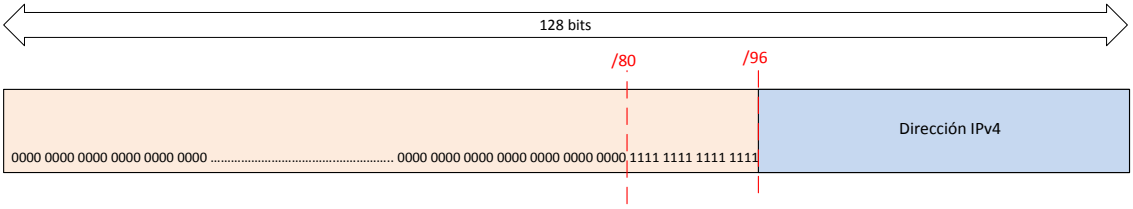


Figura 8 Tipo de dirección mapeada a IPv4

Un interface configurado con IPv6 puede tener múltiples direcciones IPv6, pero al menos deber tener una dirección de *local-link*.

Hay algunas direcciones IPv6 *unicast* especiales[6] que son:

Dirección IPv6	Descripción
::/0	Se utiliza para especificar una ruta estática por defecto, Es la equivalencia a 0.0.0.0/0 en IPv4
::/128	Dirección inespecífica, se utiliza para indicar que la ausencia de una dirección IPv6
::1/128	Dirección de loopback. Equivalente a la dirección 127.0.0.1 en IPv4
FC00::/7[7]	Dirección local única (ULA) . Cumple la misma función que las direcciones privadas en IPv4 y no son enrutables por Internet.
2001:0DB8::/32[8]	Dirección con propósito de documentación

[6] RFC 5156, Special-Use IPv6 Address
[7] RFC 4193, Unique Local IPv6 Unicast Address
[8] RFC 3849, IPv6 Address Prefix Reserved for Documentation

DIRECCIONES *MULTICAST*

Las direcciones *multicast* a diferencia de en IPv4, en IPv6 son la base de muchas funciones, como la de sustituir a la direcciones de difusión o servir para la autoconfiguración de direcciones.

La direcciones *multicast* tienen el siguiente formato:

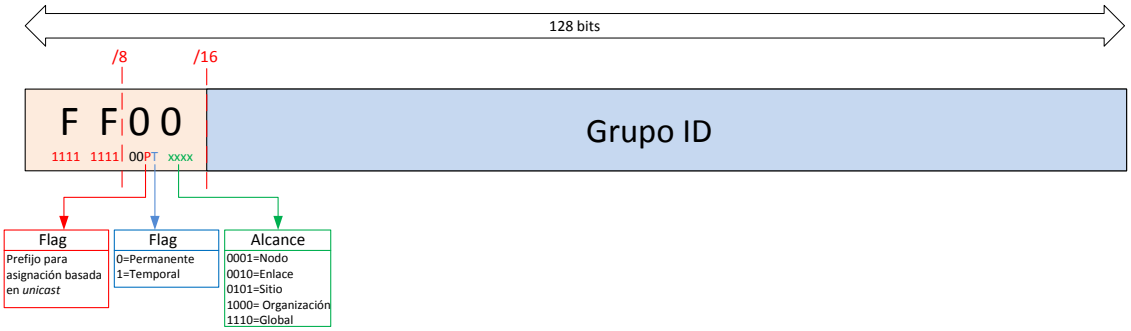


Figura 9 Tipo de dirección *multicast*

Los *flags* nos indica el prefijo, el tiempo de vida y el alcance de la dirección.

Hay algunas direcciones IPv6 *multicast*[9] reservadas son:

Dirección IPv6	Descripción
FF02::1	Indica todos los nodos de un enlace local
FF02::2	Indica todos los encaminadores de un enlace.
FF02::9	Indica a todos los encaminadores RIP de un enlace.
FF02::1:FFxx:xxxx	Indica a la dirección *multicast* de un nodo para la solicitud de autoconfiguración de host y descubrimiento de vecinos. El xx:xxxx son los 24 bits más a la derecha de la dirección *unicast* o *anycast* del nodo.
FF05::101	Indica todos los servidores NTP.

DIRECCIONES *ANYCAST*

Las direcciones *anycast* son igual que las direcciones *unicast* y pueden ser globales o especificas, y nos permiten indicar mediante un protocolo de IGP el destino de la dirección *anycast.* Así , por ejemplo si enviamos un paquete DNS a una dirección *anycast*, la red enviará este paquete al servidor DNS más cercano al origen de la petición, evitando trafico innecesario por otras redes. Existen direcciones especificas para poder indicar los servicios más cercanos, como puede ser, los servidores DNS, que se indicaran por las direcciones *anycast* FEC0:0:0:0:FFFF::1 , FEC0:0:0:0:FFFF::2, FEC0:0:0:0:FFFF::3.

Anycast ha supuesto una mejora en el rendimiento de las redes, al poder indicar los servicios más cercanos a un nodo de una manera muy sencilla y a la vez evitar de limitar los famosos ataques por DoS, ya que los ataques a las direcciones *anycast*, siempre serán las más cercanas al atacante , permitiendo operar sin problemas al

[9] RFC 3306, Unicast-Prefix-based IPv6 Multicast Address

resto de servicios *anycast*, ya que la decisión de donde llega cada dirección *anycast*, está en la red no en la dirección propiamente dicho.

ID INTERFACE

Hemos visto en los tipos de direcciones que el indicador de un nodo concreto en las redes IPv6 es el ID Interface. Este número, que normalmente será de de 64 bits, puede ser configurado manualmente, dándole un valor concreto como se hacía en IPv4, pero para facilitar la autoconfiguración de direcciones IPv6, sea definido una método de generar este identificador de tal manera que sea único en cada red, este método sea llamado EUI-64.

Todas las tarjetas de red del mercado disponen del un único identificar de acceso al medio o MAC de 48 bits o 6 octetos. Los 3 primeros octetos de una MAC son asignados por el IEEE a cada fabricante para evitar posibles duplicidades de direcciones MAC y el resto de bits, el fabricante asigna una única dirección a cada uno de los interfaces que fabrica.

Para generar una dirección EUI-64 para la autoconfiguración de la parte ID Interface de una dirección IPv6, según se especifica en el RFC 4291[10], se realiza los siguientes pasos:

1. Se divide la dirección MAC por la mitad , generando dos parte de 3 octetos cada una.
2. Se le añade en medio dos octetos consecutivos fijos que son, FF:FE.
3. Al primer octeto, se le cambia de valor del segundo bit de menor peso.
4. Se unen todos los octetos, generando una dirección de 64 bits.

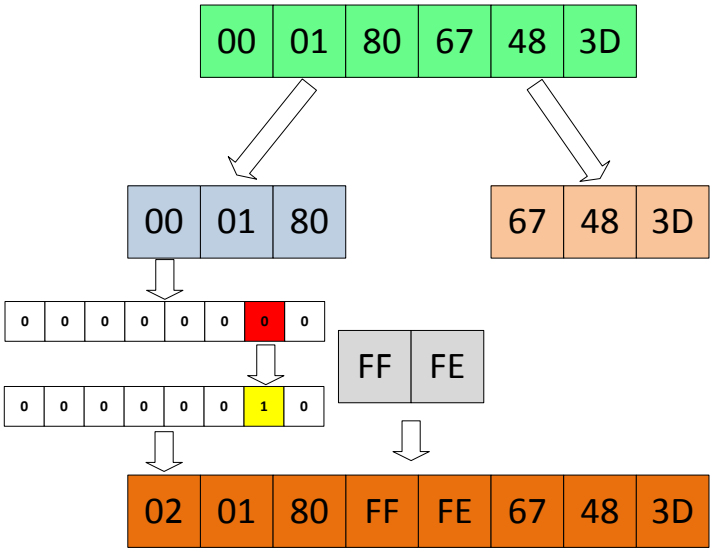


Figura 10 Generación de una dirección EUI64

De esta manera hemos generado los 64 bits necesarios para especificar un único nodo de red.

[10] https://tools.ietf.org/html/rfc4291#appendix-A

DESCUBRIMIENTO DE VECINOS

Como hemos comentado anteriormente, en IPv6 desaparece ARP, entonces, ¿cómo podemos comunicarnos con los nodos de nuestro segmento de red local, si no conocemos su direcciones MAC o de nivel de enlace?. Dado que ARP ocasionaba graves problemas de seguridad, como la posibilidad de realizar *ARP Spoofing*, a la hora de diseña IPv6 se prescindido de este método de resolución de direcciones de nivel de enlace y se opto por utilizar *multicast.*

Así, se diseño un método de resolución utilizando el protocolo ICMPv6 (ICMP para IPv6) y las direcciones *multicast.* A esto se le conoce como descubrimiento de vecinos (*Neighborn Discovery*). Sean definido 4 nuevos tipos de paquetes ICMPv6 para los procesos de descubrimiento de vecinos.

Mensaje ICMPv6	Tipo	Descripción
Solicitud de encaminador (Router Solicitation - RS)	133	Se envía cuando un nodo esta encendiendo y envía un mensaje RS para que los encaminadores que hay en el enlace local generen inmediatamente un mensaje RA.
Notificación de un encaminador (Router Advertisement - RA)	134	Los RA's contienen información del prefijo de red del enlace local, valor de MTU, un límite de saltos sugerido, etc. Los RA's se envían periódicamente o en respuesta a un mensaje RS
Solicitud de vecino (Neighbor solicitation - NS)	135	Un nodo envía un NS para determinar la dirección de enlace local de un vecino. Un NS se puede utilizar para la detección de dirección duplicadas (Duplicate Address Deteccion - DAD) También se usa NS para comprobar si un vecino está disponible.
Notificación de un vecino (Neighbor Advertisement - NA)	136	Un NA es una respuesta a un mensaje NS con los datos solicitados.

El funcionamiento es el siguiente: cuando un nodo desea establecer una comunicación con otro nodo, del cual solo conoce su dirección IPv6, necesita saber a qué dirección de enlace o nivel 2 debe enviar el paquete, al igual que en IPv4. Entonces el nodo envía un NS a la dirección *multicast* FF02::1:FFxx:xxxx . El paquete NS tendrá como dirección IPv6 la del nodo solicitante y la dirección IPv6 de destino será la dirección *multicast* FF02::1:FF+24 bits de menor peso del ID interface del nodo solicitado, la dirección de enlace local del nodo solicitante y la consulta de la dirección de enlace local del nodo solicitado. El nodo solicitado, responderá con un NA, que tendrá como dirección IPv6 origen la del nodo solicitado, la dirección IPv6 destino del nodo solicitante y la dirección de enlace local del nodo solicitado.

Los ICMPv6 RS y RA, sirven para obtener información de los vecinos y así poder usar la autoconfiguración que nos ofrece IPv6.

AUTOCONFIGURACIÓN IPV6

En IPv6 también cambian el modo de asignar dinámicamente direcciones IP. Antes, en IPv4, solo teníamos un método de poder asignar direcciones IP dinámicamente a requerimientos de los nodos mediante DHCP. En IPv6 sean ampliado los métodos de configuración dinámica o autoconfiguración de las direcciones IP.

El primer método que veremos será de autoconfiguración sin estado (*stateless*) o SLAAC[11].

Este método permite que un nodo pueda configurar el mismo su dirección IPv6 y demás parámetros de red necesarios como puerta de enlace, MTU, etc. utilizando el protocolo ICMPv6 y los encaminadores. El modo de funcionamiento es el siguiente:

- El interface de un nodo es inicializado al arrancar el sistema.
- Este interface genera una dirección de enlace local para sí mismo.
- El nodo envía un paquete ICMPv6 RS, para descubrir un encaminador.
- El encaminador responde con un paquete ICMPv6 RA, indicando el prefijo de red y su longitud, rutas, el tiempo de uso, MTU.
- El nodo con el prefijo de red recibido y utilizando el EUI-64, genera una dirección global para este interface.

El inconveniente de este método de autoconfiguración es que no provee de información adicional como los servidores DNS, nombre de dominio y opciones de vendedor, para lo cual nos tenemos que apoyar en un servidor DHCPv6. Para esto, el encaminador configura el bit O[12] a 1 en el mensaje RA que envía al nodo y hace que este requerirá información adicional al DCHPv6..

DHCP ha evolucionado y sea adaptado a IPv6 pasándose a llamar DHCPv6[13]. Este protocolo utiliza UDP en los puertos 546 para clientes y 547 para servidores, direcciones *multicast*, FF01::1:2 para indicar todos los agentes de reenvió y servidores DHCPv6 y FF05::1:3 para indicar todos los servidores DHCPv6 y las direcciones de enlace local para el intercambio de mensajes entre clientes y el servidor. DHCPv6 utiliza el método de autoconfiguración con estado (*statefull*). Los modos para solicitar la configuración IPv6 a un servidor DHCPv6 pueden ser:

1. Un encaminador envía un mensaje RA con el bit M a 1 al nodo, que le indica a este que debe configurarse mediante DHCPv6.
2. El nodo tiene activado la configuración mediante DHCPv6.

Una novedad en DHCPv6 es la utilización del DUID (DHCP Unique Identifier), que provee a cliente y servidores de un identificador único para estos se puedan identificar inequívocamente los mensajes entre ellos.

[11] RFC4862, "IPv6 Stateless Address Autoconfiguration".
[12] RFC4861, "Neighbor Discovery for IP version 6 (IPv6)".
[13] RFC 3315, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".

METODOS DE TRANSICIÓN IPV4 → IPV6

La parte más importante de todo este proyecto será la correcta elección de los métodos de transición de IPv4 a IPv6. Se nos dará casos donde debido a circunstancias de entorno, progresión futura, prestaciones, etc. debamos utilizar unos u otros tipos de métodos de transición.

¿Por qué tener que utilizar métodos de transición?. Obviamente, partimos que un entorno empresarial en producción 24 horas al días, 365 días al año, donde las paradas por motivos técnicos son muy costosas tanto por operatividad como el impacto económico en la plataforma de negocio on-line. Plantearnos un cambio total de infraestructuras en única operación a la par que resultaría muy complicada, se asumirían riesgos muy grandes que afectarían a los servicios de negocio de la compañía. Por esto, durante el proceso de implantación y hasta el de operación, utilizaremos técnicas de transición de IPv4 a IPv6, que nos permitirán realizar estos procesos por fases e ir validando cada operación realizada y gestionar toda la transición en eventos más pequeños y manejables.

Sean desarrollado distintos métodos de poder coexistir redes IPv4 con redes IPv6, que son:

DOBLE PILA

Quizás este es el método más popular a la vez que versátil. Definido en el RFC 4213, consiste en que los dispositivos con pila TCP/IP, puedan utilizar tanto protocolo IPv4 como IPv6, simultáneamente. El único inconveniente es la sobrecarga de trabajo en los dispositivos que conlleva el tener que gestionar dos procesos IP simultáneamente, a la vez que la monitorización y resolución de problemas se hace más compleja. Pero en contraste, permite realizar una transición fácilmente, al tener la posibilidad de estar usando ambos protocolos a la vez.

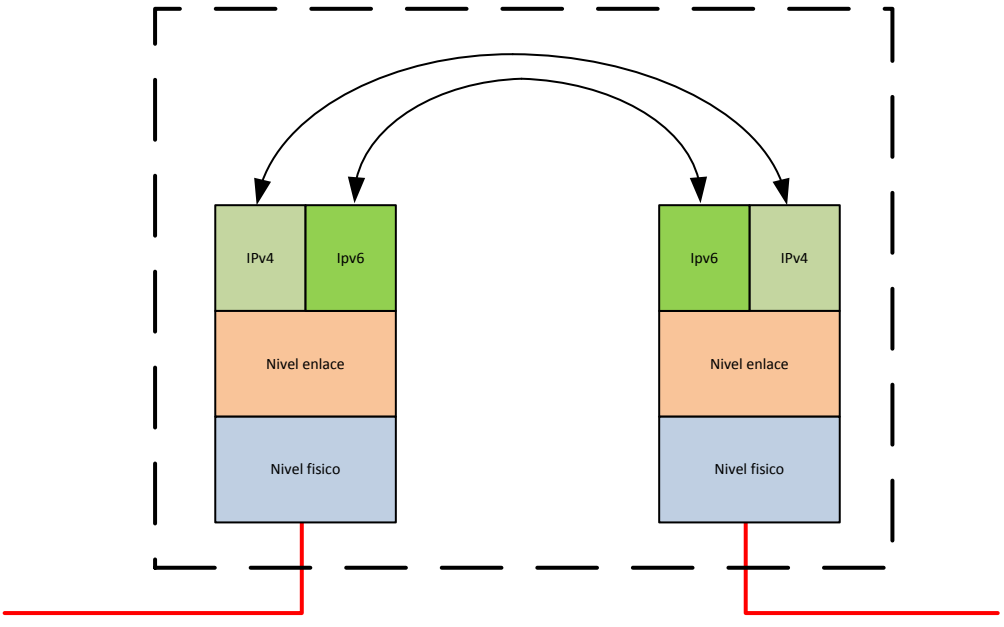


Figura 11 Dispositivo encaminador con doble pila

En los dispositivos con doble pila, son la aplicaciones las encargadas de seleccionar con que versión de IP se usara, dependiendo de la prioridad del protocolo dentro de la pila, de la respuesta a una consulta DNS o dependiendo del tipo de paquete con que se inicio la comunicación.

En la configuración de doble pila, se puede configurar las aplicaciones para que utilicen preferentemente uno de los dos protocolo.

EN IPv6 sea definido un nuevo conjunto de registros en la resolución de nombres DNS[14]. Así para la resolución de nombres a direcciones IPv6 sea establecido el nuevo registro AAAA. Dentro de una misma zona, pueden cohabitar el mismo nombre para diferente tipo de dirección IP y los registros AAAA y A. Los registros AAAA pueden ser consultados bajo IPv4 y los registros A pueden ser consultados bajo IPv6[15].

La selección del protocolo de comunicación mediante DNS dependerá de si la respuesta a una petición DNS, es un registro AAAA, para utilizar IPv6 y se utilizara IPv4 en el caso de que la respuesta DNS sea un registro del tipo A. Un ejemplo de este funcionamiento son los exploradores Web. En estas aplicaciones lo normal es indicar el nombre DNS del servidor al cual nos queremos conectar. Si en el equipo que ejecuta el explorador Web tenemos habilitado la doble pila, dependerá del tipo de respuesta DNS recibida en el explorador para que este elija con que versión del protocolo IP se inicia la comunicación.

La selección del protocolo mediante tipo de paquetes dependerá de que con qué tipo de paquete se inicio la comunicación. Si se recibe un paquete IPv6 se responderá con IPv6, si el paquete recibido es IPv4, entonces se utilizará IPv4.

Un dispositivo puede tener ambas pilas cargadas y activadas o puede tener ambas cargadas pero solo una activada.

En la actualidad tenemos este método de transición ampliamente desplegado. Un ejemplo lo tenemos en la Web[16] del Gobierno Español para el fomento de IPv6, que funciona con doble pila IP. También muchas empresas, sobre todo las dedicadas al *hosting* en Internet, llevan muchos años dando servicio con doble pila IP, como la empresa Host Virtual[17] . Esto nos indica, que este método de transición es el que más ampliamente ha sido aceptado, por su estabilidad y sencillez de implantación en Internet.

La ventaja del método de transición de doble pila, es que debido a que no hace ninguna interferencia con la pila actual de IPv4, esto es, el protocolo IPv4, tablas de rutas, protocolos de enrutamiento no se modifica ni se cambian su configuración, un problema que nos encontráramos en la pila de IPv6 no afectaría a los servicios sobre IPv4, por lo cual lo hace ideal para un despliegue progresivo y total de redes IPv6.

[14] RFC 3596 DNS Extensions to Support IP Version 6
[15] RFC 4472 Considerations with IPv6 DNS
[16] http://www.ipv6.es/es-ES/transicion/casos/Paginas/Casos.aspx
[17] http://www.vr.org/ipv6

TUNEL IPV6-TO-IPV4 (6TO4)

Si nos encontrásemos en la situación que deseamos conectar dos redes IPv6 a través de una red IPv4, tenemos la posibilidad de tunelizar el trafico IPv6 dentro de paquetes IPv4, creando un túnel entre dos dispositivos con doble pila.

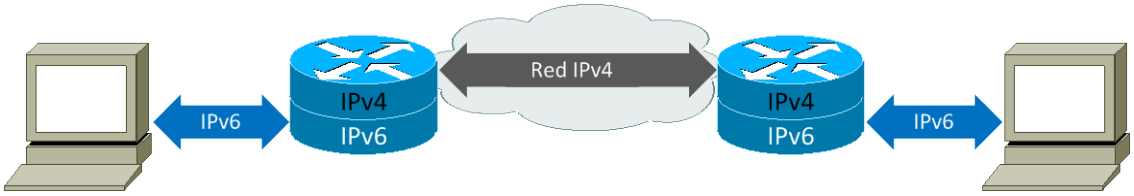


Figura 12 Túnel 6to4

IPv6 es encapsulado dentro de paquetes IPv4 y atraviesa el túnel dentro de una red IPv4, hasta el otro extremo donde es desencapsulado y transportado a la red IPv6. Los túneles son de creación automática.

La forma de realizar la comunicación entre dos islas de redes IPv6 separadas por redes en IPv4, consiste en utilizar un prefijo IPv6 2002:"*IPv4*"::/48[18] en el interface. Así, en las redes IPv6 se dispondrá de una ruta para llegar a las redes IPv6 a través de la dirección IPv6 del túnel construida con el prefijo de red 2002::/16 y la dirección IPv4. Cuando un paquete llega al encaminador, este encapsula el paquete IPv6 dentro de un paquete IPv4 y mediante la tabla de rutas[19] y decodificando la dirección IPv4 a partir de la dirección IPv6 del túnel y sabemos la dirección IPv4 donde tenemos que entregar el paquete, dado que los bits del 48 al 64 de la dirección IPv6 del túnel nos indican la dirección IPv4 del extremo del túnel. Hecho esto, el encaminador construye un paquete IPv4 con dirección origen su interface IPv4 y dirección destino IPv4 del extremo del túnel. Dentro del paquete se encapsula el paquete IPv6 y se envía a través de la red IPv4 hasta su destino. Una vez recibido el paquete en el extremo del túnel, el encaminador desencapsula el paquete y envía dicho paquete por el interface IPv6.

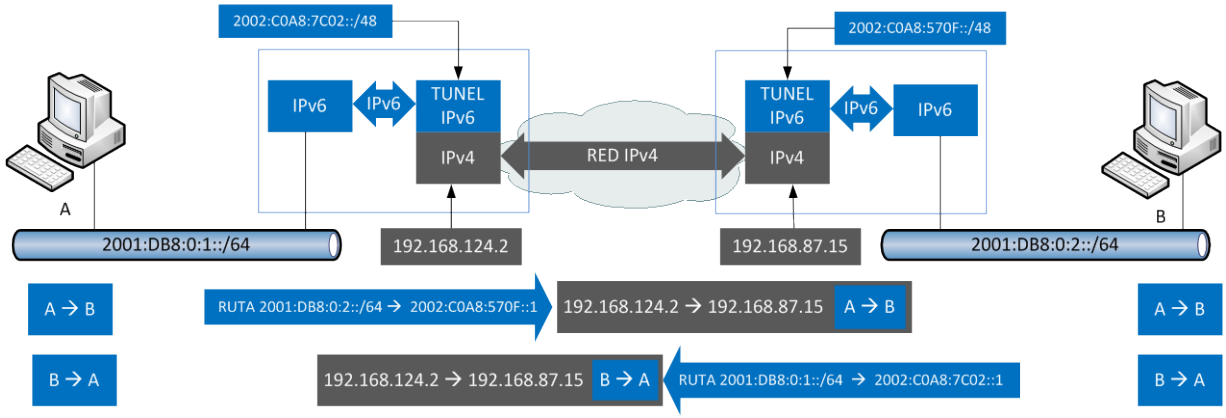


Figura 13 Descripción de un túnel 6to4

[18] RFC 6343 "Advisory Guidelines for 6to4 Deployment"
[19] RFC 3964 "Security Considerantions for 6to4"

TRANSLACIÓN DE PROTOCOLO

Existe la posibilidad de comunicar redes IPv4 e IPv6 mediante la translación de direcciones, similar a NAT de IPv4 pero más completa.

Se diseñaron dos métodos de translación que son *Network Address Tranlation-Protocol Translation* (NAT-PT), depreciado en el RFC 4966 por sus limitaciones y problemas con DNS y *Network Address Translation 64* (NAT64) que junto a DNS64 nos permite comunicar fácilmente redes IPv4-IPv6, por lo cual explicaremos su funcionamiento.

NAT64 se ha definido en dos modos de funcionamiento, con estado (*stateful*) especificado en el RFC 6146 y sin estado (*stateless*) especificado en el RFC 6145. Cada uno de estos tipos está pensado para un método de conexión.

NAT64 sin estado de conexión, está pensado para tipos de translaciones 1:1, donde hay un número limitado de nodos. Esto método no permite la conservación de direcciones IPv4 ya que necesitaremos tanta direcciones IPv4 como IPv6 y hay que tener en cuenta que en una sola red IPv6 hay 18 trillones de direcciones posible. Permite la conectividad *end-to-end* completa. Una comunicación *end-to-end*, permite que la comunicaciones entre nodos sea totalmente transparente, esto es, los nodos intermedios no modifican los paquetes y permite además que un nodo se pueda conectar con cualquier otro nodo. Internet se diseño originalmente con esta concepción de *end-to-end*. La translación requiere una asignación estática o por DHCP en ambos protocolos.

NAT64 con estado, es una traducción de 1:N, por lo que no tiene limitación en el numero de nodos, por lo que es adecuado para NAT masivo (CGN), ideal para los ISP. Este método permite la conservación de direcciones IPv4. Al utilizar sobrecarga de direcciones, no permite una conectividad *end-to-end* de direcciones. Permite que los nodos puedan ser configurados con cualquier método de autoconfiguración, DHCPv6, autoconfiguración sin estado (SLAAC), etc.

Como vemos, el mejor método para realizar una transición de IPv4 a IPv6 es NAT64 con estado, que aunque tiene las limitaciones propias del NAT de IPv4 (dificultad en las comunicaciones *end-to-end)*, permite una comunicación muy sencilla y sin grandes configuraciones, entre redes IPv4 e IPv6 ideal para que un ISP con una red IPv6 nativa pueda seguir teniendo conectividad con Internet IPv4.

DNS64 nos permitirá sintetizar respuestas de registro del tipo A en registros AAAA, para que los nodos de una red IPv6 puedan seguir resolviendo nombres de redes IPv4. Esto será necesario dado que debemos coexistir con redes IPv4 en Internet y solo conoceremos sus registros A.

