“Diseño, puesta en marcha y pruebas funcionales de un backbone MPLS/MPBGP con direccionamiento IPv6”

Tesis presentada para cumplir con los requisitos finales para la obtención del título de Ingeniería en Sistemas

Autor : Emanuel Braile

Tutores : Ingeniero Abel Crespo , Ingeniero Ricardo Furch

Septiembre 2013

Dedicatoria

Esta tesis de Ingeniería, y toda la carrera universitaria la pude lograr gracias al apoyo incondicional de mi familia, a mis hermanos, que siempre me acompañaron y ayudaron también a que todo esto sea posible, estando siempre presentes.

A mis padres, que pusieron todas sus energías para que pueda culminar mis estudios, y no quedarme en el camino bajo ninguna circunstancia. A ustedes dedico principalmente este trabajo de tesis, ya que son mis ideales de todo lo que soy; y no me alcanzaría la vida para devolverles todo lo que me han dado.

Quiero agradecer también a mis amigos, que considero parte de mi familia, los cuales muchas veces me hicieron ver las cosas de otra manera, y me acompañaron en todo el proceso de la vida de estudiante; compartiendo momentos inolvidables.

A los profesores, por llamarlos en general de algún modo, ya que todos mis educadores dentro de la institución fueron grandes maestros: programadores, ingenieros, magisters, doctores, licenciados y la lista sigue...

A la Empresa "Aguas del Colorado" por darme la oportunidad de ser parte, dar mi aporte y a la vez aprender. Al Ingeniero Electrónico Ricardo Furch, quien me guió meticulosamente conjuntamente con el Ingeniero Electrónico Aldo Abel Crespo para desarrollar esta Tesis que aquí les presento.

A los integrantes de la Comisión Evaluadora, al Ingeniero Electrónico Ernesto Daniel Berges, a la Magister María Fernanda Papa y al Licenciado en Sistemas de Información Guillermo Javier Lafuente; quienes aceptaron dedicarle parte de su tiempo a la evaluación de este trabajo.

A todos ustedes va esta dedicatoria, y a la Facultad de Ingeniería de la Universidad Nacional de La Pampa que me ha dado una educación privilegiada, de excelente nivel, y sin dejar de decirlo, me educó gratuitamente, algo que los Argentinos tenemos que saber valorar.

Saludo a todos ustedes, y a todas las personas que me acompañaron en el proceso, logrando que no me sienta nunca solo y logre concretar el sueño de graduarme con un título de grado.

Les agradezco desde lo mas profundo de mi corazón, por darme todo lo que me han dado, los saludo muy atentamente.

Emanuel Braile, Septiembre 2013.

Resumen

El propósito de este trabajo de tesis es ofrecer una alternativa viable y efectiva al problema de encaminamiento de datagramas de red extremo a extremo, cuando ambos extremos de la comunicación poseen al menos una interfaz con dirección de red de 128 bits perteneciente al Protocolo de Internet versión 6.

La solución propuesta, gira en torno a la tecnología disponible en el área de comunicaciones de la Empresa Aguas del Colorado , no obstante, es una opción conveniente bajo un contexto de dispositivos marca Cisco Systems, los cuales poseen un sistema operativo bajo licencia , y el rango de alternativas que solucionan la problemática no es muy amplio.

La solución es implementar un modelo topológico de red con el protocolo llamado Cisco 6PE (propietario de Cisco Systems) , y configurando una serie de protocolos que en conjunto, proporcionan los resultados esperados.

Se presentará al lector un modelo de red (representativo de la estructura interna de la Empresa) que permita implementar encaminamiento dinámico de datagramas extremo a extremo, con soporte al protocolo de Internet en sus dos versiones: versión 4 (IPv4) y versión 6 (IPv6) .

Este modelo, debe ser compatible y debe coexistir con la tecnología utilizada actualmente en la empresa, ya que se ofrecen servicios que deben estar las 24 horas del día disponibles, sin cortes ni interrupciones.

Para esta tarea, se utilizará un Software de simulación llamado "Gns3" en la plataforma de Sistema Operativo Linux, con el objetivo de crear el modelo y simular un entorno de red virtual que nos sirva de base para las primeras pruebas de funcionamiento y configuraciones.

Otra de las tareas será desarrollar contenido teórico en relación a los protocolos de comunicaciones mas utilizados, principalmente aquellos que participan en el encaminamiento de paquetes , estos son (sus siglas) : OSPF, BGP, MPLS y VPN/VRF .

Luego se realizarán pruebas en los dispositivos de red reales disponibles en el laboratorio de la empresa, verificando el funcionamiento, y capturando resultados.

Finalmente se presentarán conclusiones, basadas en las configuraciones utilizadas y las alternativas que se plantearon dentro del esquema de la solución propuesta.

De acuerdo a lo expresado en los párrafos previos, se espera demostrar que es posible brindar una solución estable para el actual problema de agotamiento de números IPv4 , siendo la mejor solución con menor costo de impacto en el contexto actual de la empresa.

Índice General

Capítulo 1: Introducción

Capítulo 2: Protocolo de Internet versión 4 y factores condicionantes

Capítulo 3: Fundamentos Protocolo de Internet versión 6 (IPv6)

Capítulo 4: IPv6 y Protocolos asociados

Capítulo 5: Conocimiento general de la red

Capítulo 6: Software de Emulación y Protocolo Cisco Express Forwarding (CEF)

Capítulo 7: Protocolos utilizados y Solución Propuesta

Capítulo 8: Pruebas de Laboratorio

Índice de Figuras

Capítulo 6: Software de Emulación y Protocolo Cisco Express Forwarding (CEF)

Capítulo 7: Protocolos utilizados y Solución Propuesta

Capítulo 8: Pruebas de Laboratorio

Capítulo 1: Introducción

1.0 Descripción de Empresa Aguas del Colorado (ADC)

La empresa AGUAS DEL COLORADO SAPEM es una Sociedad Anónima con participación Estatal mayoritaria, constituida en la Provincia de La Pampa, República Argentina, por Ley Provincial Nº 2.223. Su capital societario accionario está constituido del siguiente modo:

- El 60% por acciones clase "A" suscriptas por el Estado Provincial
- El 20% por acciones clase "B" pertenecientes a los Municipios y Comisiones de Fomento
- El 20% restante por acciones de clase "C", estando destinadas por el acto constitutivo a personas de derecho público estatal y no estatal (Cooperativas, Mutuales o Personas Jurídicas)

La empresa se rige por las normas derivadas del derecho privado para las Sociedades Comerciales en Argentina expresadas en la ley Nº 19.550 y sus modificatorias. Su conformación interna incluye la definición de dos sectores derivados de los preceptos originales con los que se creó la empresa. Un sector encargado de mantener y operar la infraestructura para la distribución del agua proveniente del Río Colorado a través de un acueducto de más de 490 km, y otro sector encargado de mantener, operar y actualizar la infraestructura de telecomunicaciones que incluye más de 1800 Km de red de Fibra Óptica para interconectar 44 localidades en la provincia de La Pampa. Esta red de área amplia se conecta al norte y al sur de la provincia a proveedores internacionales de acceso a Internet (ISP). Adicionalmente, la empresa inauguró recientemente un Centro de Datos de última generación destinado a albergar equipamiento propio y de otros organismos del estado provincial relacionados con los servicios informáticos que prestan.

De ahora en más se indicará como ADC al Área de Comunicaciones de la empresa Aguas del Colorado, lugar en que se realizó la pasantía rentada.

A continuación, en la sección 1.1, se describirá con mayor detalle los servicios que presta ADC, en la sección 1.2 se abordará la situación actual respecto del número de direcciones IPv4 disponibles (direcciones no asignadas) y las acciones correctivas tendientes a eliminar riesgos relacionados con el agotamiento de direcciones IPv4, que afecten el servicio de los usuarios de Aguas del Colorado SAPEM. En la sección 1.3 se describirán los objetivos a cumplimentar relacionados a la problemática introducida en las secciones anteriores. Finalmente, en la sección 1.4 se presentará sintéticamente la estructura del presente trabajo y su justificación.

1.1 Prestación de Servicios

ADC esta conformada por un grupo de profesionales con sólidos conocimientos tecnológicos, que trabajan empeñados en lograr las mejores soluciones en redes, datos y telefonía para sustentar el desarrollo de las telecomunicaciones en la Provincia de La Pampa. El área se encarga de la operación, administración y explotación de la Red de Fibra Óptica del Gobierno de la provincia de La Pampa. Participa del Plan Estratégico Digital instrumentando el INTERNET PAMPEANO. Ofrece soluciones y asesoramiento en telecomunicaciones al gobierno provincial y entre sus múltiples alcances, brinda Internet a las localidades de la provincia por convenios

con los prestadores locales (mayoritariamente cooperativas y entidades de servicios de cable). Asimismo, presta servicios a entidades públicas con presencia en toda la provincia.

Si bien la prestación de servicios se logró resumir en un párrafo, las tareas de mantenimiento, operación, administración y gestión de la red, constituyen un arduo trabajo que exige el conocimiento de la infraestructura de Internet global y de sus protocolos asociados. El volumen de información respecto de la infraestructura de Internet y los protocolos que la soportan es inconmensurable y en este contexto es necesario sumar recursos humanos calificados para constituir grupos de trabajo dedicados a estudiar lo que demanda un área de elevada dinámica.

1.2 Estado Actual de ADC

Antes de describir el estado actual de ADC se realizará una breve descripción de la evolución del protocolo de red en Internet en su versión 4 (IPv4). Ello es necesario porque el estado actual de la empresa respecto del esquema de direcciones de Internet, no es ajeno a la situación global de Internet en lo que respecta a los problemas de escalabilidad del protocolo IPv4.

Para conectar una computadora a Internet se necesita de una dirección de Internet. En el año 1981 se definió el *Request For Comment* 791 [1] que entre otros aspectos especifica el formato de direcciones de Internet denominado IPv4. Allí se definieron redes basadas en clases y se optó por direcciones de Internet cuya longitud es de 32 bits. Si bien 2^32 da como resultado un número de direcciones muy grande, el hecho de definir clases de redes A, B y C; creó un problema que se visualizó a los pocos meses en que Internet comenzó a operar. El principal inconveniente fue que la asignación de redes basadas en clases por parte del IANA (Internet Assigned Numbers Authority) [2] inutilizaba casi todo el espectro de direcciones de Clase A. Las redes de Clase B fueron rápidamente asignadas y bajo este panorama IANA comenzó a suministrar redes de Clase C. Inmediatamente el IETF (Internet Engineering Task Force) [3] intervino para definir un parche que mitigue la situación anterior. Bajo ese precepto surgió el RFC 917 en el año 1984, en que se definió el concepto de subred. La creación de subredes a partir de una red basada en clases, constituyó una mejora respecto de la optimización del uso de direcciones IPv4. Pero aún con la introducción del RFC 917 otro problema comenzó a acentuarse, la demanda de redes de Clase C incrementó exponencialmente el número de rutas en los routers del núcleo de Internet. El IETF no tuvo otra alternativa que aplicar un cambio radical respecto de la definición de redes basadas en clases, es así como el RFC 1519 define una política de asignación de direcciones IPv4 denominada CIDR y dejó obsoleto el concepto de redes basadas en clase. Todo el espectro de direcciones IPv4 fue re-definido y ello permitió que hasta el presente IPv4 sea el protocolo dominante en Internet.

La definición de subredes y la re-definición del espacio de direcciones en IPv4 (CIDR - Classless Inter-Domain Routing), fueron esfuerzos para mantener la vigencia de IPv4. Otro esfuerzo adicional del IETF fue la definición de NAT (Network Address Translation), mediante NAT computadoras en una red de área local o en una red de área amplia se configuran con direcciones privadas IPv4 según lo especifica el RFC 1918 pero utilizan un conjunto variable y reducido de direcciones IPv4 públicas para el acceso a Internet. Si bien esta modalidad permite reducir el número de direcciones IPv4 públicas empleadas, tiene como desventaja la afectación de protocolos destinados a proveer seguridad en una comunicación de datos e introduce una demora en el procesamiento de datagramas IPv4 en el router de borde de la red o redes consideradas, entre otros inconvenientes. A pesar de todos los esfuerzos expresados

en párrafos anteriores, IPv4 ha llegado al límite de su máxima definición en lo que se refiere a direcciones IPv4.

ADC dispone de un total de aproximadamente 20.000 direcciones IPv4 y considerando que se trata de una empresa con pocos años de existencia, en la actualidad sólo dispone de 2000 direcciones IPv4 libres. Ello significa que en poco tiempo los bloques de direcciones asignados por LACNIC (Latin America & Caribbean Network Information Centre) [4] a ADC se agotaran por completo. Bajo esta perspectiva la empresa debe anticipar la contingencia y comenzar a experimentar con la nueva versión del protocolo de Internet denominado IPv6 [5]. A tal fin ADC gestionó y obtuvo un bloque de direcciones IPv6 pero la tarea no culmina con la adquisición del bloque IPv6. En una red de área amplia bajo TCP/IP, interaccionan diversos protocolos que son fuertemente dependientes del protocolo de red utilizado. Migrar de una plataforma basada en IPv4 a IPv6 significa una migración de protocolos de encaminamiento (protocolos de borde interior y de borde exterior), la re-configuración de servicios que la empresa presta a sus usuarios, y numerosos aspectos adicionales.

1.3 Objetivos Propuestos

Teniendo en cuenta las consideraciones expresadas en la sección anterior, el objetivo principal de la Práctica Profesional Supervisada se puede resumir como:

> *Adecuar un núcleo de red basado en la tecnología MPLS [6] bajo IPv4, para que publique rutas basadas en el protocolo IPv6, y provea todos los servicios relacionados al transporte de datos utilizando para ello un esquema de asignación de direcciones basado en IPv6.*

Para lograr el objetivo propuesto es necesario cumplimentar con las siguientes etapas operativas:

a. Diseñar una topología de red para interconectar un número determinado de dispositivos de conmutación de paquetes en capa 3, con soporte de protocolos de encaminamiento dinámicos (de borde interior y de borde exterior). La topología se construirá sobre una plataforma de virtualización denominada GNS3 [6], que se ejecutará sobre un núcleo Linux bajo la arquitectura i386. El diseño, configuración y ejecución de la topología, permitirá extraer conclusiones sobre el funcionamiento y operación del protocolo IPv6, y los protocolos de encaminamiento dinámicos (OSPF [7] y BGP [8]), entre otros.

b. Cuando los resultados de las pruebas en (a) se consideren satisfactorias, los archivos de configuración serán respaldados para su posterior utilización en dispositivos reales (routers). Para ello se construirá una topología idéntica a la de (a.) pero basada en equipamiento real. El diseño propuesto debe ser escalable respecto del número de abonados a servir y se deben poder agregar clientes y/o proveedores de Internet sin dificultad con respecto a las configuraciones realizadas.

c. Desarrollar contenido teórico en relación a los protocolos de comunicación que se utilizarán. Para ello será necesario presentar ejemplos prácticos sobre configuraciones realizadas, y luego explicar detalles de su funcionamiento.

d. Diseñar un plan de direccionamiento IPv6 que incluya: implementación de una red basada en IPv6 cliente de ADC. Delegar un prefijo de red según IPv6, y establecer conectividad a un Sistema Autónomo remoto y/o local a través del núcleo de red de ADC.

e. Finalmente se presentarán las conclusiones cuyo objetivo será describir los beneficios de la implementación de IPv6 en un núcleo de red y en un ambiente de producción real como lo es el de la empresa considerada.

1.4 Estructura del Informe

A los efectos de abordar la temática presentada en la sección anterior es necesario considerar el estudio de los siguientes tópicos:

El capítulo 2 tratará sobre el protocolo de Internet IPv4 y los problemas asociados a la escalabilidad en la actualidad.

El capítulo 3 introducirá la nueva versión del protocolo de Internet, IPv6, sus fundamentos, enfatizando las mejoras relativas al protocolo IPv4.

El capítulo 4 presentará una serie de protocolos relativos al funcionamiento base de Ipv6. Entre aquellos cuya finalidad sea el encaminamiento entre un origen y destino, los abordaremos en capítulos posteriores para ejemplificar su uso en este trabajo.

El capítulo 5 revelara información acerca de la infraestructura de red (interna y bordes) de la empresa, resumiendo la tecnología y dispositivos utilizados cotidianamente.

El capítulo 6, abarcara detalles del Software de emulación GNS3 (Graphical Network Simulator) que se utilizo para pruebas y configuraciones de routers virtuales.

En el capítulo 7 veremos protocolos de red utilizados en teoría y practica, y se desarrolla la solución propuesta, dando una introducción al protocolo de cisco 6PE.

En el capítulo capítulo 8 , se resumirá brevemente el trabajo ejecutado en laboratorio, de forma tal de brindar detalles acerca de las conexiones y configuraciones correspondientes.

Se profundiza la configuración de BGP con Route Reflector (Reflector de Rutas).

Luego se analiza y pone en practica como alternativa de esquema de encaminamiento el uso de Sub-Interfaces , incluyendo pruebas de conectividad y verificaciones basadas en capturas de tablas de encaminamiento de los dispositivos afectados.

Como consecuencia del total de contenido y actividades previamente expuestas en los capítulos mencionados, se presentan las conclusiones finales.

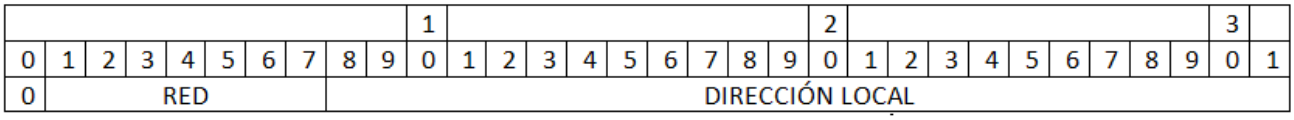
Capítulo 2: Protocolo de Internet versión 4 y factores condicionantes

2.0 Introducción

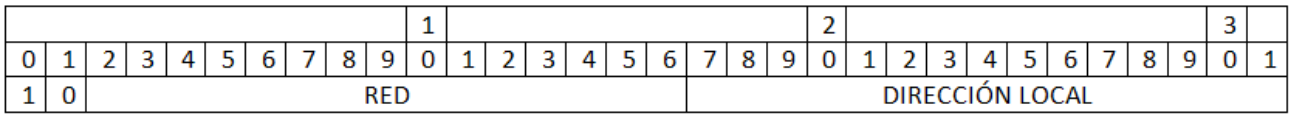
Para conectarse a Internet, cada dispositivo debe poseer al menos una interfaz de red identificada con una dirección IPv4 globalmente única. IPv4 posee un límite teórico de más de cuatro mil millones de direcciones únicas (4.000.000.000), pero en la práctica es improbable que pueda soportar más de 250 millones de direcciones únicas en el mundo.
En este capítulo, en la sección 2.1, se tratará sobre el eminente agotamiento del espacio de direcciones IPv4, el inminente colapso de la estructura de rutas en los routers del núcleo de Internet y el problema de interoperabilidad entre aplicaciones extremo a extremo a través de dominios en el que las direcciones IPv4 no son globalmente únicas. En la misma sección (2.1.1) se abordarán los mecanismos implementados por el IETF para extender la vida útil del protocolo IPv4. En la sección 2.1.2 se realizará una breve descripción sobre las medidas correctivas adoptadas por el IETF. La sección 2.2 tratará sobre el estado actual del protocolo IPv4 y finalmente en la sección 2.3 se realizarán algunas consideraciones finales relativas al presente capítulo.