El modo de funcionamiento de DNS64 es el siguiente:

- Un nodo con pila IPv6, realiza una petición de resolución de nombre a un DNS64, enviándole una consulta DNS de un registro AAAA.
- El servidor DNS64 realiza la consulta, ya sea por recursión o por delegación a otros servidores DNS para localizar el registro solicitado.
- Si la respuesta obtenida está vacía, entonces el servidor DNS64 realiza la misma petición pero cambiando el tipo de registro AAAA por un tipo de registro A.
- Si obtiene respuesta a la consulta, que será una dirección IPv4, entonces el servidor DNS 64 utilizara un prefijo IPv6 preestablecido para crear una dirección IPv4 mapeada y devolver una respuesta al nodo en IPv6.

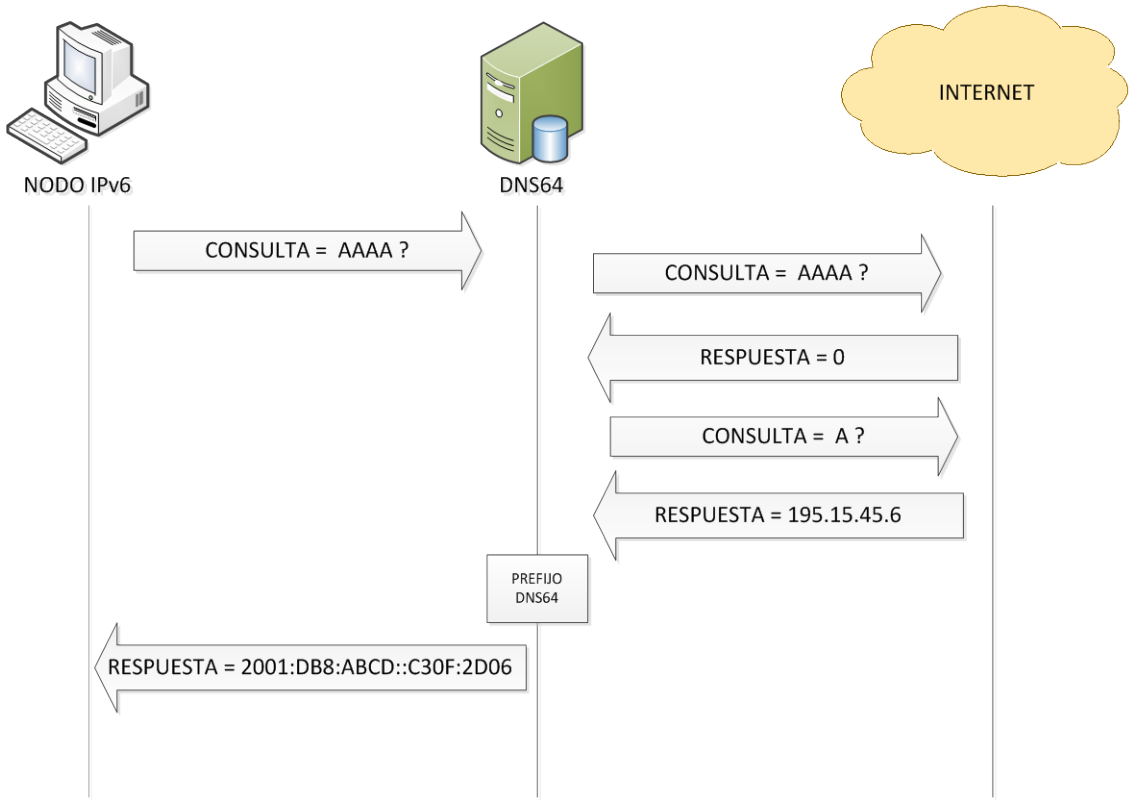


Figura 14 Funcionamiento DNS64

METODOLOGIA DE GESTIÓN DEL PROYECTO

Para realización de este proyecto de migración, dividiremos este en fases, que nos permitirá ir marcados las pautas necesarias que hay que cumplir en cada una de estas fases. Esto es necesario para una correcta organización de los procesos en los que estaremos inmersos dentro de cada una de las fases.

Análisis y planificación

Diseño de la red IPv6

Implantación

Operación y optimización

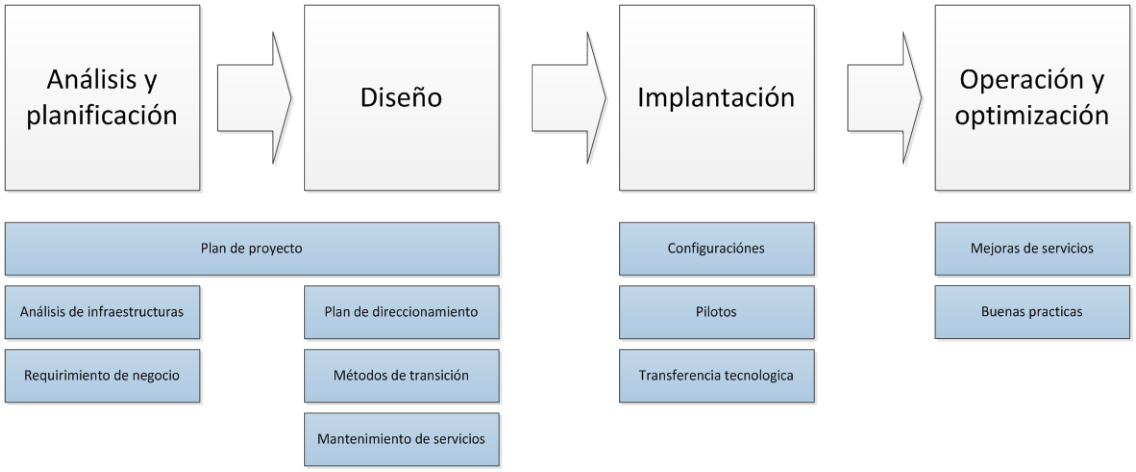


Figura 15 Metodología del proyecto

FASE DE ANÁLISIS Y PLANIFICACIÓN

PREPARACIÓN DEL PROYECTO

REQUERIMIENTOS DE NEGOCIO Y SERVICIOS ESTRATÉGICOS

La dirección de la empresa, en un intento de aumentar las ventas y seguir en el crecimiento de la empresa, desea potenciar la venta online y ofrecer más servicios que la competencia hoy en día. Para ello primero desea ampliar el número de tiendas on-line, expandiéndose hacia otras gamas como los electrodomésticos y bricolaje, pero no desea que mantener el mismo nombre para estos dos nuevas tienda, que dispondrán cada una de nombre y dominio propio. También se desea dar la posibilidad a los clientes habituales (registrados), de llamar al personal del departamento comercial o al soporte técnico directamente desde la pagina web utilizando VoIP, evitándoles así gastos de llamada al 902 habilitado actualmente. Otro factor donde la dirección de la empresa es ser pioneros en el ámbito de Internet, siendo el primer portal de ventas-online que trabaja sobre IPv6. Dentro de los planes estratégicos de la empresa, también está la apertura de más tiendas en toda España, con el objetivo de cubrir el 100% del territorio así como la implantación de dos nuevos centros de distribución

PLAN DE PROYECTO

Viendo las necesidades plantadas por la dirección de la empresa, la gerencia del área de sistemas y telecomunicaciones, después de evaluar los requerimientos, realiza las siguientes conclusiones:

- Para aumentar el número de dominios requiere aumentar las direcciones publicas asignadas actualmente debido a la estructura de los balanceadores.
- La empresa tiene asignado un rango publico que es 194.25.147.208 / 29 , suficiente para el servicio Web actual y SMTP, pero insuficiente para ampliar a 3 servicios web más dado qué no se puede utilizar hosts virtuales debido a que no tiene compatibilidad con SSL/TLS y los certificados digitales que actualmente dispone la empresa.
- El ISP ha comunicado que RIPE NCC, no otorga direccionamiento IPv4 y que cualquier cambio o ampliación de direcciones IP se realizara sobre IPv6.
- La utilización de tecnologías de VoIP sobre NAT, es muy problemática, pero no imposible.
- No se puede establecer un túnel IPSEC desde el servidor de comercio electrónico contra el servidor de transacciones del banco dado que tenemos un NAT entre ambos. Se podría realizar con un túnel IPSEC en modo agresivo, pero el banco no soporta este tipo de túneles.

Todos estos inconvenientes, llevan a pensar en la idoneidad de realizar la transición de la red IPv4 de la empresa a IPv6, por lo cual es expone:

- La migración a IPv6, se deberá realizar tarde o temprano, porque si no cada día que pase las redes antiguas de IPv4 quedaran más aislada del mundo de Internet.
- IPv6 ofrece muchas mejoras sobre IPv4.
- El agotamiento de IPv4 es real.

ANÁLISIS DE LAS INFRAESTRUCTURAS DE RED

Para realizar una correcta transición de IPv4 a IPv6, necesitamos conocer al detalle todas la infraestructuras TIC de la empresa. Es necesario descubrir e inventariar cualquier dispositivos que necesite de las comunicaciones LAN o WAN, para una correcta transición, así que dividiremos el análisis de las infraestructuras de la empresa en dos entornos que serán, redes LAN y redes WAN.

Tendremos en cuenta que en los dos Centros de Distribución poseen las mismas infraestructuras de redes y sistemas, al igual que las cinco tiendas son iguales entre ellas.

En una primera parte realizaremos un descubrimiento e inventario de todos los dispositivos de red, servidores y equipos que puedan verse afectados por la transición a IPv6. En una segunda parte, analizaremos la estructura física y lógica de la red para tener un amplio conocimiento de ella.

En el Anexo 2, se muestra el esquema de la estructura LAN/WAN de la red IPv4 de la empresa NetMania.

INVENTARIO DE REDES LAN

Las redes LAN de la empresa en cada ubicación está formada por todo el dispositivos de red, servidores y equipos de microinformática.

Los equipamientos que tenemos por ubicación y función son:

Sede Central

Dispositivo	Características	Unid.	Función
FortiGate 800	14 Interfaces 1000 Mbps TX FortiOS 4.3.10	2	Cortafuegos en alta disponibilidad que protegen las redes internas y crean una DMZ de servicios de Internet.
Juniper SSG140	6 Interfaces 10/100 Mbps TX 2 Interface 1000 Mbps TX ScreenOS versión 6.3.0	2	Cortafuegos en alta disponibilidad que protegen las redes internas aislando la DMZ de estas.
Cisco Catalyst 6506	8 Interfaces 1000 Mbps SX 96 Interfaces 10/100/1000 Mbps TX IOS versión 12.3SX	1	Matriz de conmutación con procesamiento de nivel 3 para la interconexión de todos los dispositivos del CPD.
Cisco Catalyst 2960	48 Interfaces 10/100 Mbps TX 2 Interfaces 1000 Mbps SX IOS Versión 12.2(52)SE2 LAN BASE	4	Conmutadores de planta para acceso de los equipos de microinformática.
F5 BIG-IP 1600 LTM	4 Interfaces 1000 Mbps TX LTM 10.1.0	2	Balanceador de tráfico en alta disponibilidad para la granja de servidores Web
WebInternet	Servidor Ultra Sun Solaris S.O. Solarios 10.0 Apache 2.0	4	Granja de servidores Web para la venta por Internet
SMTPInternet	Servidor Ultra Sun Solaris S.O. Solarios 10.0	1	Pasarela SMTP para el correo electrónico corporativo
ProxyInternet	Servidor HP DL 380 S.O. Debían 6.0.1 Squid 3.1.6	1	Servidor cache de acceso a Internet para los usuarios corporativos y filtrado de contenidos.
BBDDInternet	Servidor Ultra Sun Solaris S.O. Solarios 10.0 Oracle 10.0	1	Base de datos para servicios de Internet
WebIntranet	Servidor HP DL 380 Windows 2008 IIS 7.0	1	Servidor Web para la Intranet Corporativo con soporte ASP
EcommerceServer	Servidor Ultra Sun Solaris S.O. Solarios 10.0	1	Servidor de comercio electrónico seguro
DNS	Servidor Ultra Sun Solaris S.O. Solarios 10.0 BIND 9.0.3	1	Servidor DNS para resolución de nombres.
DHCP	Servidor HP DL 320 S.O. Red Hard 5.3 DHCP Server	1	Servidor DHCP para la autoconfiguración IP de los equipos microinformáticos de la sede central
Windows AD	Servidor DELL T480 S.O Windows 2008	1	Controlador de dominio de Windows Active Directory.
CorreoCorpo	Servidor HP DL 380 S.O Windows 2008 R2 Microsoft Exchange Server 2010	1	Correo electrónico corporativo
BBDDIntranet	Servidor Ultra Sun Solaris S.O. Solarios 10.0 Oracle 10.0	1	Base de datos para servicios de Intranet
TPVNetServer	Servidor HP DL 380 S.O Windows 2003 SP 2	1	Servidor de consolidación de ventas de los TPV de tiendas
PC-WINXP	S.O. Windows XP SP3 Software ofimático MS-Office	60	PC de escritorio para los usuarios corporativos

Centros de distribución

Cada CD dispone de los siguientes dispositivos y equipos:

Dispositivo	Características	Unid.	Función
Cisco Catalyst 2950	25 Interfaces 10/100 Mbps TX IOS Versión 12.3	1	Conmutador para la conectividad de nivel 2 de los dispositivos de red del Centro
FTPGesTran	Servidor HP DL 380 S.O Debian 6.0	1	Servidor de gestión de envíos.
PrintTrans	Impresora Laserjet 8000	3	Impresora para impresión de etiquetas y documentación de envió con JetDirect 600N para conexión a la red.
PC-WINXP	S.O. Windows XP SP3 Software ofimático MS-Office	5	PC de escritorio para la gestión del centro de distribución.

Tiendas

Cada tienda dispone de los siguientes dispositivos y equipos:

Dispositivo	Características	Unid.	Función
Cisco Catalyst 2950	24 Interfaces 10/100/1000 Mbps TX IOS Versión 12.3	1	Conmutador para la conectividad de nivel 2 de los dispositivos de red de la tienda
TPVNet	Terminales de punto de venta S.O. Windows XP SP2	5	Terminales de venta
PrintFac	Impresora Laserjet 2400	1	Impresora para impresión de facturas con JetDirect 620N para conexión a la red.
ServerTPV	Servidor DELL 1420 S.O. Windows 2003	1	Servidor para gestión de los terminales de venta
PC-WINXP	S.O. Windows XP SP3 Software ofimático MS-Office	2	PC de escritorio para la gestión de la tienda

INVENTARIO DE REDES WAN

Las redes WAN de la empresa, esta formadas por los siguientes elementos:

SEDE CENTRAL

Se dispone de una conexión a Internet suministrada por el ISP TeleNet, está compuesta por dos encaminadores Cisco 2811, con un caudal de 50 Mbps . Se tienen configurado los protocolo BGP en el lado ISP y OSPF en el lado cliente para provee de rutas dinámicas y disponer de caminos redundantes para caso de pérdida de conectividad por uno de los encaminadores . Estos encaminadores están conectados mediante una conexión FastEthernet con los cortafuegos Fortinet en el cual se sitúa el rango de direcciones IP públicas.

Para la conexión con los Centros de Distribución, disponemos de una conexión *Frame Relay*, provisionado con el operador de telecomunicaciones TeleComA. Para esta conexión disponemos de un encaminador Cisco 2611XM con dos circuitos virtuales, uno a cada centro. Este equipamiento es propiedad de NetMania, teniendo solo alquilado las líneas y circuitos FR. El caudal contratado es de 2 Mbps

Para la conexión de las tiendas, se dispone de una interconexión mediante MPLS/IP provisionada por el operador TeleComB. Se disponen de dos encaminadores Cisco 7203 en configuración HSRP, con una caudal de 10 Mbps . Estos encaminadores están conectados mediante *FastEthernet* a los cortafuegos.

Dispositivo	Características	Unid.	Función
Cisco 2811	2 Interfaces 10/100 Mbps TX IOS Versión 12.4	2	*Router* Internet, recibe rutas BGP del ISP y propagan OSPF hacia el cortafuego, para disponer de rutas redundantes.
Cisco 2611 XM	2 Interfaces 10/100 Mbps TX 2 Interfaces V.34 Frame Relay IOS Versión 12.3	1	*Router* de conexión con los centros de distribución
Cisco 7203	4 Interfaces 10/100 Mbps TX IOS Versión 12.3	2	*Router* MPLS/IP para conexión de las tiendas.

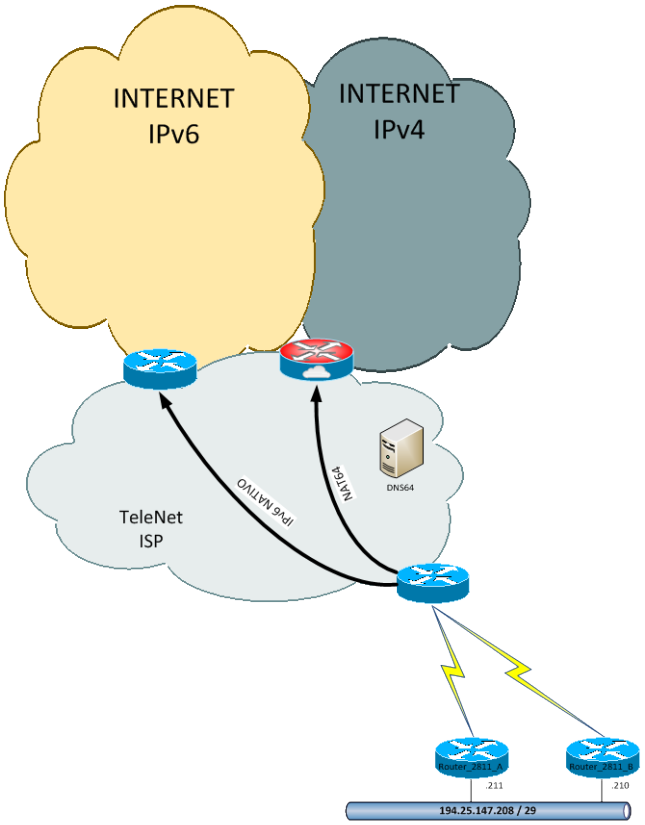


Figura 16 Red WAN Internet

La tecnología MPLS/IP utilizada en esta red, es un protocolo de red basado en etiquetas. Combina la potencia de ATM con la flexibilidad de IP, permitiendo realizar Ingeniería de tráfico y QoS. MPLS/IP se basa en etiquetar el trafico IP y utilizar estas etiquetas y el protocolo BGP para encaminar el trafico.

CENTROS DE DISTRIBUCIÓN

Los centros de distribución están conectados a la Sede Central mediante FR a través de un encaminador Cisco 2610 con interface FR y un circuito virtual contra dicha sede. Este encaminador se conecta a la red LAN del centro mediante una conexión FastEthernet contra un puerto del conmutador Cisco Catalyst 2524XL.

Dispositivo	Características	Unid.	Función
Cisco 2610	1 Interfaces 10/100 Mbps TX 1 Interfaces V.34 Frame Relay IOS Versión 12.3	2	*Router* de conexión con la Sede Central

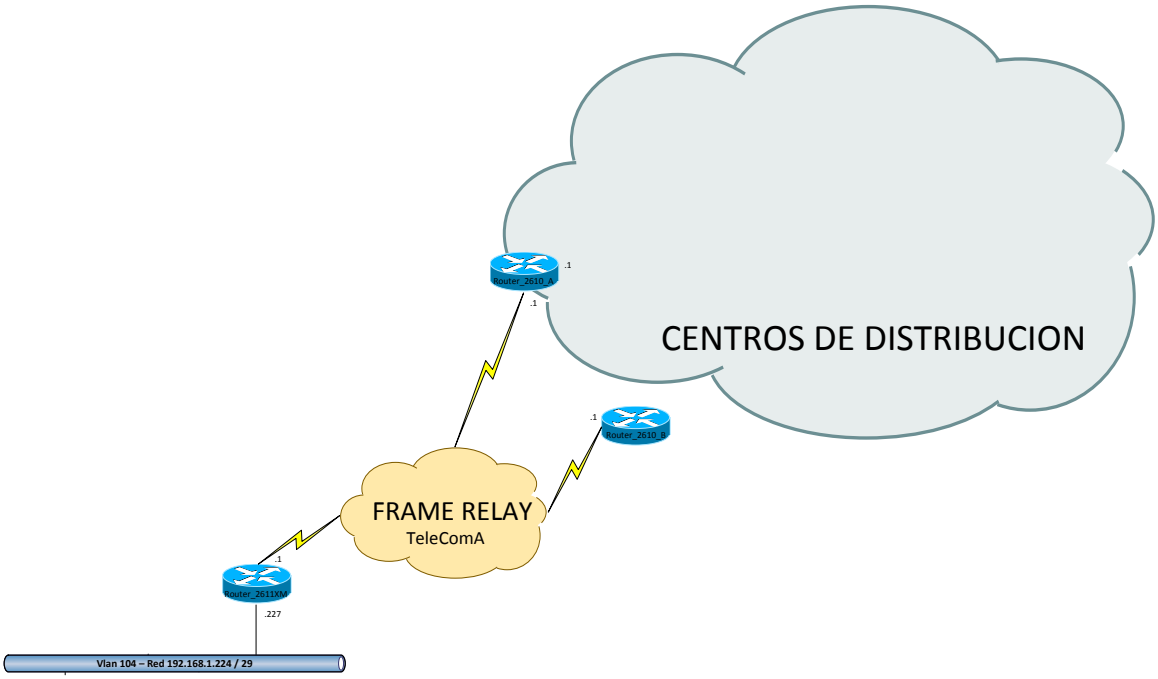


Figura 17 Red WAN Centros de Distribución

TIENDAS

Las tiendas disponen cada una de un encaminador Cisco 1801 del operador TeleComB, para la conexión a la MPLS/IP contra la Sede Central. Este encaminador está conectado mediante FastEtehrnet a un puerto del conmutador Cisco Catalyst 2924.

Dispositivo	Características	Unid.	Función
Cisco 1801	1 Interfaces 10/100 Mbps TX 1 Interfaces V.34 Frame Relay IOS Versión12.4	5	*Router* de conexión con la Sede Central

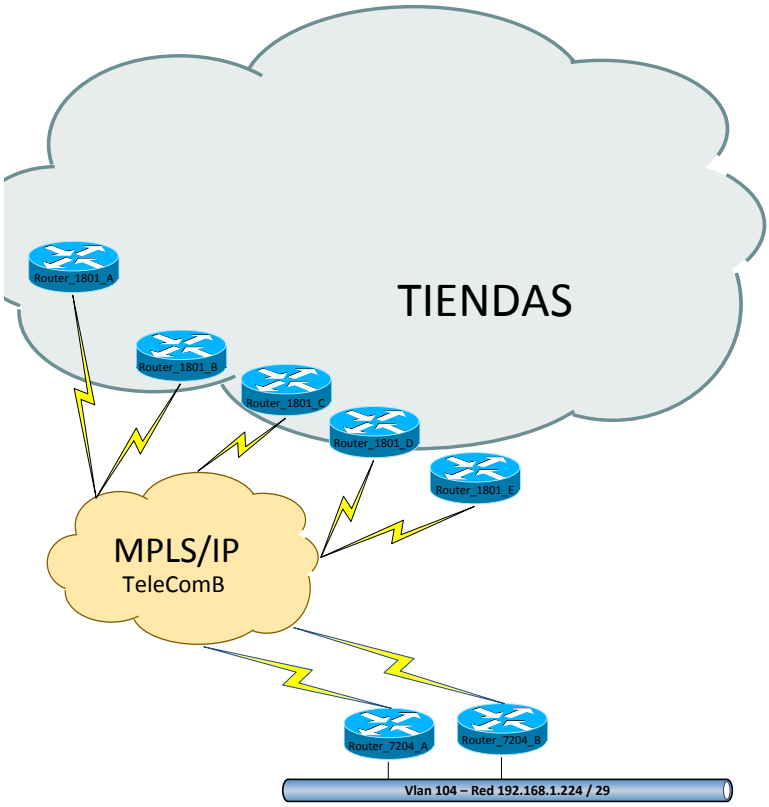


Figura 18 Red WAN Tiendas

ESTRUCTURA FÍSICA DE LA RED

Realizaremos una breve descripción de la estructuras física de cada ubicación:

- Sede Central: En este sitio está ubicado el CPD y las oficinas centrales. En el CPD se encuentran el equipo Catalyst 6506 que actúa de núcleo de red, 2 Fortinet 850, 2 Juniper SSG140, los encaminadores de conectividad WAN y los enlaces de fibra óptica de cada planta en un armario rack de 19". Contiguo a este están los armarios de los servidores de sistemas. En cada planta, se encuentra un armario de distribución de cableado horizontal donde se encuentran instalados 1 Catalyst 2948 que proveen conectividad de nivel 2 a los equipos de cada planta y se encuentran conectados con el núcleo de red mediante 1 cable de dos fibra óptica multimodo cada uno. Todos los equipos están en estado operativo. La estructura de cableado horizontal en el CPD y en cada planta está formado por cableado de categoría 6. La estructura de cableado vertical CPD-Plantas está formado por 2 mangueras de 12 fibras ópticas multimodo.
- Centros de Distribución: En cada centro hay un armario rack de 19" donde se ubican el conmutador Catalsyt 2950 que da conectividad de nivel 2 a los sistemas, un encaminador Cisco 2610 para la conectividad WAN, el servidor de datos del CD y el cableado estructurado del Centro. Los equipos del centro se conectan mediante un cableado estructurado de categoría 5.
- Tiendas de venta: En cada tienda hay un armario de 19", donde están instalados el conmutador Catalyst 2624, para la conectividad e nivel 2, el encaminador Cisco 1801 para la conexión a la MPLS/IP y el servidor de datos de la tienda. Los TPV y ordenadores se encuentran conectados mediante un cableado de categoría 5.

ESTRUCTURA LÓGICA DE LA RED

La estructura lógica de la red , con su división en subredes IP es la siguiente:

SEDE CENTRAL

El núcleo de la red, lo forma un Catalyst 6505 que dispone de una matriz de conmutación de alta velocidad de Nivel 2 y un modulo de procesamiento de Nivel 3 que le provee de capacidad de enrutamiento IP. Es un equipo modular que además dispone de 1 módulo de 8 puertos de fibra óptica SX para la conexión con las plantas y 2 módulos de puertos 10/100/1000 BaseTX para dar servicio a los dispositivos y servidores del CDP. En este equipo se realiza la segmentación de las redes IP en VLAN's de nivel 2 y provee de enrutamiento entre las mismas. Las VLAN's forman un dominio de VTP que se propaga por los conmutadores de planta para mantener una configuración común de VLAN's en todos los dispositivos de conmutación de la sede.

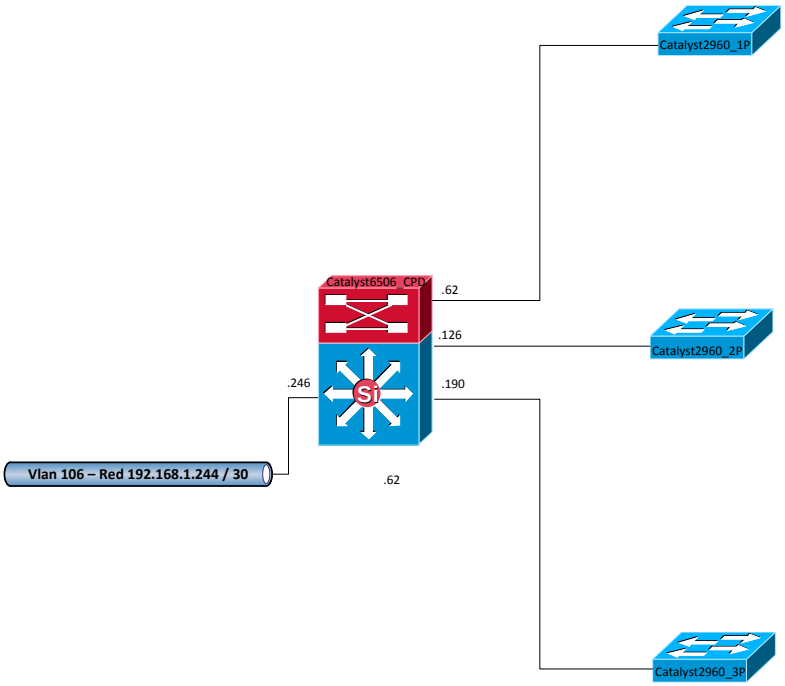


Figura 19 Núcleo de red

Los cortafuegos están configurados en alta disponibilidad , esto es, cada pareja de cortafuego funciona como un único equipo, que en caso de fallo del equipo principal, el equipo en modo *backup*, asume la gestión del tráfico con la misma configuración que el principal, dado que se sincronizan las configuraciones entre ellos. Los cortafuegos Fortinet y Juniper, forman dos DMZ's en dos niveles de seguridad, el primer nivel aísla todo el trafico de Internet hacia la granja de servidores Web del resto de redes y el segundo nivel, controla el flujo de tráfico desde la DMZ de primer nivel hacia los servicios corporativos y también hacia las sedes remotas para solo permitir tráficos autorizados hacia ellas. Sean seleccionado dos grupos de cortafuegos de diferente fabricante para evitar que una posible vulnerabilidad en uno de los fabricantes permitiese a un atacante hacerse con ambos grupos de cortafuegos. El cortafuego Fortinet , mantiene la conectividad con Internet y provee de NAT para las peticiones

smtp, http y https de los clientes de Internet hacia la DMZ de 1º nivel, que es donde están los servicios web de la empresa para estos clientes. Las redes remotas se conectan a la Sede Central a través de la DMZ de 2º nivel, ubicada en el cortafuego Juniper y esto permite tener un control del tráfico que se desea que envíen y reciban dichas redes remotas.

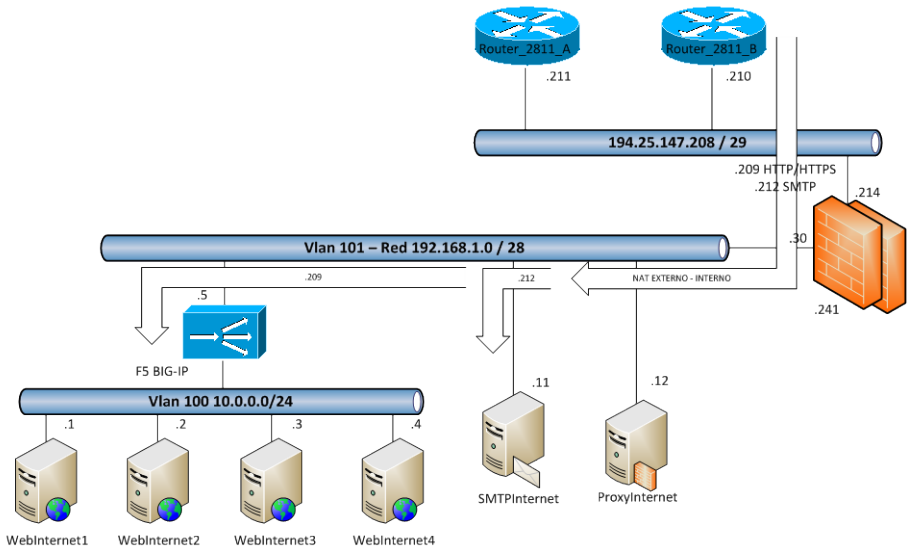


Figura 20 Flujo del tráfico NAT

En la DMZ de 1º nivel, se encuentra los servicios de Internet, Web y SMTP, así como el servicio proxy de navegación por Internet de los usuarios corporativos y filtrado de contenidos. Los servicios Web están formados por una granja de 4 servidores web, con dos F5 BIG-IP 1600 LTM (Local Traffic Management) en alta disponibilidad, que balancea las peticiones de cliente entre los cuatros servidores web.

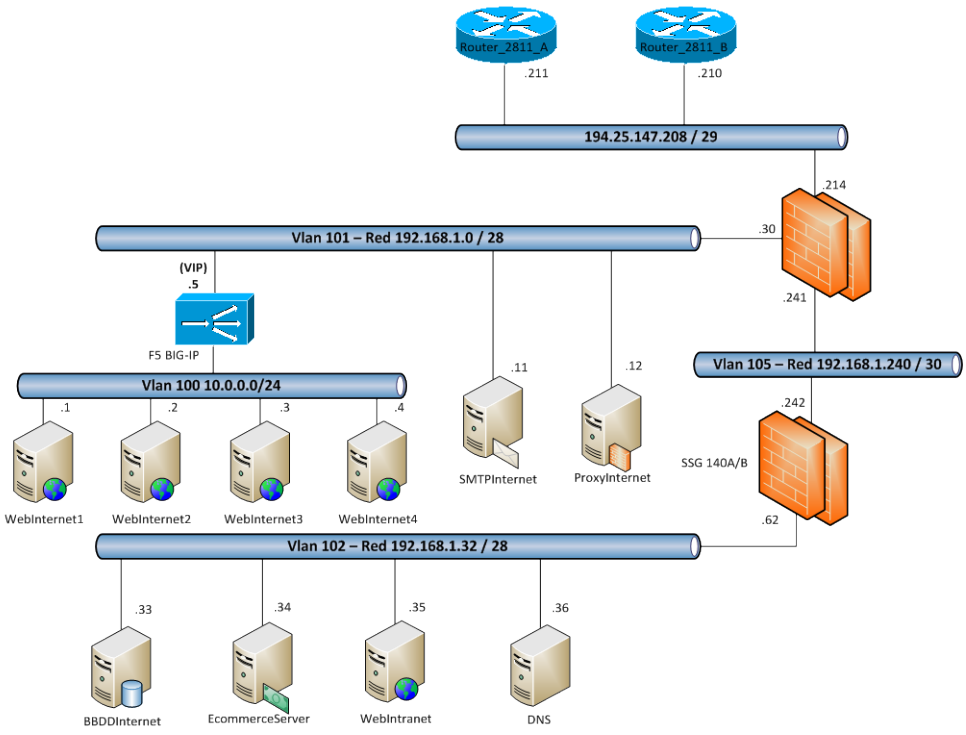


Figura 21 DMZ 1º y 2º Nivel con dos cortafuegos

Los servidores Web esta aislados en una vlan accesible solo por los balanceadores de tráfico. Estos balanceadores tienen configurados una IP Virtual (VIP) que atiende a dos grupos de balanceo, uno para el protocolo http y otro para el protocolo https para las transacciones comerciales. Cada grupo de balanceo tiene configurado los cuatro servidores Web con una política de round-robin .

Para la gestión de la electrónica de red y de los servidores de sistemas, hay implantada una red de gestión *out-band,* solo es accesible desde los equipos de sistemas y telecomunicaciones que disponen de una segunda tarjeta de red conectada a este segmento de red.

Se dispone de un servidor DHCP para la autoconfiguración IP de los equipos de usuarios. Los dispositivos de red así como los servidores disponen de direcciones IP configuradas estáticamente.

Hay un servidor DNS para la resolución de nombres del dominio interno, para resoluciones de nombres de dominios de Internet hace la tarea de reenviador. El dominio de la empresa Netmania.es es gestionado por el ISP que actúa de agente registrador para dicho dominio.

La segmentación de la redes IP y su asignación por VLAN's es:

Segmento IP	Nº Vlan	Asignación
10.0.0.0 / 24	100	Granja de servidores Web
192.168.1.0 / 28	101	DMZ 1º Nivel , Servidores y VIP Servicios Web
192.168.1.32 / 28	102	DMZ 2º Nivel, Servidores
192.168.1.48 / 28	103	Red de Servidores Corporativos
192.168.1.64 / 27	10	Red de gestión *out-band*
192.168.1.224 / 29	104	Redes de interconexión WAN
192.168.1.240 / 30	105	Red interconexión cortafuegos
192.168.1.244 / 30	106	Red interconexión red corporativa
192.168.2.0 / 26	110	Red de usuarios de administración y facturación
192.168.2.64 / 26	111	Red de usuarios de gestión comercial
192.168.2.128 / 26	112	Red de usuarios de sistemas y telecomunicaciones

RED IP PUBLICA

Se tiene asignado un direccionamiento público para los servicios de Internet. Para ofrecer los servicios, el cortafuegos Fortinet realiza una translación de direcciones publicas a privadas de cada servicio público hacia una dirección IP interna. El direccionamiento de la red IP publica es el siguiente

Dirección IP	Asignación
194.25.147.209	Dirección de resolución DNS para el dominio NetMania.es (NAT)
194.25.147.210	Dirección IP router principal ISP
194.25.147.211	Dirección IP router backup ISP
194.25.147.212	Dirección IP resolución DNS para servicio SMTP
194.25.147.213	LIBRE
194.25.147.214	Dirección IP cortafuego Fortinet.

El ISP trabaja con BGP en sus encaminadores, excepto en los interfaces de los clientes que en nuestro caso trabaja con OSPF para inyectar una ruta por defecto y proveer de tolerancia a fallos en caso de caída uno de los dos encaminadores que dan servicio a la compañía.

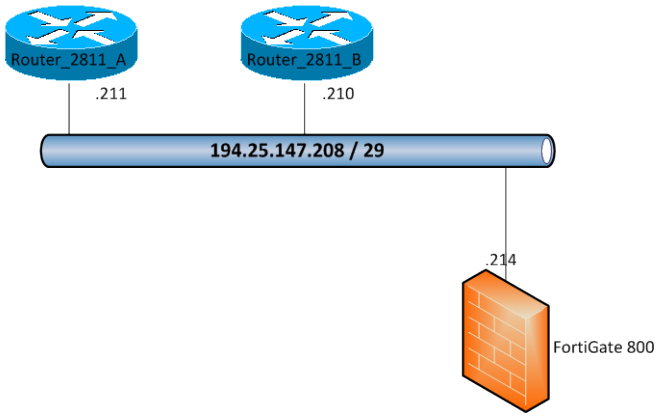


Figura 22 Direccionamiento publico

CENTROS DE DISTRIBUCIÓN

Los Centros de Distribución disponen de un encaminador Cisco 2610, con un interface V.35 para la comunicación mediante un circuito de FR con la sede central y con un interface FastEthernet conectado a conmutador Cisco Catalyst 2950 para la conectividad de nivel 2. Todos los dispositivos y equipos tiene las direcciones IPv4 configuradas estáticamente.

Las redes IP asignadas a los Centros de Distribución son:

Segmento IP	Asignación
192.168.4.0 / 26	Centro de Distribución de Madrid
192.168.4.120/30	Red IP FR DLCI 101 Sede Central - CD Madrid
192.168.4.32/ 26	Centro de Distribución de Barcelona
192.168.4.124/30	Red IP FR DLCI 201 Sede Central - CD Barcelona

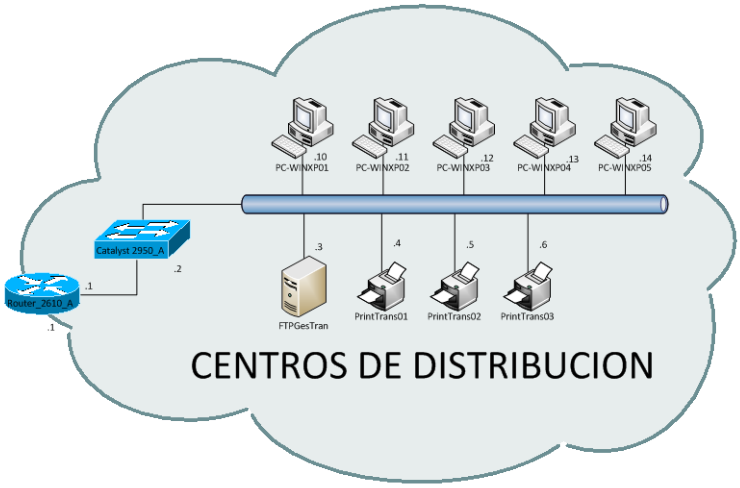


Figura 23 Red Centros de distribución

TIENDAS

Todas las tiendas tienen el mismo tipo de configuración, solo cambian la asignación IP de las subredes. En los encaminadores Cisco 1800 y Cisco 7203 de la red MPLS/IP, solo se asigna la dirección IP de la parte LAN por parte de la compañía *NetMania*, dado que la red IP de la parte WAN MPLS/IP, es responsabilidad de la compañía TeleCom B y tiene su propia infraestructura IP. Los encaminadores 7203 están configurados mediante el protocolo HSPR para proveer tolerancia a fallo en caso de caída de comunicación de uno de los equipos. El protocolo HSRP nos provee de una única puerta de enlace, compartida con varios equipos. Estos equipos crean una dirección IP y MAC virtual que es anunciada por el equipo que tenga función de MASTER, mientras que el resto de los equipos que forman el grupo HSRP estarán en estado STANDBY, que están a la espera de que el equipo MASTER no responda para que entonces el equipo con más prioridad STANDBY asuma la función del MASTER y realice la función de puerta de enlace de su segmento IP.

TeleCom B realiza el transporte de las redes de la compañía mediante una MPLS VPN, para la crear una única red virtual entre la sede central y las 5 redes de las tiendas. Todos los equipos tiene las direcciones IPv4 configuradas estáticamente.

Las redes IP asignadas a los Centros de Distribución son:

Segmento IP	Asignación
192.168.3.0 / 28	Red IP de la tienda de Madrid
192.168.3.16 / 28	Red IP de la tienda de Barcelona
192.168.3.32 / 28	Red IP de la tienda de Sevilla
192.168.3.48 / 28	Red IP de la tienda de Valencia
192.168.8.64 / 28	Red IP de la tienda de Bilbao

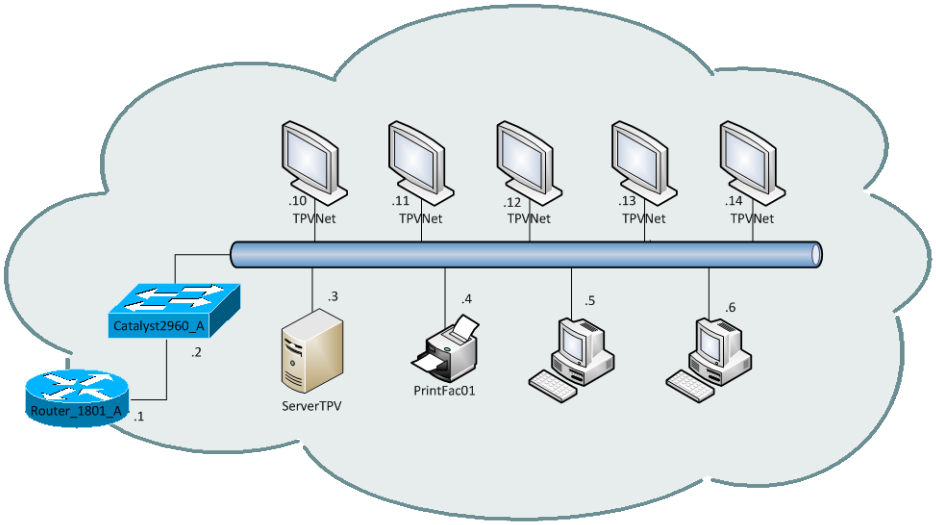


Figura 24 Red Tiendas

COMPROBACIÓN DE SOPORTE DE IPV6

Para una correcta transición de IPv4 a IPv6, debemos comprobar que los dispositivos de red como los sistemas operativos de servidores y PC soportan el protocolo IPv6 y en caso contrario, que debemos hacer para solventar este problema, que podrías ser una actualización de software de los dispositivos y servidores, sustitución de aquellos que no soporten IPv6, métodos alternativos para que funcionen equipos en IPv6, etc.

DISPOSITIVOS DE RED

Analizaremos el soporte de IPv6 de cada dispositivo de red por fabricante y modelo.

CISCO SYSTEM

Cisco System es una de las grandes compañía mundiales y referente en los entornos de redes tanto LAN como MAN y WAN. Disponemos diferentes encaminadores y conmutadores de este fabricante. Estos dispositivos disponen de un firmware propio llamado IOS , que provee de funcionalidades a los dispositivos. Para comprobar que los dispositivos soporta IPv6, debemos comprobar si el IOS lo soporta y si no es así, debemos encontrar que versión de IOS de cada tipo de dispositivo es compatible IPv6.

Cisco System dispone en su web[20] un servicio (Software Advisor) que nos permite buscar y ver las características de cada versión de IOS. Mediante esta página buscaremos que versión de IOS de cada dispositivo necesita para soportar IPv6 y si en caso de tener que actualizar el IOS, que requerimientos de memoria Flash y RAM necesitamos para pueda soportar dicho IOS.

Dispositivo	IOS	Ubicación	Soporta IPv6	IOS con soporte IPv6	¿Requiere actualizado hardware?
Router 2811_A	12.4(4)T7- ADVANCED IP SERVICES	Sede Central	SI	-	No
Router 2811_B	12.4(4)T7- ADVANCED IP SERVICES	Sede Central	SI	-	No
Router 2611XM	12.3(18) IP BASE	Sede Central	NO	12.3(26) IP PLUS	Si, Ampliar memoria Flash a 48 Mb
Router 7203_A	12.3(14)YX16 PDSN R2.0 BASIC	Sede Central	SI	-	-
Router 7203_B	12.3(14)YX16 PDSN R2.0 BASIC	Sede Central	SI	-	-
Catalyst 6506_CPD	12.2.(33)SXI6 IP SERVICES	Sede Central	Si	-	-
Catalyst 2960_1P	12.2(52)SE2 LAN BASE	Sede Central	Si	-	-
Catalyst 2960_2P	12.2(52)SE2 LAN BASE	Sede Central	Si	-	-
Catalyst 2960_3P	12.2(52)SE2 LAN BASE	Sede Central	Si	-	-
Router 2610_A	12.2(36) IP PLUS	CD Madrid	NO	12.2(2)T1 IP PLUS	-
Catalyst 2950_A	12.1(22)EA1	CD Madrid	NO	NO DISPONE	Completo
Router 2610_B	12.2(36) IP PLUS	CD Barcelona	NO	12.2(2)T1 IP PLUS	
Catalyst 2950_B	12.1(22)EA1	CD Barcelona	NO	NO DISPONE	Completo
Router 1801_A	12.3(8)Y12 ADVANCED IP SERVICES	Tienda Madrid	SI	-	-
Catalyst 2960_A	12.2(50)SE2 LAN BASE	Tienda Madrid	SI	-	-
Router 1801_B	12.3(8)Y12 ADVANCED IP SERVICES	Tienda Barcelona	SI	-	-

[20] http://tools.cisco.com/Support/Fusion/FusionHome.do?mySession=832619&myStep=6

Catalyst 2960_B	12.2(55)SE4 LAN BASE	Tienda Barcelona	SI	-	-
Router 1801_C	12.3(8)Y12 ADVANCED IP SERVICES	Tienda Sevilla	SI	-	-
Catalyst 2960_C	12.2(55)SE4 LAN BASE	Tienda Sevilla	SI	-	-
Router 1801_D	12.3(8)Y12 ADVANCED IP SERVICES	Tienda Valencia	SI	-	-
Catalyst 2960_D	12.2(58)SE1 LAN BASE	Tienda Valencia	SI	-	-
Router 1801_E	12.3(8)Y12 ADVANCED IP SERVICES	Tienda Bilbao	SI	-	-
Catalyst 2960_E	12.2(58)SE1 LAN BASE	Tienda Bilbao	SI	-	-

Observamos que la gran mayoría del equipamiento Cisco de la compañía, soporta IPv6, con lo que solo habrá que realizar las configuraciones pertinentes en dichos equipos. Hay cierto equipamiento que debido a su antigüedad, habrá que actualizar su IOS, para que estos soporten IPv6, lo cual realizaremos descargándonos a través de la pagina web de Cisco, las imágenes de las IOS necesarias para el soporte de IPv6. En alguno de estos equipos, se deberá además realizar una actualización de *hardware* del mismo. En este caso , se debe ampliar la memoria flash, dado que al actualizar el fichero del IOS , este puede ser más grande que la memoria flash que dispone el equipo , por lo cual, para que se pueda actualizar con un fichero de IOS de tamaño superior a la memoria flash, esta se debe ampliar al tamaña mínimo requerido.

Pero hemos detectado que los Catalyst 2950 no soportan IPv6, debido a lo antiguo que son (son los primeros equipos comprados por la compañía y que no se actualizaron en los programas de mantenimiento de la red), por lo que se debe analizar si se sustituyen o si no es posible, habrá que indicar qué medidas se toman para poder mantener la conectividad con el resto de la red de NetMania.

F5

F5 es una compañía especializada en *appliance,* equipos personalizados y optimizados, para la ejecución de sus aplicaciones de gestión de tráfico. La empresa NetMania dispone de dos balanceadores de tráfico (o de carga) BIG-IP 1600 para su granja de servidores Web. Esto permite evitar sobrecarga los servidores, repartiendo la carga según sesiones de clientes entre los distintos servidores Web, sin sobrecargar un único servidor.

El equipo BIG-IP 1600, dispone de 4 interfaces 1000 base TX para la conexión a la red de clientes (Internet-> DMZ) y a la red de la granja de servidores. Este equipo está basado en Linux GNU y sobre él se ejecuta la aplicación de gestión de tráfico *Local Traffic Management"* (LTM) versión 10.1.0. Esta aplicación es la encargada de realizar el balaceo de carga entre los servidores y dependiendo del tipo de trafico reciban (http, https). La configuración esta optimizada para que el trafico http y https mantenga persistencia de sesión en cada servidor, esto es, cada cliente se dirige a un servidor Web y mientras ese cliente mantenga la sesión TCP estabilizada, cualquier nueva petición http o https se enviará al mismo servidor. El balanceo de trafico de cliente sigue una política de *round robbin*, que significa que cada nueva conexión de cliente se va repartiendo entre los servidores en modo rotativo, 1→2→3→4→1→2→... además en caso de que un servidor supere un número máximo de conexiones permitidas, este no recibe más peticiones hasta que se liberen las sesiones actuales, esto puede venir dado, por el hecho que ciertos clientes pueden mantener las sesiones muchos más activas y si da la casualidad que estás caen en un mismo

servidor, este tendrá menos recursos disponibles que otros servidores web, cuyos clientes han cerrado más rápidamente las sesiones, liberando los recursos del servidor.

En cuanto al soporte de IPv6, sea comprobado que F5 desde sus primeras versiones de la aplicación LTM soporta IPv6. El único requerimiento es disponer de la licencia de IPv6 GATEWAY para LTM. Se comprueba que se dispone de dicha licencia.

Dispositivo	Versión	Ubicación	Soporta IPv6	LTM con soporte IPv6	¿Requiere actualizado hardware?
BIG-IP 1600 LTM	10.1.0	Sede Central	Si	-	-

FORTINET

Fortinet es una empresa de fabricación de equipamiento de seguridad de red. Disponemos de dos cortafuego modelo FortiGate 800C configurados en alta disponibilidad, que nos ofrece seguridad entre la red de Internet y las redes internas, creando la DMZ de 1º Nivel. Aparte, este equipo nos realiza la translación de dirección de IPv4 publicas hacia las direcciones de red privadas, necesario para hacer público los servicios de los servidores web y correo electrónico.

Estos equipos disponen de un sistema operativo llamado FortiOS. Fortinet[21] informa que a partir de la versión 3.0 del firmware FortiOS se soporta IPv6.

Dispositivo	Versión	Ubicación	Soporta IPv6	FortiOS con soporte IPv6	¿Requiere actualizado hardware?
FortiGate 800	FortiOS 4.3.10	Sede Central	Si	-	-

JUNIPER

Juniper es el siguiente competidor de Cisco System en negocio del equipamiento de red, tanto en la parte de interconexión de redes como en sistemas de seguridad.

En este caso, nuestro equipamiento Juniper está orientado a la seguridad de la red de compañía, al igual que el equipamiento de Fortigate. Con los dos equipo SSG140 en alta disponibilidad, sea creado un segundo nivel de DMZ, que permite aumentar el aislamiento entre las redes internas e Internet y creando una DMZ de 2º nivel.

El firmware de estos equipos se llama ScreenOS. Se comprueba mediante el datasheet del SSG140[22], que este equipo soporta IPv6.

Dispositivo	Versión	Ubicación	Soporta IPv6	ScreenOS con soporte IPv6	¿Requiere actualizado hardware?
SSG 140	ScreenOS 6.3.0	Sede Central	Si	-	-

[21] http://www.fortinet.com/press_releases/080225.html
[22] http://www.juniper.net/us/en/local/pdf/datasheets/1000181-en.pdf

HP

La compañía dispone de varias impresoras HP conectadas a las redes LAN, 6 en los centros de distribución para la impresión de etiquetas y documentación de envíos y 5 en las tiendas para la impresión de facturas a clientes. Estas impresoras disponen de unos módulos llamados JetDirect para la impresión en red mediante el protocolo LPD. Comprobamos que los JetDirect actuales no soportan IPv6, por lo cual buscamos un modulo JetDirect compatibles con dichas impresoras y que soporte IPv6[23]. El modulo compatible con todas las impresoras y que tiene soporte IPv6 es el JetDirect 635N.