2.1 Crisis de direcciones IPv4: Medidas Correctivas

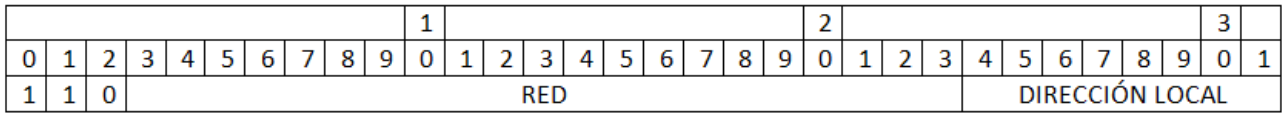
Internet, creció desde unas pocas redes a una red global que actualmente conecta a cientos de millones de personas en el mundo. En 1981 el RFC 791 definió direcciones de Internet basada en "clases" tal como lo ilustra la Figura 2.1:



a) Estructura de direcciones IPv4 Clase "A"



b) Estructura de direcciones IPv4 Clase "B"



c) Estructura de direcciones IPv4 Clase "C"

Figura 2.1: Estructura de direcciones IPv4 definidas por el RFC 791

El lector puede observar que la mitad del espacio de direcciones se reservó para 126 redes de clase "A" cada una de ellas con capacidad para albergar 2^{24} dispositivos en red. Pronto quedó en evidencia que, en el supuesto que existieran organizaciones de tamaña envergadura respecto de sus necesidades de consumo de direcciones, no existían (ni existen) tecnologías de red para hacerlo posible. Respecto de las redes de clase "B" (tal como se puede deducir de la Figura 2.1 a,b,c) el RFC 791 considero que 16.383 redes, era un número suficiente para

satisfacer la demanda de organizaciones medianas. Cada red de clase "B" podría alojar un máximo de 2^{16} interfaces de red, pero al igual que en el caso de las redes de Clase "A" las limitaciones tecnológicas lo impedían. Por último el RFC 791 definió un total de 2^{21} redes de clase "C", cada una de ellas con capacidad de conectar un máximo cercano a las 256 interfaces de red (ver Fig. 2.1 a, b, c).

De acuerdo a lo expresado en el párrafo anterior, es evidente que un esquema de direcciones como el planteado en el RFC 791 no resultó escalable conforme Internet comenzó a expandirse y ello quedó evidenciado en el RFC 917 redactado el año 1982 en donde se introdujo el término "subred". Mediante la definición de subredes, en una red IPv4, fue posible aumentar el número de direcciones IPv4 utilizadas en redes IPv4 de clase "A" y "B". Asimismo se tuvieron que definir nuevos conceptos relacionados con subredes tal como dirección de subred y dirección de difusión en cada subred (RFC 922).

A finales de la década de 1980, la expansión y comercialización de la antigua red de investigación derivó en la conexión de un gran número de nuevas organizaciones de acuerdo al plan de direccionamiento dado por el RFC 791. Nuevas organizaciones solicitaban redes de clase "B" y la tasa de demanda crecía exponencialmente. Ante esta situación, el IETF y el grupo de trabajo ROAD (acrónimo de *ROuting and ADdressing)* examinaron esta situación. En enero de 1992 el grupo identificó tres problemas:

1. Agotamiento del espacio de redes de Clase "B"

2. Crecimiento de las tablas de rutas en los routers del núcleo de Internet, más allá de las posibilidades que brindaba el software y Hardware de esa época

3. Eventual agotamiento del espacio de direcciones IPv4

El grupo ROAD predijo que los problemas 1 y 2 se experimentarían entre los años 1993 y 1995 y el trabajo del grupo culminó con el RFC 1338 que más tarde derivó en el RFC 1519. El RFC 1519 reestructuró por completo el espacio de direcciones IPv4 utilizando el concepto de redes IPv4 sin clases o por su acrónimo del inglés CIDR *(Classless Inter-Domain Routing)*.

CIDR proveyó y aún provee un mecanismo para disminuir la tasa de crecimiento de las rutas en los routers del núcleo de Internet, a la vez que redujo la tasa de consumo de direcciones IPv4. El grupo ROAD considero que el agotamiento del espacio de direcciones IPv4, era un problema a largo plazo, y que se debería trabajar en un nuevo esquema para solucionarlo (año 1992). No es el objetivo del informe extenderse en una explicación detallada respecto de CIDR, el lector interesado puede consultar el RFC 1519 [3] y aquellos RFC´s que lo sucedieron a los efectos de entender el mecanismo.

En diciembre del año 1991 el RFC 1287 titulado *"Towards the Future Internet Architecture"* expresaba la preocupación del IETF por los problemas de escalabilidad de IPv4 y sentaba amplias recomendaciones para hacer de Internet una arquitectura escalable; siendo el primer documento que introdujo el concepto de NAT *(Network Address Traslation)*. Concretamente en el RFC 1287 se propone reemplazar el campo de 32 bits en el campo dirección fuente, por un campo de la misma longitud pero con un significado diferente. En vez de utilizar una dirección IPv4 globalmente única, utilizar otra dirección de la misma longitud, cuyo significado sea único para una pequeña región, o región administrativa. Luego pasarelas o routers en la frontera con

Internet debían reescribir la dirección fuente por una dirección IPv4 de significado global antes de que el datagrama cruzara la frontera.

Finalmente en mayo de 1994 mediante el RFC 1631 (informativo) se especificó claramente la operación que debía llevar a cabo NAT. Posteriormente el RFC 1631 fue declarado obsoleto y sucedido por el RFC 3022. Aunque existen diversas funcionalidades de NAT para el propósito de este informe, el lector debe asimilar que en el caso general que se trata de conectar computadoras u otros dispositivos en red utilizando direcciones IPv4 con sentido local. Cuando uno o más computadoras, buscan acceso a Internet, el router de borde (entre el dominio administrativo e Internet) reescribe la dirección fuente por una de significado global a efectos de que se logre el acceso a la red de redes o Internet.

Hasta aquí se ha descrito la problemática del plan de direccionamiento dado en el RFC 791 y la reacción del IETF para alargar la vida del protocolo IPv4. En la próxima sección se tratará sobre el resultado de las medidas correctivas y algunas de las consecuencias aparejadas tras su implementación.

2.2 Resultado de las Medidas Correctivas

En la sección anterior se introdujeron brevemente algunas de las medidas correctivas que el IETF tuvo que implementar para extender la vida útil de IPv4 como protocolo de red a Internet.

Si bien NAT permitió (y aún permite) preservar el recurso escaso, liberando direcciones IPv4, tuvo consecuencias negativas relacionadas fundamentalmente con aplicaciones de red y con aspectos de seguridad de la información en Internet.

El uso de NAT implicó que muchas aplicaciones, por ejemplo VoIP basada en el protocolo de sesión SIP, no pudieran ser utilizadas efectivamente, funcionando sólo en intranets (redes que cuya gestión y administración depende de una organización). Además de VoIP, aplicaciones multimedia tal como videoconferencias, vídeo bajo demanda, e IPTV, no funcionan correctamente a través de NAT. Para una autenticación basada en Kerberos se necesita de la dirección fuente del emisor y dependiendo de la configuración, NAT puede removerla. IPSec (protocolo seguro para Internet) asegura autenticación de los datos, integridad y confidencialidad, sin embargo cuando se utiliza NAT, cambia direcciones en el encabezado de IPv4. En síntesis, diversas aplicaciones y protocolos aún hoy son afectadas/os por la introducción de NAT.

CIDR permitió evitar el colapso del crecimiento exponencial en el número de entradas de los routers del núcleo de Internet, pero aún así, desde el año 1994 hasta la fecha el número de rutas se incrementó hasta llegar a un total de aproximadamente 500.000 en la actualidad. Ello significa que un datagrama IPv4 que ingrese a un router del núcleo de Internet, en el peor caso, será encaminado luego de medio millón de comprobaciones. Vale aclarar que los routers en el núcleo de Internet disponen de una base de datos dinámica para que todos los bloques CIDR sean globalmente alcanzados.

2.3 Estado Actual

IPv4 ha sido el protocolo de red que ha sostenido la infraestructura de Internet por más de 30 años, pero ha llegado al fin de su vida útil. El agotamiento de direcciones IPv4 es un hecho que se acentúa en mayor o menor grado de acuerdo a la región geográfica en el mundo.
Las organizaciones que administran las direcciones del protocolo de Internet, dependen de IANA y se denominan *Regional Internet Registries* o por su acrónimo RIRs [12]. IANA creó cinco RIRs para administrar las direcciones de Internet, ellos son:

- AfriNIC (África y regiones en el Océano Índico)
- APNIC (Asia/Pacifico)
- ARIN (América del Norte y regiones del Caribe)
- LACNIC (América Latina y regiones del Caribe)
- RIPE NCC (Europa, Medio Oriente y Asia Central)

A continuación y a los efectos de ilustrar el estado actual de direcciones IPv4 en lo que respecta a cada uno de los RIRs, se presenta la Fig. 2.2

Registry	Advertised /32s	(/8s)	Unadvertised /32s	(/8s)	Allocated /32s	(/8s)	Reserved /32s	(/8s)	Available /32s	(/8s)	Total /32s	(/8s)
AFRINIC	46275840	2.76	7580416	0.45	53856256	3.21	760576	0.05	62537984	3.73	117154816	6.98
APNIC	725318780	43.23	124601732	7.43	849920512	50.66	3985152	0.24	14290944	0.85	868196608	51.75
ARIN	1065893192	63.53	622644664	37.11	1688537856	100.64	4855296	0.29	35909120	2.14	1729302272	103.07
RIPENCC	656364900	39.12	107880916	6.43	764245816	45.55	1354440	0.08	14843392	0.88	780443648	46.52
LACNIC	133334952	7.95	14468696	0.86	147803648	8.81	424960	0.03	38459136	2.29	186687744	11.13
IANA	0	0.00	0	0.00	0	0.00	592708864	35.33	20466432	1.22	613175296	36.55
TOTAL	2627187664	156.59	877176424	52.28	3504364088	208.88	604089288	36.01	186507008	11.12	4294960384	256.00

Figura 2.2: Adjudicación de recursos IPv4 por RIRs (10/07/2013)

A los efectos de lograr un mayor entendimiento, a continuación se realizará una breve explicación del significado de los datos dados en la Figura 2.2.

La primer columna comprende todos los RIRs definidos por IANA. La segunda columna expresa el número de direcciones IPv4 publicadas (detectadas en los routers del núcleo de Internet), esta columna está inherentemente relacionada con la tercera, que expresa el mismo número pero en relación a prefijos /8 asignados por IANA a los RIRs.

La cuarta columna expresa el número de direcciones IPv4 no publicadas (no detectadas en los routers del núcleo de Internet). Estas direcciones adjudicadas por los RIRs a los ISP *(Internet Service Provider)* o bien no son utilizadas o por el contrario, son utilizadas pero no publicadas por estar encubiertas por dispositivos que implementan NAT.

La quinta columna expresa el número total de direcciones adjudicadas que mediante una simple suma se puede constatar que incluye las direcciones publicadas y las no publicadas (en cada RIR).

La décima columna brinda el número total de direcciones no asignadas (libres) para cada uno de RIR´s, mientras que la duodécima columna expresa el total de direcciones (asignadas, reservadas y libres) para cada uno de los RIR´s.

LACNIC, en la actualidad sólo dispone de aproximadamente 38,5 millones de direcciones IPv4, número considerado escaso y que según las predicciones del mismo organismo se adjudicarán por completo durante 2014. A continuación se expresarán las consideraciones finales para este capítulo.

2.4 Consideraciones Finales

El IETF consideró que las medidas adoptadas (descriptas en las secciones previas) constituían una solución para el corto y mediano plazo. Por este motivo en el año 1994 creó un grupo de trabajo destinado a proveer una solución definitiva para permitir que Internet sea escalable. El IETF tuvo en claro que la solución no se trataría de parches adicionales al protocolo IPv4, sino que por el contrario se tendría que definir una nueva versión del protocolo de Internet. Bajo esta perspectiva se elaboró el RFC 2460 (1998) que definió al nuevo protocolo de Internet IPv6 y que luego fue actualizado por los RFCs 5095, 5722, 5871, 6437, 6564, 6935 y 6949. En esta dirección, el capítulo 3 abordará las principales características del nuevo protocolo de red en Internet y las razones que hacen de IPv6, la única alternativa válida para que Internet continúe creciendo sin obstáculos.

Capítulo 3: Fundamentos de Protocolo de Internet versión 6 (IPv6)

3.0 Introducción Protocolo de Internet versión 6 (IPv6)

El Protocolo de Internet versión 6 (IPv6) es una versión del protocolo de Internet, definida en el RFC 2460 y diseñada con el fin de reemplazar al actual protocolo de Internet versión 4 (IPv4) del cual nos referimos en el capítulo 2 a modo de introducción.
Diseñado por Steve Deering de Xerox PARC y Craig Mudge, esta destinado a sustituir a IPv4, cuyo límite en el número de direcciones de red admisibles está empezando a restringir el crecimiento de Internet y su uso, especialmente en China, India, y otros países asiáticos densamente poblados. El nuevo estándar mejorará el servicio globalmente; por ejemplo, proporcionará a cada dispositivo electrónico, la posibilidad de tener sus direcciones de internet propias y permanentes [1].
En la semana del 3 de febrero del 2011, la IANA (Agencia Internacional de Asignación de Números de Internet, por sus siglas en inglés) entregó el último bloque de direcciones disponibles (33 millones) a la organización encargada de asignar IPs en Asia (Apnic), un mercado que está en auge y no tardará en consumirlas todas. [2]
Puede apreciarse en la Figura 3.1, información actualizada de la disponibilidad de direcciones IPv4 otorgada por LacNic en su web [3]:

Figura 3.1: Reporte de terminación de direcciones IPv4

Podemos apreciar de la Figura 3.1, que se encuentran disponibles para todo Latino-América un total de 43.414.016 (cuarenta y tres millones, cuatrocientos catorce mil dieciséis) direcciones

IPv4. Actualmente LACNIC como RIR (de Regional Internet Registry – o en castellano Registro Regional de Internet) es responsable del registro, distribución y asignación del 11.13 / 8s (186.730.240) de direcciones asignadas para latinoamérica. La utilización de este espacio de direcciones, hasta la fecha de 18/04/2013 se muestra en la Figura 3.2:

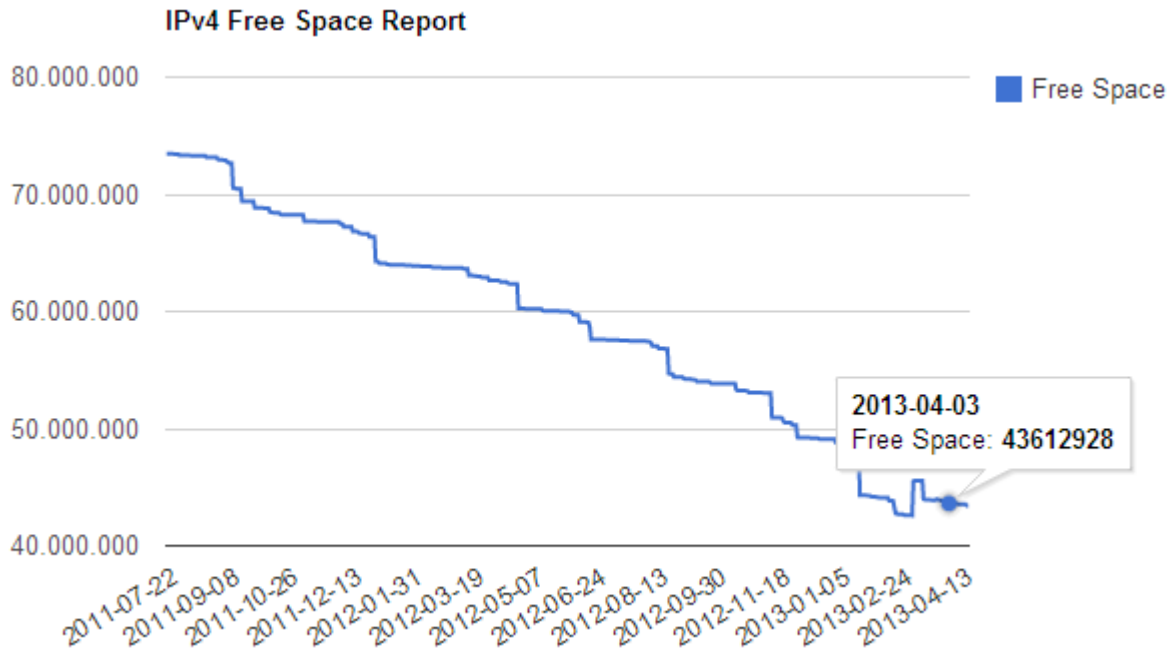


Figura 3.2: Reporte de espacio de direcciones IPv4 libre

LACNIC a adoptado como política, que al momento que el stock de direcciones sea inferior a 4.194.304, se considerará el stock de LACNIC como agotado. También cuando el stock de direcciones disponibles alcance 2.097.152 de direcciones, LACNIC cambiará las políticas relacionadas con el agotamiento del espacio de direcciones IPv4. Con la información obtenida por LACNIC, hasta la fecha, tenemos:

- Total asignado a LACNIC: 143.316.224 direcciones
- Total Libre: 43.414.016 (0,30 % disponible)

3.1 IPv4 versus IPv6 : Cantidad de Direcciones

Como se vió en el capítulo 1, en la figura 2.1 acerca de las clases de redes, IPv4 posibilita una cantidad de direcciones de red diferentes, dependiendo de la clase de red elegida (Clase A, B,C). La cantidad de direcciones posibles para cada clase de red IPv4 , es un número inadecuado para dar una dirección única a cada persona del planeta, y mucho menos a cada vehículo, teléfono, PDA, etcétera.
En cambio, IPv6 admite 40.282.366.920.938.463.463.374.607.431.768.211.456 (2128 o 340 sextillones de direcciones) —cerca de 6,7 × 1017 (670 mil billones) de direcciones.

3.2 Cambios y nuevas características

En muchos aspectos, IPv6 es una extensión conservadora de IPv4. La mayoría de los protocolos de transporte y aplicación necesitan pocos o ningún cambio para operar sobre IPv6;

las excepciones son los protocolos de aplicación que integran direcciones de capa de red, como FTP o NTPv3, NTPv4. IPv6 especifica un nuevo formato de paquete, diseñado para minimizar el procesamiento del encabezado de paquetes. Debido a que las cabeceras de los paquetes IPv4 e IPv6 son significativamente distintas, los dos protocolos no son ínter-operables. Algunos de los cambios de IPv4 a IPv6 mas relevantes son:

Direcciones más grandes: El interés de los diseñadores era que direcciones más largas permiten una entrega jerárquica, sistemática y en definitiva mejor de las direcciones y una eficiente agregación de rutas. Por ejemplo, cambiando el prefijo anunciado por unos pocos routers es posible en principio reasignar la numeración de toda la red, ya que los identificadores de nodos (los 64 bits menos significativos de la dirección) pueden ser auto-configurados independientemente por un nodo. El tamaño de una subred en IPv6 es de (máscara de subred de 64-bit), el cuadrado del tamaño de la Internet IPv4 entera. Así, las tasas de utilización del espacio de direcciones será probablemente menor en IPv6, pero la administración de las redes y el encaminamiento serán más eficientes debido a las decisiones de diseño inherentes al mayor tamaño de las subredes y la agregación jerárquica de rutas. Vemos la siguiente figura 3.3 que ejemplifica una dirección IPv6 :

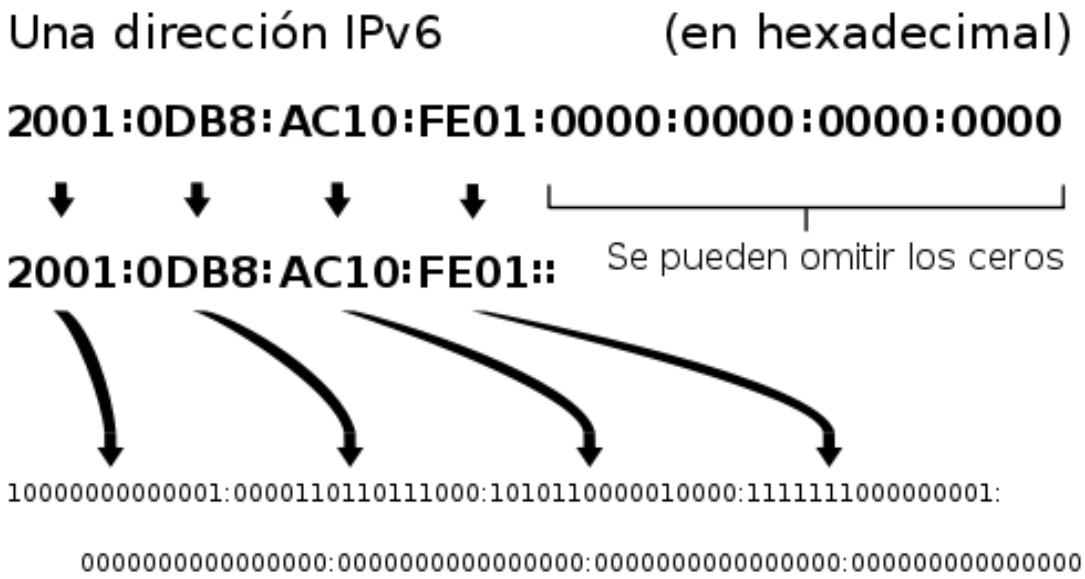


Figura 3.3: Una ilustración de una dirección IP (versión 6), en hexadecimal y binario.