Dispositivo	Modelo	Ubicación	Soporta IPv6	JetDirect con soporte IPv6	¿Requiere actualizado hardware?
PrintTrans01	HP 8000 con Jedirect 600N	CD Madrid	No	635N	Si, completo
PrintTrans02	HP 8000 con Jedirect 600N	CD Madrid	No	635N	Si, completo
PrintTrans03	HP 8000 con Jedirect 600N	CD Madrid	No	635N	Si, completo
PrintTrans04	HP 8000 con Jedirect 600N	CD Barcelona	No	635N	Si, completo
PrintTrans05	HP 8000 con Jedirect 600N	CD Barcelona	No	635N	Si, completo
PrintTrans06	HP 8000 con Jedirect 600N	CD Barcelona	No	635N	Si, completo
PrintFac01	HP 2410 con Jedirect 620N	Tienda Madrid	No	635N	Si, completo
PrintFac02	HP 2410 con Jedirect 620N	Tienda Barcelona	No	635N	Si, completo
PrintFac03	HP 2410 con Jedirect 620N	Tienda Sevilla	No	635N	Si, completo
PrintFac04	HP 2410 con Jedirect 620N	Tienda Valencia	No	635N	Si, completo
PrintFac05	HP 2410 con Jedirect 620N	Tienda Bilbao	No	635N	Si, completo

SISTEMAS OPERATIVOS DE SERVIDORES Y EQUIPOS INFORMÁTICOS

Los sistemas operativos de los servidores y equipos informáticos necesitan soportar IPv6 para poder seguir funcionando normalmente con las aplicaciones ofimáticas y corporativas. Comprobaremos que cada tipo de sistema operativo si este soportado IPv6 y sino, que debemos hacer para poder funcionar con este protocolo.

DEBIAN 6.0 (LINUX)

Se disponen de un total de 3 servidores sobre los cuales se ejecuta el sistema operativo Debian 6.0 (Squeeze), una distribución de Linux bajo licencia GNU.

Este sistema operativo, soporta IPv6 completamente[24], por lo cual solo se deberá configurar adecuadamente. Permite la ejecución en *Dual Stack* de la pila de protocolos IPv4 e IPv6.

SOLARIS 10.0

Sun, fue una de las grandes compañías de servidores y aplicaciones, promotora del sistema operativo Solaris y del entorno de desarrollo de aplicaciones Java. Recientemente Sun fue adquirida por la compañía especialidad en software de SGBD Oracle, integrando así en una única compañía todos los niveles de negocios de las TIC, equipos, sistema operativo, aplicaciones y base de datos, lo cual le permite dar soluciones completas a problemas complejos en entornos empresariales. Oracle está manteniendo el desarrollo de los sistema operativo Solaris, aunque no se descarta en el futuro que prescinda de ellos o que cambie el enfoque de los mismo.

[23] http://h10010.www1.hp.com/wwpc/us/en/sm/WF06a/18972-18972-236253-34213-236264-500078.html?dnr=1
[24] http://wiki.debian.org/DebianIPv6

En nuestro caso , disponemos de 9 servidores con el sistema operativo Solaris versión 10.1. Al igual que con Debian, este sistema operativo soporta perfectamente IPv6[25].

REDHAT 5.3

Red Hat es otra distribución de Linux/GNU, la cual está instalada en 1 servidores en su versión 5.3.

RedHat 5.3 soporta IPv6, estando certificado por el Departamento de Defensa de EEUU, recomendando un kernel 2.6.x o superior[26].

WINDOWS SERVER 2003

Se disponen de 6 servidores basados en el sistema operativo Windows 2003 de Microsoft. Estos servidores gestión el entorno de TPV de las tiendas y consolidan los datos en un servidor de la sede central.

Microsoft , en su página de productos y servicios soportados en IPv6[27], no indica dicho sistema operativo, esto es, por que solo se detallan los productos que actualmente están en el portfolio de venta comercial de Microsoft. Windows 2003 dejo de comercializarse el 13/03/2007[28], pero hemos comprobado que dicho sistema operativo soporta IPv6[29].

WINDOWS SERVER 2008

Se disponen de 2 servidores basados en el sistema operativo Windows 2008 de Microsoft. Estos servidores gestión el Directorio Activo de la compañía y el correo electrónico basado en Exchange 2010.

Según la página de productos y servicios soportados en IPv6[30] de Microsoft, el sistema operativo Windows Server 2008 soportan IPv6.

WINDWOS XP SP3

La compañía tiene homologado como sistema operativo de equipos de escritorio al versión Windows XP SP3 de Microsoft.

Al igual que con el sistema operativo Windows 2003, aunque no se indique en la página de productos soportados en IPv6, Windows XP si puede operar con IPv6[31].

[25] http://docs.oracle.com/cd/E19253-01/816-4554/ipv6-ref-83/index.html
[26] http://www.redhat.com/mirrors/LDP/HOWTO/html_single/Linux+IPv6-HOWTO/#SYSTEMCHECK-KERNEL
[27] http://technet.microsoft.com/en-us/network/hh994905.aspx
[28] http://support.microsoft.com/lifecycle/default.aspx?LN=es-es&x=7&y=11&p1=3198
[29] http://support.microsoft.com/kb/325449
[30] http://technet.microsoft.com/en-us/network/hh994905.aspx
[31] http://support.microsoft.com/kb/2478747

SERVICIOS DE RED

Los servicios de red que actualmente se disponen, deben ser migrados o adecuados para soportar IPv6 son los siguientes:

DHCP

La asignación de direcciones IPv4 dentro de la compañía se realiza de dos maneras, estáticamente para equipamiento de red, servidores, dispositivos que requieran disponer de una asignación fija para poder ser localizados por otros servicios y redes de usuarios que no superen los 14 nodos, y dinámicamente a todas aquellas redes de usuarios finales de más de 14 nodos.

El servidor DHCP es la versión 4.1 de ISC. Este servicio se ejecuta sobre un servidor con sistema operativo RedHat 5.3 y esta soportado sobre IPv6[32].

DNS

Se dispone de un DNS BIND versión 9.5 de ISC, que tiene configurada de una zona principal para el dominio *netmania.es* para la resolución de direcciones IP de las redes internas de la compañía. Este DNS realiza el reenvió de peticiones DNS del resto de dominios (Dominios de Internet) a un DNS de nuestro ISP. El ISP mantiene la zona principal del dominio *netmania.es* para las peticiones provenientes de Internet. Este servicio se ejecuta en un servidor con sistema operativo Solaris 10.0.

Se comprueba que esta versión de DNS soporta IPv6. Puede soportar DNS64 a partir de la versión 9.8

PROXY INTERNET

Para que los usuarios tanto de la sede central, centros de distribución y tiendas puedan navegar por Internet, se dispone de un servidor proxy (cache) Squid ejecutándose sobre un servidor con sistema operativo Debian 6.0, con gestión de paginas negras (blacklist) para el control de acceso y uso optimo del acceso a Internet.

Squid[33] soporta IPv6 en versiones 3.1 y superiores.

[32] https://access.redhat.com/knowledge/docs/en-US/Red_Hat_Enterprise_Linux/6/html/Deployment_Guide/s1-dhcp_for_ipv6_dhcpv6.html
[33] http://wiki.squid-cache.org/Features/IPv6

INTERACCIÓN CON TERCEROS

La transición de IPv4 a IPv6, no solo afecta a la compañía *NetMania*, sino que también afecta a terceros con los que mantenemos relaciones de servicios cliente/proveedor. Deberemos comprobar hasta qué punto de viabilidad técnica como económica nos puede afectar estas relaciones en el proceso de la transición. Nuestros proveedores de servicios a nivel de red son:

- TeleNet ISP: Proveedor de servicios de Internet, hosting y LIR del dominio *Netmania.es*.
- TeleCom A: Proveedor de servicios de telecomunicaciones con el cual disponemos unos circuitos FR con los centros de distribución.
- TeleCom B: Proveedor de servicios de conectividad MPLS/IP para la interconexión de la sede central con las 5 tiendas.

Analizaremos que servicios de nuestros proveedores pueden ser migrados a IPv6 y cuáles no.

SERVICIOS TELENET ISP

TeleNet ISP, nos proporciona la conectividad con Internet así como nuestro rango publico de direcciones IPv4.

Puesto en conversaciones con su departamento comercial y de ingeniería, sobre la posibilidad de una transición de IPv4 a IPv6, hemos observado lo siguiente:

- TeleNet ISP, ya nos comunico la imposibilidad de ampliar nuestro rango publico de IPv4.
- TeleNet ISP, cuenta con una red propia de Internet sobre IPv6, AS asignado por la IANA para esta red, DNS64 y NAT64 hacia Internet sobre IPv4, lo que permite que clientes suyos sobre IPv6 puedan seguir teniendo conectividad con toda la red de Internet sobre IPv4.
- Para que la red IPv6 de *NetMania* sigua siendo visible por Internet IPv4, se deberá realizar un mapeo NAT64 en los encaminadores de translación de NAT64 que disponen.
- TeleNet ISP, no pone ningún impedimento a que la compañía haga la transición de IPv4 a IPv6.
- El Departamento de Ingeniería de TeleNet ISP, nos ayudara en todo los procesos de adaptación, configuración transición y pruebas.
- El Departamento Comercial nos indica que los cargos de toda la transición será el coste del nuevo registro en RIPE del direccionamiento IPv6 de la compañía y un 40% de las horas totales de Ingeniería. RIPE es una de las cinco agencias regionales (RIR) encargada de la gestión del los recursos de Internet. RIPE[34] se encarga de la gestión del área geográfica de Europa y el oeste y ciertas partes de Asia.

[34] http://www.ripe.net/lir-services/ncc/one_sheet_October_2012_final.pdf

SERVICIOS TELECOM A

TeleCom A ,empresa de telecomunicaciones de nivel internacional, provee a la compañía del servicio de conexión FR con los centros de distribución mediante dos circuitos virtuales. Trasladada la consulta sobre la transición de la compañía de IPv4 a IPv6, TeleCom A nos ha indicado lo siguiente:

- TeleCom A solo nos provee de las líneas de FR con los correspondientes circuitos virtuales en configuración punto-multipunto.
- Los encaminadores de la red FR son propiedad de la compañía *NetMania*.
- TeleCom A nos indica que ellos no realizaran ninguna operativa sobre su red, dado que los protocolos IPv4 e IPv6 se encapsulan dentro de FR y por tanto no afecta al funcionamiento de la misma.

SERVICIOS TELECOM B

TeleCom B, empresa de telecomunicaciones de ámbito nacional, provee a la compañía de un servicio de transporte sobre MPLS/IP entre la sede central y las 5 tiendas distribuidas por el territorio nacional. Sobre la necesidad de la compañía de realizar una transición a IPv6, nos indica lo siguiente:

- Toda la red de TeleCom B está basada en IPv4.
- TeleCom B hoy por hoy, no tiene planes de tener una red MPLS/IP en IPv6.
- Desde TeleCom B nos comentan que están dispuesto a realizar cualquier configuración en la parte de cliente en los encaminadores CPE, pero no en su red.
- A la pregunta de si sería posible configurar entres los CPE de la compañía túneles 6to4, nos indica que no habría ningún problema y que no habría coste económico, dado que los trabajos de mejoras en encaminadores de clientes están incluidos en el contrato de mantenimiento de TeleCom B con la compañía NetMania.

CONCLUSIONES

Después de analizar el estado de las infraestructuras de red , servidores y servicios de red, llegamos a las siguientes conclusiones:

- Debido a que un gran número de fabricantes, llevan años implementado el protocolo IPv6 dentro de sus equipos y software, nos encontramos que la mayoría del equipamiento de la compañía soporta IPv6.
- Se han detectado un número muy reducido de dispositivos de red que no soportan IPv6, debido principalmente a su antigüedad, pero que pueden ser reemplazados por elementos más actuales que si soportan IPv6 sin mucho coste. Hay otros elementos solo requieren una pequeña actualización de hardware poco costosa.
- El proveedor TeleCom B no soporta IPv6, pero podremos conectar las redes de las tiendas en IPv6 con la sede central mediante túneles 6to4.
- TeleNet ISP , nos permite estar conectados y recibir trafico de las redes de Internet en IPv4 mediante translación NAT64 y en IPv6 nativamente.
- TeleNet ISP, nos permitirá el uso de DNS64 para resolución de nombres en IPv4.
- Podemos utilizar un modelo de transición de doble pila (*Dual-Stack*) en todos los dispositivos de red.
- Actualmente, el modelo de transición en doble pila, está ampliamente desplegado sobre todo en organismos públicos y universidades tanto del ámbito nacional e internacional así como en grandes corporaciones que están involucradas en el despliegue de IPv6.
- Debido a que durante la transición de IPv4 a IPv6 con el método de doble pila, mantendremos la operatividad actual de la red IPv4, podremos enfrentarnos a posibles problemas de errores de software, bugs de fabricantes sin que la producción actual se vea afectada.
- El área de Sistemas por su parte, a verificado que las aplicaciones corporativas como bases de datos, servidores web, correo electrónico y entorno SAP, son compatibles con IPv6. De esta parte se encarga el área de sistemas en un proyecto paralelo al nuestro.

Por todo esto, llegamos a la conclusión de la fiabilidad del proyecto de transición a IPv6 y pasamos a la fase de diseño y planificación de la red de *NetMania* en IPv6.

DISEÑO DE LA TRANSICIÓN A IPV6

En esta fase realizaremos el diseño para la transición a IPv6.

DIRECCIONAMIENTO IPV6

TeleNet ISP nos proveerá de un rango de direccionamiento IPv6 y procederá a su registro en RIPE. El prefijo asignado será un /48 de acuerdo con las recomendaciones de IAB /IESG vigentes en la actualidad. Esta longitud de prefijo otorga a NetMania las suficientes redes para el despliegue actual y futuros crecimientos.

En este proyecto propondremos que el segmento asignado por TeleNet ISP a NetMania es el : 2A00:2380:A8::/48

PLAN DE DIRECCIONAMIENTO

El nuevo diseño de la red IPv6 de NetMania no contempla la nueva creación de segmentos de redes IP.

Todas las subredes de NetMania tendrán un prefijo /64.

ESTRUCTURA DEL PLAN DE DIRECCIONAMIENTO

Es adecuado realizar un buen plan de direccionamiento, bajo unos criterios de escalabilidad, organización y jerarquía. Así propondremos el uso de una estructura de direccionamiento que será la siguiente:

Del prefijo de red asignado, disponemos 16 bits para la organización de nuestras subredes. Estos 16 bits los dividiremos en tres bloque, el primero bloque está compuesto por 1 bit y nos indica si las subredes son internas o externas a la organización, para futuros usos como la movilidad IP, el segundo bloque nos servirá para la realización de una división por ubicaciones. Este bloque a su vez se divide en dos bloques de 6 y 2 bits, los primeros 6 bits indica la provincia y los siguientes 2 bits indica el tipo de sede dentro de la provincia. El segundo bloque de 7 bits nos servirá para indicar el numero de la vlan dentro de cada sede. Hemos establecido como premisa para este plan de direccionamiento que la empresa podrá crecer en todas las provincias siempre con el mismo tipo de sedes.

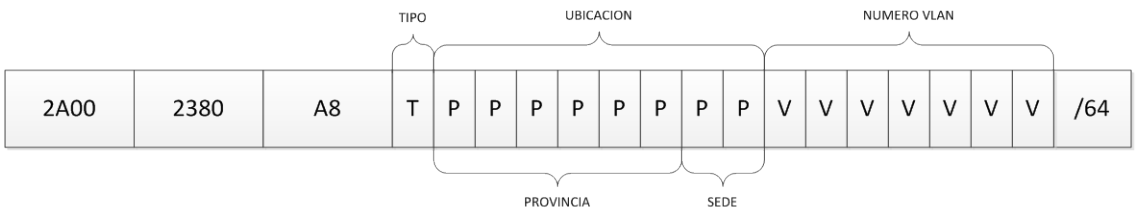


Figura 25 Plan de direccionamiento

Con este plan tendremos que, con el prefijo /55 nos referiremos a todas las redes de una provincia concreta, con el prefijo /57 indicaremos una sede concreta dentro de una provincia y con el prefijo /64 será una red especifica de una sede en una provincia.

La asignación de bits para la ubicación será:

Bits provincia

Provincia	Bits						DEC	HEX
Madrid	0	0	0	0	0	1	1	1
Barcelona	0	0	0	0	1	0	2	2
Sevilla	0	0	0	0	1	1	3	3
Valencia	0	0	0	1	0	0	4	4
Bilbao	0	0	0	1	0	1	5	5

Bits tipo de sede

Tipo de sede	Bits		DEC	HEX
Oficinas Centrales	0	1	1	1
Centro de distribución	1	0	2	2
Tienda	1	1	3	3

Con este plan, si nos quisiéramos referir por ejemplo, a la vlan 10 de la Sede Central de Madrid, el numero de red sería el siguiente:

	Provincia	Sede	VLAN	Dirección de red IPv6
Binario	000001	01	0001010	**000001010001010**

La dirección de la subred IPv6 resultante sería: 2A00:2380:A8:28A::/64

Este plan de direccionamiento nos permite tener 64 provincias, con 4 tipos de sede en cada provincia y con 128 subredes (vlan) en cada sede de 2^{64} dispositivos cada una.

REDES DE ENLACES PUNTO A PUNTO

En la red de NetMania existen varias redes punto a punto, que son las cuales solo tienen dos dispositivos en el segmento de red, como las redes de interconexión de dispositivos de red y los enlaces FR. En los planes de direccionamiento de IPv4, era lo adecuado disponer de un conjunto de redes con una máscara de red /30, que abarcar solo dos direcciones IP, para la asignación a este tipo de redes. Con esto se conseguía un aprovechamiento de las direcciones IP. En IPv6 al seguir con las mismas infraestructuras de red, seguimos que esta demanda de redes con dos únicos dispositivos. Podríamos tomar una red con prefijo /64 y dedicarla para segmentarla en subredes con prefijo /127 y así disponer de una multitud de redes para las conexiones punto a punto. Aunque esto puede parecer lo idóneo, no es así. Tal como se describe en el RFC 3627 dedicado a este tema, utilizar un prefijo /127 para redes punto a punto nos puede ocasionar muchos problemas sino tenemos en cuenta otras consideraciones. El problema radica en la introducción en IPv6 de las direcciones *anycast* de una subred descrito en los RFC 2526 y RFC 2373. Como ya hemos comento las direcciones *anycast* se utilizan para disponer de servicios cercanos a nuestras redes. Estas direcciones *anycast* utilizan unas direcciones especificas para indicar servicios y/o funcionalidades dentro de una subred. El problema de escoger un prefijo /127, es que podemos entrar en conflicto con una dirección *anycast* predeterminada. En un ejemplo, si tomáramos para una red de interconexión entre dos

dispositivos la subred 2A00:2380:A:1C0A:: /127, un dispositivo de un enlace punto a punto tendría la dirección IPv6 2A00:2380:A:1C0A::1/127, y no habría problemas, pero al configurar el otro dispositivo del enlace con la dirección 2A00:2380:A:1C0A::0/127 nos encontraríamos que sería imposible, dado que esta es la dirección *anycast Subnet-Router*. Así nos pasaría con todas las subredes con prefijo /127 que coincidiera con alguna dirección IPv6 *anycast* reservada. Para evitar estos problemas y para adecuarnos a las recomendaciones IAB/IESG, en todos los enlaces punto a punto usaremos subredes con prefijo /64.

Para esto reservaremos la red 2A00:2380:A8:0::/57, dado que nuestro plan de direccionamiento no prevé utilizar esta red. Esto nos permitirá dispone 2^7 subredes para los enlaces punto a punto.

ASIGNACIÓN ESTATICA DE DIRECCIONES IPV6

El actual plan de direccionamiento IPv4, contempla la asignación estática de direcciones IP a dispositivos de red y servidores. Este directriz se seguirá manteniendo con las siguientes consideración:

- Usaremos los caracteres alfabéticos hexadecimales para las direcciones IP estáticas, preferentemente.
- Intentaremos crear nombres o secuencias fáciles de memorizar.
- Los caracteres más fáciles se utilizaran con fines comunes, por ejemplo, la dirección IPv6 terminada en los dígitos hexadecimales BACA, se puede utilizar para todas las puertas de enlaces de las subredes.
- Los dispositivos con múltiples interfaces utilizaran una secuencia consecutiva de caracteres, por ejemplo, 2001:DB8:A:1234::AAAA , 2001:DB8:A:1234::BAAA, 2001:DB8:A:1234::CAAA
- Para aumentar la seguridad en nuestra red, IPv6 nos da la ventaja de que en una única red /64 hay millones de direcciones IP posibles, lo que complica a un atacante la posibilidad de realizar un escaneo de direcciones IP con el fin de encontrar posibles equipos victimas. Está claro que los atacantes intentaran encontrar una manera de cómo evitar esto, y la forma más sencilla, es utilizar la ingeniería social y pensar que los administradores de red pondrán direcciones IP estáticas sencillas para sus dispositivos y servidores, lo que les permitirá localizar fácilmente sus equipos, como por ejemplo, las direcciones IP más baja, :: 1, ::2, ::3, etc. Una manera de evitar que estos sean fácilmente localizados, es incluir en toda nuestra infraestructura un número fijo en el ID interface para todos los dispositivos y servidores. Así, podemos tomar el numero 5AA5 e incluirlo en los primeros 16 bits del identificador de interface. Un ejemplo seria la dirección IP de un servidor Web. Si establecemos que los servidores Web son la dirección IP 2001:DB8:A:1234::BBBx, pues solo debemos agregar el numero elegido al principio del identificador del interface en toda nuestra organización, para ocultar un poco más nuestras direcciones IPv6, que sería de la siguiente manera, 2001:DB8:A:1234:5AA5::BBB1. Ahora un atacante si solo escanease los primeros 2^{16} bits de una subred, no encontraría ningún dispositivo dado que este equipo estaría sobre los 6 trillones de direcciones después.

Una propuesta de direcciones estáticas para los ID interface es:

Descripción	ID Interface
Puerta de enlace de una subred por defecto	BACA
Servidor Web	BBBx
DNS	DDxx
Servidor Base de Datos	BDxx
Interface de enlace punto a punto	1 y 2
Servidor de propósito general	CCxx
Servidor Directorio Activo	ADxx
Servidor FTP	FFxx
IP Gestión de Dispositivo de Red	Ax
Impresora de red	Bx
PC de usuario con IP estática	Exxx

DIRECCIONAMIENTO

Según lo propuesto anteriormente, se propone el siguiente direccionamiento para la red de NetMania incluido en el Anexo 1. Así mismo en el Anexo 4 se muestra el esquema de la red con el direccionamiento IPv6.

METODOS DE TRANSICIÓN

Para una realización progresiva y por etapas de la transición a IPv6, nos basaremos en el modelo de transición de doble pila, que nos permitirá coexistir las redes IPv4 e IPv6 hasta que este ultima este totalmente desplegada, con una única excepción en la red WAN de TeleCom B dado que este proveedor no nos provee de soporte de IPv6 en su red.

Para poder comunicar las tiendas con el resto de sedes e infraestructuras, utilizaremos túneles 6to4. Esto permitirá que nuestra red pueda ser desplegada en IPv6 sin tener en cuenta la red de TeleCom B. Además, cuando en un futuro TeleCom B opere con IPv6, se podrá adaptar a nuestra infraestructura sin ningún tipo de problema.

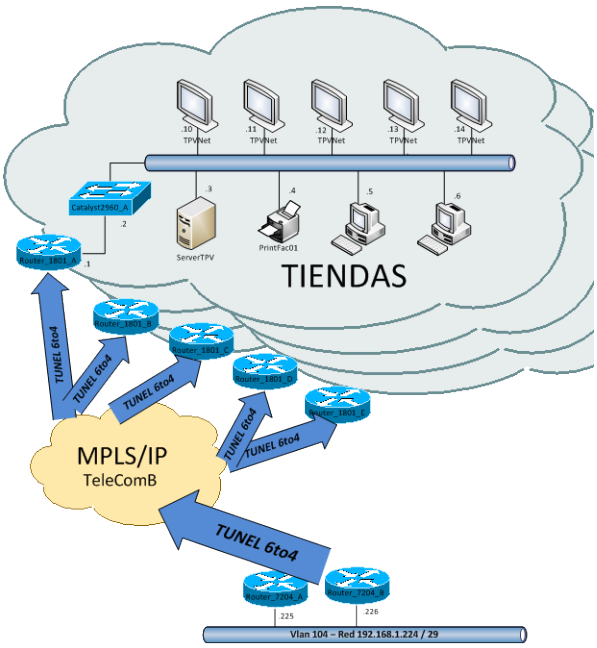


Figura 26 Túneles 6to4 en red WAN TeleCom B

MANTENIMIENTO DE LOS SERVICIOS SOBRE IPV4

Nuestro plan de transición, no puede obviar que cuando se realice todavía quedara más del 84% de los sistemas de Internet sobre IPv4. Para seguir dando servicio a estas redes, nuestro proveedor TeleNet ISP se encargara de realizar la translación NAT64 en su CGN. Así, TeleNet ISP seguirá manteniendo nuestro rango de IP publicas en los CGN conectados a Internet IPv4. Realiza un mapeo en la translación NAT64 para preserva las direcciones IPv4 actuales y en producción de NetMania y traducirlas a las nuevas direcciones IPv6 de los servicios Web.

TeleNet ISP mantendrán dos CGN, uno para las translaciones 6→4 y otro para las translaciones 4 →6 que dependerán de quien inicie la comunicación IP. Un CGN es un dispositivo de red que realiza NAT de forma masiva. Estos dispositivos son ampliamente utilizados por ISP para evitar el agotamiento del direccionamiento IPv4. Un ejemplo de CGN son los utilizados en las redes de telefonía móvil. Con la explosión de los terminales inteligentes para la conexión a Internet y a las redes sociales, los operadores evitan tener que asignar direccionamiento IPv4 publico a estos terminales conectándolos a Internet mediante un CGN. Esto permite que millones de dispositivos móviles con direcciones de clase privada[35] conectarse a Internet con un rango pequeño de direcciones públicas y permitir la conservación de direcciones públicas.

Si una persona en Internet desea conectarse a NetMania, los DNS64 de TeleNet ISP le resolverán la dirección IPv4 publica (194.25.147.209) que esta anunciándose en un CGN. El CGN recibirá la petición de comunicación, y sabrá donde enviarla, dado que tendrá un mapeo de la IPv4 de NetMania a la IPv6 de NetMania. El CGN tendrá un prefijo de red configurado para formar una dirección IPv4 mapeada.

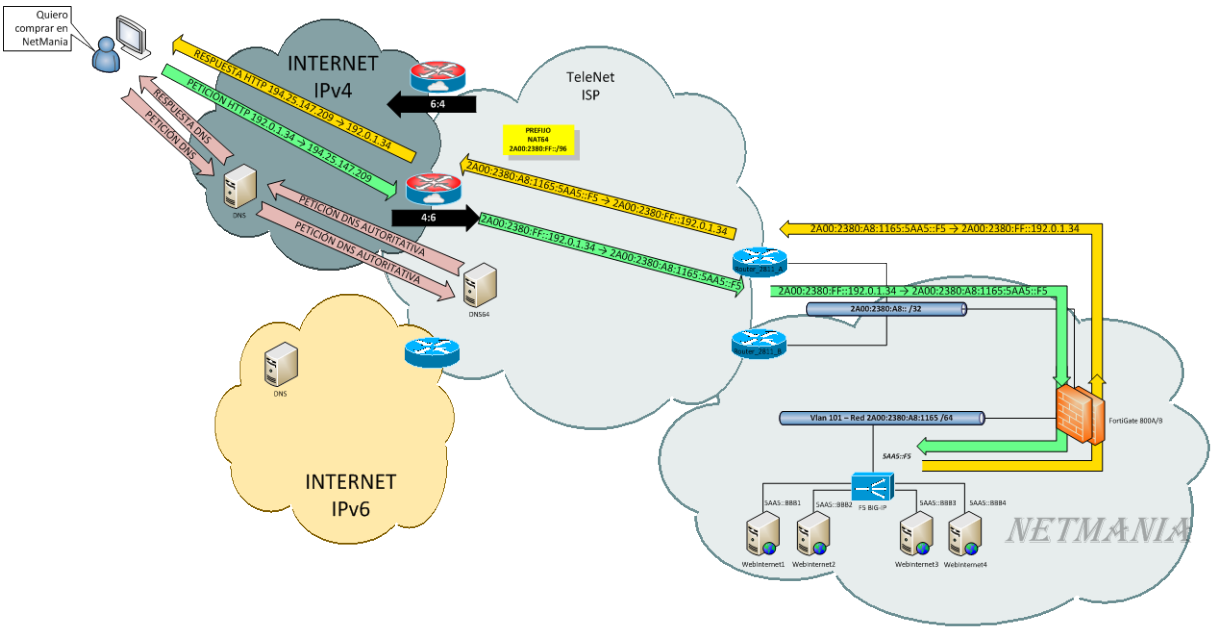


Figura 27 Translación de trafico IPv4 a IPv6

[35] RFC 1918, "Address Allocations for Private Internets"

En la situación inversa, nos encontraremos que desde la red de NetMania necesitaremos conectarnos a servicios en Internet sobre IPv4 existentes en la actualidad y que no están sobre IPv6. Para ello, TeleNet ISP dispone de un segundo CGN para la translación masiva de direcciones IPv6 a IPv4. En este modo no se realiza ningún mapeo estático, sino que al igual en NAT de IPv4 se hace una sobrecarga de direcciones para preservar direccionamiento IPv4. Se dispone de un pool de direcciones IPv4 en el CGN que servirá para realizar la translación 6 →4 sin estado, esto es, al igual que en IPv4 se rompe el modelo *end-to-end*, imposibilitando una comunicación completa entre los nodos.

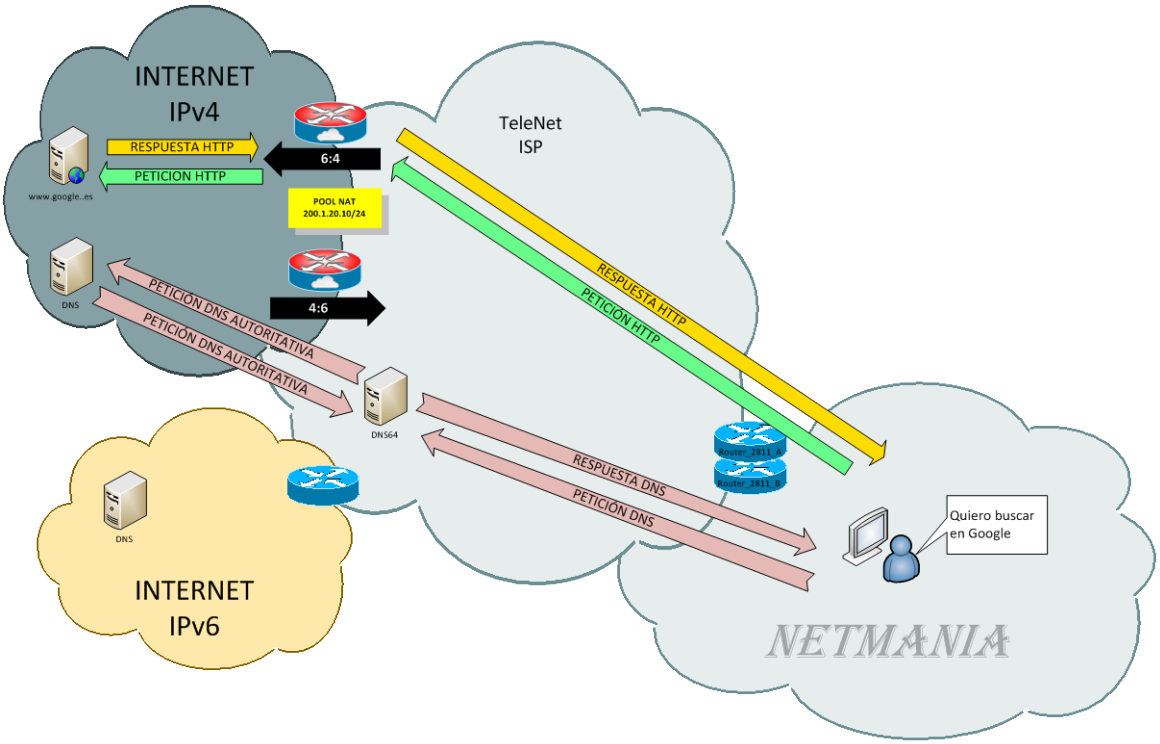


Figura 28 Translación de trafico IPv6 a IPv4

PLANIFICACIÓN DE LA TRANSICIÓN A IPV6

Una vez que hemos realizado el trabajo de cómo será la red de NetMania en IPv6, realizaremos una planificación de los trabajos necesarios para el desarrollo del proyecto.

Dividiremos los trabajos a realizar en EDT y realizaremos una estimación de los tiempos necesarios para la realización de cada EDT y los recursos necesarios para la realización de los mismo.

En plan de proyecto detallado se incluye en el Anexo 3.

RECURSOS HUMANOS

Los recursos humanos necesarios para el desarrollo del proyecto son:

Recurso	Cometido
Jefe de Proyecto	Sera la persona encargada de la gestión del proyecto, cumplimiento de los plazos y calidad, redacción de los documentos y procedimientos así como la asignación de las mismas a los recursos.
Ingeniero de soporte de TeleNet ISP	Persona de apoyo de la compañía TeleNet ISP. Actuara como interlocutor entre su compañía y NetMania, Realizara las operaciones de configuración o las delegara en otros Ingenieros de su compañía.
Ingeniero de soporte de TeleCom B	Persona de apoyo de la compañía TeleCom B. Actuara como interlocutor entre su compañía y NetMania, Realizara las operaciones de configuración o las delegara en otros Ingenieros de su compañía.
Ingeniero de Telecomunicaciones experto en Cisco (CCIE).	Persona encargada de la configuración y administración de todo lo relacionado con equipamiento Cisco.
Ingeniero de Telecomunicaciones experto en F5.	Persona encargada de la configuración y administración de los balanceadores F5
Ingeniero de Telecomunicaciones, experto seguridad en FortiNet y Juniper	Persona encargada de la configuración y administración de los cortafuegos FortiNet y Juniper.
Ingeniero Informático de Sistemas, experto en Linux y Microsoft.	Persona encargada de la configuración y administración de los servidores basados en Linux/Unix y Windows
Técnico de soporte	Persona de soporte de atención a usuarios encargada de configuración de equipos de usuarios basados en Windows.

IMPLANTACIÓN DE IPV6

En esta fase, acometeremos las tareas de configuración de todos los elementos involucrados en la transición a IPv6, esto es, todos aquellos dispositivos que dispongan de una pila TCP/IP según la planificación programada.

CONFIGURACIÓN DE DISPOSITIVOS DE RED

Se deberá especificar cómo se debe adecuar las configuraciones de los dispositivos existentes para que soporte IPv6 en modo de doble pila.

NUCLEO DE RED CATALYST 6505

Primero se deberá activar la capacidad de enrutamiento IPv6 con el comando:

```
Catalyst_6505_CPD#configure terminal
Catalyst_6505_CPD(config)#ipv6 unicast-routing
Catalyst_6505_CPD(config)#ipv6 cef
Catalyst_6505_CPD(config)#end
```

En cada interface de nivel 3 de cada segmento IP se configurara la IPv6 correspondiente.

Vlan 10

```
Catalyst_6505_CPD#configure terminal
Catalyst_6505_CPD(config)#interface vlan 10
Catalyst_6505_CPD(config-if)#ipv6 address 2A00:2380:A8:28A:5AA5::BACA/64
Catalyst_6505_CPD(config)#end
```

Vlan 103

```
Catalyst_6505_CPD#configure terminal
Catalyst_6505_CPD(config)#interface vlan 103
Catalyst_6505_CPD(config-if)#ipv6 address 2A00:2380:A8:2E7:5AA5::BACA/64
Catalyst_6505_CPD(config)#end
```

Vlan 106

```
Catalyst_6505_CPD#configure terminal
Catalyst_6505_CPD(config)#interface vlan 106
Catalyst_6505_CPD(config-if)#ipv6 address 2A00:2380:A8:2EA:5AA5::BACA/64
Catalyst_6505_CPD(config)#end
```

Vlan 110

```
Catalyst_6505_CPD#configure terminal
Catalyst_6505_CPD(config)#interface vlan 110
Catalyst_6505_CPD(config-if)#ipv6 address 2A00:2380:A8:2EE:5AA5::BACA/64
Catalyst_6505_CPD(config)#end
```

Vlan 111

```
Catalyst_6505_CPD#configure terminal
Catalyst_6505_CPD(config)#interface vlan 111
```

```
Catalyst_6505_CPD(config-if)#ipv6 address 2A00:2380:A8:2EF:5AA5::BACA/64
Catalyst_6505_CPD(config)#end
```

Vlan 112

```
Catalyst_6505_CPD#configure terminal
Catalyst_6505_CPD(config)#interface vlan 112
Catalyst_6505_CPD(config-if)#ipv6 address 2A00:2380:A8:2F0:5AA5::BACA/64
Catalyst_6505_CPD(config)#end
```

Se agregaran las rutas IPv6 correspondiente.

```
Catalyst_6505_CPD#configure terminal
Catalyst_6505_CPD(config)#ipv6 route ::/0 2A00:2380:A8:2EA:5AA5::B
Catalyst_6505_CPD(config)#end
```

CORTAFUEGOS

Los cortafuegos que disponemos están configurados en alta disponibilidad, esto es, dos equipos funcionan como uno solo, copiándose la configuración del nodo activo que está funcionando al nodo pasivo que esta de respaldo. Debido a esto solo se deberá configurar el nodo activo para que ambos nodos dispongan de la misma configuración, excepto en la configuración de las IP de gestión que cada dispositivo tiene la suya propia y por tanto se deben configurar en cada uno de ellos.

FORTIGATE 800

Configuraremos IPv6 en los cortafuegos FortiGate 800, para ello habilitamos IPv6 en el cortafuego.

```
FortiGate_A#config system global
FortiGate_A#set gui-ipv6 enable
FortiGate_A#end
```

Configuramos IPv6 en los interfaces Ethernet.

Zona Untrust

```
FortiGate_A#config system interface
FortiGate_A#edit interface_untrust
FortiGate_A#config ipv6
FortiGate_A#set ip6-address 2A00:2380:A8:8000:5AA5::BACA/64
FortiGate_A#end
```

Zona DMZ 1º Nivel

```
FortiGate_A#config system interface
FortiGate_A#edit interface_untrust
FortiGate_A#config ipv6
FortiGate_A#set ip6-address 2A00:2380:A8:2E5:5AA5::BACA/64
FortiGate_A#set ip6-alloaccess ping
FortiGate_A#end
```

Zona Trust

```
FortiGate_A#config system interface
```

```
FortiGate_A#edit interface_untrust
FortiGate_A#config ipv6
FortiGate_A#set ip6-address 2A00:2380:A8:2E9:5AA5::A/64
FortiGate_A#set ip6-alloaccess ping
FortiGate_A#end
```

Gestión (FortiGate_A)

```
FortiGate_A#config system interface
FortiGate_A#edit interface_management
FortiGate_A#config ipv6
FortiGate_A#set ip6-address 2A00:2380:A8:28A:5AA5::A21/64
FortiGate_A#set ip6-allowaccess ping ssh https
FortiGate_A#end
```

Gestión (FortiGate_B)

```
FortiGate_A#config system interface
FortiGate_A#edit interface_management
FortiGate_A#config ipv6
FortiGate_A#set ip6-address 2A00:2380:A8:28A:5AA5::A22/64
FortiGate_A#set ip6-allowaccess ping ssh https
FortiGate_A#end
```

Configuramos enrutamiento IPv6.

```
FortiGate_A#config router static6
FortiGate_A#edit 1
FortiGate_A#set device interface_trust
FortiGate_A#dst 2A00:2380:A8::/49
FortiGate_A#set gateway 2A00:2380:A8:2E9:5AA5::B
FortiGate_A#end
```

Configuramos enrutamiento por OSPFv3 hacia el ISP.

```
FortiGate_A#config router ospf6
FortiGate_A#config area
FortiGate_A#edit 0.0.0.0
FortiGate_A#next
FortiGate_A#end
FortiGate_A#config ospf6-interface
FortiGate_A#edit interface_untrust
FortiGate_A#set area-id 0.0.0.0
FortiGate_A#set interface_trust
FortiGate_A#next
FortiGate_A#set router id 172.0.0.10
FortiGate_A#end
```

SSG140

Configuraremos IPv6 en los cortafuegos SSG140, para ello habilitamos IPv6 en el cortafuego.

```
SSG140_A(Master)#set envar ipv6=yes
SSG140_A(Master)#reset
SSG140_A(Master)#reset save-config yes
```

Configuramos IPv6 en los interfaces Ethernet.

Zona DMZ 2º Nivel

```
SSG140_A(Master)#set interface ethernet4 ipv6 mode router
SSG140_A(Master)#set interface ethernet4 ipv6 enable
SSG140_A(Master)#set interface ethernet4 ipv6 2A00:2380:A8:2E6:5AA5::B/64
SSG140_A(Master)#set interface ethernet4 ipv6 ra transmit
```

Zona WAN

```
SSG140_A(Master)#set interface ethernet3 ipv6 mode router
SSG140_A(Master)#set interface ethernet3 ipv6 enable
SSG140_A(Master)#set interface ethernet3 ipv6 2A00:2380:A8:2E8:5AA5::B/64
SSG140_A(Master)#set interface ethernet3 ipv6 ra transmit
```

Zona Untrust

```
SSG140_A(Master)#set interface ethernet5 ipv6 mode router
SSG140_A(Master)#set interface ethernet5 ipv6 enable
SSG140_A(Master)#set interface ethernet5 ipv6 2A00:2380:A8:2E9:5AA5::B/64
SSG140_A(Master)#set interface ethernet5 ipv6 ra transmit
```

Zona Trust

```
SSG140_A(Master)#set interface ethernet1 ipv6 mode router
SSG140_A(Master)#set interface ethernet1 ipv6 enable
SSG140_A(Master)#set interface ethernet1 ipv6 2A00:2380:A8:2EA:5AA5::B/64
SSG140_A(Master)#set interface ethernet1 ipv6 ra transmit
```

Gestión (SSG140_A)

```
SSG140_A(Master)#set interface ethernet6 ipv6 mode router
SSG140_A(Master)#set interface ethernet6 ipv6 enable
SSG140_A(Master)#set interface ethernet6 ipv6 2A00:2380:A8:28A:A21::B/64
SSG140_A(Master)#set interface ethernet6 ipv6 ra transmit
SSG140_A(Master)#set interface ethernet6 manage ssh
```

Gestión (SSG140_B)

```
SSG140_B(Backup)#set interface ethernet6 ipv6 mode router
SSG140_B(Backup)#set interface ethernet6 ipv6 enable
SSG140_B(Backup)#set interface ethernet6 ipv6 2A00:2380:A8:28A:A22::B/64
SSG140_B(Backup)#set interface ethernet6 ipv6 ra transmit
SSG140_B(Backup)#set interface ethernet6 manage ssh
```

Configuramos enrutamiento IPv6.

```
SSG140_A(Master)#set vrouter trust-vr route ::0/0 interface ethernet5
SSG140_A(Master)#set vrouter trust-vr route 2A00:2380:A8:2E5:0/55 interface ethernet5
SSG140_A(Master)#set vrouter trust-vr route 2A00:2380:A8:300:0/55 interface ethernet3
SSG140_A(Master)#set vrouter trust-vr route 2A00:2380:A8:400:0/55 interface ethernet3
SSG140_A(Master)#set vrouter trust-vr route 2A00:2380:A8:600:0/55 interface ethernet3
SSG140_A(Master)#set vrouter trust-vr route 2A00:2380:A8:800:0/55 interface ethernet3
SSG140_A(Master)#set vrouter trust-vr route 2A00:2380:A8:A00:0/55 interface ethernet3
SSG140_A(Master)#set vrouter trust-vr route 2A00:2380:A8:200:0/55 interface ethernet1
```

Ahora solo se deben modificar las políticas de seguridad que se disponen en IPv4 para que sirvan para IPv6. Para ello solo debemos incluir en la política de IPv4 las direcciones IPv6 correspondientes.

```
SSG140_A(Master)#set policy id:number_policy from zone_source to zone_destination

ipv6_address_source ipv6_address_destination service permit
```

BALANCEADORES

Los balanceadores de trafico F5, se deberán configurarse al igual que otros dispositivos en modo doble-pila para poder balancear peticiones de clientes de Internet entre los cuatros servidores Web de la granja de servidores.

Configuramos los interfaces de nivel 3.

```
***** bigip_base.conf *******
vlan external {
  tag 101
  interfaces 1.1
}
vlan internal {
  tag 100
  interfaces 1.2
}
self 2A00:2380:A8:2E5:5AA5::A {
  netmask ffff:ffff:ffff:ffff::
  vlan external
  allow default
}
self 2A00:2380:A8:2E4:5AA5::B {
  netmask ffff:ffff:ffff:ffff::
  vlan internal
  allow default
}
route default inet6 {
   gateway  2A00:2380:A8:2E5:5AA5::BACA}
```

Configuramos la nueva IPv6 virtual, los nuevos pool de servidores, los servicios y servidores en IPv6.

```
******** bigip.conf  **********
node 2A00:2380:A8:2E5:5AA5::F5 {
  screen VIP-IPv6
}
;  Pools
pool http-ipv6 {
  monitor all http
  members {
     2A00:2380:A8:2E4:5AA5::BBB1.http {}
     2A00:2380:A8:2E4:5AA5::BBB2.http {}
     2A00:2380:A8:2E4:5AA5::BBB3.http {}
     2A00:2380:A8:2E4:5AA5::BBB4.http {}
  }
}
pool https-ipv6 {
  monitor all http
  members {
     2A00:2380:A8:2E4:5AA5::BBB1.https {}
     2A00:2380:A8:2E4:5AA5::BBB2.https {}
     2A00:2380:A8:2E4:5AA5::BBB3.https {}
     2A00:2380:A8:2E4:5AA5::BBB4.https {}
  }
}
;Virtuals Servers
virtual http1-ipv6 {
  pool http-ipv6
  destination 2A00:2380:A8:2E4:5AA5::BBB1.http
  ip protocol tcp
```

```
  persist cookie
  profiles {
     http {}
     tcp {}
  }
}
virtual http2-ipv6 {
  pool http-ipv6
  destination 2A00:2380:A8:2E4:5AA5::BBB2.http
  ip protocol tcp
  persist cookie
  profiles {
     http {}
     tcp {}
  }
}
virtual http3-ipv6 {
  pool http-ipv6
  destination 2A00:2380:A8:2E4:5AA5::BBB3.http
  ip protocol tcp
  persist cookie
  profiles {
     http {}
     tcp {}
  }
}
virtual http4-ipv6 {
  pool http-ipv6
  destination 2A00:2380:A8:2E4:5AA5::BBB4.http
  ip protocol tcp
  persist cookie
  profiles {
     http {}
     tcp {}
  }
}
virtual https1-ipv6 {
  pool https-ipv6
  destination 2A00:2380:A8:2E4:5AA5::BBB1.https
  ip protocol tcp
  persist ssl
  profiles {
     https {}
     tcp {}
  }
}
virtual https2-ipv6 {
  pool https-ipv6
  destination 2A00:2380:A8:2E4:5AA5::BBB2.https
  ip protocol tcp
  persist ssl
  profiles {
     https {}
     tcp {}
  }
}
virtual https3-ipv6 {
  pool https-ipv6
  destination 2A00:2380:A8:2E4:5AA5::BBB3.https
  ip protocol tcp
  persist ssl
  profiles {
     https {}
```

```
      tcp {}
   }
}
virtual https4-ipv6 {
   pool https-ipv6
   destination 2A00:2380:A8:2E4:5AA5::BBB4.https
   ip protocol tcp
   persist ssl
   profiles {
      https {}
      tcp {}
   }
}
```

ENCAMINADORES

Describiremos las configuraciones a realizar en los encaminadores de la red de NetMania.

INTERNET

TeleNet ISP se encargara de configurar los encaminadores Router_2811_A y Router_2811_B. Estos encaminadores serán configurados con OSPFv3 para proveer de tolerancia a fallos en la conexión de Internet. Se propagaran una ruta por defecto hacia la red de NetMania dando al encaminador Router_2811_A menor coste que el encaminador ROUTER_2811_B. En caso de caída del encaminador Router_2811_A, automáticamente se enviará el tráfico hacia el encaminador Router_2811_B.

La configuración de los interfaces del lado de la red de NetMania, se realizara de acuerdo a lo diseñado en este proyecto. La configuración de los interfaces hacia el lado de la red de TeleNet ISP, será de acuerdo al criterio de TeleNet ISP.

Router_2811_A

Activamos la capacidad de enrutamiento IPv6 con el comando:

```
Router_2811_A#configure terminal
Router_2811_A(config)#ipv6 unicast-routing
Router_2811_A(config)#ipv6 cef
Router_2811_A(config)#end
```

Se configurara la dirección IPv6 en el interface correspondiente.

```
Router_2811_A#configure terminal
Router_2811_A(config)#interface fastethernet0/0
Router_2811_A(config-if)#ipv6 address 2A00:2380:A8:8000:5AA5::A/64
Router_2811_A(config)#end
```

Se agregaran las rutas IPv6 correspondiente.

```
Router_2811_A#configure terminal
Router_2811_A(config)#ipv6 route 2A00:2380:A8::/49 2A00:2380:A8:8000:5AA5::BACA
Router_2811_A(config)#end
```

Configuramos el enrutamiento por OSPFv3.

```
Router_2811_A#configure terminal
Router_2811_A(config)#ipv6 router ospf 1
Router_2811_A(config-rtr)#redistribute
Router_2811_A(config-rtr)#router-id 172.0.0.1
Router_2811_A(config-rtr)#exit
Router_2811_A(config)#interface fastethernet0/0
Router_2811_A(config-if)#ipv6 ospf 1 area 0.0.0.0
Router_2811_A(config-if)#ipv6 ospf 1 cost 10
Router_2811_A(config-if)#exit
Router_2811_A(config)#end
```

Router_2811_B

Activamos la capacidad de enrutamiento IPv6 con el comando:

```
Router_2811_B#configure terminal
Router_2811_B(config)#ipv6 unicast-routing
Router_2811_B(config)#ipv6 cef
Router_2811_B(config)#end
```

Se configurara la dirección IPv6 en el interface correspondiente.

```
Router_2811_B#configure terminal
Router_2811_B(config)#interface fastethernet0/0
Router_2811_B(config-if)#ipv6 address 2A00:2380:A8:8000:5AA5::B/64
Router_2811_B(config-if)#end
```

Se agregaran las rutas IPv6 correspondiente.

```
Router_2811_B#configure terminal
Router_2811_B(config)#ipv6 route 2A00:2380:A8::/49 2A00:2380:A8:8000:5AA5::BACA
Router_2811_B(config)#end
```

Configuramos el enrutamiento por OSPFv3 con mayor coste.

```
Router_2811_B#configure terminal
Router_2811_B(config)#ipv6 router ospf 1
Router_2811_B(config-rtr)#redistribute
Router_2811_B(config-rtr)#router-id 172.0.0.2
Router_2811_B(config-rtr)#exit
Router_2811_B(config)#interface fastethernet0/0
Router_2811_B(config-if)#ipv6 ospf 1 area 0.0.0.0
Router_2811_B(config-if)#ipv6 ospf 1 cost 100
Router_2811_B(config-if)#exit
Router_2811_B(config)#end
```

CENTROS DE DISTRIBUCIÓN

La configuración de los encaminadores de la red WAN de los CD será la siguiente:

Encaminador Router_2611_XM en Sede Central:

Activamos la capacidad de enrutamiento IPv6 con el comando:

```
Router_2611XM#configure terminal
Router_2611XM(config)#ipv6 unicast-routing
Router_2611XM(config)#ipv6 cef
Router_2611XM(config)#end
```

Se configurara la dirección IPv6 en el interface correspondiente.

```
Router_2611XM#configure terminal
Router_2611XM(config)#interface fastethernet0/0
Router_2611XM(config-if)#ipv6 address 2A00:2380:A8:2E8:5AA5::CD/64
Router_2611XM(config-if)#exit
Router_2611XM(config)#interface serial0/0.1
Router_2611XM(config-subif)#ipv6 address 2A00:2380:A8:1:5AA5::1/64
Router_2611XM(config-subif)#frame-relay map ipv6 2A00:2380:A8:1:5AA5::2 102
Router_2611XM(config-subif)#exit
Router_2611XM(config)#interface serial0/0.2
Router_2611XM(config-subif)#ipv6 address 2A00:2380:A8:w:5AA5::1/64
Router_2611XM(config-subif)#frame-relay map ipv6 2A00:2380:A8:2:5AA5::2 202
Router_2611XM(config-subif)#exit
Router_2611XM(config)#end
```

Se agregaran las rutas IPv6 correspondiente.

```
Router_2611XM#configure terminal
Router_2611XM(config)#ipv6 route 2A00:2380:A8:300::/52 2A00:2380:A8:1:5AA5::2
Router_2611XM(config)#ipv6 route 2A00:2380:A8:500::/52 2A00:2380:A8:2:5AA5::2
Router_2611XM(config)#ipv6 route ::/0 2A00:2380:A8:2E8:5AA5::BACA
Router_2611XM(config)#end
```

Encaminador Router_2610_A en CD Madrid:

Activamos la capacidad de enrutamiento IPv6 con el comando:

```
Router_2610_A#configure terminal
Router_2610_A(config)#ipv6 unicast-routing
Router_2610_A(config)#ipv6 cef
Router_2610_A(config)#end
```