3.3 Encabezado de Paquetes: procesamiento simplificado en los routers

Se realizaron modificaciones en la cabecera de los paquetes, con el objetivo de simplificarlo; así como en el proceso de reenvío de paquetes para hacer el procesamiento de los mismos más simple y por ello más eficiente. En concreto:

• El encabezado del paquete en IPv6 es más simple que el utilizado en IPv4, así los campos que son raramente utilizados han sido movidos a opciones separadas; en efecto, aunque las direcciones en IPv6 son 4 veces más largas, el encabezado IPv6 (sin opciones) es solamente el doble de largo que el encabezado IPv4 (sin opciones).

• Los routers IPv6 no realizan fragmentación. Los nodos IPv6 requieren ya sea hacer descubrimiento de MTU (Maximum Transfer Unit), realizar fragmentación extremo a extremo o enviar paquetes menores al MTU mínimo de IPv6 de 1280 bytes.

• El encabezado IPv6 no está protegido por una suma de comprobación (checksum); la protección de integridad se asume asegurada tanto por el checksum de capa de enlace y por un checksum de nivel superior (TCP, UDP). En efecto, los routers IPv6 no necesitan re-calcular la suma de comprobación cada vez que algún campo del encabezado (como el contador de saltos o Tiempo de Vida) cambian. Esta mejora puede no resultar de gran importancia en routers que utilizan hardware dedicado para computar este cálculo y así pueden hacerlo a velocidad de linea (wirespeed), pero es relevante para routers por software.

• El campo Tiempo de Vida de IPv4, conocido como TTL (Time To Live), pasa a llamarse Límite de saltos, reflejando el hecho de que ya no se espera que los routers computen el tiempo en segundos que tarda en atravesarlo (que en cualquier caso siempre resulta menor de 1 segundo). Se simplifica como el número de saltos entre routers que se permite realizar al paquete IPv6.

Hasta aquí llegamos en cuanto a características del protocolo IPv6 y principales diferencias con respecto a su predecesor en su versión 4 . Veremos a continuación, en el capítulo 4, una serie de protocolos utilizados que resultan cruciales en lo que respecta a IPv6. Estos son:

- Protocolo de Mensajes de Control de Internet Versión 6 (ICMPv6) [6]
- Protocolo Descubrimiento de Vecinos (Neighbor Discovery Protocol o NDP)
- Protocolo Descubrimiento subscriptores de grupos (Multicast Listener Discovery Protocol Versión 2 o MLDv2)
- Internet Protocol Security (Ipsec)

3.4 El papel de APNIC en agotamiento de IPv4 [4]

En los últimos años, APNIC (Asia Pacific Network Information Centre) ha ido construyendo conciencia en la comunidad acerca del agotamiento de IPv4 y el despliegue de IPv6. Personal de APNIC da presentaciones en conferencias regionales y foros internacionales con las estadísticas publicadas para guiar a quienes deben tomar decisiones. APNIC ha estado distribuyendo IPv6 desde 1999 y ofrece talleres de capacitación para los operadores de red desde el año 2006. IPv6 se ha desplegado a través de la propia red de APNIC en Australia. Hay un esfuerzo en curso para recuperar direcciones IPv4 no utilizadas dentro de la región Asia-Pacífico para la redistribución a redes que todavía necesitan IPv4.

Capítulo 4: IPv6 y Protocolos Asociados

4.0 Introducción

Del conjunto de protocolos de Internet , los que están mas ligados a IPv6 son ICMPv6 y el Descubrimiento de vecinos (Neighbor Discovery Protocol o NDP). En cuanto a los protocolos de encaminamiento para IPv6, se adoptan los mismos protocolos de encaminamiento para redes IPv4, realizando las modificaciones pertinentes en cuanto a configuraciones de manera tal de operar con IPv6. A continuación se describirán dichos protocolos.

4.1 Protocolo de Mensajes de Control de Internet Versión 6 (Internet Control Message Protocol o ICMPv6)

ICMPv6 (o ICMP para IPv6) [6] es una nueva versión de ICMP y es un protocolo importante en la arquitectura IPv6 que debe estar completamente soportado por todas las implementaciones y nodos IPv6.
ICMPv6 combina funciones que anteriormente estaban subdivididas en varias partes de diferentes protocolos tales como ICMP (Internet Control Message Protocol), IGMP (Internet Group Management Protocol) o ARP (Address Resolution Protocol) y además introduce algunas simplificaciones eliminando tipos de mensajes obsoletos actualmente.
ICMPv6 es un protocolo de propósito múltiple y está diseñado para realizar funciones tales como detectar errores encontrados en la interpretación de paquetes, realizar diagnósticos, realizar funciones como descubrimiento de vecinos (Neighbor Discovery) y detectar direcciones IPv6 multicast. Por esta razón, los mensajes ICMPv6 están subdivididos en dos clases: mensajes de error y mensajes informativos. Los mensajes ICMPv6 son enviados dentro de paquetes IPv6 los cuales a su vez pueden llevar las extensiones de cabecera de IPv6.

Ver anexo 21: RFC 4443 ICMPv6 (ICMP for IPv6) March 2006

Formato de los Paquetes

Los paquetes ICMPv6 tienen el formato Tipo, Código y Checksum. Los 8 bits del campo Tipo indican el tipo de mensaje. Si el bit de mayor peso tiene el valor 0 (valores entre 0 y 127) entonces es un mensaje de error, por el contrario si el bit de mayor peso es 1 (valores entre 128 y 255) entonces es un mensaje informativo. Los 8 bits del campo Código dependen del tipo de mensaje, y son utilizados para crear un nivel adicional de clasificación de mensajes, de tal forma que los mensajes informativos en función del campo Código se puedan subdividir en varios tipos. El campo Checksum es usado para detectar errores en los mensajes ICMP y en algunos de los mensajes IPv6.

Mensajes de Error

Los mensajes de error de ICMPv6 son similares a los mensajes de error de ICMPv4. Se dividen en 4 categorías: destino inaccesible, paquete demasiado grande, tiempo excedido y problemas de parámetros:

1 - Destination Unreachable (Destino Inalcanzable)
2 - Packet Too Big (Paquete Demasiado Grande)
3 - Time Exceeded (Tiempo Agotado)
4 - Parameter Problem (Problema de Parámetros)

Mensajes Informativos

El segundo tipo de mensajes ICMP son los mensajes informativos. Estos mensajes se subdividen en tres grupos: mensajes de diagnóstico, mensajes para la administración de grupos multicast y mensajes de descubrimiento de vecinos (Neighbor Discovery).
Cada mensaje ICMPv6 esta precedido por una cabecera IPv6 y cero o mas extensiones de cabecera IPv6.

4.2 Protocolo de Descubrimiento de Vecinos (Neighbor Discovery Protocol o NDP)

Neighbor Discovery Protocol (NDP) es un protocolo de IPv6, y es equivalente al protocolo Address Resolution Protocol (ARP o Protocolo de Resolución de direcciones) en IPv4, aunque también incorpora las funcionalidades de otros protocolos de esta versión. Consiste en un mecanismo con el cual un nodo que se acaba de incorporar a una red, descubre la presencia de otros nodos en el mismo enlace, además de ver sus direcciones IP. Este protocolo también se ocupa de mantener limpios los caches donde se almacena la información relativa al contexto de la red a la que está conectado un nodo.
Así cuando una ruta hacia un cierto nodo falla, el router correspondiente buscará rutas alternativas. Emplea los mensajes de ICMPv6, y es la base para permitir el mecanismo de auto-configuración en IPv6.

Ver Anexo 23: RFC 4861 Neighbor Discovery in IPv6 Septiembre 2007

Tipos de paquetes

• **Solicitud de router:** es generado por una interfaz cuando esta es activada, para pedir a los nodos que se anuncien. Tipo en paquete ICMPv6 = 133.

• **Anunciación de router:** producido por los nodos periódicamente (entre cada 4 y 1800 segundos), o bien se produce por una "solicitud de router", de esta manera informa de su presencia así como de otros parámetros de enlace y de Internet, como prefijos (uno o varios), tiempos de vida y configuración de direcciones. Tipo en paquete ICMPv6 = 134.

• **Solicitud de vecino:** lo generan los nodos para determinar la dirección de capa de enlace de sus vecinos, o para asegurarse de que el nodo vecino es alcanzable, aunque también se genera para detectar las direcciones IP duplicadas. Tipo en paquete ICMPv6 = 135.

• **Anunciación de vecino:** los nodos lo producen como respuesta a la"solicitud de vecino", principalmente, aunque también para indicar cambios de direcciones en el nivel de enlace. Tipo en paquete ICMPv6 = 136.

• **Re-dirección:** los nodos generan este paquete para informar a los routers de que existe una ruta mejor para llegar a un determinado destino. Es equivalente, en parte a "ICMP redirect". Tipo en paquete ICMPv6 = 137.

Vecinos distantes ahora pueden estar conectados, debido a esta nueva característica que incorpora el nuevo protocolo.

Nota 1: un router es equivalente a un dispositivo encaminador de paquetes.

4.3 Protocolo de Descubrimiento de Subscriptores de Grupos (Multicast Listener Discovery Protocol Versión 2 o MLDv2)

MLD es utilizado por los routers IPv6 para descubrir la presencia de oyentes de multidifusión en los enlaces directamente conectados, y descubrir qué direcciones de multidifusión son de interés para los nodos vecinos.
MLDv2 esta diseñado para ser interoperable con MLDv1. MLDv2 añade la posibilidad de que un nodo informe interés en escuchar paquetes con una dirección de multidifusión en particular, sólo desde una dirección de origen específica o de todas las fuentes a excepción de la dirección de origen específica.

Se presentarán a continuación, una serie de capturas de paquetes, que tienen como objetivo, analizar el protocolo MLDv2.
Estas capturas fueron obtenidas con el Software llamado “Wireshark” (ver Nota 2), configurado en modo promiscuo en las interfaces de los routers que utilizamos en la simulación, de forma tal de filtrar todo el tráfico entrante y saliente. Pasamos entonces a ver las capturas .

Nota 2: Wireshark es el nombre del software que se utilizó, antes conocido como Ethereal. Es un analizador de protocolos muy robusto que permite capturar paquetes y ver exhaustivamente que información circula por la red. Puede descargarse libremente desde la web del autor (http://www.wireshark.org/download.html).

A continuación, veremos las Figuras 4.1, 4.3, 4.4, 4.5, 4.6, y 4.7 las cuales representan las capturas obtenidas con el Software Wireshark.

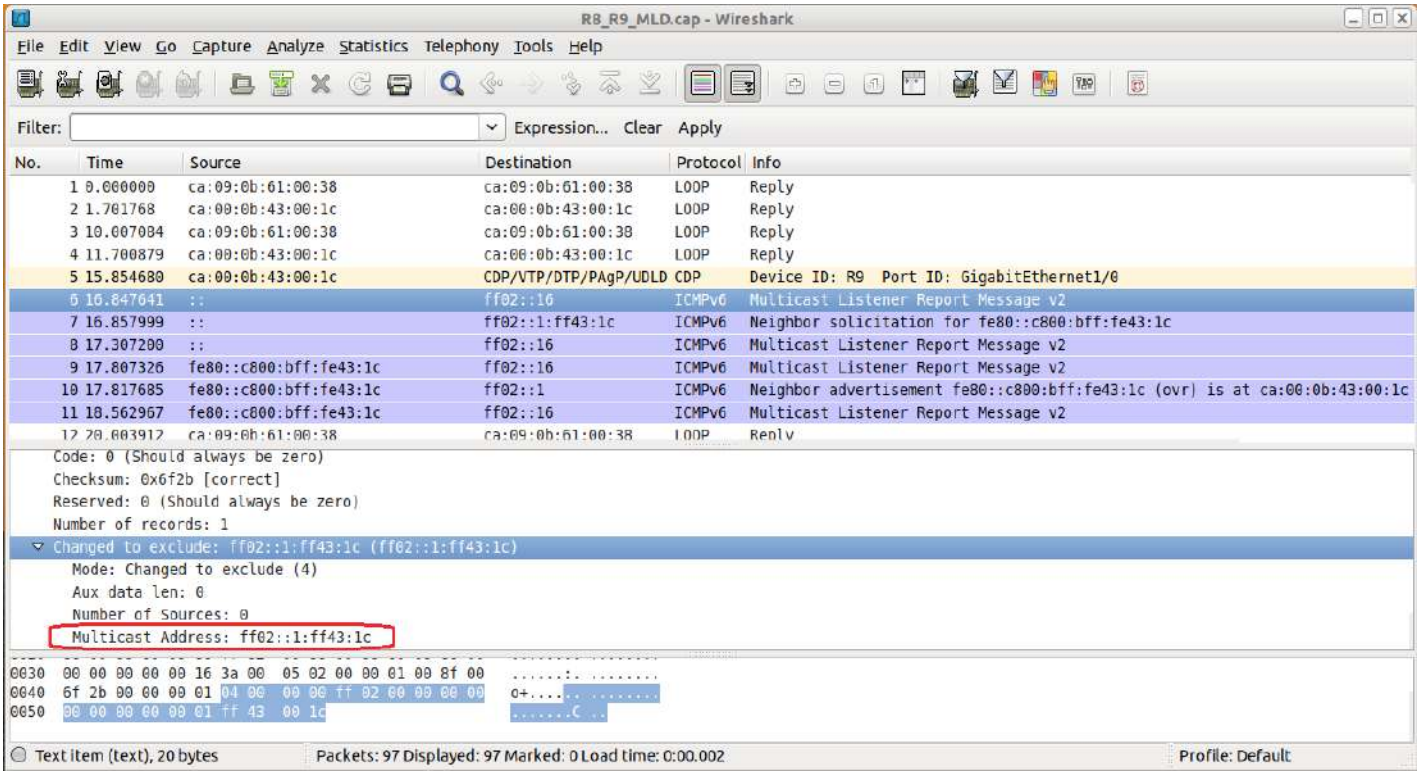


Figura 4.1: campo Changed to exclude de ICMPv6. La dirección multicast marcada en rojo se excluye de las direcciones de las cuales queremos recibir paquetes (ya que es la propia dirección de la interfaz)

Nota 3: para mas información, ver :

- Anexo 18 : RFC 3810 MLDv2 for IPv6 June 2004
- Anexo 7 : RFC 2711 IPv6 router Alert Option October 1999
- Anexo 17: RFC 3513 IPv6 Addressing Architecture April 2003

MLDv2 es un sub-protocolo de ICMPv6, es decir, los tipos de mensajes MLDv2 son un subconjunto de mensajes ICMPv6, y los mensajes MLDv2 son identificados como paquetes IPv6 con un valor Next Header de 58 (ver figura 4.4).
Todos los mensajes MLDv2 deben ser enviados con una dirección IPv6 link-local de origen, un IPv6 Hop Limit de 1 (ver figura 4.6), y un IPv6 router Alert option en el Hop-by-Hop Options header (ver figura 4.5). El router Alert option es necesario para causar a los routers a examinar mensajes MLDv2 enviados a una dirección multicast ipv6 en la cual los propios routers no tienen interés.
MLDv2 Reports pueden ser enviados con una dirección de origen no especificada ::,
unspecified address (Anexo 17), si aun no se ha adquirido una dirección link-local IPv6 válida para la interfaz de salida. Hay 2 tipos de mensajes MLD en lo que respecta al protocolo MLDv2 :

• **Multicast Listener Query (Type = decimal 130)**

• **Version 2 Multicast Listener Report (Type = decimal 143)**. (ver figura 4.3) . Estos mensajes son enviados por nodos ip para reportar (a los routers vecinos) el estado actual de

escucha multicast (multicast listening state), o cambios en el estado de la escucha multicast, o de sus interfaces.
La Figura 4.2 muestra el formato de los mensajes Reports:

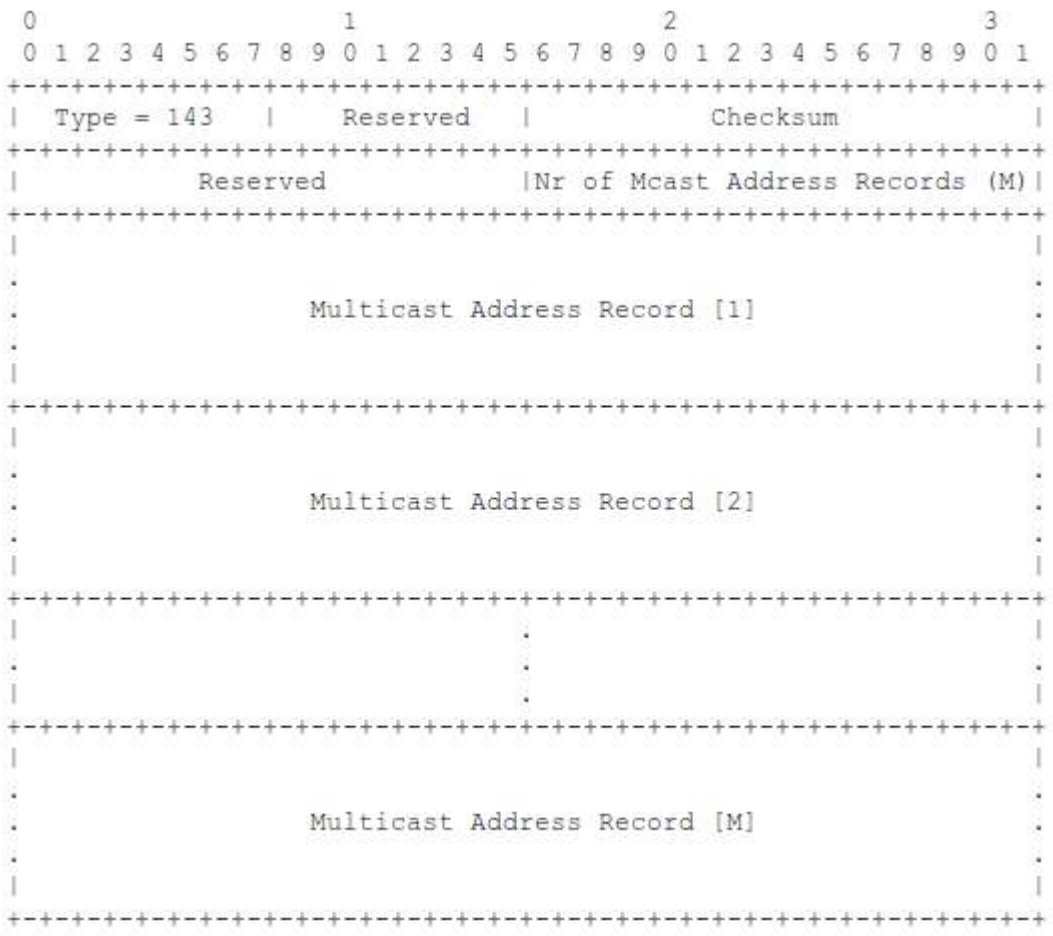


Figura 4.2: formato del paquete MLDv2 "REPORT"

Para mayor detalle del paquete y sus opciones, ver el RFC 3810 (Anexo 18).