Se configurara la dirección IPv6 en el interface correspondiente.

```
Router_2610_A#configure terminal
Router_2610_A(config)#interface fastethernet0/0
Router_2610_A(config-if)#ipv6 address 2A00:2380:A8:300:5AA5::BACA/64
Router_2610_A(config-if)#exit
Router_2610_A(config)#interface serial0/0.1
Router_2610_A(config-subif)#ipv6 address 2A00:2380:A8:1:5AA5::2/64
Router_2610_A(config-subif)#frame-relay map ipv6 2A00:2380:A8:1:5AA5::1 101
Router_2610_A(config)#end
```

Se agregaran las rutas IPv6 correspondiente.

```
Router_2610_A#configure terminal
Router_2610_A(config)#ipv6 route ::/0 2A00:2380:A8:1:5AA5::1
Router_2610_A(config)#end
```

Encaminador Router_2610_B en CD Barcelona:

Activamos la capacidad de enrutamiento IPv6 con el comando:

```
Router_2610_B#configure terminal
Router_2610_B(config)#ipv6 unicast-routing
Router_2610_B(config)#ipv6 cef
Router_2610_B(config)#end
```

Se configurara la dirección IPv6 en el interface correspondiente.

```
Router_2610_B#configure terminal
Router_2610_B(config)#interface fastethernet0/0
Router_2610_B(config-if)#ipv6 address 2A00:2380:A8:500:5AA5::BACA/64
Router_2610_B(config-if)#exit
Router_2610_B(config)#interface serial0/0.1
Router_2610_B(config-subif)#ipv6 address 2A00:2380:A8:2:5AA5::2/64
Router_2610_B(config-subif)#frame-relay map ipv6 2A00:2380:A8:2:5AA5::1 201
Router_2610_B(config)#end
```

Se agregaran las rutas IPv6 correspondiente.

```
Router_2610_B#configure terminal
Router_2610_B(config)#ipv6 route ::/0 2A00:2380:A8:2:5AA5::1
Router_2610_B(config)#end
```

TIENDAS

La configuración de los encaminadores WAN que interconecta las tiendas será en modo túnel 6to4. Estas son las configuraciones que se traspasaran al proveedor TeleCom B para que configure los encaminadores correctamente. Necesitamos saber las direcciones IPv4 de cada terminación de los túneles 6to4 y estas han sido remitidas por TeleCom B, las cuales son:

Dirección IP	Asignación
10.250.85.76	Router Central Madrid IP HSRP 7203
10.28.56.45	Router_1801_A (Tienda Madrid)
10.8.56.189	Router_1801_B (Tienda Barcelona)
10.46.203.5	Router_1801_C (Tienda Valencia)
10.41.5.85	Router_1801_D (Tienda Sevilla)
10.48.60.195	Router_1801_E (Tienda Bilbao)

Encaminador Router_7203_A en Sede Central:

Activamos la capacidad de enrutamiento IPv6 con el comando:

```
Router_7203_A#configure terminal
Router_7203_A(config)#ipv6 unicast-routing
Router_7203_A(config)#ipv6 cef
Router_7203_A(config)#end
```

Se configurara la dirección IPv6 en el interface de la red LAN.

```
Router_7203_A#configure terminal
Router_7203_A(config)#interface fastethernet0/1
Router_7203_A(config-if)#ipv6 address 2A00:2380:A8:2E8:5AA5::A/64
Router_7203_A(config-if)#standby 2 ipv6 2A00:2380:A8:2E8:5AA5::AB/64
Router_7203_A(config-if)#standby 2 ipv6 preempt
Router_7203_A(config-if)#standby 2 ipv6 priority 10
Router_7203_A(config-if)#exit
Router_7203_A(config)#end
```

Se configurara el túnel 6to4.

```
Router_7203_A#configure terminal
Router_7203_A(config)#interface tunel1
Router_7203_A(config-if)#ipv6 address 2002:0AFA:554C::/128
Router_7203_A(config-if)#tunnel source interface fa0/0
Router_7203_A(config-if)#tunnel mode ipv6ip 6to4
Router_7203_A(config-if)#exit
Router_7203_A(config)#end
```

Se agregaran las rutas IPv6 correspondiente.

```
Router_7203_A#configure terminal
Router_7203_A(config)#ipv6 route 2002::/16 tunnel1
Router_7203_A(config)#ipv6 route 2A00:2380:A8:380::/52 2002:0A1C:382D::
Router_7203_A(config)#ipv6 route 2A00:2380:A8:580::/52 2002:0A08:38BD::
Router_7203_A(config)#ipv6 route 2A00:2380:A8:780::/52 2002:0A2E:CD05::
Router_7203_A(config)#ipv6 route 2A00:2380:A8:980::/52 2002:0A29:0555::
Router_7203_A(config)#ipv6 route 2A00:2380:A8:B80::/52 2002:0A30:36C3::
Router_7203_B(config)#ipv6 route::/0 2A00:2380:A8:2E8:5AA5::BACA
Router_7203_A(config)#end
```

Encaminador Router_7203_B en Sede Central:

Activamos la capacidad de enrutamiento IPv6 con el comando:

```
Router_7203_B#configure terminal
Router_7203_B(config)#ipv6 unicast-routing
Router_7203_B(config)#ipv6 cef
Router_7203_B(config)#end
```

Se configurara la dirección IPv6 en el interface de la red LAN.

```
Router_7203_B#configure terminal
Router_7203_B(config)#interface fastethernet0/1
Router_7203_B(config-if)#ipv6 address 2A00:2380:A8:2E8:5AA5::B/64
Router_7203_B(config-if)#standby 2 ipv6 2A00:2380:A8:2E8:5AA5::AB/64
Router_7203_B(config-if)#standby 2 ipv6 priority 50
Router_7203_B(config-if)#exit
Router_7203_B(config)#end
```

Se configurara el túnel 6to4.

```
Router_7203_B#configure terminal
Router_7203_B(config)#interface tunel1
Router_7203_B(config-if)#ipv6 address 2002:0AFA:554C::/128
Router_7203_B(config-if)#tunnel source interface fa0/0
Router_7203_B(config-if)#tunnel mode ipv6ip 6to4
Router_7203_B(config-if)#exit
Router_7203_B(config)#end
```

Se agregaran las rutas IPv6 correspondiente.

```
Router_7203_B#configure terminal
Router_7203_B(config)#ipv6 route 2002::/16 tunnel1
Router_7203_B(config)#ipv6 route 2A00:2380:A8:380::/52 2002:0A1C:382D::
Router_7203_B(config)#ipv6 route 2A00:2380:A8:580::/52 2002:0A08:38BD::
Router_7203_B(config)#ipv6 route 2A00:2380:A8:780::/52 2002:0A2E:CD05::
Router_7203_B(config)#ipv6 route 2A00:2380:A8:980::/52 2002:0A29:0555::
Router_7203_B(config)#ipv6 route 2A00:2380:A8:B80::/52 2002:0A30:36C3::
Router_7203_B(config)#ipv6 route::/0 2A00:2380:A8:2E8:5AA5::BACA
Router_7203_B(config)#end
```

Encaminador Router_1801_A en la tienda de Madrid:

Activamos la capacidad de enrutamiento IPv6 con el comando:

```
Router_1801_A#configure terminal
Router_1801_A(config)#ipv6 unicast-routing
Router_1801_A(config)#ipv6 cef
Router_1801_A(config)#end
```

Se configurara la dirección IPv6 en el interface correspondiente.

```
Router_1801_A#configure terminal
Router_1801_A(config)#interface fastethernet0/1
Router_1801_A(config-if)#ipv6 address 2A00:2380:A8:380:5AA5::BACA/64
Router_1801_A(config)#end
```

Se configurara el túnel 6to4.

```
Router_1801_A#configure terminal
Router_1801_A(config)#interface tunel1
Router_1801_A(config-if)#ipv6 address 2002:0A1C:382D::/128
Router_1801_A(config-if)#tunnel source interface fa0/0
Router_1801_A(config-if)#tunnel mode ipv6ip 6to4
Router_1801_A(config-if)#exit
Router_1801_A(config)#end
```

Se agregaran las rutas IPv6 correspondiente.

```
Router_1801_A #configure terminal
Router_1801_A(config)#ipv6 route 2002::/16 tunnel1
Router_1801_A(config)#ipv6 route 2A00:2380:A8:580::/52 2002:0A08:38BD::
Router_1801_A(config)#ipv6 route 2A00:2380:A8:780::/52 2002:0A2E:CD05::
Router_1801_A(config)#ipv6 route 2A00:2380:A8:980::/52 2002:0A29:0555::
Router_1801_A(config)#ipv6 route 2A00:2380:A8:B80::/52 2002:0A30:36C3::
Router_1801_A(config)#ipv6 route ::/0 2002:0AFA:554C
Router_1801_A(config)#end
```

Encaminador Router_1801_B en la tienda de Barcelona:

Activamos la capacidad de enrutamiento IPv6 con el comando:

```
Router_1801_B#configure terminal
Router_1801_B(config)#ipv6 unicast-routing
Router_1801_B(config)#ipv6 cef
Router_1801_B(config)#end
```

Se configurara la dirección IPv6 en el interface correspondiente.

```
Router_1801_B#configure terminal
Router_1801_B(config)#interface fastethernet0/1
Router_1801_B(config-if)#ipv6 address 2A00:2380:A8:580:5AA5::BACA/64
Router_1801_B(config)#end
```

Se configurara el túnel 6to4.

```
Router_1801_B#configure terminal
Router_1801_B(config)#interface tunel1
Router_1801_B(config-if)#ipv6 address 2002:0A08:38BD::/128
Router_1801_B(config-if)#tunnel source interface fa0/0
Router_1801_B(config-if)#tunnel mode ipv6ip 6to4
Router_1801_B(config-if)#exit
Router_1801_B(config)#end
```

Se agregaran las rutas IPv6 correspondiente.

```
Router_1801_B #configure terminal
Router_1801_B(config)#ipv6 route 2002::/16 tunnel1
Router_1801_B(config)#ipv6 route 2A00:2380:A8:380::/52 2002:0A1C:382D::
Router_1801_B(config)#ipv6 route 2A00:2380:A8:780::/52 2002:0A2E:CD05::
Router_1801_B(config)#ipv6 route 2A00:2380:A8:980::/52 2002:0A29:0555::
Router_1801_B(config)#ipv6 route 2A00:2380:A8:B80::/52 2002:0A30:36C3::
Router_1801_B(config)#ipv6 route ::/0 2002:0AFA:554C
Router_1801_B(config)#end
```

Encaminador Router_1801_C en la tienda de Valencia:

Activamos la capacidad de enrutamiento IPv6 con el comando:

```
Router_1801_C#configure terminal
Router_1801_C(config)#ipv6 unicast-routing
Router_1801_C(config)#ipv6 cef
Router_1801_C(config)#end
```

Se configurara la dirección IPv6 en el interface correspondiente.

```
Router_1801_C#configure terminal
Router_1801_C(config)#interface fastethernet0/1
Router_1801_C(config-if)#ipv6 address 2A00:2380:A8:780:5AA5::BACA/64
Router_1801_C(config)#end
```

Se configurara el túnel 6to4.

```
Router_1801_C#configure terminal
Router_1801_C(config)#interface tunel1
Router_1801_C(config-if)#ipv6 address 2002:0A2E:CD05::/128
Router_1801_C(config-if)#tunnel source interface fa0/0
Router_1801_C(config-if)#tunnel mode ipv6ip 6to4
Router_1801_C(config-if)#exit
Router_1801_C(config)#end
```

Se agregara las rutas IPv6 correspondiente.

```
Router_1801_C#configure terminal
Router_1801_C(config)#ipv6 route 2002::/16 tunnel1
Router_1801_C(config)#ipv6 route 2A00:2380:A8:380::/52 2002:0A1C:382D::
Router_1801_C(config)#ipv6 route 2A00:2380:A8:580::/52 2002:0A08:38BD::
Router_1801_C(config)#ipv6 route 2A00:2380:A8:980::/52 2002:0A29:0555::
Router_1801_C(config)#ipv6 route 2A00:2380:A8:B80::/52 2002:0A30:36C3::
Router_1801_C(config)#ipv6 route ::/0 2002:0AFA:554C
Router_1801_C(config)#end
```

Encaminador Router_1801_D en la tienda de Sevilla:

Activamos la capacidad de enrutamiento IPv6 con el comando:

```
Router_1801_D#configure terminal
Router_1801_D(config)#ipv6 unicast-routing
Router_1801_D(config)#ipv6 cef
Router_1801_D(config)#end
```

Se configurara la dirección IPv6 en el interface correspondiente.

```
Router_1801_D#configure terminal
Router_1801_D(config)#interface fastethernet0/1
Router_1801_D(config-if)#ipv6 address 2A00:2380:A8:980:5AA5::BACA/64
```

```
Router_1801_D(config)#end
```

Se configurara el túnel 6to4.

```
Router_1801_D#configure terminal
Router_1801_D(config)#interface tunel1
Router_1801_D(config-if)#ipv6 address 2002:0A29:0555::/128
Router_1801_D(config-if)#tunnel source interface fa0/0
Router_1801_D(config-if)#tunnel mode ipv6ip 6to4
Router_1801_D(config-if)#exit
Router_1801_D(config)#end
```

Se agregara las rutas IPv6 correspondiente.

```
Router_1801_D#configure terminal
Router_1801_D(config)#ipv6 route 2002::/16 tunnel1
Router_1801_D(config)#ipv6 route 2A00:2380:A8:380::/52 2002:0A1C:382D::
Router_1801_D(config)#ipv6 route 2A00:2380:A8:580::/52 2002:0A08:38BD::
Router_1801_D(config)#ipv6 route 2A00:2380:A8:780::/52 2002:0A2E:CD05::
Router_1801_D(config)#ipv6 route 2A00:2380:A8:B80::/52 2002:0A30:36C3::
Router_1801_D(config)#ipv6 route ::/0 2002:0AFA:554C
Router_1801_D(config)#end
```

Encaminador Router_1801_E en la tienda de Bilbao:

Activamos la capacidad de enrutamiento IPv6 con el comando:

```
Router_1801_E#configure terminal
Router_1801_E(config)#ipv6 unicast-routing
Router_1801_E(config)#ipv6 cef
Router_1801_E(config)#end
```

Se configurara la dirección IPv6 en el interface correspondiente.

```
Router_1801_E#configure terminal
Router_1801_E(config)#interface fastethernet0/1
Router_1801_E(config-if)#ipv6 address 2A00:2380:A8:B80:5AA5::BACA/64
Router_1801_E(config)#end
```

Se configurara el túnel 6to4.

```
Router_1801_E#configure terminal
Router_1801_E(config)#interface tunel1
Router_1801_E(config-if)#ipv6 address 2002:0A30:36C3::/128
Router_1801_E(config-if)#tunnel source interface fa0/0
Router_1801_E(config-if)#tunnel mode ipv6ip 6to4
Router_1801_E(config-if)#exit
Router_1801_E(config)#end
```

Se agregara las rutas IPv6 correspondiente.

```
Router_1801_E#configure terminal
Router_1801_E(config)#ipv6 route 2002::/16 tunnel1
Router_1801_E(config)#ipv6 route 2A00:2380:A8:380::/52 2002:0A1C:382D::
Router_1801_E(config)#ipv6 route 2A00:2380:A8:580::/52 2002:0A08:38BD::
Router_1801_E(config)#ipv6 route 2A00:2380:A8:780::/52 2002:0A2E:CD05::
Router_1801_E(config)#ipv6 route 2A00:2380:A8:980::/52 2002:0A29:0555::
Router_1801_E(config)#ipv6 route ::/0 2002:0AFA:554C
Router_1801_E(config)#end
```

CONMUTADORES

Los conmutadores de la red de NetMania, solo requieren configurar una dirección IPv6 de gestión, pero necesaria para poder configurarlos en remoto.

Las configuraciones de los conmutadores en la Sede Central será:

1º Planta

```
Catalyst2960_1#configure terminal
Catalyst2960_1#(config)#interface vlan 10
Catalyst2960_1# (config-if)#ipv6 address 2A00:2380:A8:28A:5AA5::A4/64
Catalyst2960_1# (config-if)#ipv6 enable
Catalyst2960_1# (config-if)#exit
Catalyst2960_1# (config)#ipv6 route ::/0 2A00:2380:A8:28A:5AA5::BACA
Catalyst2960_1#(config)#end
```

2º Planta

```
Catalyst2960_2#configure terminal
Catalyst2960_2#(config)#interface vlan 10
Catalyst2960_2# (config-if)#ipv6 address 2A00:2380:A8:28A:5AA5::A5/64
Catalyst2960_2# (config-if)#ipv6 enable
Catalyst2960_2# (config-if)#exit
Catalyst2960_2# (config)#ipv6 route ::/0 2A00:2380:A8:28A:5AA5::BACA
Catalyst2960_2#(config)#end
```

3º Planta

```
Catalyst2960_3#configure terminal
Catalyst2960_3#(config)#interface vlan 10
Catalyst2960_3# (config-if)#ipv6 address 2A00:2380:A8:28A:5AA5::A6/64
Catalyst2960_3# (config-if)#ipv6 enable
Catalyst2960_3# (config-if)#exit
Catalyst2960_3# (config)#ipv6 route ::/0 2A00:2380:A8:28A:5AA5::BACA
Catalyst2960_3#(config)#end
```

Las configuraciones de los conmutadores en los CD será:

CD Madrid

```
Catalyst2960_A#configure terminal
Catalyst2960_A#(config)#interface vlan 1
Catalyst2960_A# (config-if)#ipv6 address 2A00:2380:A8:301:5AA5::A1/64
Catalyst2960_A# (config-if)#ipv6 enable
Catalyst2960_A# (config-if)#exit
Catalyst2960_A# (config)#ipv6 route ::/0 2A00:2380:A8:301:5AA5::BACA
Catalyst2960_A#(config)#end
```

CD Barcelona

```
Catalyst2960_B#configure terminal
Catalyst2960_B#(config)#interface vlan 1
Catalyst2960_B# (config-if)#ipv6 address 2A00:2380:A8:501:5AA5::A1/64
Catalyst2960_B# (config-if)#ipv6 enable
Catalyst2960_B# (config-if)#exit
Catalyst2960_B# (config)#ipv6 route ::/0 2A00:2380:A8:501:5AA5::BACA
Catalyst2960_B#(config)#end
```

Las configuraciones de los conmutadores en las tiendas será:

Tienda Madrid

```
Catalyst2960_A#configure terminal
Catalyst2960_A#(config)#interface vlan 1
Catalyst2960_A#(config-if)#ipv6 address 2A00:2380:A8:381:5AA5::A1/64
Catalyst2960_A#(config-if)#ipv6 enable
Catalyst2960_A#(config-if)#exit
Catalyst2960_A#(config)#ipv6 route ::/0 2A00:2380:A8:381:5AA5::BACA
Catalyst2960_A#(config)#end
```

Tienda Barcelona

```
Catalyst2960_B#configure terminal
Catalyst2960_B#(config)#interface vlan 1
Catalyst2960_B#(config-if)#ipv6 address 2A00:2380:A8:581:5AA5::A1/64
Catalyst2960_B#(config-if)#ipv6 enable
Catalyst2960_B#(config-if)#exit
Catalyst2960_B#(config)#ipv6 route ::/0 2A00:2380:A8:581:5AA5::BACA
Catalyst2960_B#(config)#end
```

Tienda Sevilla

```
Catalyst2960_C#configure terminal
Catalyst2960_C#(config)#interface vlan 1
Catalyst2960_C#(config-if)#ipv6 address 2A00:2380:A8:781:5AA5::A1/64
Catalyst2960_C#(config-if)#ipv6 enable
Catalyst2960_C#(config-if)#exit
Catalyst2960_C#(config)#ipv6 route ::/0 2A00:2380:A8:781:5AA5::BACA
Catalyst2960_C#(config)#end
```

Tienda Valencia

```
Catalyst2960_D#configure terminal
Catalyst2960_D#(config)#interface vlan 1
Catalyst2960_D#(config-if)#ipv6 address 2A00:2380:A8:981:5AA5::A1/64
Catalyst2960_D#(config-if)#ipv6 enable
Catalyst2960_D#(config-if)#exit
Catalyst2960_D#(config)#ipv6 route ::/0 2A00:2380:A8:981:5AA5::BACA
Catalyst2960_D#(config)#end
```

Tienda Bilbao

```
Catalyst2960_E#configure terminal
Catalyst2960_E#(config)#interface vlan 1
Catalyst2960_E#(config-if)#ipv6 address 2A00:2380:A8:B81:5AA5::A1/64
Catalyst2960_E#(config-if)#ipv6 enable
Catalyst2960_E#(config-if)#exit
Catalyst2960_E#(config)#ipv6 route ::/0 2A00:2380:A8:B81:5AA5::BACA
Catalyst2960_E#(config)#end
```

CONFIGURACIÓN DE SISTEMAS OPERATIVOS

En este punto, se indicara como se deben configurar correctamente los sistemas operativos de servidores y los equipos informáticos de la red de NetMania. No se indicara la configuración de cada servidor, sino la manera de configurar cada uno dependiendo de su sistema operativo. Solo se deberá incluir los parámetros concretos, dirección IPv6, puerta de enlace, etc. de cada servidor para realizar la configuración correcta.

SERVIDORES

Mostraremos como se debe configurar cada tipo de sistema operativo en los servidores correspondientes.

DEBIAN 6.0

Iniciamos sesión como superusuario en el servidor que deseamos configurar.
Editamos el fichero /etc/network/interfaces, donde añadimos la siguiente configuración.

```
# vi /etc/network/interfaces
iface eth0 inet6 static
pre-up modprobe ipv6
address ipv6-address
netmask prefix
gateway ipv6-route default
```

Añadimos los servidores DNS IPv6 al fichero /etc/resolv.conf

```
#vi /etc/resolv.conf
nameserver dns-ipv6-address
```

Restauramos el servicio de red.

```
# /etc/init.d/networking restart
```

SOLARIS 10.0

Iniciamos sesión como superusuario en el servidor que deseamos configurar y creamos un fichero de configuración para una dirección IPv6 para el interface.

```
#touch /etc/hostname6.interface
```

Añadimos la dirección IPv6 al fichero de configuración.

```
#vi /etc/hostname6.interface
inet6 ipv6_address-local-link up
addif inet ipv6-address-global-link up
.....
```

Creamos la ruta IPv6 por defecto

```
#/usr/sbin/route -p add -inet6 default ipv6-route-default
```

Reiniciamos el servidor

```
#reboot -- -r
```

REDHAT 5.3

Iniciamos sesión como superusuario en el servidor que deseamos configurar.
Editamos el fichero /etc/sysconfig/network, donde añadimos la siguiente configuración.

```
# vi /etc/sysconfig/network
NETWORKING= yes
NETWORKING_IPV6= yes
```

Editamos el fichero /etc/sysconfig/network-scripts/init.ipv6-global y añadimos la siguiente configuración.

```
# vi etc/sysconfig/network-scripts/init.ipv6-global
IPV6INIT=yes
IPV6_AUTOCONF=no
IPV6ADDR=ipv6-address/prefix
```

Añadimos los servidores DNS IPv6 al fichero /etc/resolv.conf

```
#vi /etc/resolv.conf
nameserver dns-ipv6-address
```

Creamos la ruta IPv6 por defecto

```
#route -A -inet6 add default gw ipv6-route-default
```

Restauramos el servicio de red.

```
# /etc/init.d/networking restart
```

WINDOWS 2003

Para configurar los servidores Windows 2003 en IPv6, primero debemos instalar la pila del protocolo en el sistema, dado que no viene instalada por defecto, para ello desde el panel de propiedades del interface de red, añadimos el protocolo IPv6.

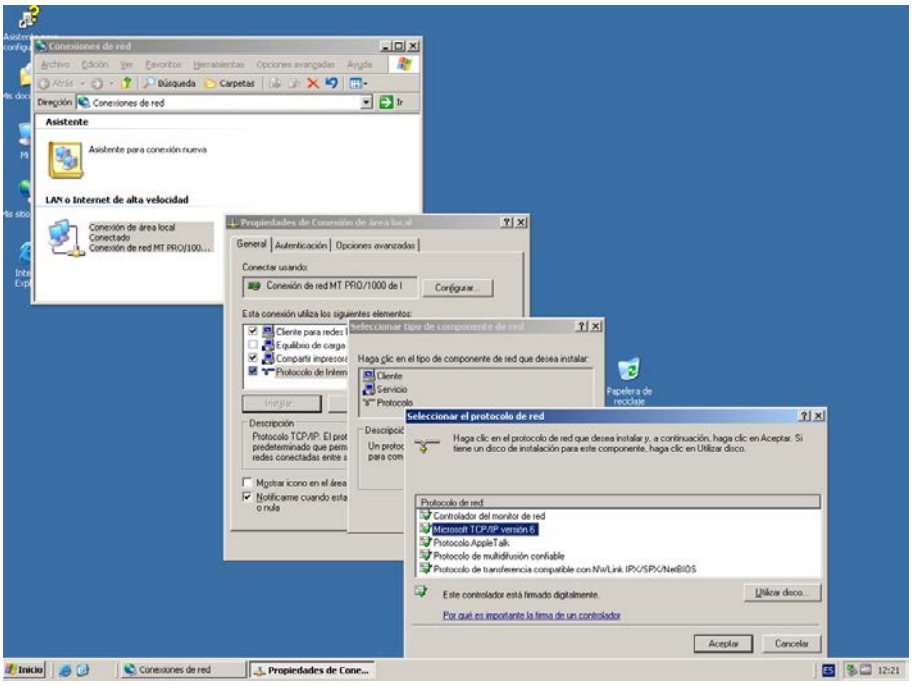


Figura 29 Instalación del protocolo IPv6 en un servidor Windows 2003

Una vez que hemos instalado el protocolo IPv6 en el servidor, debemos configurarlo mediante línea de comandos, para ello ejecutamos el comando ***"cmd"***, y en la ventana de comandos escribimos C:\netsh , para entrar en modo configuración de red.

Para configurar la dirección IPv6, hacemos lo siguiente:

```
netsh> interface ipv6
netsh interface ipv6> add address "nombre_interface" ipv6_address_global_link
```

Configuramos los DNS.

```
netsh interface ipv6> add dns "nombre_interface" dns-ipv6-address
```

La configuración de la ruta por defecto se realizara mediante RA de los encaminadores, para facilitar la autoconfiguración en caso de modificación de la dirección IPv6 de estos.

WINDOWS 2008

En los servidores Windows 2008 viene por defecto instalada la pila IPv6. Para configurar de IPv6 en los servidores Windows 2008 se seguirán los siguientes pasos:

Abrimos Panel de Control → Centro de redes y recursos compartidos.

Pulsamos sobre *Cambiar configuración del adaptador.*

Sobre el interface de red, pulsamos con el botón derecho del ratón y elegimos la opción de *Propiedades*.

En la pantalla de propiedades nos posicionamos sobre el protocolo IPv6 y pulsamos el botón de *Propiedades*.