Para asegurar la inter-operabilidad con nodos que implementan MLDv1, una implementación de MLDv2 debe también soportar los dos tipos de mensajes siguientes :

• **Version 1 Multicast Listener Report (Type = decimal 131)** [RFC 2710]

• **Version 1 Multicast Listener Done (Type = decimal 132)** [RFC 2710]

Tipos no reconocidos de mensajes deben ser silenciosamente ignorados. Otros tipos de mensajes podrían ser utilizados por nuevas versiones o extensiones de MLD, por Multicast Routing Protocols, o para otros usos.

A continuación mas capturas del protocolo MLDv2.

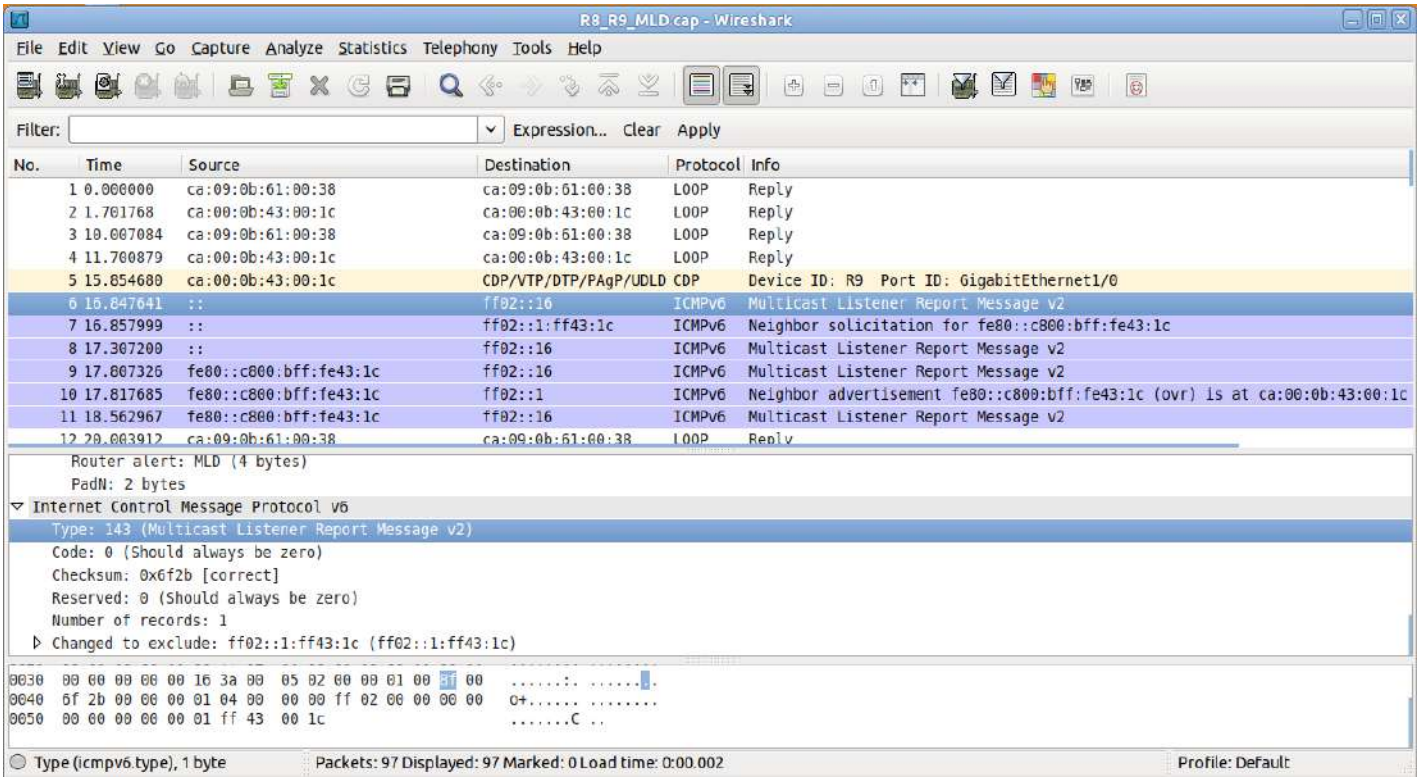


Figura 4.3: captura del protocolo MLDv2.

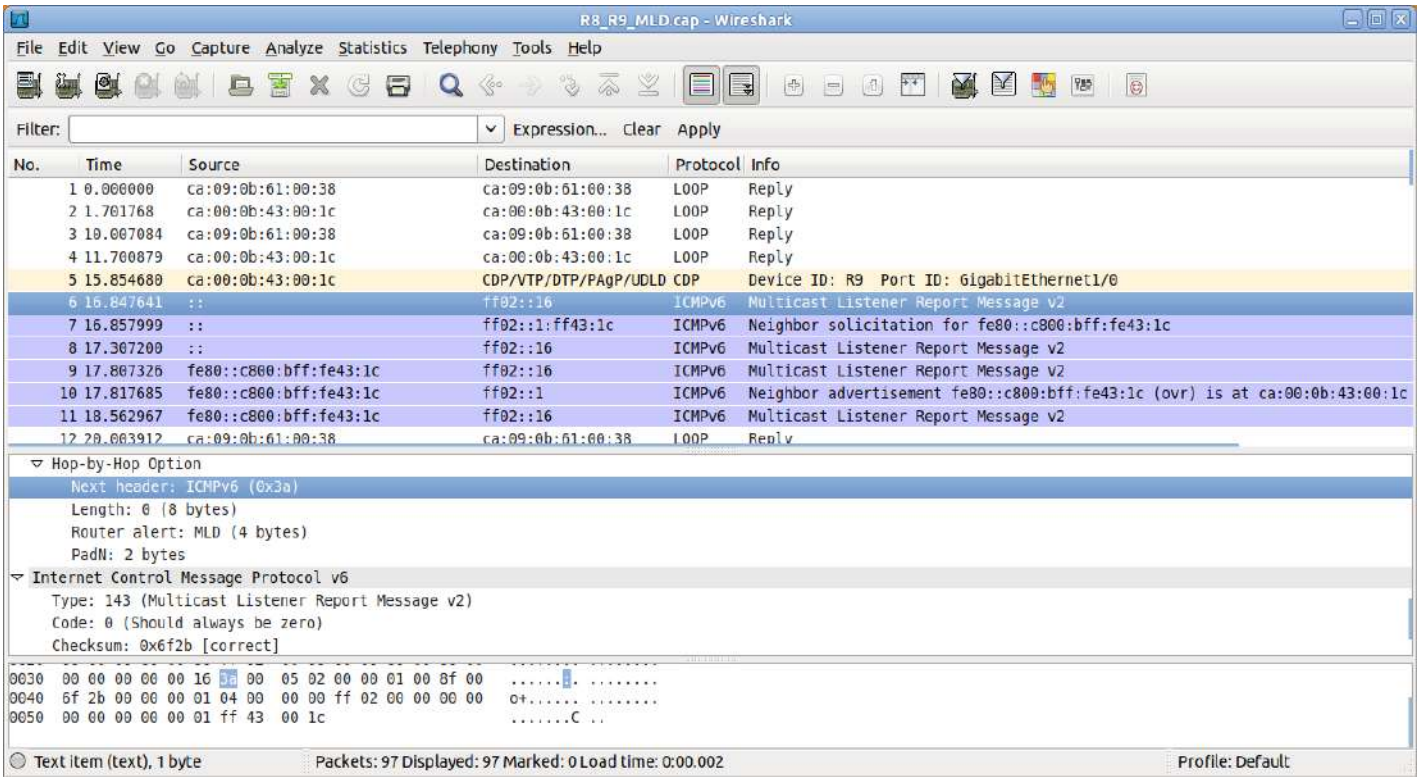


Figura 4.4: Next Header de ICMPv6 con el valor en hexadecimal 0x3a, que corresponde con el valor 58 en decimal.

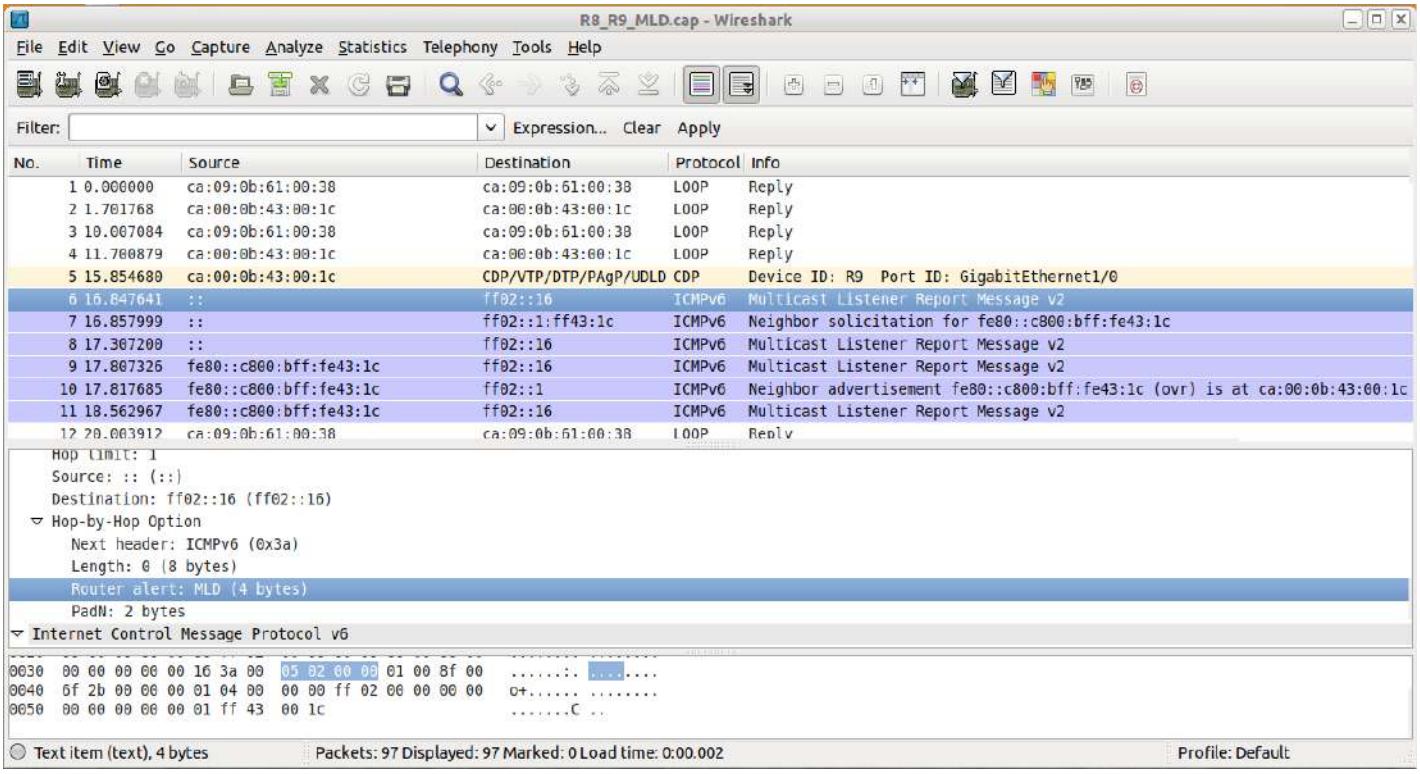


Figura 4.5: campo Router Alert

Puede observarse en la figura 4.5 , que en el paquete número 6 se envía un mensaje REPORT perteneciente al protocolo MLDv2, con dirección de origen :: (esta red) y dirección destino ff02::16.

Esta última dirección, es una link-local utilizada para conocer todos los routers compatibles con MLDv2, y se relaciona con IPv6 multicast routing. Vemos también el campo Type de ICMPv6 con valor 143.

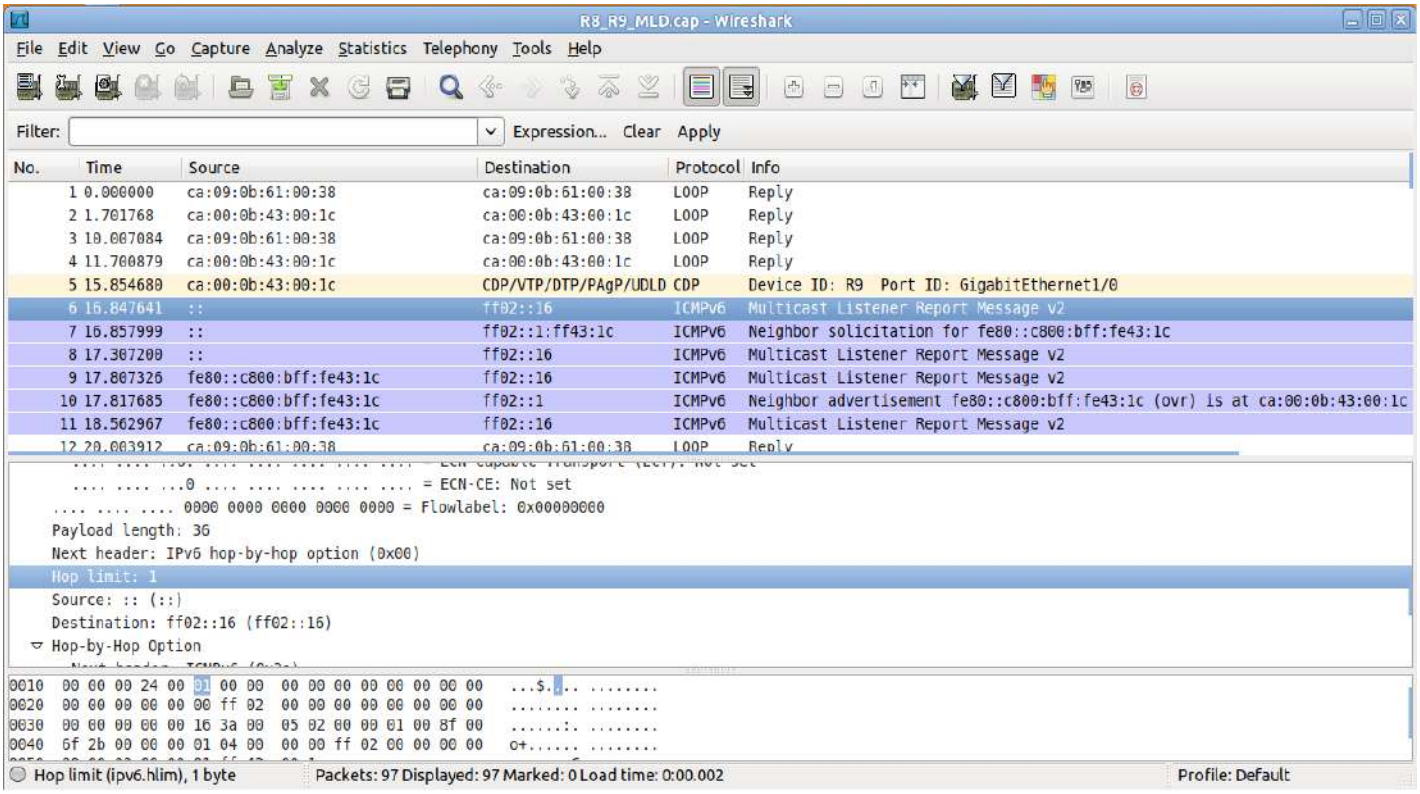


Figura 4.6: apreciamos el campo Hop Limit con valor 1

En el dispositivo de salida, IPv6 multicast routing debe estar habilitado. Luego el paquete numero 7 tiene un Neighbor Solicitation (ICMPv6 type 135) con dirección destino ff02::1:ff43:1c (dirección tentativa, falta verificar), vemos la captura (Figura 4.7) :

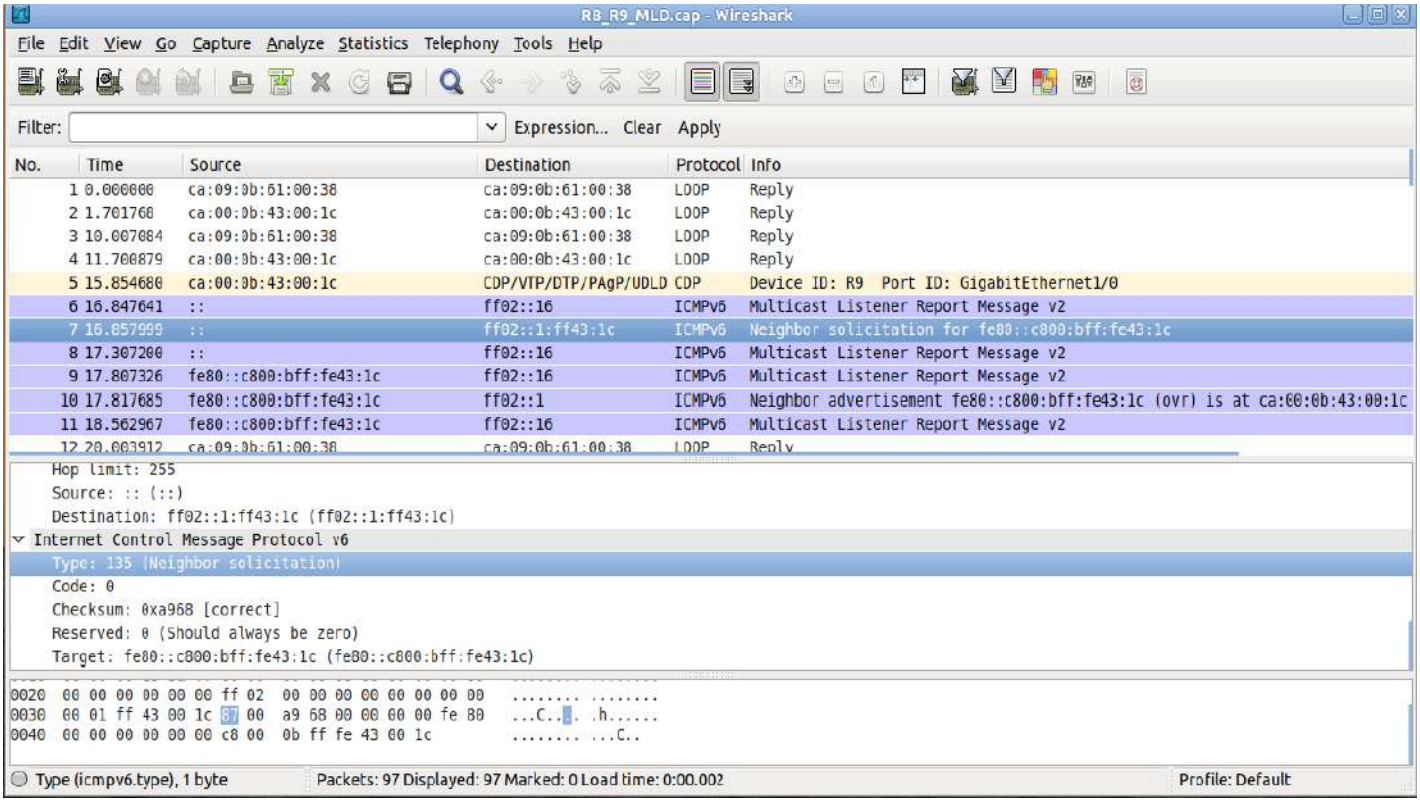


Figura 4.7: solicitud de vecino ICMPv6 campo type: 135

A modo de resumen del protocolo, podemos decir que antes que la dirección link-local pueda asignarse a una interfaz y utilizarse, el nodo debe verificar que esta dirección "tentativa" no esté en uso por otro. En concreto, se envía un mensaje de solicitud de vecino que contiene la dirección tentativa como destino. Si otro nodo ya esta utilizando esa dirección, devolverá un anuncio de vecino informando. Si otro nodo intenta utilizar la misma dirección, este nodo enviará también una solicitud de vecino para el mismo destino. El número exacto de veces que la solicitud de vecino es retransmitida y el tiempo de retardo entre solicitudes consecutivas es específico del enlace y puede ser fijado por el administrador del sistema.