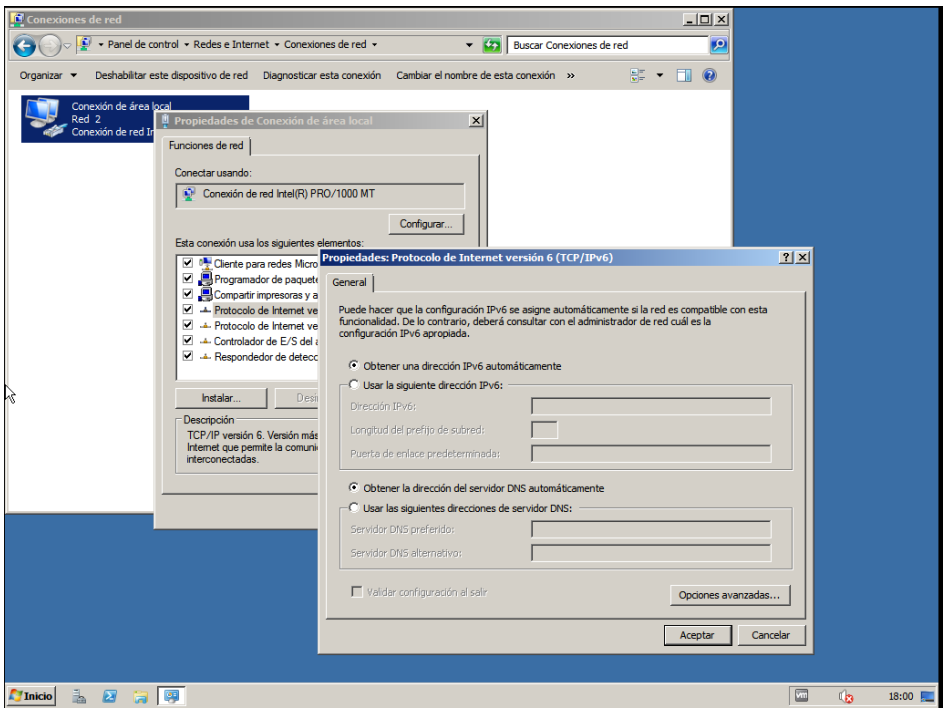


Figura 30 Pantalla de configuración de IPv6 en un servidor Windows 2008

Ahora solo debemos configurar correctamente la dirección IPv6, longitud del prefijo, la puerta de enlace predeterminada y los servidores DNS en IPv6.

Una vez configuradas todas las opciones pulsamos el botón de *Aceptar* y cerramos el resto de ventanas, con lo cual tendremos el protocolo IPv6 funcionando correctamente.

EQUIPOS INFORMATICOS Y TPV

Los equipos informáticos de usuarios así como los TPV, están basado en Windows XP SP3. La manera de configurar IPv6 en estos equipos es similar a la realizada en los servidores Windows 2003.

Para instalar el protocolo IPv6 en el servidor, debemos hacerlo mediante línea de comandos, para ello ejecutamos el comando ***"cmd"***, y en la ventana de comandos escribimos:

```
C:\>ipv6 install
```

Esto provoca que se instale la pila IPv6. Ahora deberemos configurar los equipos dependiendo si la asignación de IP será estática o dinámica. Para equipos que deben tener la IP estática, realizaremos lo siguiente. Desde la ventana de comandos, ejecutamos lo siguiente.

Para configurar la dirección IPv6, hacemos lo siguiente:

```
netsh> interface ipv6
netsh interface ipv6> add address "nombre_interface" ipv6_address_global_link
```

Configuramos los DNS.

```
netsh interface ipv6> add dns "nombre_interface" dns-ipv6-address
```

La configuración de la ruta por defecto se realizara mediante RA de los encaminadores, para facilitar la autoconfiguración en caso de modificación de la dirección IPv6 de estos.

En los equipos que utilicen la autoconfiguración por DHCPv6 no deberemos realizar nada, dado que al instalar la pila IPv6, por defecto esta en modo autoconfiguración.

CONFIGURACIÓN DE SERVICIOS DE RED

DNS

Para configurar el DNS interno para operar correctamente con IPv6 realizaremos las siguientes modificaciones en los ficheros de configuración de BIND. Se da por hecho que el servidor tiene la configuración de doble pila correctamente configurada.

Primero configuramos el servidor para que escuche IPv6, para ello editamos en fichero *named.conf*, y añadimos las siguientes líneas:

```
#vi named.conf
options {
        listen-on-v6 { any; };
};
```

Agregamos los DNS externos para las búsquedas recursivas.

```
#vi named.conf
options {
        forwarders { ipv6_address;};
};
```

Modificamos los ficheros de zona local agregando los registro AAAA concretos.

```
#vi db.netmania.es

$ORIGIN netmania.es
name_server    AAAA    ipv6_address
.....
```

DHCP

Como hemos visto, el servicio DHCP en IPv6 puede ser sustituido por la autoconfiguración sin estado, aunque con limitaciones que deben ser suplidas por un servidor DHCP. En este caso, hemos evaluado la posibilidad de eliminar el servidor de DHCP, para pasar todo este trabajo a la electrónica de red y utilizar el modo de *Stateless+DHCPv6*. En este modo de autoconfiguración sin estado, la electrónica de red , a través de la puerta de enlace de cada segmento IP, proveerá la capacidad de autoconfiguración de equipos , enviando el prefijo de red, MTU y el servidor DHCPv6, que será la misma electrónica de red, y permitirá configurar opciones no disponible por este método. Así, solo deberemos configurar correctamente los interface de nivel 3 del núcleo de red , en la Sede Central y los encaminadores en los CD y tiendas. En el futuro no será necesario el uso de DHCPv6 para que los equipos se puedan autoconfigurar. Esto será posible cuando el RFC 6106 se implemente en los dispositivos, debido que en dicho RFC se define el modo de enviar en mensajes RA, una lista de servidores DNS. El actual servidor de DHCP se reutilizara para en un futuro sea un servidor de monitorización de red basado en NAGIOS.

La configuración en el núcleo de red de la sede Central será:

Primero se deberá activar y configurar el servidor DHCPv6:

```
Catalyst_6505_CPD#configure terminal
Catalyst_6505_CPD(config)#ipv6 dhcp pool IPV6_DHCPPOOL
Catalyst_6505_CPD(config)#domain-name netmania.es
Catalyst_6505_CPD(config)#nameserver 2A00:2380:A8:2E6:5AA5::DD01
Catalyst_6505_CPD(config)#.....(opciones futuras) ......
Catalyst_6505_CPD(config)#end
```

En cada interface de nivel 3 de cada segmento IP con equipos informáticos configuramos:

Vlan 110

```
Catalyst_6505_CPD#configure terminal
Catalyst_6505_CPD(config)#interface vlan 110
Catalyst_6505_CPD(config-if)#ipv6 nd other_config_flag
Catalyst_6505_CPD(config-if)#ipv6 dhcp server IPV6_DHCPPOOL
Catalyst_6505_CPD(config)#end
```

Vlan 111

```
Catalyst_6505_CPD#configure terminal
Catalyst_6505_CPD(config)#interface vlan 110
Catalyst_6505_CPD(config-if)#ipv6 nd other_config_flag
Catalyst_6505_CPD(config-if)#ipv6 dhcp server IPV6_DHCPPOOL
Catalyst_6505_CPD(config)#end
```

Vlan 112

```
Catalyst_6505_CPD#configure terminal
Catalyst_6505_CPD(config)#interface vlan 110
Catalyst_6505_CPD(config-if)#ipv6 nd other_config_flag
Catalyst_6505_CPD(config-if)#ipv6 dhcp server IPV6_DHCPPOOL
Catalyst_6505_CPD(config)#end
```

En el restos de encaminadores, tanto en CD como en tiendas configuraremos los siguientes parámetros:

```
encaminador#configure terminal
encaminador(config)#ipv6 dhcp pool IPV6_DHCPPOOL
encaminador(config)#domain-name netmania.es
encaminador(config)#nameserver 2A00:2380:A8:2E6:5AA5::DD01
encaminador(config)#interface fastethernet0/0
encaminador(config-if)#ipv6 nd other_config_flag
encaminador(config-if)#ipv6 dhcp server IPV6_DHCPPOOL
encaminador(config)#end
```

PROXY

Dado que en IPv6 no sea implementado NAT nativo, esto es, NAT entre redes IPv6, (no lo confundamos con NAT entre redes IPv6 e IPv4 como hemos visto anteriormente), esta funcionalidad no será usada en redes IPv6, por lo cual su función se reducirá a cache y filtrado de contenidos.

Para ello solo deberemos incluir en el fichero de configuración, las mismas reglas que con IPv4, pero en formato de IPv6, de la siguiente manera:

```
#vi squid.conf
acl localnet_ipv6 src 2A00:2380:A8::/48
http_access allow localnet_ipv6
```

IMPRESIÓN EN RED

Debido a que debemos sustituir todos los dispositivos JetDirect para impresión mediante LPR, deberemos configurar de nuevo todos los JetDirect con la IPv4 actual y la IPv6 asignada. Para ello se utilizara los menus[36] incorporados en las impresoras para la configuración del interface MIO (JetDirect Interno).

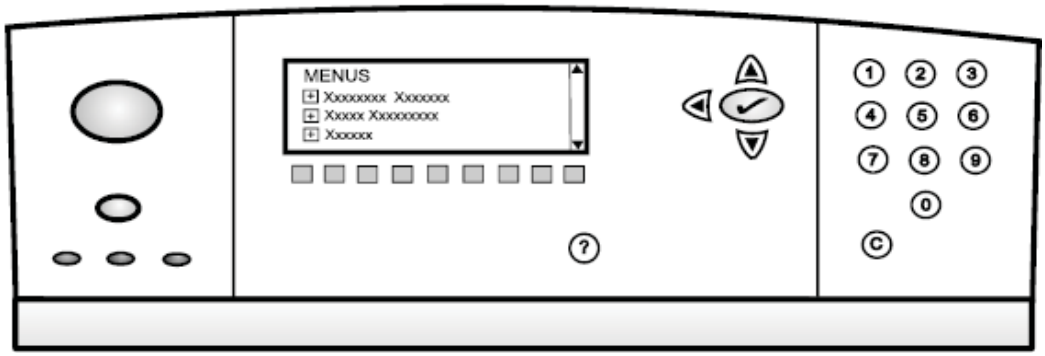


Figura 31 Panel de control de JetDirect mediante menús.

La configuración de los dispositivos JetDirect 635 mediante los menús, se realizara de la siguiente manera:

```
Menú Principal        →Sub-menus            Valor.(Descripción)
-------------------------------------------------------------------------------
  TCP/IP
    |------------->Enable                   ON. Activamos el protocolo TCP/IP.
    |
    |------------->IPv4 Settings -->Config Method
    |                                    |
    |                                    |
    |                                Manual Settings
    |                                    |
    |                                    |-->Manual. Configuración de IPv4.
    |                                    |
    |                                    |-->Default IP. Dirección IPv4.
    |                                    |
    |                                    |-->Subnet Mask. Mascara de red IPv4.
    |                                    |
    |                                    |-->Default Gateway. Puerta de enlace IPv4.
    |
    |
    |--------> IPv6 Settings ---->Enable --> ON. Activa IPv6
                        |
                        |
                        |-------> Manual Settings
                                          |
                                          |
                                          |-->Enable. Configuración de IPv6.
                                          |
```

[36] http://h20000.www2.hp.com/bizsupport/TechSupport/CoreRedirect.jsp?redirectReason=DocIndexPDF&prodSeriesId=500078&targetPage=http%3A%2F%2Fbizsupport1.austin.hp.com%2Fbc%2Fdocs%2Fsupport%2FSupportManual%2Fc00399328%2Fc00399328.pdf

```
                    |-->Address. Dirección IPv6.
              DHCPv6 Policy
                    |
                    |-->Router Speficied. Puerta de enlace IPv6.
```

Solo será necesario configurar estos parámetros, con los datos concretos de cada impresora, dado que el resto son innecesarios para poder imprimir mediante LPR.

VERIFICACIÓN DE LA OPERATIVIDAD DE IPV6

Una vez que se realice todo la implantación en las infraestructuras de red de la pila IPv6 y con todos los dispositivos y equipos operando modo de doble pila se realizaran las verificaciones necesarias para realizar la aceptación de la operatividad de la red de NetMania sobre IPv6. Utilizaremos una serie de herramientas, como generadores de trafico IPER, equipos Windows para emular a los clientes y analizadores de red como WireShark para comprobar que las pruebas se realizan correctamente y se obtienen los resultados deseados. Las listas de verificaciones a realizar son:

1. Configuración de IPv6 mediante DHCPv6.
   Se comprobara que los equipos informáticos que deben configurar sus dirección IPv6 de forma automática, lo hacen correctamente. Se simularan situaciones donde la carga de tráfico en la redes es media-alta.
2. Resolución DNS de nombres IPv6 e IPv4.
   Se comprobara que desde los equipos informáticos y servidores se resuelve correctamente nombres de dominio locales y de Internet mediante el DNS local. Además se comprobara la correcta operatividad de la translación de nombres bajo DNS64.
3. Operatividad de la Intranet Corporativa.
   Dado que todas las aplicaciones de gestión corporativa se ejecutan en el servidor WebIntranet, sobre un servidor Web Apache 2.0, se comprobara que los distintos navegadores del mercado, como Internet Explorer, Mozilla Firefox y Chrome, pueden acceder correctamente a las aplicaciones Web mediante IPv6. Se deberá comprobar que las aplicaciones Web, tienen configurado las llamadas mediante nombres DNS y no mediante direcciones IPv4.
4. Operatividad de la navegación hacia Internet.
   Con los mismos navegadores que indicamos en el punto anterior, se comprobara que se navega correctamente a Internet, tanto directamente como utilizando el servidor cache ProxyInternet.
5. Operatividad del correo corporativo.
   Se comprobara que los servidores de correo electrónico, pueden enviar y recibir mensajes utilizando el cliente de correo electrónico corporativo (Outlook 2007) e IPv6. Se deberá utilizar registros DNS para correo que solo resuelvan direcciones IPv6.
6. Simulación de carga de trafico de Internet hacia los servidores Web.
   Mediante la instalación de una serie de equipos de generación de tráfico en la parte WAN de Internet (con la ayuda de TeleNet ISP), se generara trafico IPv6 para comprobar el correcto funcionamiento de los cortafuegos, balanceadores y servidores Web.
7. Impresión bajo IPv6.
   Se enviaran trabajos de impresión a las impresoras de red bajo IPv6, para comprobar su correcto funcionamiento.
8. Transferencias FTP
   Se comprobara que es posible el envió de fichero mediante IPv6 de los diferentes servidores FTP de la empresa.
9. Terminales TPV
   Se comprobara el correcto funcionamiento de los terminales TPV bajo IPv6.

OPERACIÓN EN IPV6

Una vez realizada las labores de verificación de la operatividad de IPv6 en la red de NetMania, solo nos queda pasar dicho entorno a producción. Para ello nos basaremos en los DNS tanto interno como externos, dado que ellos serán los encargados de indicar a los clientes con tipo de dirección IP trabajar.

La primera labor será eliminar de los DNS internos todos los registros A de los servicios que utilizamos como Web, Correo, FTP, etc.

Una vez realizado esto, TeleNet ISP deberá realizar lo cambio en su entorno, necesario para que los usuarios en Internet IPv4 puedan conectarse a los servicios Web de NetMania. Para ellos se realizaran las siguientes tareas:

- Inclusión en el DNS64 de TeleNet ISP, de la zona NetMania.
- Inclusión en esta zona de los registros A del NAT64.
- Creación de los registros AAAA de NetMania, Web y SMTP.

Todos estos trabajos se realizan fuera del horario normal y preferentemente entre 3 y 5 A.M que es cuando menos actividad de usuarios hay.

Una vez, que la red este operativa en IPv6, solo nos quedara ir deshabilitando las pilas IPv4 de los dispositivos en la medida de lo posible, dado que puede haber equipos que necesiten siempre IPv4 para funcionar correctamente.

Con todo esto, habremos llegado a la parte final del proyecto ,donde solo nos quedara la realizar la transferencia de conocimientos al resto de personal técnico, tanto de telecomunicaciones como de sistemas y la realización de la documentación pertinente para dejar correctamente documentado el entorno de red IPv6.

MANUAL DE BUENAS PRACTICAS EN IPV6

En este nuevo entorno, deberemos seguir una serie de buenas prácticas y recomendaciones para mantener un entorno de red seguro y estable.

- Todos las subredes serán de 64 Bits en direcciones host.
- Usar dígitos hexadecimales fácilmente reconocibles para facilitar la localización de redes.
- Utilizar un prefijo en el ID Interface, para evitar direcciones IPv6 sencillas y fáciles de encontrar por atacantes a nuestra red.
- Utilizar el método de configuración sin estado en la medida de lo posible, para facilitar la renumeración de redes.
- En redes que no requieren conectividad total (con Internet) y que requiere un plus de seguridad, como las redes de gestión, utilizaremos el prefijo de direcciones locales únicas (ULA's) FC00::/7.
- En los encaminadores y cortafuegos se bloquearan los prefijos no enrutables por Internet, como las direcciones ULA, de documentación, etc. y se descartara este tráfico para evitar ruido de fondo.
- Seleccionar correctamente el filtrado del trafico ICMPv6. Dado que no podemos fragmentar los paquetes IPv6 y es necesario utilizar "*Path MTU Discovery*" mediante ICMPv6, habrá que habilitar este en los cortafuegos y encaminadores y deshabilitar otros ICMPv6 que no sean necesarios.

ESTIMACIÓN ECONÓMICA

La propuesta económica para realizar la transición de IPv4 a IPv6 la dividiremos en recursos humanos y materiales.

RECURSOS HUMANOS

Realizaremos una valoración del coste de los recursos necesarios para la ejecución del proyecto.

Recurso	Cantidad	Precio/unidad	Total
Ingeniero de soporte de TeleNet ISP	52	120 € - 60%	2.496 €
Ingeniero de Telecomunicaciones experto en Cisco (CCIE).	106	140 €	14.840 €
Ingeniero de Telecomunicaciones experto en F5.	64	80 €	5.120 €
Ingeniero de Telecomunicaciones experto en FortiGate y Juniper	100	124 €	12.400 €
Ingeniero Informático de Sistemas experto en Linux y Microsoft.	118	100 €	11.800 €
Técnico de soporte	124	55 €	6.820 €
Total Recursos			53.476 €

RECURSOS MATERIALES

Realizaremos una valoración los materiales y equipos necesarios para la ejecución del proyecto.

Recurso	Cantidad	Precio/unidad	Total
Actualización de memoria Flash a 48 MB para Cisco 2610	2	87	174 €
Cisco Catalyst 2960 24 Puertos 10/100/1000 Mbps	2	975 €	1.950 €
HP JetDirect 635N	11	477 €	5.247 €
Total material			7.398 €

El coste total del proyecto de la transición de la redes de la empresa NetMania de IPv4 a IPv6 sería de 60.874 €

GLOSARIO

TFC: Trabajo de Fin de Carrera.

IETF: Internet Enginer Task Force.

IANA: Internet Asignament Number .

RIR: Regional Internet Registrer.

LIR/ISP: Local Internet Registrer / Internet Service Provider.

RFC: Request For Comment.

IPv4: Internet Protocol versión 4.

IPv6: Internet Protocol versión 6.

VLSM: Variable Lenght Subnet Mask.

CIDR: Classless Inter Domain Routing.

ULA: Unique Local Unicast.

TIC: Tecnologías de la Informática y las Comunicaciones.

IGP: Internal Gateway Protocol.

NTP: Network Time Protocol.

CPE: Customer Premises Equipment.

HSRP: Hot Standby Router Protocolo.

MAC: Media Access Control.

NAT: Network Address Translation.

IOS: Internetworking Operating System.

LPD: Line Printer Daemon Protocol.

VIP: Virtual IP Address.

CGN: Carrier-grade NAT.

BIBLIOGRAFICA

- Inventing the Internet. Janet Abbate Cambridge (Mass.) MIT Press, cop. 1999 ISBN 0262011727.
- IPv6 para Todos. Guillermo Cicleo, Roque Gadliano, Chistian O'Flaherty, Cesar Olvera, Jordi Palet, Marlela Rocha, Alvaro Vives. ISOC.Ar. 2009. ISBN 978-987-25392-1-4.
- Global IPv6 Strategies: From Business Analysis to Operational Planning. Patrick Grossetete, Ciprian Popoviciu, Fred Wettling. Cisco Systems, Inc. 2008. ISBN 978-1-58705-343-6.
- DNS and BIND on IPv6. Cricket Liu. O'Reilly Media, Inc. Mayo 2011. ISBN 978-1-4493-0519-2.
- Preparing an IPv6 Addressing Plan. http://www.surfnet.nl/Documents/handleiding_201012_IPv6_nummerplan_EN.pdf. SURFnet. Marzo 2011.
- ARIN: The IANA IPv4 Address Free Pool Is Now Depleted: https://www.arin.net/knowledge/v4-v6.html
- APNIC IPv4 exhaustion: http://www.apnic.net/community/ipv6-program/ipv4-exhaustion
- RIPE Network Coordination Centre: http://www.ripe.net/
- [RFC 791] "Internet Protocol" , Defense Advanced Research Projects Agency, Septiembre 1981.
- [RFC 1918] "Address Allocations for Private Internets", Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, E. Lear. Febrero 1996.
- [RFC2373] "IP Version 6 Addressing Architecture", R. Hinden, S. Deering. Julio 1998.
- [RFC 2460] "Internet Protocol, Version 6 (IPv6) Specification", R. Hinden, S. Deering. Diciembre 1998.
- [RFC 2526] "Reserved IPv6 Subnet Anycast Addresses", D. Jonhson, S. Deering. Marzo 1999.
- [RFC 3177] "IAB/IESG Recommendations on IPv6 Addrress Allocations to Site", IAB, IESG. Septiembre 2001.
- RFC 3306] "Unicast-Prefix-based IPv6 Multicast Address", B. Haberman, D. Thaler. Agosto 2002
- [RFC 3315] "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, M. Carney. Julio 2003.
- [RFC 3578] "IPv6 Global Unicast Address Format", R. Hinden, S. Deering, E. Nordmark. Agosto 2003.
- [RFC 3596] "DNS Extensions to Support IP Version 6", S. Thomson, C. Huitema, V. Ksinant, M. Souissi. Octubre 2003.
- [RFC 3627] "Use of /127 Prefix Length Between Routers Considered Harmful", P. Savola. Septiembre 2003.
- [RFC 3849] "Pv6 Address Prefix Reserved for Documentation", M. Huston, A. Lord, p: Smith. Julio 2004.
- [RFC 3879] "Deprecating Site Local Addresses", C. Huitema, B. Carpenter. Septiembre 2004.

- [RFC 3964] "Security Considerantions for 6to4", P. Savola, C. Patel. Diciembre 2004.
- [RFC 4193] "Unicast-Prefix-based IPv6 Multicast Address", B. Haberman, D. Thaler. Agosto 2002.
- [RFC 4213] "Basic Transition Mechanisms for IPv6 Hosts and Routers", E. Nordmark, R. Gilligan. Octubre 2005.
- [RFC 4291] " IP Version 6 Addressing Architecture", R. Hinden, S. Deering. Febrero 2006.
- [RFC 4472] "Operational Considerations and Issues with IPv6 DNS", A. Durand, J. Ihren, P. Savola. Abril 2006.
- [RFC 4786] "Operation of anycast services", J. Abley, K. Lindqvist. Diciembre 2006.
- [RFC4861] "Neighbor Discovery for IP version 6 (IPv6)", T. Narten, E. Nordmark, W. Simpson, H. Soliman. Septiembre 2007.
- [RFC4862] "IPv6 Stateless Address Autoconfiguration", S. Thomson, T. Narten, T. Jinmei. Septiembre 2007.
- [RFC4966] " Reasons to Move the Network Address Translator-Protocol Translator (NAP-PT) to Historic Status". Julio 2007
- [RFC 5156] "Special-Use IPv6 Address", M. Blanchet. Abril 2008.
- [RFC 6106] "IPv6 Router Advertisement Options for DNS Configuration", J. Jeong, S. Park, L. Beloeil, S. Madanapalli. Noviembre 2010.
- [RFC 6052] "IPv6 Addressing of IPv4/IPv6 Translators", C. Bao, C. Huitema, M. Bagnulo, M. Boucadair, X. Li. Octubre 2002.
- [RFC 6144] "Framework for IPv4/IPv6 Translation", F. Baker, X. Li, K. Yin. Abril 2011.
- [RFC 6145] "IP/ICMP Translation Algorithm", X. Li, C. Bao, F. Baker. Abril 2011.
- [RFC 6146] "Stateful NAT64: Interwork Address and Protocol Translation from IPv6 Clients to IPv4 Servers", M. Bagnulo, P. Matthews, I. van Beijnum. Abril 2011.
- [RFC 6147] "DNS64: DNS Extensions for Interwork Address Tranlation from IPv6 Clients to IPv4 Servers".
- [RFC 6343] "Advisory Guidelines for 6to4 Deployment", B. Carpenter. Agosto 2011.