Luego se ve en el paquete número 9, que ya se estableció una dirección link-local válida en la interfaz, la misma se utiliza como dirección de origen para enviar un paquete REPORT de MLDv2 , de esta forma se suscribe a la dirección multicast.

A continuación tenemos una anunciación de vecino en el paquete 10, como respuesta a la solicitud de vecino enviada previamente, pero esta vez a la dirección ff02::1 . El protocolo NDP (neighbor discovery protocol) usa esta dirección (ff02::1) para enviar un paquete en multicast y que todos los hosts en el enlace local lo reciban.

La dirección ff02::2 también es utilizada para mensajes multicast, con la diferencia que esta última seria para todos los routers (all routers) y no para todos los hosts.

De esta forma se conoce la vecindad de hosts y routers en un nodo.

4.4 Seguridad de Nivel de Red obligatoria

Internet Protocol Security (IPsec), es el protocolo para cifrado y autenticación IP, y pertenece al protocolo base en IPv6.

El soporte IPsec es obligatorio en IPv6; a diferencia de IPv4, donde es opcional (pero usualmente implementado). Sin embargo, actualmente no se está utilizando normalmente IPsec excepto para asegurar el tráfico entre routers de BGP Ipv6.

Para cumplir el objetivo de este trabajo, no nos adentraremos en lo que respecta a IPsec, pero dejamos en claro que puede resultar una alternativa conveniente si se desea cifrar la información que viaja entre dos nodos BGP garantizando una comunicación segura.

Aquí concluye el capítulo 4. En el siguiente capítulo, se mostrara los resultados del relevamiento, que trae al plano del lector, los dispositivos de red presentes en la empresa Aguas del Colorado, los cuales resultan cruciales al momento de examinar posibles soluciones a la problemática planteada.

Capítulo 5: Conocimiento general de la red

5.0 Introducción

En este capítulo, se darán detalles acerca de la infraestructura de red utilizada en la Empresa Aguas del Colorado, haciendo hincapié tanto en el software de los equipos (Versiones de sistema operativo utilizado) como en el hardware (tipo de interfaces disponibles, alimentación eléctrica, etc).

En cuanto a los protocolos de comunicaciones, en este capítulo solo se mencionaran los que se utilizan en la actualidad, ya que en el capítulo 7 expandiremos acerca de ellos.

Este tipo de información es trivial, ya que depende del tipo de tecnología disponible, las opciones que analizaremos como alternativa de solución, seleccionando aquellas que resulten viables para la actual problemática de agotamiento de direcciones IPv4 , y la inclusión del nuevo protocolo IP versión 6.

Se introduce a que es un backbone , ya que este tipo de modelo de red es el que implementó ADC en la actualidad. Luego veremos el tipo de hardware y software, para finalmente en el capítulo 7, detallar ampliamente la solución propuesta a la problemática planteada.

5.1 ¿ Qué es un backbone ?

La palabra backbone se refiere a las principales conexiones troncales de Internet. Una conexión troncal, esta compuesta de un gran número de routers comerciales, gubernamentales, universitarios y otros de gran capacidad interconectados que llevan los datos a través de países, continentes y océanos del mundo mediante cables de fibra óptica.

El término backbone también se refiere al cableado troncal o subsistema vertical en una instalación de red de área local que sigue la normativa de cableado estructurado.

Figura 5.1: Cableado vertical, troncal o backbone

5.1.1 Tipos de backbone

Según el tipo de conexiones, cableado, y acceso al medio, existen 2 tipos: cascada y colapsado.

En el primero, todos los puestos de trabajo (host, terminales) están conectados a un enlace troncal con el cuarto de equipos (ER – por sus siglas en Inglés "Equipment Room"); esta arquitectura es casi obsoleta y genera mucho tráfico innecesario en la red.

Figura 5.2: backbone en cascada (también llamado topología Bus)

En el colapsado existen varios tramos que salen del ER, permitiendo una mejor distribución de servicios, sin saturar ningún sector de la red y dando una mejor calidad de señal a los tramos lejos al ER.

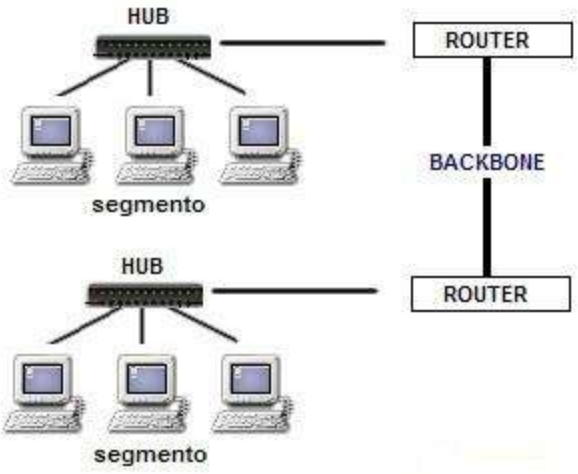


Figura 5.3: backbone conectando 2 segmentos

5.2 Relevamiento de hardware y Software

En este punto veremos la diversidad de equipos de red, los cuales utilizaremos para desplegar una topología que incluya encaminamiento IPv6, y luego, los protocolos de red que se utilizaron. En cuanto a hardware, tenemos los siguientes:

Routers: Cisco c3925 , Cisco c7201 , Cisco c2921 , Cisco c7609.

Tipos de Enlace: Fibra Óptica (ver Figura 5.5) y Cobre (RJ-45, ver Figura 5.4)

Figura 5.4: conector RJ-45 patchcord

Figura 5.5: cable jumper fibra óptica

En cuanto a los routers, describiremos brevemente características generales, las cuales tendrán mas relevancia en lo que respecta a este proyecto de tesis, ya que no tendría sentido extenderse en detalles que no hacen al propósito buscado. Podemos decir lo siguiente:

Cisco 3925: es un equipo de gran utilidad para utilizar como router de Borde de una red. Denominado por Cisco como "Integrated Services Router (ISR) Cisco 3925" , es un equipo que proporciona datos de alta seguridad, voz, vídeo y servicios de aplicación para pequeñas sucursales. Veremos a continuación, que tipos de interfaz y alimentación de energía nos provee este equipo:

- 3 puertos integrados Ethernet 10/100/1000 con 2 puertos capaces de RJ-45 o conectividad SFP (ver Nota 4)
- 2 ranuras para módulos de servicio

- 4 ranuras para Tarjetas de interfaz WAN de alta velocidad mejorada (EHWIC - Enhanced High-speed WAN interface cards)

- 4 ranuras de procesador de señal digital (DSP a bordo)

- 1 slot para Módulo de Servicios Internos

- Fuentes de alimentación duales integradas.

La distribución de energía esta totalmente integrada a los módulos con soporte 802.3af (Power over Ethernet) .

Nota 4: Un transceptor es un dispositivo que cuenta con un transmisor y un receptor que comparten parte de la circuitería o se encuentran dentro de la misma caja.

Un transceptor SFP, del inglés small form-factor pluggable transceptor (en español, transceptor de factor de forma pequeño conectable) es un dispositivo compacto y conectable en caliente (ver Nota 5) utilizado para las aplicaciones de comunicaciones de datos y telecomunicaciones. Están diseñados para soportar Sonet, canal de Fibra, Gigabit Ethernet y otros estándares de comunicaciones.

Nota 5: Conexión en caliente, traducido del inglés hot-plug, es la capacidad que tienen algunos periféricos de poder enchufarse o desenchufarse al ordenador, sin apagar el mismo, y funcionar correctamente.

Vemos la Figura 5.6 del equipo en cuestión:

Figura 5.6: Cisco 3925 Integrated Services Router

Estos equipos de red, utilizan un sistema operativo de Cisco (algo que resulta obvio), el Cisco IOS (se explica en el capítulo 6). Puede verse la versión del IOS disponible, desde la consola

escribiendo el siguiente comando: `#show version`. Vemos en la Figura 5.7, las versiones de IOS y el archivo de imagen del sistema.

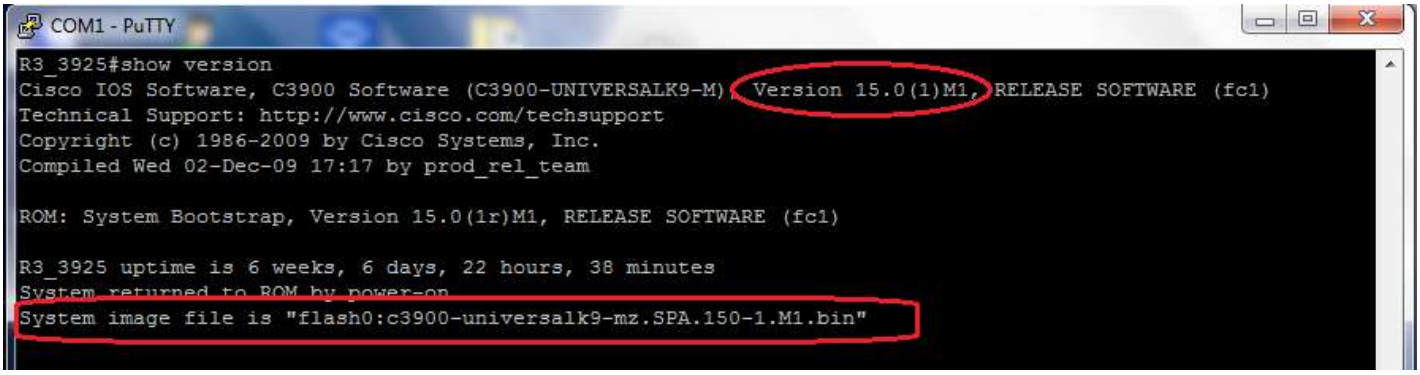


Figura 5.7: Salida del comando #show version del Cisco 3925 Integrated Services Router

Puede verse la versión del IOS: Version 15.0 (1) M1 , el archivo de Imagen del sistema: "flash0:c3900-universalk9-mz.SPA.150-1.m1.bin". Además tiene una imagen de IOS universal que le permite desplegar nuevos servicios rápidamente.

Cisco c7201: este equipo, ofrece hasta dos millones de paquetes por segundo (Mpps) en Cisco Express Forwarding (CEF).

Dispone de:

- 4 puertos Gigabit Ethernet (GE) integrado .
- 1 puerto Ethernet de cobre de 10/100-Mbps dedicado para la gestión.
- 1 puerto USB para almacenamiento general y el almacenamiento de token de seguridad
- una única ranura de adaptador de Cisco 7000
- flujo de aire de adelante hacia atrás.

Vemos en la Figura 5.8 , el Cisco c7201 :

Figura 5.8: Cisco 7201

Podemos ver en la siguiente Figura 5.9, información acerca del IOS que tiene instalado, y el archivo de imagen del sistema.

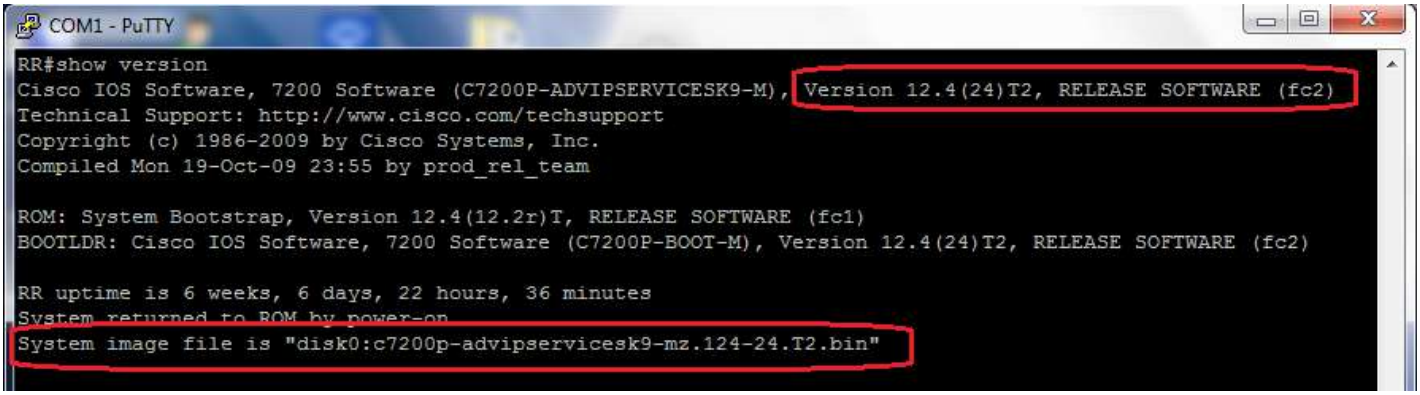


Figura 5.9: Salida del comando #show version del Cisco c7201

Puede verse que tiene el IOS Version 12.4 (24)T2, y el archivo de Imagen de Sistema: "disk0:c7200p-advipservicesk9-mz.124-24.T2.bin" como se ve, se encuentra en disk0.

Cisco 2921 (Integrated Services Router): este equipo proporciona datos de alta seguridad, voz, video y servicios de aplicaciones para pequeñas oficinas. Las características clave incluyen:

- 3 puertos integrados Ethernet 10/100/1000 con 1 puerto capaz de RJ-45 o conectividad SFP
- 1 ranura para módulo de servicio
- 4 Tarjeta de interfaz WAN de alta velocidad mejorada (EHWIC)
- 3 ranuras de procesador de señal digital a bordo
- 1 ranura del módulo de servicio interno de servicios de aplicaciones
- Distribución de energía totalmente integrado a los módulos de soporte 802.3af Power over Ethernet (PoE) y Cisco PoE mejorada.

Vemos en la Figura 5.10 el Cisco 2921:

Figura 5.10: Cisco 2921

Podemos ver en la Figura 5.11, información acerca del IOS que tiene instalado, y el archivo de imagen del sistema.

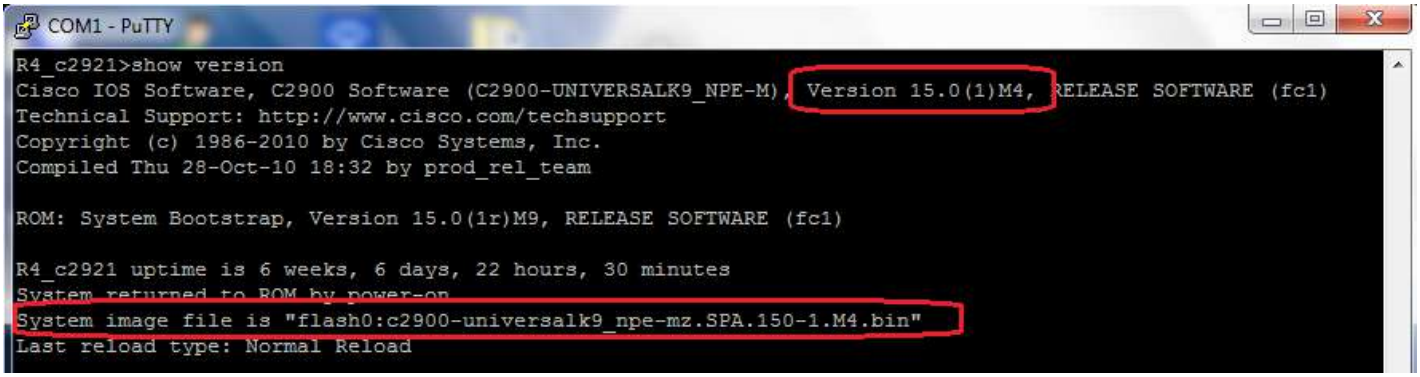


Figura 5.11: Salida del comando #show version del Cisco c2921

Puede verse que tiene el IOS Version 15.0 (1)M4 , y el archivo de Imagen de Sistema: "flash0:c2900-universalk9_npe-mz.SPA.150-1.M4.bin" como se ve, se encuentra en flash0.

Cisco 7609-S Router

El Cisco 7609-S Router es un router de alto rendimiento desplegado en el borde de la red, donde el rendimiento, servicios IP, redundancia y capacidad de recuperación frente a fallos son críticos (Fuentes de alimentación y módulos de ventilación redundantes). Permite a los proveedores de servicios Carrier Ethernet desplegar una infraestructura de red avanzada que admite una amplia gama de vídeo IP y triple-play (voz, video y datos).

Con una tasa de transmisión de hasta 400 Mpps distribuidos y un rendimiento total de 720 Gbps, el Cisco 7609-S ofrece un rendimiento y fiabilidad con opciones de redundancia en los procesos de encaminamiento y alimentación energética.

Es un equipo con numerosas características y aplicaciones, para mayor información, consultar el sitio oficial de cisco en la dirección web:

http://www.cisco.com/en/US/prod/collateral/routers/ps368/ps367/product_data_sheet0900aecd8057f3d2.html

Figura 5.12: Cisco 7609-S Router

Resúmen del capítulo

En lo que respecta a tipos de enlace, se utilizan enlaces de fibra óptica, de 1 y 10 Gigabits por segundo para los enlaces internos del backbone, y enlaces de fibra y de cobre para los clientes según necesidad de ancho de banda y plan contratado.

En cuanto a protocolos de red utilizados actualmente, se describirá teóricamente y con ejemplos de configuración en el capítulo 7. Estos son:

- **Open Shortest Path First** (OSPF version 2 para IPv4)

- **BGP** (del inglés Border Gateway Protocol)

Capítulo 6: Software de Emulación y Protocolo Cisco Express Forwarding (CEF)

6.0 Introducción

La utilización de un Software de emulación resulta de gran utilidad, cuando el objetivo de un proyecto es ofrecer una solución estable, viable, y eficiente frente a una problemática. Las ventajas que nos ofrece un software de emulación son variadas, podemos destacar las siguientes:

- Permite analizar diferentes soluciones sin costo alguno (mediante la emulación virtual), y seleccionar que alternativas se adaptan mejor a nuestra problemática
- Evaluar la complejidad en cuanto a las configuraciones de los equipos (con el software de emulación GNS3 podemos emular diferentes equipos de marca Cisco)
- Integración de todos los equipos de una topología en el mismo software, de forma tal de no tener que moverse a cada equipo para las configuraciones individuales
- Probar equipos que no se dispone, y realizar comparaciones entre distintos equipos. De esta manera, se tiene un panorama global de que equipos presentan ventajas con respecto a otros, y cuales se adaptan mejor para una tarea específica.

A continuación, veremos el software de emulación que se utilizó, denominado GNS3.

6.1 Software de Emulación: GNS3 (Graphical network simulator 3)

GNS3 (graphical network simulator 3) es un simulador gráfico de red basado en la IOS de Cisco Systems. Con este simulador podemos crear un laboratorio 100% operativo de dispositivos Cisco, solo necesitamos disponer de las imágenes IOS de cada uno de los routers, switches o firewalls a usar. Resulta bastante útil para la preparación de certificaciones CCNA, CCNP, CCIE y otras, ademas de volcar entornos de clientes y realizar pruebas reales. Además es un programa de código abierto y compatible con muchos sistemas operativos. (Ver logotipo en Figura 6.1).