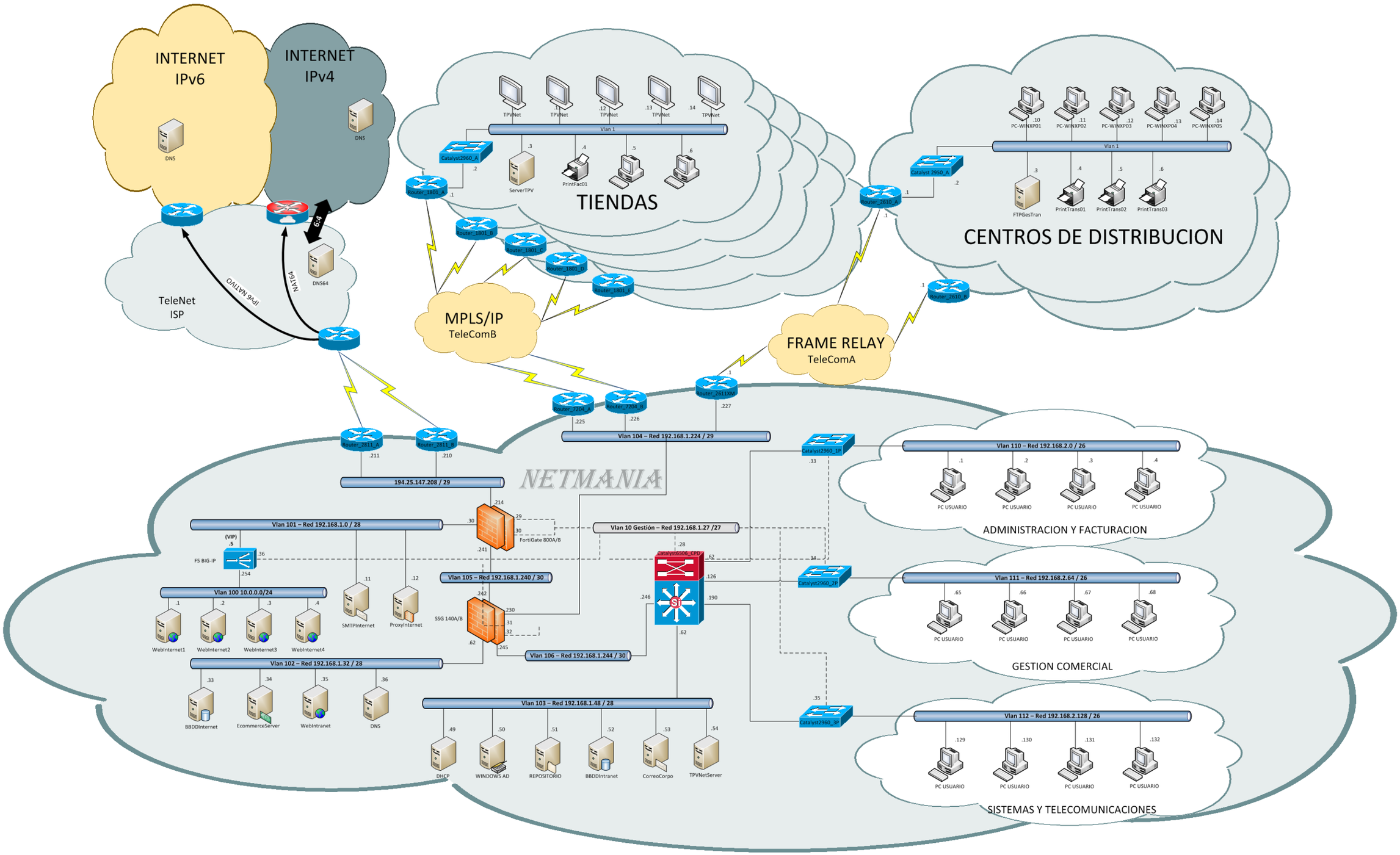
ANEXOS

1.- DIRECCIONAMIENTO IPV6 RED NETMANIA

Red	Subred	Dirección IP	Descripción
2A00:2380:A8:280::/57 Oficinas Centrales Madrid	2A00:2380:A8:2E4::/64 Vlan 100	2A00:2380:A8:2E4:5AA5::BACA	Balanceador F5
		2A00:2380:A8:2E4:5AA5::BBB1	WebInternet 1
		2A00:2380:A8:2E4:5AA5::BBB2	WebInternet 2
		2A00:2380:A8:2E4:5AA5::BBB3	WebInternet 3
		2A00:2380:A8:2E4:5AA5::BBB4	WebInternet 4
	2A00:2380:A8:2E5::/64 Vlan 101	2A00:2380:A8:2E5:5AA5::BACA	Puerta de enlace Vlan 101
		2A00:2380:A8:2E5:5AA5::B1	Balanceador F5
		2A00:2380:A8:2E5:5AA5::CAFE	SMTPInternet
		2A00:2380:A8:2E5:5AA5::AAAA	ProxyInternet
	2A00:2380:A8:2E6::/64 Vlan 102	2A00:2380:A8:2E6:5AA5::BACA	Puerta de enlace Vlan 102
		2A00:2380:A8:2E6:5AA5::DD01	DNSv6
		2A00:2380:A8:2E6:5AA5::BBB1	WebIntranet
		2A00:2380:A8:2E6:5AA5::CC01	EcommenServer
		2A00:2380:A8:2E6:5AA5::BD01	BBDDInternet
	2A00:2380:A8:2E7::/64 Vlan 103	2A00:2380:A8:2E7:5AA5::BACA	Puerta de enlace Vlan 103
		2A00:2380:A8:2E7:5AA5:CC01	Nagios
		2A00:2380:A8:2E7:5AA5::AD01	Windows AD
		2A00:2380:A8:2E7:5AA5::CC02	Repositorio
		2A00:2380:A8:2E7:5AA5::BD01	BBDDIntraNet
		2A00:2380:A8:2E7:5AA5::CC03	CorreoCorpo
		2A00:2380:A8:2E7:5AA5::CC04	TPVNetServer
	2A00:2380:A8:2E8::/64 Vlan 104	2A00:2380:A8:2E8:5AA5::BACA	Puerta de enlace Vlan 104
		2A00:2380:A8:2E8:5AA5::A	Router_7203_A
		2A00:2380:A8:2E8:5AA5::B	Router_7203_B
		2A00:2380:A8:2E8:5AA5::AB	Router_7203_HSRP
		2A00:2380:A8:2E8:5AA5::CD	Router_2611XM
	2A00:2380:A8:2E9::/64 Vlan 105	2A00:2380:A8:2E9:5AA5::A	FortiGate 800
		2A00:2380:A8:2E9:5AA5::B	SSG140
	2A00:2380:A8:2EA::/64 Vlan 106	2A00:2380:A8:2EA:5AA5::A	Catalyst6506_CPD
		2A00:2380:A8:2EA:5AA5::B	SSG140
	2A00:2380:A8:2EE::/64 Vlan 110	2A00:2380:A8:2EE:5AA5::	Gateway Vlan 112
		2A00:2380:A8:2EE:+DHCPv6	PC Usuarios
	2A00:2380:A8:2EF::/64 Vlan 111	2A00:2380:A8:2EF:5AA5::	Gateway Vlan 112
		2A00:2380:A8:2EF:+DHCPv6	PC Usuarios
	2A00:2380:A8:2F0::/64 Vlan 112	2A00:2380:A8:2F0:5AA5::BACA	Gateway Vlan 112
		2A00:2380:A8:2F0:+DHCPv6	PC Usuarios
	2A00:2380:A8:28A::/64 Vlan 10 Gestión Dispositivos de red	2A00:2380:A8:28A:5AA5::BACA	Catalyst6506_CPD
		2A00:2380:A8:28A:5AA5::A21	FortiGate 800_A
		2A00:2380:A8:28A:5AA5::A22	FortiGate 800_B
		2A00:2380:A8:28A:5AA5::A31	SSG140_A
		2A00:2380:A8:28A:5AA5::A32	SSG140_B
		2A00:2380:A8:28A:5AA5::F5	Balanceador F5
		2A00:2380:A8:28A:5AA5::A4	Catalyst2960_1P
		2A00:2380:A8:28A:5AA5::A5	Catalyst2960_2P
		2A00:2380:A8:28A:5AA5::A6	Catalyst2960_3P
2A00:2380:A8:300::/57 CD Madrid	2A00:2380:A8:301::/64 Vlan 1	2A00:2380:A8:301:5AA5::BACA	Router_2610_A
		2A00:2380:A8:301:5AA5::F1	FTPGestTran
		2A00:2380:A8:301:5AA5::A1	Catalyst2960_A
		2A00:2380:A8:301:5AA5::B1	PrintTrans01
		2A00:2380:A8:301:5AA5::B2	PrintTrans02
		2A00:2380:A8:301:5AA5::B3	PrintTrans03
		2A00:2380:A8:301:5AA5::Exxx	PC Usuarios
2A00:2380:A8:500::/52 CD Barcelona	2A00:2380:A8:501::/64 Vlan 1	2A00:2380:A8:501:5AA5::BACA	Router_2610_B
		2A00:2380:A8:501:5AA5::F1	FTPGestTran
		2A00:2380:A8:501:5AA5::A1	Catalyst2960_B
		2A00:2380:A8:501:5AA5::B1	PrintTrans01
		2A00:2380:A8:501:5AA5::B2	PrintTrans02
		2A00:2380:A8:501:5AA5::B3	PrintTrans03
		2A00:2380:A8:501:5AA5::Exxx	PC Usuarios

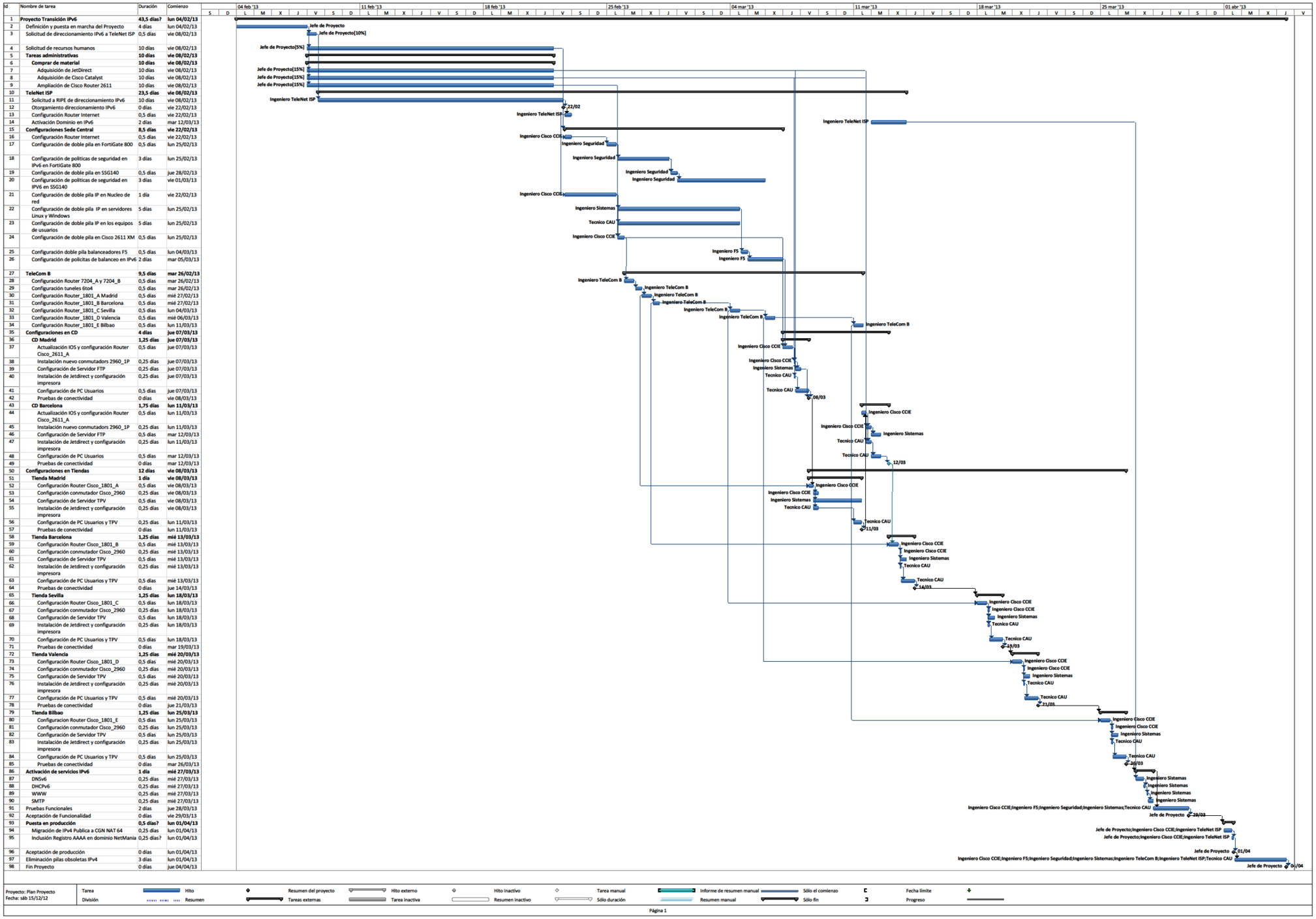
Red	Subred	Dirección IP	Descripción
2A00:2380:A8:380::/52 **Tienda Madrid**	2A00:2380:A8:381::/64 Vlan 1	2A00:2380:A8:381:5AA5::BACA	Router_1801_A
		2A00:2380:A8:381:5AA5::A1	Catalyst2960_A
		2A00:2380:A8:381:5AA5::CC1	ServerTPV_A
		2A00:2380:A8:381:5AA5::B1	PrintFac01
		2A00:2380:A8:381:5AA5::Exxx	PC Usuarios
		2A00:2380:A8:381:5AA5::EExx	TPV's
2A00:2380:A8:580::/52 **Tienda Barcelona**	2A00:2380:A8:581::/64 Vlan 1	2A00:2380:A8:581:5AA5::BACA	Router_1801_B
		2A00:2380:A8:581:5AA5::A1	Catalyst2960_B
		2A00:2380:A8:581:5AA5::CC1	ServerTPV_B
		2A00:2380:A8:581:5AA5::B1	PrintFac02
		2A00:2380:A8:581:5AA5::Exxx	PC Usuarios
		2A00:2380:A8:581:5AA5::EExx	TPV's
2A00:2380:A8:780::/52 **Tienda Sevilla**	2A00:2380:A8:781::/64 Vlan 1	2A00:2380:A8:781:5AA5::BACA	Router_1801_C
		2A00:2380:A8:781:5AA5::A1	Catalyst2960_C
		2A00:2380:A8:781:5AA5::CC1	ServerTPV_C
		2A00:2380:A8:781:5AA5::B1	PrintFac03
		2A00:2380:A8:781:5AA5::Exxx	PC Usuarios
		2A00:2380:A8:781:5AA5::EExx	TPV's
2A00:2380:A8:980::/52 **Tienda Valencia**	2A00:2380:A8:981::/64 Vlan 1	2A00:2380:A8:981:5AA5::BACA	Router_1801_D
		2A00:2380:A8:981:5AA5::A1	Catalyst2960_D
		2A00:2380:A8:981:5AA5::CC1	ServerTPV_D
		2A00:2380:A8:981:5AA5::B1	PrintFac04
		2A00:2380:A8:981:5AA5::Exxx	PC Usuarios
		2A00:2380:A8:981:5AA5::EExx	TPV's
2A00:2380:A8:B80::/52 **Tienda Bilbao**	2A00:2380:A8:B81::/64 Vlan 1	2A00:2380:A8:B81:5AA5::BACA	Router_1801_E
		2A00:2380:A8:B81:5AA5::A1	Catalyst5960_E
		2A00:2380:A8:B81:5AA5::CC1	ServerTPV_E
		2A00:2380:A8:B81:5AA5::B1	PrintFac05
		2A00:2380:A8:B81:5AA5::Exxx	PC Usuarios
		2A00:2380:A8:B81:5AA5::EExx	TPV's
2A00:2380:A8:8000::/49 **Redes externas**	2A00:2380:A8:8000::/64 Conexión TeleNet ISP	2A00:2380:A8:8000:5AA5::BACA	FortiGate 800
		2A00:2380:A8:8000:5AA5::A	Router_2811_A
		2A00:2380:A8:8000:5AA5::B	Router_2811_B
2A00:2380:A8:FF00::/52 **Redes Punto a Punto**	2A00:2380:A8:1::/64 Madrid - CD Madrid	2A00:2380:A8:1:5AA5::1	Router_2611XM
		2A00:2380:A8:1:5AA5::2	Router_2610_A
	2A00:2380:A8:2::/64 Madrid - CD Barcelona	2A00:2380:A8:2:5AA5::1	Router_2611XM
		2A00:2380:A8:2:5AA5::2	Router_2610_B

2.- ESQUEMA LOGICO DE LA RED IPV4 DE NETMANIA

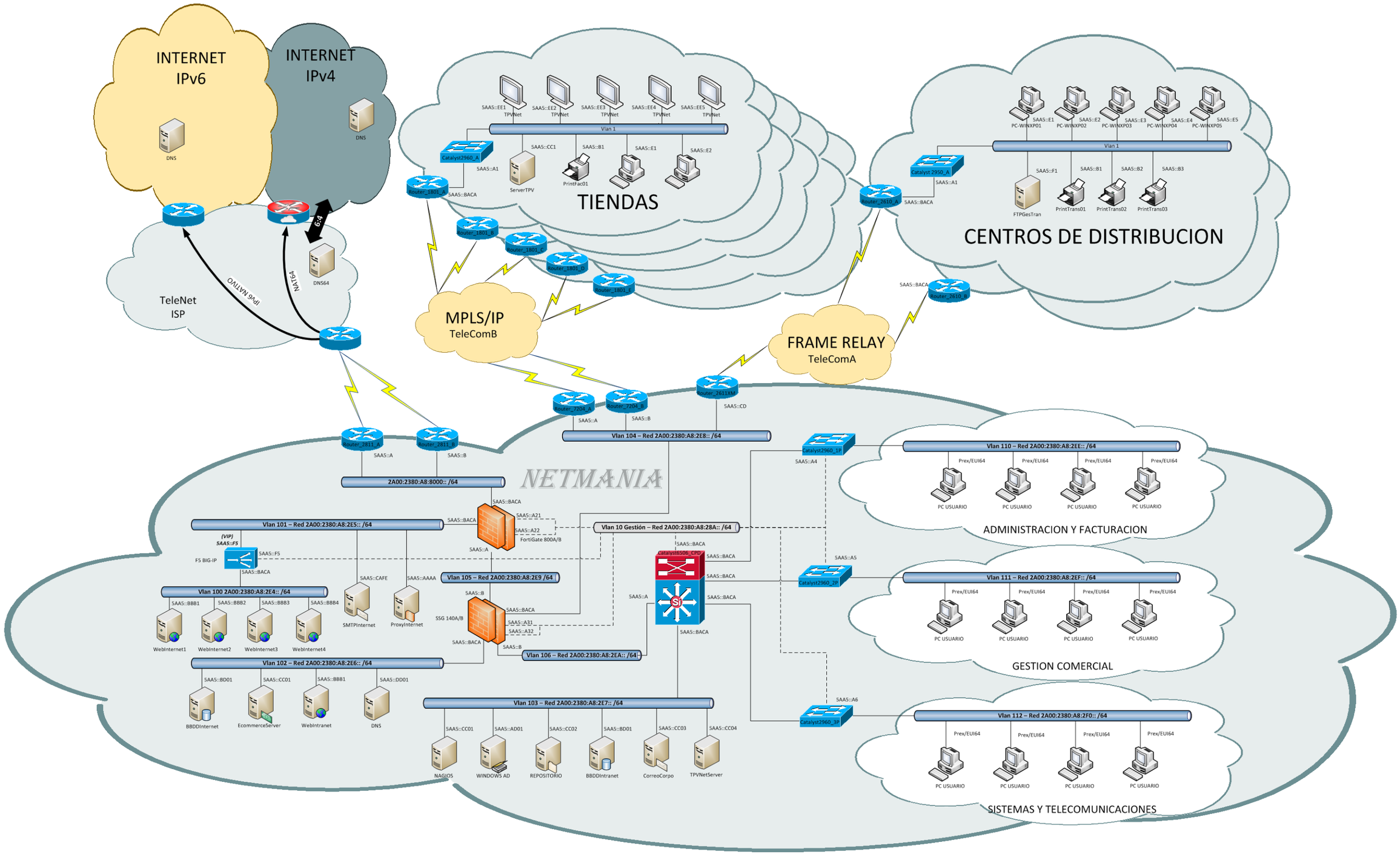


3.- PLAN DE PROYECTO DE TRANSICIÓN A IPV6

Id	Nombre de tarea	Duración	Comienzo
1	**Proyecto Transición IPv6**	**43,5 días?**	**lun 04/02/13**
2	Definición y puesta en marcha del Proyecto	4 días	lun 04/02/13
3	Solicitud de direccionamiento IPv6 a TeleNet ISP	0,5 días	vie 08/02/13
4	Solicitud de recursos humanos	10 días	vie 08/02/13
5	**Tareas administrativas**	**10 días**	**vie 08/02/13**
6	**Comprar de material**	**10 días**	**vie 08/02/13**
7	Adquisición de JetDirect	10 días	vie 08/02/13
8	Adquisición de Cisco Catalyst	10 días	vie 08/02/13
9	Ampliación de Cisco Router 2611	10 días	vie 08/02/13
10	**TeleNet ISP**	**23,5 días**	**vie 08/02/13**
11	Solicitud a RIPE de direccionamiento IPv6	10 días	vie 08/02/13
12	Otorgamiento direccionamiento IPv6	0 días	vie 22/02/13
13	Configuración Router Internet	0,5 días	vie 22/02/13
14	Activación Dominio en IPv6	2 días	mar 12/03/13
15	**Configuraciones Sede Central**	**8,5 días**	**vie 22/02/13**
16	Configuración Router Internet	0,5 días	vie 22/02/13
17	Configuración de doble pila en FortiGate 800	0,5 días	lun 25/02/13
18	Configuración de políticas de seguridad en IPv6 en FortiGate 800	3 días	lun 25/02/13
19	Configuración de doble pila en SSG140	0,5 días	jue 28/02/13
20	Configuración de políticas de seguridad en IPV6 en SSG140	3 días	vie 01/03/13
21	Configuración de doble pila IP en Nucleo de red	1 día	vie 22/02/13
22	Configuración de doble pila IP en servidores Linux y Windows	5 días	lun 25/02/13
23	Configuración de doble pila IP en los equipos de usuarios	5 días	lun 25/02/13
24	Configuración de doble pila en Cisco 2611 XM	0,5 días	lun 25/02/13
25	Configuración doble pila balanceadores F5	0,5 días	lun 04/03/13
26	Configuración de policitas de balanceo en IPv6	2 días	mar 05/03/13
27	**TeleCom B**	**9,5 días**	**mar 26/02/13**
28	Configuración Router 7204_A y 7204_B	0,5 días	mar 26/02/13
29	Configuración tuneles 6to4	0,5 días	mar 26/02/13
30	Configuración Router_1801_A Madrid	0,5 días	mié 27/02/13
31	Configuración Router_1801_B Barcelona	0,5 días	mié 27/02/13
32	Configuración Router_1801_C Sevilla	0,5 días	lun 04/03/13
33	Configuración Router_1801_D Valencia	0,5 días	mié 06/03/13
34	Configuración Router_1801_E Bilbao	0,5 días	lun 11/03/13
35	**Configuraciones en CD**	**4 días**	**jue 07/03/13**
36	**CD Madrid**	**1,25 días**	**jue 07/03/13**
37	Actualización IOS y configuración Router Cisco_2611_A	0,5 días	jue 07/03/13
38	Instalación nuevo conmutadors 2960_1P	0,25 días	jue 07/03/13
39	Configuración de Servidor FTP	0,25 días	jue 07/03/13
40	Instalación de Jetdirect y configuración impresora	0,25 días	jue 07/03/13
41	Configuración de PC Usuarios	0,5 días	jue 07/03/13
42	Pruebas de conectividad	0 días	vie 08/03/13
43	**CD Barcelona**	**1,75 días**	**lun 11/03/13**
44	Actualización IOS y configuración Router Cisco_2611_A	0,5 días	lun 11/03/13
45	Instalación nuevo conmutadors 2960_1P	0,25 días	lun 11/03/13
46	Configuración de Servidor FTP	0,5 días	mar 12/03/13
47	Instalación de Jetdirect y configuración impresora	0,25 días	lun 11/03/13
48	Configuración de PC Usuarios	0,5 días	mar 12/03/13
49	Pruebas de conectividad	0 días	mar 12/03/13
50	**Configuraciones en Tiendas**	**12 días**	**vie 08/03/13**
51	**Tienda Madrid**	**1 día**	**vie 08/03/13**
52	Configuración Router Cisco_1801_A	0,5 días	vie 08/03/13
53	Configuración conmutador Cisco_2960	0,25 días	vie 08/03/13
54	Configuración de Servidor TPV	0,5 días	vie 08/03/13
55	Instalación de Jetdirect y configuración impresora	0,25 días	vie 08/03/13
56	Configuración de PC Usuarios y TPV	0,25 días	lun 11/03/13
57	Pruebas de conectividad	0 días	lun 11/03/13
58	**Tienda Barcelona**	**1,25 días**	**mié 13/03/13**
59	Configuración Router Cisco_1801_B	0,5 días	mié 13/03/13
60	Configuración conmutador Cisco_2960	0,25 días	mié 13/03/13
61	Configuración de Servidor TPV	0,5 días	mié 13/03/13
62	Instalación de Jetdirect y configuración impresora	0,25 días	mié 13/03/13
63	Configuración de PC Usuarios y TPV	0,5 días	mié 13/03/13
64	Pruebas de conectividad	0 días	jue 14/03/13
65	**Tienda Sevilla**	**1,25 días**	**lun 18/03/13**
66	Configuración Router Cisco_1801_C	0,5 días	lun 18/03/13
67	Configuración conmutador Cisco_2960	0,25 días	lun 18/03/13
68	Configuración de Servidor TPV	0,5 días	lun 18/03/13
69	Instalación de Jetdirect y configuración impresora	0,25 días	lun 18/03/13
70	Configuración de PC Usuarios y TPV	0,5 días	lun 18/03/13
71	Pruebas de conectividad	0 días	mar 19/03/13
72	**Tienda Valencia**	**1,25 días**	**mié 20/03/13**
73	Configuración Router Cisco_1801_D	0,5 días	mié 20/03/13
74	Configuración conmutador Cisco_2960	0,25 días	mié 20/03/13
75	Configuración de Servidor TPV	0,5 días	mié 20/03/13
76	Instalación de Jetdirect y configuración impresora	0,25 días	mié 20/03/13
77	Configuración de PC Usuarios y TPV	0,5 días	mié 20/03/13
78	Pruebas de conectividad	0 días	jue 21/03/13
79	**Tienda Bilbao**	**1,25 días**	**lun 25/03/13**
80	Configuración Router Cisco_1801_E	0,5 días	lun 25/03/13
81	Configuración conmutador Cisco_2960	0,25 días	lun 25/03/13
82	Configuración de Servidor TPV	0,5 días	lun 25/03/13
83	Instalación de Jetdirect y configuración impresora	0,25 días	lun 25/03/13
84	Configuración de PC Usuarios y TPV	0,5 días	lun 25/03/13
85	Pruebas de conectividad	0 días	mar 26/03/13
86	**Activación de servicios IPv6**	**1 día**	**mié 27/03/13**
87	DNSv6	0,25 días	mié 27/03/13
88	DHCPv6	0,25 días	mié 27/03/13
89	WWW	0,25 días	mié 27/03/13
90	SMTP	0,25 días	mié 27/03/13
91	Pruebas Funcionales	2 días	jue 28/03/13
92	Aceptación de Funcionalidad	0 días	vie 29/03/13
93	**Puesta en producción**	**0,5 días?**	**lun 01/04/13**
94	Migración de IPv4 Publica a CGN NAT 64	0,25 días	lun 01/04/13
95	Inclusión Registro AAAA en dominio NetMania	0,25 días?	lun 01/04/13
96	Aceptación de producción	0 días	lun 01/04/13
97	Eliminación pilas obsoletas IPv4	3 días	lun 01/04/13
98	Fin Proyecto	0 días	jue 04/04/13



4.- ESQUEMA LOGICO DE LA RED IPV6 DE NETMANIA



Esta página esta intencionadamente en blanco