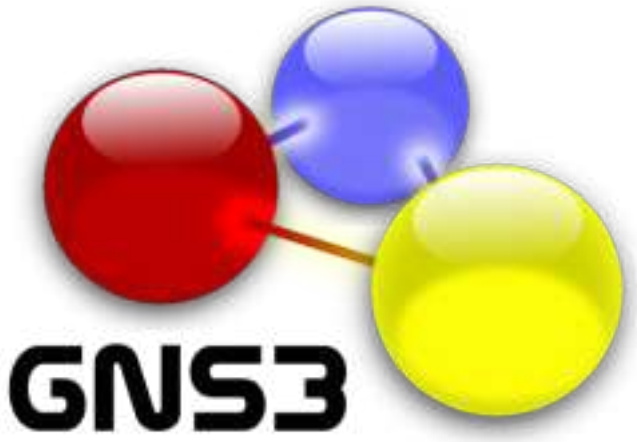


Figura 6.1: Logotipo Software de Simulaciones IOS GNS3

6.2 Cisco IOS

Cisco IOS es el software utilizado en la gran mayoría de routers y switches (conmutadores) de Cisco Systems (algunos conmutadores obsoletos ejecutaban CatOS). IOS es un paquete de funciones de encaminamiento, conmutación, trabajo de Internet y telecomunicaciones que se integra estrechamente con un sistema operativo multi-tarea.
La interfaz de línea de comandos de IOS (IOS CLI) proporciona un conjunto fijo de comandos de múltiples palabras. El conjunto disponible se determina mediante el "modo" y el nivel de privilegios del usuario actual. El modo "Global configuration" proporciona comandos para cambiar la configuración del sistema y el modo "interface configuration" a su vez, proporciona comandos para cambiar la configuración de una interfaz específica. A todos los comandos se les asigna un *nivel de privilegios*, de 0 a 15, y pueden ser accedidos por usuarios con los privilegios necesarios. A través de la CLI, se pueden definir los comandos disponibles para cada nivel de privilegio.

Arranque del IOS

Al arrancar un dispositivo de Cisco este realiza un Bootstrap (comprobación de Hardware). Después intentara cargar una imagen IOS desde la memoria Flash o desde un servidor TFTP. En el caso de no hallarla, ejecutará una versión reducida de la IOS ubicada en la ROM.
Tras el arranque del sistema localizará la configuración del mismo, generalmente en texto simple. Puede estar ubicada en la memoria NVRAM o en un servidor de TFTP. En el caso de no encontrarla iniciará un asistente de instalación (modo Setup). En la Figura 6.2 puede quedar mas claro:

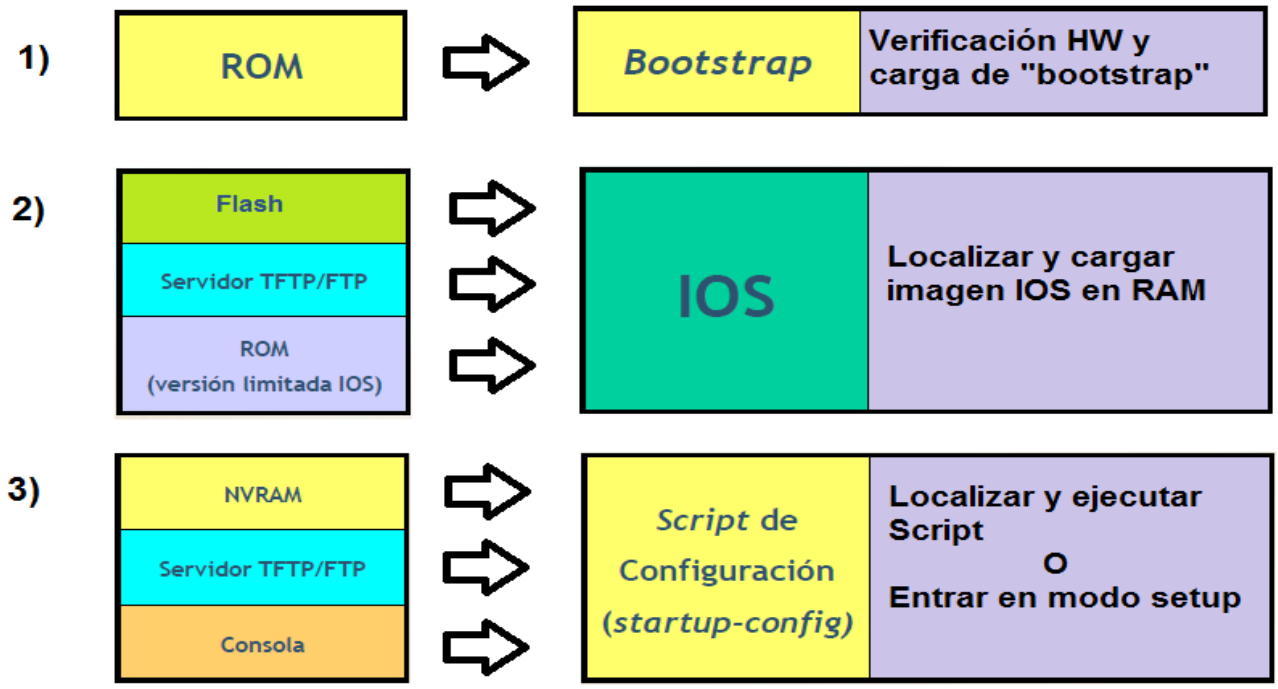


Figura 6.2: Proceso de Arranque del IOS

Sistema de Archivos: IOS File System (IFS) puede acceder y almacenar distintos tipos de datos en:

- Bootflash
- Flash: se usa para almacenar imágenes completas del software Cisco IOS. Guarda copia del sistema operativo (como se vió en el capítulo 4)
- Flh
- Nvram es uno de los componentes de configuración interna de un router. Se usa para almacenar un archivo de configuración de respaldo/inicio
- RCP
- Slo
- Slot1
- System
- TFTP

Modos de configuración

- **Modo USER EXEC:** Modo sin privilegios en el que no podemos modificar ni leer la configuración del equipo. Básicamente, solo podemos utilizar: show, ping, telnet, traceroute. Debemos escribir "*enable"* en el terminal, para acceder al siguiente modo.

- **Modo PRIVILEGED EXEC: Modo de visualización con privilegios.** Debemos escribir "*configure terminal"* en el terminal, para acceder al siguiente modo.

- **Modo de Configuración Global o CONFIGURE:** Permite configurar aspectos simples del equipo como pueden ser el nombre, alias de comandos, reloj, etc.
  Escribiremos en el terminal de consola: "*interface, line, router…"* dependiendo de lo que queramos configurar.

- **Modos de configuración específicos:** Permiten configurar protocolos, interfaces o en general aspectos mas complejos del equipo.

6.3 CEF (Cisco Express Forwarding)

Es una característica del Cisco IOS que permite un modo de conmutación mas rápido en los dispositivos Cisco. ¿ Qué es CEF y como trabaja? Lo vemos a continuación.

Introducción a CEF

Una tarea esencial en los dispositivos de capa 3 (routers y switches layer 3), es la toma de decisiones respecto de donde deben reenviar los paquetes que reciben.
Este proceso de decisión es el que toma el nombre de "conmutación" (Switching en inglés), y es diferente del proceso de conmutación que se realiza en un switch Ethernet (capa 2).
Cuando un dispositivo capa 3 "conmuta" ejecuta las siguientes operaciones: Decidir si debe o no reenviar un paquete después de verificar que la red de destino del paquete es "alcanzable". Si el destino es alcanzable, ¿cuál es el próximo salto y que interfaz debe utilizarse para

alcanzar este destino?, ¿se debe o no modificar la dirección MAC con la que se encapsula el paquete?. Los routers y switches layer 3 Cisco IOS ofrecen la posibilidad de operar con diferentes opciones o modos de conmutación. CEF es uno de los modos de conmutación disponibles.

Tomando como base de referencia la tabla de encaminamiento IP, CEF crea su propia tabla de reenvío que se denomina Forwarding Information Base (FIB). La FIB es una tabla organizada de modo diferente que la tabla de encaminamiento, y es la que se utiliza para definir a que interfaz se debe reenviar el paquete; de este modo, CEF ofrece varios beneficios:

- Tiene mejor rendimiento que el modo de conmutación por defecto de los dispositivos (fast-switching) y requiere menos ciclos de CPU para realizar la misma tarea.

- Cuando esta habilitado este modo de conmutación, es posible utilizar otras características avanzadas, como NBAR (Network Based Application Recognition).

- Esencialmente, CEF es un modo de conmutación de tráfico mas rápido que otros disponibles.

Habilitación y des-habilitación de CEF

CEF se encuentra deshabilitado por defecto en todos los dispositivos Cisco, excepto en los routers de la serie 7xxx, 6500 y 12000. Los routers de las series 2600, 3600, 3800 incorporan esta característica a partir de Cisco IOS 12.2(11)T. Para habilitar este modo de conmutación se debe operar desde el modo de configuración global:

```
router#configure terminal
router(config)#ip cef
```

Para deshabilitar esta función el proceso es igualmente simple:

```
router(config)#no ip cef
```

Monitoreo del status de CEF : Como es habitual, Cisco IOS ofrece un conjunto de comandos show que permiten verificar el estado y operación de CEF:

`show ip cef` es el comando que permite verificar las entradas de la tabla FIB.

Un ejemplo del comando lo vemos en la Figura 6.3 en la siguiente página .

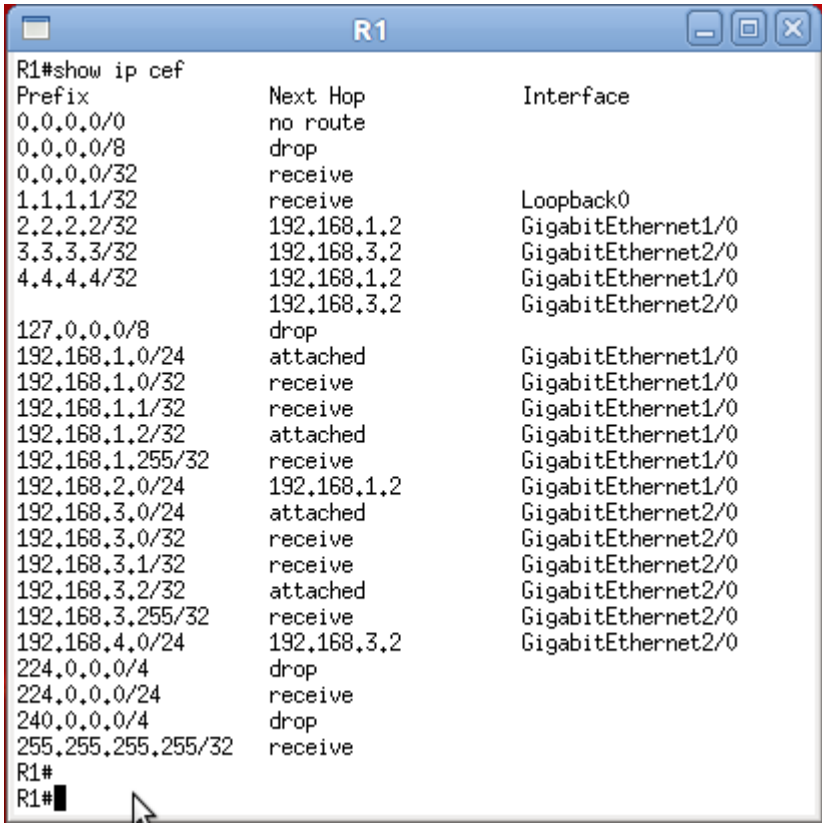


Figura 6.3: salida del comando show ip cef

Pueden apreciarse los prefijos ip con el siguiente salto asignado, y a través de que interfaz (Figura 6.4):

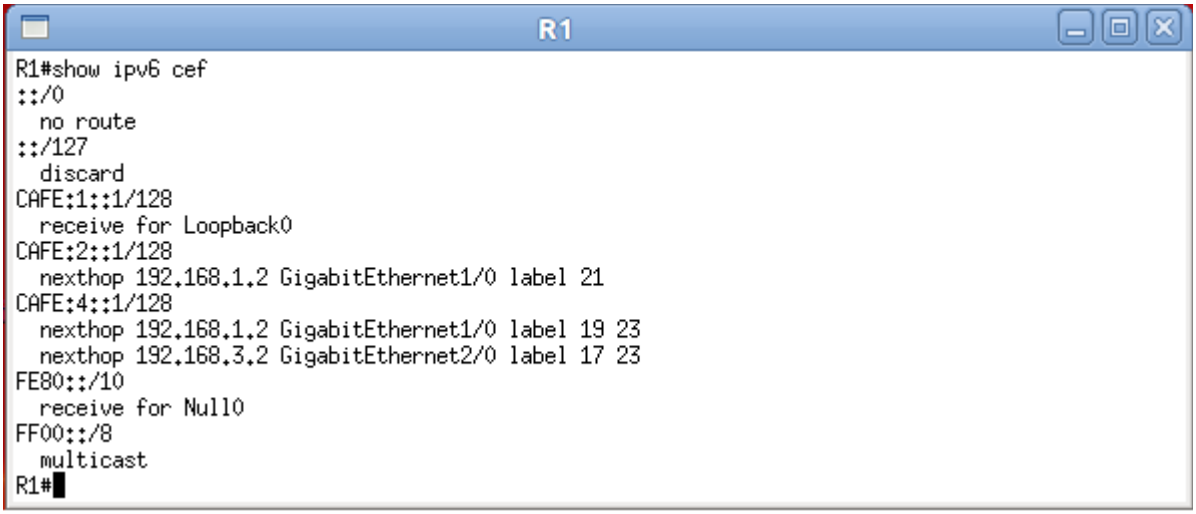


Figura 6.4: salida del comando show ipv6 cef

Concluimos de este capítulo, que el Software de Emulación GNS3 resulta muy útil para realizar análisis de redes, y representa una herramienta imprescindible en un entorno de tecnología Cisco Systems.

Capítulo 7: Protocolos utilizados y Solución Propuesta

7.0 Introducción

Del relevamiento realizado, se obtuvo como resultado una visualización general de los nodos principales que componen el backbone, y los protocolos de red mas utilizados. Estos son:

- **Open Shortest Path First** (OSPF versión 2 para IPv4)
- **BGP** (del inglés Border Gateway Protocol)
- **Multi Protocol Label Switching** (MPLS)
- **Virtual Private Network** (VPN) y **Virtual Routing and Forwarding** (VRF)

Para la inclusión del protocolo IPv6, se continuarán utilizando los mismos protocolos, haciendo las adaptaciones correspondientes. Para obtener un entorno de pruebas, el cual nos permita realizar configuraciones y pruebas de conectividad, se utiliza una topología piloto, implementando protocolos de capa 3: OSPF (para el encaminamiento interno del núcleo) y BGP para el encaminamiento en los routers de borde. La publicación de rutas sera a través de BGP con Route Reflector. En la sección 7.7 se verán capturas y pruebas de funcionamiento. A continuación la topología, luego los protocolos y solución propuesta.

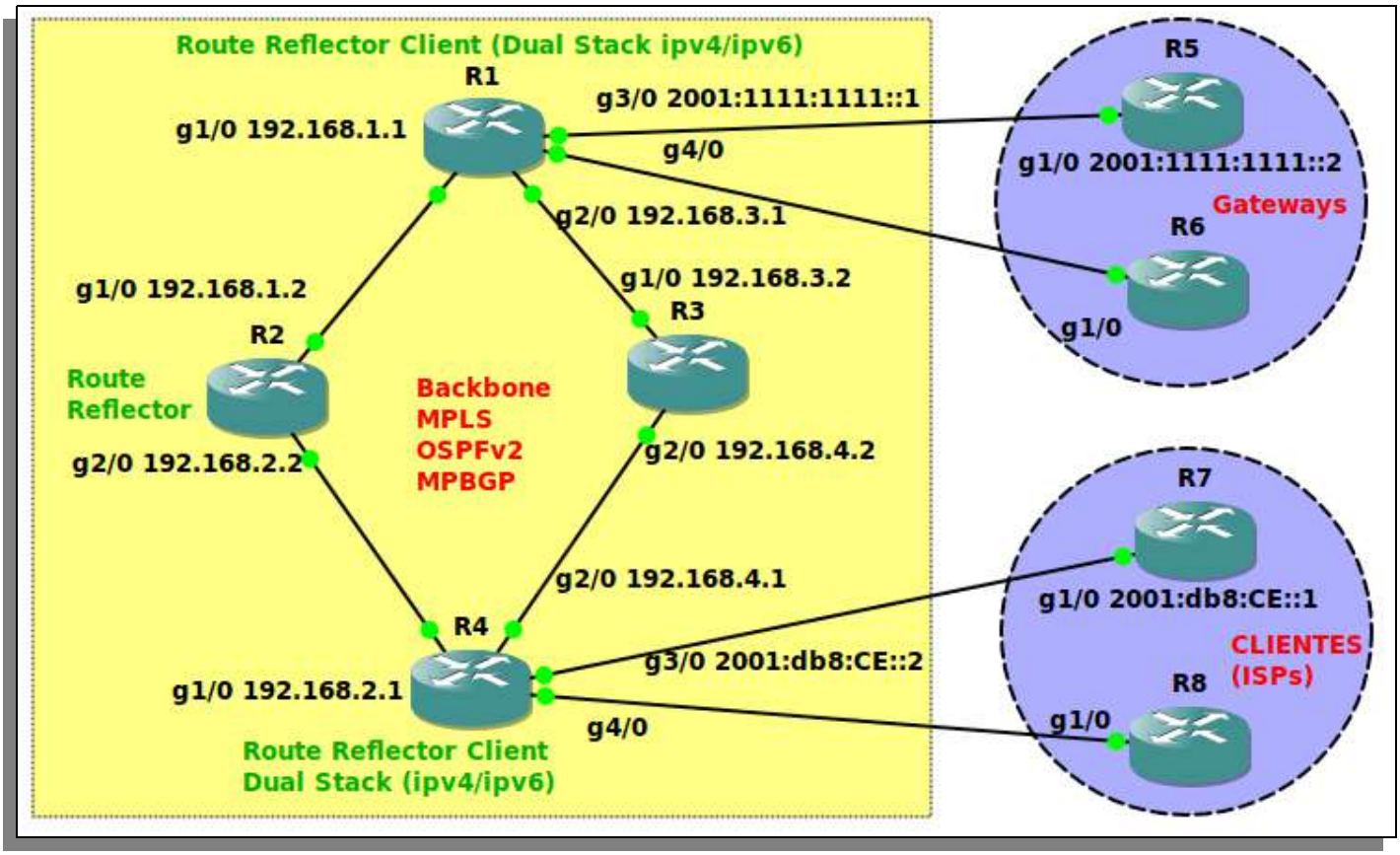


Figura 7.1: topología presentada con GNS3

La topología que muestra la figura 7.1, nos indica que tenemos los routers R1, R2, R3 y R4 representando el Backbone MPLS que pertenecería a la Empresa ADC, la cual representa al sistema autónomo 65000 (se escogió este valor arbitrariamente). Tiene como IGP a OSPFv2 (para IPv4).

Luego tenemos los routers R7 y R8 que representan Clientes que se conectan al Backbone de la Empresa (como por ejemplo proveedores de internet), y los routers R5 y R6 representan los Gateways que utiliza la empresa para salir a la nube de Internet (podrían ser un sistema autónomo remoto).

De la comunicación Backbone-Clientes, y Backbone-Gateways se encarga el protocolo de pasarela exterior llamado BGP, con soporte para VPN/VRF y familia de direcciones IPv6.

También puede apreciarse que el Router 2 esta configurado como reflector de rutas (RR), configuración que se explica en detalle en el capítulo 8. Los routers fronterizos R1 y R4 se configuran doble pila IPv4/IPv6. La palabra Gx/x en los enlaces punto-a-punto de los routers indican el numero de interfaz. Pasamos entonces a ver los protocolos aquí expuestos.

7.1 Open Shortest Path First (OSPF)

Open Shortest Path First (frecuentemente abreviado OSPF) es un protocolo de encaminamiento jerárquico de pasarela interior o IGP (Interior Gateway Protocol), que usa el algoritmo Dijkstra enlace-estado (LSA - Link State Algorithm) para calcular la ruta más corta posible (se computa localmente en cada router para rellenar la tabla de encaminamiento partiendo de la base de datos de la topología de la red). Usa cost como su medida de métrica. Además, construye una base de datos enlace-estado (link-state database, LSDB) idéntica en todos los routers de la zona. OSPF es probablemente el tipo de protocolo IGP mas utilizado en grandes redes.

A lo largo del tiempo, se han ido creando nuevas versiones, como OSPFv3 que soporta IPv6 o como las extensiones multidifusión para OSPF (MOSPF), aunque no están demasiado extendidas. OSPF puede "etiquetar" rutas y propagar esas etiquetas por otras rutas.

Ver Anexo 5: RFC 2328 OSPF Version 2 April 1998 ; y Anexo 25 : RFC 5340 OSPF for IPv6 July 2008

Configurando OSPFv2 en router 1: Comandos de configuración

```
R1>en
R1#configure terminal
R1(config)#router ospf 1
R1(config-router)#router-id 1.1.1.1
R1(config-router)#log-adjacency-changes
R1(config-router)#redistribute connected
R1(config-router)#network 1.1.1.1 0.0.0.0 area 0 → red de loopback
R1(config-router)#network 192.168.1.0 0.0.0.255 area 0 → enlazamos con R2
R1(config-router)#network 192.168.3.0 0.0.0.255 area 0 → enlazamos con R3
```

Se debe realizar el mismo procedimiento para R2 , R3 y R4. Veamos como queda la Base de datos OSPF en R2 en la siguiente Figura 7.2:

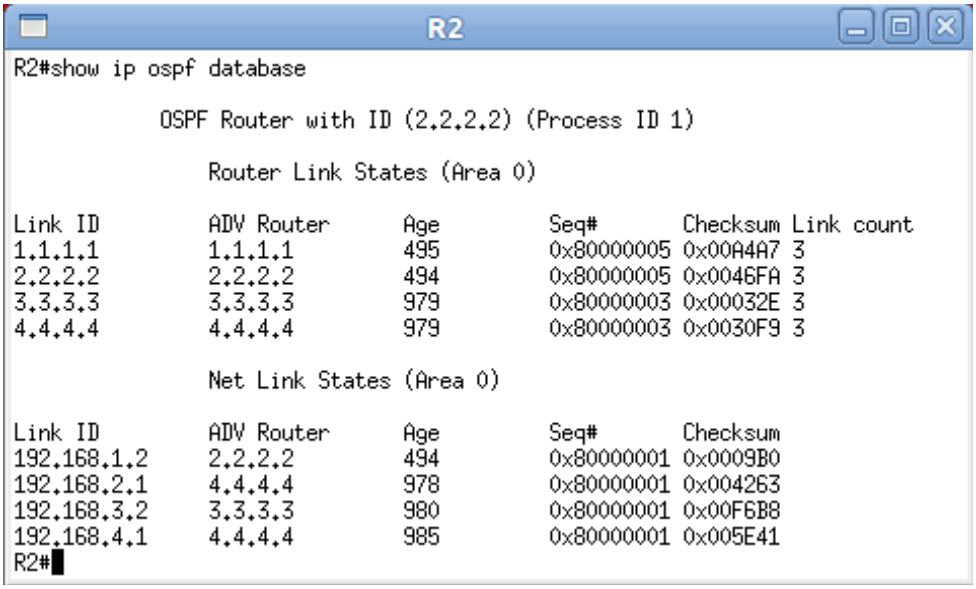


Figura 7.2: Base de Datos OSPF en R2

La ejecución del comando `#show ip ospf database`, tiene como salida:

- **OSPF Router with ID (2.2.2.2) (Process ID 1):** nos indica el protocolo que se esta ejecutando (OSPF para IPv4), el router-id configurado previamente en dicho router, y el identificador de proceso.

- **Router Link States (Area 0):** (LSA type 1) cada dispositivo participante en OSPF envía estos avisos en los cuales anuncia el estado de cada uno de sus enlaces OSPF. Cuando se ejecuta el comando #show ip ospf database, cada línea router Link States es un tipo LSA 1 perteneciente a un router diferente (identificado por el router-id previamente configurado). Como se puede ver en la captura, tenemos:

  - **ADV Router:** El router origen de los LSA, representado por su router-id: 1.1.1.1 , 2.2.2.2 , 3.3.3.3 y 4.4.4.4

  - **Age** (edad del LSA). Número de segundos que han pasado desde que el LSA fue generado. Como puede verse, el Age con mayor valor es el que genero el mismo (es decir, es el más antiguo).

  - **Seq#** (número de secuencia de los LSA): este número inicia con 0x80000001 y sirve para detectar LSAs antiguos o duplicados

  - **Checksum**: checksum de todo el contenido del anuncio de estado de enlace.

  - **Link count (Contador de enlaces):** Número de interfaces detectadas del router.

  - **Fragment ID** (ID de Fragmento) : En OSPFv2,el Link State ID en el header contiene el router-id del ASBR. En OSPFv3 , Link State ID es el número de fragmento, y el ASBR Router ID se encuentra dentro del body del LSA. Un paquete Router-LSA puede dividirse en múltiples LSAs, así el Link State ID en el header, es el Fragment ID.

Protocolo Hello

Descubre a sus vecinos (otros routers OSPF conectados a su misma subred) utilizando un protocolo HELLO. Los mensajes HELLO sirven para:

• Descubrir los routers vecinos.

• Comprobar permanentemente accesibilidad con los vecinos.

Los mensajes HELLO se envían en un router por todas las interfaces que tienen activado el protocolo OSPF. Los mensajes HELLO se envían cada 10 segundos a través de una dirección de multicast (All-OSPF routers 224.0.0.5) y TTL=1.
Se supone que un vecino esta desconectado si no se recibe de él información de HELLO en 4 períodos (40 segundos). Los mensajes HELLO no se propagan por inundación, solo tienen sentido en la subred en la que se generan.

Protocolo HELLO: Designated Router (DR)

- Los mensajes HELLO de una subred se utilizan para elegir al DR de esa subred.
- El router Designado (DR, Designated Router) de una subred es el router representante de esa subred y se encarga de exportar la información de esa subred al resto de routers:
    - Evita que todos los routers conectados a la misma subred generen un mensaje con la información de los datos de esa subred y lo envía al resto de los routers OSPF: se ahorran mensajes.
    - El propósito del DR es permitir que la LAN sea tratada como un único nodo, a través de su nodo representante o DR.
- El DR de una subred es la dirección IP dentro de esa subred de uno de los routers que están conectados a dicha subred.
- Si en la red no hay un DR elegido, al iniciar un router enviará mensajes HELLO con el campo DR vacío (0.0.0.0) y transcurridos 40 segundos se elegirá el DR teniendo en cuenta los siguientes criterios:
    - Cada router elige como DR el router que envíe mayor número en el campo router Priority de los mensajes HELLO.
    - En caso de empate en ese campo, cada router elige como DR el que tenga mayor identificador.
- Si en la red ya hay un DR elegido, al arrancar un router recibirá mensajes HELLO con la dirección IP del DR y aprenderá la dirección IP del DR.
- En los mensajes HELLO viajará la dirección IP del DR elegido.

Protocolo HELLO: DR y BDR

- Adicionalmente al DR se elige el BDR que es un DR de backup (siguiente router que cumple los criterios de elección de DR) también a través de los mensajes HELLO.

- Una vez elegido BDR, la dirección IP del BDR de esa subred se enviará en el campo BDR de los mensajes de HELLO. Si el DR deja de funcionar, el BDR se convierte en el nuevo DR.

- Una vez elegidos DR y BDR en una subred si se conecta un router a esa subred, no se modifican los valores de DR y BDR (evita oscilaciones), incluso aunque los routers que se conecten tengan mayor prioridad o mayor identificador.

- Si en una subred solo hay conectado un router OSPF, este se elegirá como DR y no habrá BDR. Si posteriormente arrancan otros routers OSPF conectados a esa subred, se elegirá el BDR.

Formato de mensaje HELLO

Vemos en la siguiente Figura 7.3, como el mensaje de divide en dos secciones bien definidas, la cabecera y los datos :

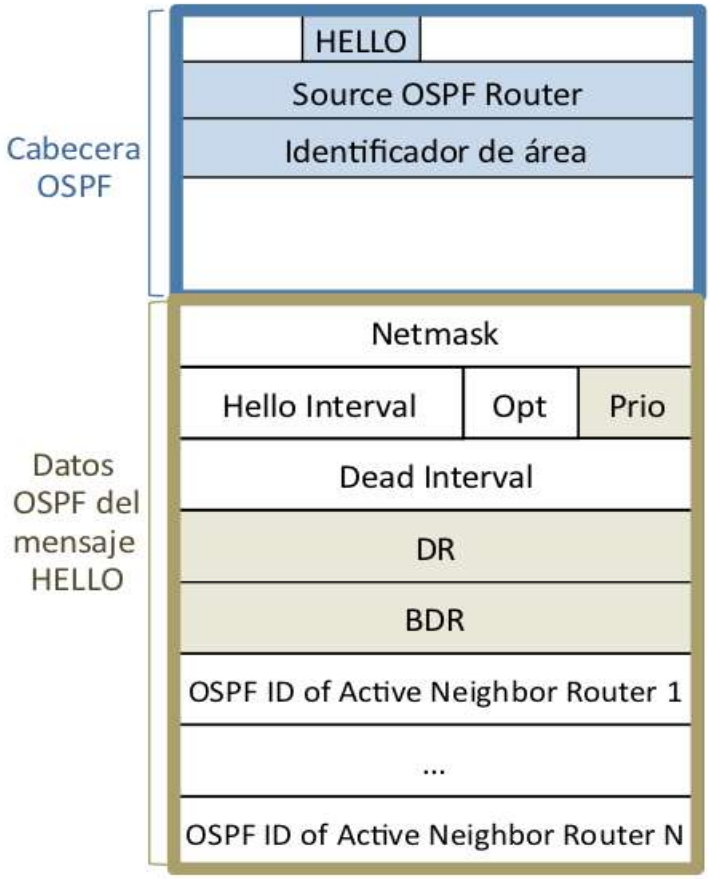


Figura 7.3: formato de mensaje hello

- **Netmask:** Mascara de la subred donde se envía el mensaje
- **Hello Interval:** intervalo en segundos entre mensajes HELLO consecutivos
- **Prio:** prioridad del router que envía el mensaje HELLO para la elección de DR/BDR.
- **Dead Interval:** período en segundos en el que se considera a un vecino OSPF desaparecido si no se recibe de él un nuevo HELLO
- **DR:** Designated Router
- **BDR:** Backup Designated Router
- **OSPF ID of Active Neighbors i:** Identificadores de los routers OSPF vecinos de los que tiene conocimiento (han enviado un HELLO).

Elección de DR y BDR

La idea del DR es que todos los routers se comuniquen con un router central, en lugar de con todos los demás. La elección del DR y BDR se realiza mediante el protocolo Hello (este proceso solo se producirá en redes broadcast o nonbroadcast multi-access, no en Protocolo punto a punto).

El DR sera el router configurado con mayor prioridad, y el que tenga la segunda prioridad mas alta será el BDR. Si todos tienen la misma prioridad, entonces se elegirá como DR al router que tenga su router-ID mas alto. Las prioridades se pueden establecer en cualquier valor de 0 a 255.
Como el router- ID es la interfaz con ip más alta, podemos configurar una ip de loopback para cambiarla. También se puede configurar una prioridad de 0, y el router no intervendrá en el proceso (Este router se designará como DRother en lugar de DR o BDR.).

En las redes multiacceso de broadcast es posible que haya mas de dos routers. OSPF elige un router designado (DR) para que sea el punto de enfoque de todas las actualizaciones del estado de enlace y de las publicaciones del estado de enlace. Debido a que la función del DR es crítica, se elige un router designado de respaldo (BDR) para que reemplace a DR en caso de que este falle. Si el tipo de red de una interfaz es broadcast, la prioridad OSPF por defecto es 1. Cuando las prioridades OSPF son iguales, la elección de OSPF para DR se decide a base del ID del router. Se selecciona el router de ID mas elevado.

El resultado de la elección puede determinarse asegurándose de que las votaciones, los paquetes hello, contengan una prioridad para dicha interfaz del router. La interfaz que registra la mayor prioridad para un router permitirá asegurar que se convertirá en DR.

Después del proceso de elección, el DR y el BDR conservan sus funciones aún cuando se agreguen a la red routers con valores de prioridad OSPF mas altos. Se modifica la prioridad OSPF introduciendo el comando de configuración de interfaz `ip ospf priority` en una interfaz que participa en OSPF. El comando `show ip ospf interface` mostrará el valor de prioridad de interfaz así como otra información clave.

Consideraciones a tener en cuenta

En la topología presentada, no tiene mucho sentido configurar manualmente el DR y BDR ya que hay solo 4 routers dentro del backbone y los enlaces son punto-a-punto a través de una conexión en serie R1-R2-R3-R4 (o conexión anillo).

Del análisis del protocolo, y la elección de DR y BDR, se concluye que no tiene gran impacto la elección de DR y BDR en una topología en estrella, topología BUS o una combinación de ellas, donde cada interfaz de cada router se ve con mas de una interfaz de otro/s router/es.

Para estos casos, una buena política de elección de DR y BDR puede significar una mejoría en el rendimiento de la red, disminuyendo el tráfico de paquetes hello, además de elegir al mejor candidato para ser DR (router mas potente, router de borde, o simplemente el router con menor costo de alcance a los demás routers, es decir, a menor cantidad de saltos). La figura 7.4 ilustra gráficamente tipos de topologías de red.

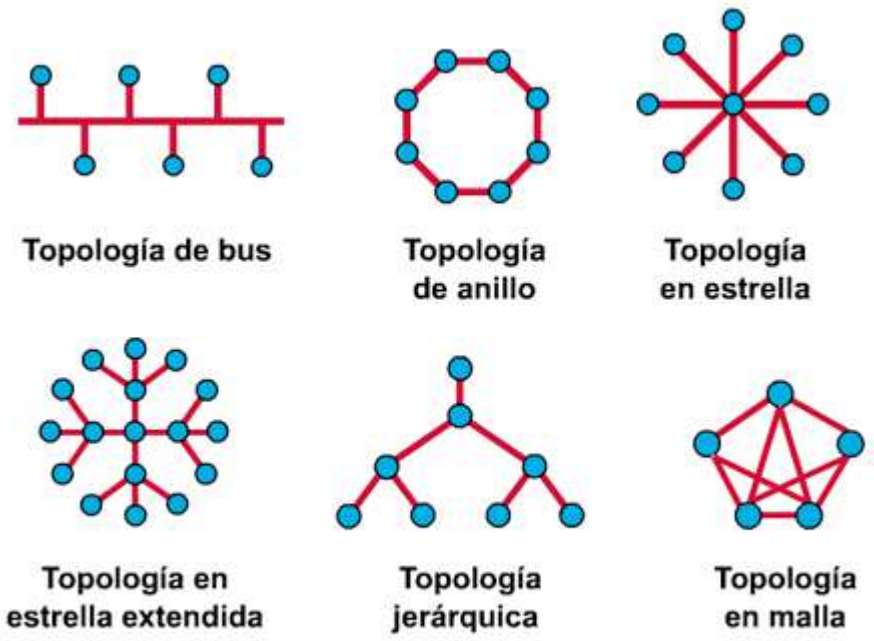


Figura 7.4: Topologías de red

Se finaliza en este punto lo relativo a información teórica del protocolo OSPF, pasaremos a ver a continuación el protocolo de borde externo BGP.

7.2 Border Gateway Protocol (BGP)

BGP o Border Gateway Protocol [13] es un protocolo mediante el cual se intercambia información de encaminamiento (tablas de rutas) entre sistemas autónomos Este intercambio de información de encaminamiento se hace entre los routers externos de cada sistema autónomo.
Cada sistema autónomo (AS) tendrá conexiones o, mejor dicho, sesiones internas (iBGP) y además sesiones externas (eBGP). BGP garantiza una elección de rutas libres de bucles.

Para conseguir una entrega fiable de la información, se hace uso de una sesión de comunicación basada en TCP en el puerto número 179. Esta sesión debe mantenerse conectada debido a que ambos extremos de la comunicación periódicamente se intercambian y actualizan información.

De modo que al principio, cada router envía al vecino toda su información de encaminamiento y después únicamente se enviarán las nuevas rutas, las actualizaciones o la eliminación de rutas transmitidas con anterioridad. Además periódicamente se envían mensajes para garantizar la conectividad.

Cuando una conexión TCP se interrumpe por alguna razón, cada extremo de la comunicación está obligado a dejar de utilizar la información que ha aprendido por el otro lado. En otras palabras, la sesión TCP sirve como un enlace virtual entre dos sistemas autónomos vecinos, y la falta de medios de comunicación indica que el enlace virtual se ha caído.

Desde este punto de vista la topología de Internet se puede considerar como un gráfico de conexión de sistemas autónomos conectados mediante enlaces virtuales.

En la Figura 7.5 podemos ver cuatro sistemas autónomos llamados AS1, AS2, AS3 y AS4 conectados por enlaces virtuales. Es decir, que mantienen sesiones BGP sobre TCP para la comunicación entre ellos.

Cada sistema autónomo contiene una o más redes que se identificaron como N1, N2 y N3 en AS1 y así sucesivamente. Simplemente observando la figura se puede mostrar que existe más de una ruta posible entre dos sistemas autónomos determinados.

Como también es posible tener uno o más de un router de borde en el mismo sistema autónomo.

BGP es la primera versión que admite encaminamiento entre dominios sin clase (CIDR) y agregado de rutas.

A diferencia de los protocolos de Gateway internos (IGP), como RIP, OSPF y EIGRP, no usa métricas como número de saltos, ancho de banda, o retardo.
En cambio, BGP toma decisiones de encaminamiento basándose en políticas de la red, o reglas que utilizan varios atributos de ruta BGP.

Vemos a continuación, la figura 7.5 antes mencionada:

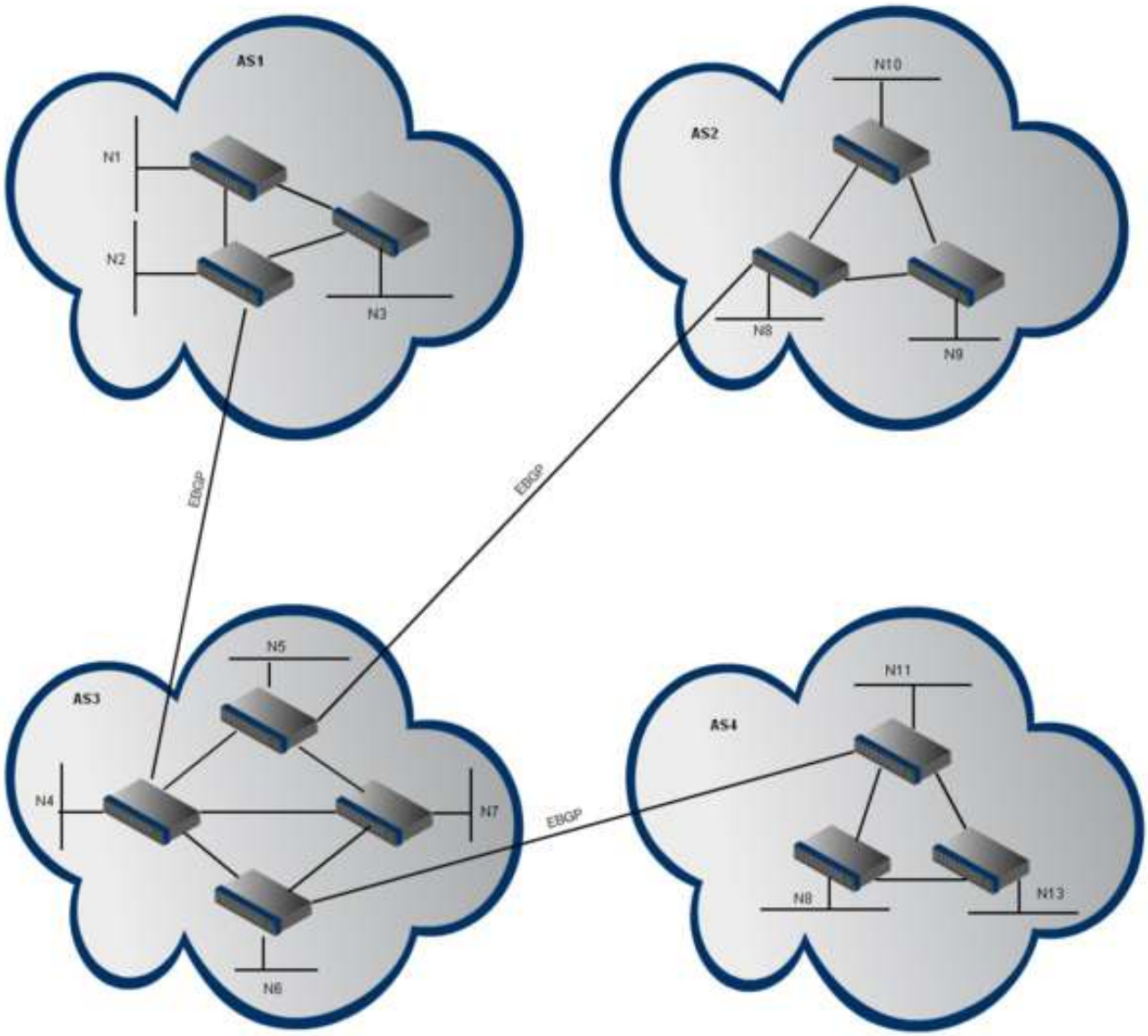


Figura 7.5: topología de varios ASs con conexiones IBGP y EBGP entre sus routers

Se debe distinguir entre External BGP (EBGP) e Internal BGP (IBGP): **EBGP** hace referencia al intercambio de información entre diferentes sistemas autónomos, sin embargo **IBGP** hace referencia al intercambio de información dentro de un mismo sistema autónomo.

7.3 Multiprotocol Label Switching (MPLS)

MPLS (siglas de Multiprotocol Label Switching) [15] es un mecanismo de transporte de datos estándar creado por el IETF y definido en el RFC 3031. Opera entre la capa de enlace de datos y la capa de red del modelo OSI. Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes. Puede ser utilizado para transportar diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP.

Paso de un paquete por la red

Cuando un paquete no etiquetado entra a un router de ingreso y necesita utilizar un túnel MPLS, el router primero determinara la Clase Equivalente de Envío (FEC), luego inserta una o mas etiquetas en el encabezado MPLS recién creado. Acto seguido el paquete salta al router siguiente según lo indica el túnel. Cuando un paquete etiquetado es recibido por un router MPLS, la etiqueta que se encuentra en el tope de la pila sera examinada. Basado en el contenido de la etiqueta el router efectuara una operación apilar (PUSH), desapilar (POP) o intercambiar (SWAP).

- En una operación SWAP la etiqueta es cambiada por otra y el paquete es enviado en el camino asociado a esta nueva etiqueta.
- En una operación PUSH una nueva etiqueta es empujada encima de otra (si existe). Si en efecto había otra etiqueta antes de efectuar esta operación, la nueva etiqueta ≪encapsula≫ la anterior.

- En una operación POP la etiqueta es retirada del paquete lo cual puede revelar una etiqueta interior (si existe). A este proceso se lo llama ≪desencapsulado≫ y es usualmente efectuada por el router de egreso con la excepción de PHP (Penultimate Hop Popping).

Durante estas operaciones el contenido del paquete por debajo de la etiqueta MPLS no es examinado, de hecho los routers de tránsito usualmente no necesitan examinar ninguna información por debajo de la mencionada etiqueta. El paquete es enviado basándose en el contenido de su etiqueta, lo cual permite ≪encaminamiento independiente del protocolo≫. En el router de egreso donde la última etiqueta es retirada, solo queda la ≪carga transportada≫, que puede ser un paquete IP o cualquier otro protocolo.

Por tanto, el router de egreso debe forzosamente tener información de encaminamiento para dicho paquete debido a que la información para el envío de la carga no se encuentra en la tabla de etiquetas MPLS. En algunas aplicaciones es posible que el paquete presentado al LER (LER = Label Edge Router) ya contenga una etiqueta MPLS, en cuyo caso simplemente se anexará otra etiqueta encima.

Un aspecto relacionado que resulta importante es PHP. En ciertos casos, es posible que la última etiqueta sea retirada en el penúltimo salto (anterior al último router que pertenece a la red MPLS); este procedimiento es llamado ≪remoción en el penúltimo salto≫ (PHP - Penultimate Hop Popping).

Esto es útil, por ejemplo, cuando la red MPLS transporta mucho tráfico. En estas condiciones los penúltimos nodos auxiliaran al último en el procesamiento de la última etiqueta de manera que este no se vea excesivamente forzado al cumplir con sus tareas de procesamiento.

Ver Anexo 10: RFC 3031 MPLS Architecture January 2001

7.4 Virtual Private Networks (VPN) y Virtual Routing and Forwarding (VRF)

MPLS es comúnmente bien utilizado para el transporte de múltiples VRF de Internet, pero surge la pregunta: ¿ Qué son las VRF ? [14]

Virtual routing and forwarding (VRF) es una tecnología incluida en routers de red IP que permite que coexistan mas de una tabla de encaminamiento en un router trabajando al mismo tiempo. Esto aumenta la funcionalidad al permitir que las redes sean segmentadas sin el uso de varios dispositivos. Dado que el tráfico es automáticamente segregado, VRF también aumenta la seguridad de la red y puede eliminar la necesidad de cifrado y autenticación.

Además, VRF requiere una tabla de reenvío que designa el siguiente salto para cada paquete de datos, una lista de dispositivos que pueden ser llamados a enviar el paquete, y un conjunto de normas y protocolos de encaminamiento que rigen la forma en que el paquete se reenvía.

Estas tablas evitan que el tráfico se pueda reenviar fuera de un camino VRF específico y así mantener el tráfico saliente que debe permanecer fuera del camino VRF.
Antes de pasar a ver en detalle el protocolo, veremos algunos conceptos generales que usaremos.

MPLS/VPN: Conceptos generales

¿ Qué es una VPN ? Es una red privada en términos lógicos, montada sobre un medio potencialmente compartido . Un conjunto de sitios a los que les es permitido comunicarse mutuamente . Es el "ámbito alcanzable" por una tabla de rutas (ver Figura 7.6).

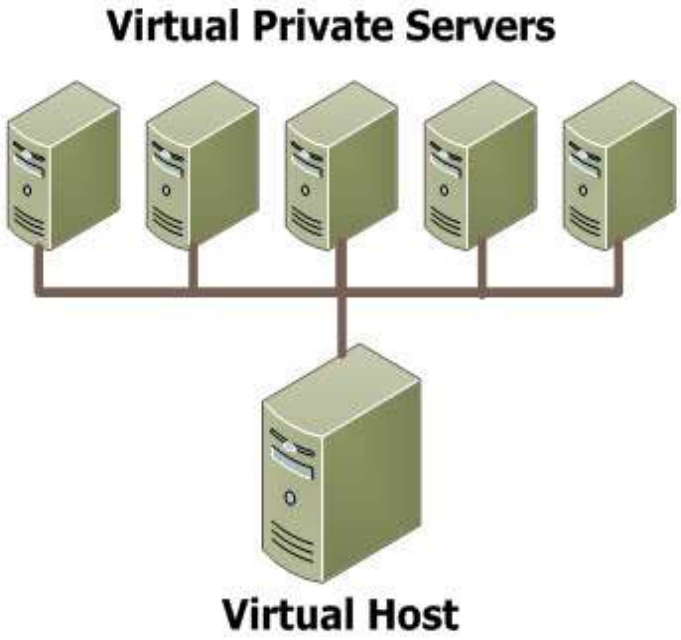


Figura 7.6: Virtual Private Server

VPN basada en la idea de "peers" (semillas)

En este tipo de arquitectura, un router de borde del backbone y router del "cliente" usan el mismo protocolo de red para dialogar, es decir, los routers de cliente (CE) y routers de backbone (PE) arman una adyacencia en los términos del protocolo común. Los routers del backbone conocen la información de direccionamiento de los routers del "cliente".

Terminología en MPLS-VPN

- Red de Proveedor (Red P): backbone controlado por un "Proveedor MPLS"
- Red de Cliente (Red C): Red bajo el control del cliente
- Router CE: Customer Edge. Parte de la Red C, que hace interfaz con la Red P
- Sitio: Conjunto de redes de la Red C, ubicadas en el ámbito de un PE. Un sitio se conecta al backbone MPLS a través de uno o mas enlaces PE/CE
- Router PE: Provider Edge Router (PE). Parte de la Red; hace interfaz con los routers CE
- Router P: Provider Router; pertenece al núcleo, no tiene conocimientos de las VPNs

MPLS-VPN : Modelo Base

Su base es el modelo de peers, pero tenemos que: routers PE reciben y mantienen información de rutas de las interfaces directamente conectadas. Esto tiene como ventaja que se reduce la cantidad de información que tiene que almacenar un PE. Para el encaminamiento interno (dentro del núcleo/backbone) se usa MPLS (no se necesita conocer información del cliente).
MPLS Multi-VRF ofrece la posibilidad de configurar y mantener mas de una instancia de una tabla de encaminamiento y reenvío en el mismo router CE.

VRF para IPv4 e IPv6

VPNs para IPv6 utilizan los mismos conceptos VRF que usa VPN IPv4 MPLS, como las address families, route distinguishers, route targets, and VRF identifiers. Los clientes que utilizan VPN IPv4 e IPv6 pueden querer compartir políticas VRF entre address families. Pueden también definirse políticas VRF aplicables para todas las address families, en lugar de definir las políticas de VRF para una address family individualmente.

Antes de Cisco IOS Release 12.2(33)SRB, una VRF se aplicaba sólo a un address family IPv4. Una relación uno-a-uno existía entre el nombre VRF y un identificador de tabla de encaminamiento y reenvío (routing and forwarding table identifier), entre un nombre VRF y un route distinguisher (RD), y entre un nombre de VRF y un ID VPN. Esta configuración se denomina single-protocol VRF.

Cisco IOS Release 12.2(33)SRB introduce soporte para una estructura múltiple address-family (multi-AF) VRF. El multi-AF VRF permite definir múltiples address families bajo la misma VRF. Dado un VRF, identificado por su nombre y un conjunto de políticas, puede aplicarse tanto a una VPN IPv4 y una VPN IPv6 al mismo tiempo. Esta VRF puede ser activada en una interfaz determinada, a pesar de que las tablas de encaminamiento y reenvío (routing and forwarding tables) son diferentes para los protocolos IPv4 e IPv6. Esta configuración se denomina multiprotocol VRF.

Virtual Routing and Forwarding (VRF)

Hay 2 componentes principales en una VRF : el route distinguisher (RD) y el route target (RT). Vemos en la figura 7.7 un ejemplo de implementación de VRF.

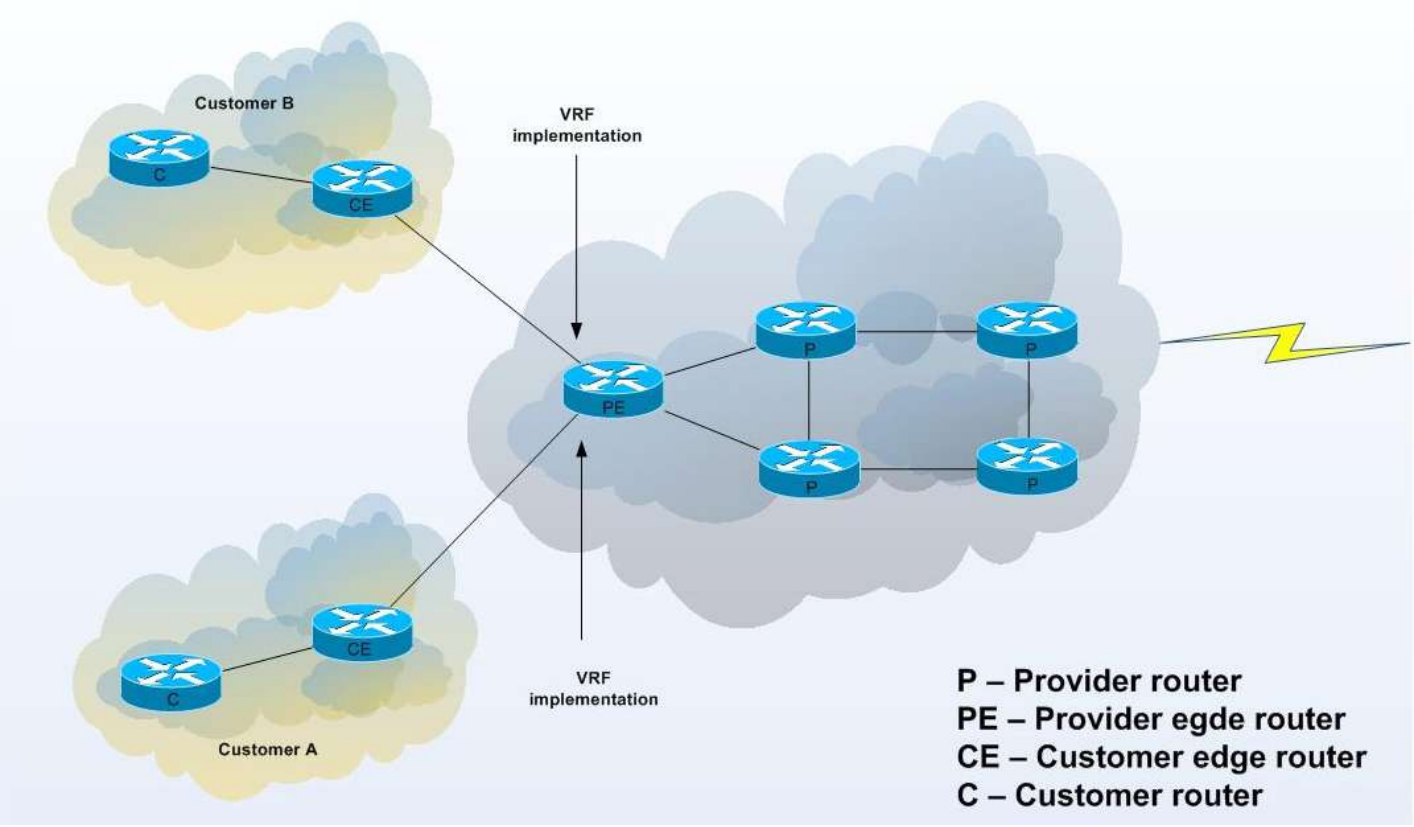


Figura 7.7: implementación de VRF MPLS

¿ Qué es el Route Distinguisher ?

El route distinguisher (RD) es un número que utiliza el protocolo MPLS para identificar una VPN en la red de un proveedor, y permitir con su uso la superposición de espacio IP.

Formato del RD

El RD es un campo de 8 octetos (64 bits), el cual se encuentra como prefijo a la dirección IP del cliente (IPv4), siendo esta última, como ya se sabe de 4 octetos, es decir 32 bits.

El campo resultante, termina siendo de 12 octetos (96 bits), y representa una dirección única "VPN-IPv4". Hay una descripción más detallada en el RFC 4364 (Ver anexo 30).

Los 8 octetos que lo conforman, están organizados de la siguiente manera: consiste en dos grandes campos, el "Type field" (2 octetos) y el "Value Field" (6 octetos); y este último a su vez esta subdividido en "Administrator Subfield" y "Assigned number subfield".

El campo "Type field" determina cómo se debe interpretar el "Value field". Los tres valores de Type, son los que presenta la siguiente Tabla 1:

Type	Formato	Características
0	Type Field (2 bytes) Administrator subfield (2 bytes) Assigned number subfield (4 bytes)	El campo "Administrator subfield" debe contener un número de sistema autónomo (se desaconseja el uso de números de sistemas autónomos privados). El valor del campo "Assigned number subfield" contiene un número asignado por el proveedor de servicios.
1	Type Field (2 bytes) Administrator subfield (4 bytes) Assigned number subfield (2 bytes)	El campo "Administrator subfield" debe contener una dirección IP numero de sistema autónomo (se desaconseja el uso de direcciones IP privadas). El valor del campo "Assigned number subfield" contiene un número asignado por el proveedor de servicios.
2	Type Field (2 bytes) Administrator subfield (4 bytes) Assigned number subfield (2 bytes)	El campo "Administrator subfield" debe contener un número de sistema autónomo de 4 bytes (se desaconseja el uso de números de sistemas autónomos privados). El valor del campo "Assigned number subfield" contiene un número asignado por el proveedor de servicios.

Tabla 1: Tipos de formatos para el número RD

Tenemos para el campo "Administrator subfield" valores de 2 bytes, que van del valor 0 al 65536 (en sistema numérico decimal).

El valor del campo "Assigned number subfield" es de 4 bytes, o sea que nos permite usar números desde el 0 hasta el 4294967296 (en decimal), siendo criterio del administrador el número utilizado.

Para el Type: 0, el campo "Administrator subfield" debe representar un número de Sistema Autónomo. Vemos a continuación como se representan dichos números.

Número de Sistema Autónomo (ASN)

Hasta el año 2007 los números de sistemas autónomos estaban definidos por un número entero de 16 bits, que permitía una cantidad máxima de 65536 asignaciones de sistemas autónomos. Debido a la demanda, se hizo necesario aumentar la posibilidad de asignaciones. La RFC 4893 (ver anexo 31) introduce los sistemas autónomos de 32-bits, que IANA ha comenzado a asignar. Vemos a continuación, como tiene organizados los ASN de 16 bits IANA en la actualidad en la Tabla 2:

ASN de 16 bits

Número de AS/bloque	Asignación
0	Reservado
1-48127	Asignado
48128-54271	Sin asignar
54272-64511	Reservado por IANA
64512-65534	Libre para uso interno (*private range*)
65535	Reservado

Tabla 2: Números de Sistemas Autónomos administrada por IANA

Asignación de ASN

Los números de Sistemas Autónomos son asignados en bloques por la Internet Assigned Numbers Authority (IANA) a Registros Regionales de Internet (RIRs). Los RIR apropiados en este caso LACNIC, asignan números de sistemas autónomos a las entidades que tienen bloques de direcciones IP delegados por LACNIC. Las entidades que quieren recibir un número de sistema autónomo deben primero llenar un formulario en RIR correspondiente a su zona geográfica.

Los números de sistemas autónomos asignados por IANA pueden se encontrados en el sitio web de IANA [11].

¿ Cómo se utiliza el RD ?

Dentro de una red MPLS, los routers de borde (PE – Provider Edge) necesitan ser configurados para asociar cada RD con las rutas que conducen a un router CE.

Un router PE puede estar configurado para asociar todas las rutas que conducen al mismo router CE con el mismo RD, o también puede configurarse para asociar diferentes rutas con diferentes RD, incluso si estos RD conducen al mismo router CE (por ejemplo, para balance de carga).

El RD tiene un solo propósito: hacer prefijos IPv4 globalmente únicos. No se utiliza para el reenvío de paquetes IP (en routers del núcleo MPLS), pero es utilizado por los routers de borde para identificar a qué VPN pertenece un paquete.

Generalmente, se utilizan números RD del Type:0 y Type:1, un ejemplo sería:

- Administrator subfield (16 bits correspondiente al numero de AS): Assigned number subfield (32 bits). Ejemplo 65000:100
- Administrator subfield (32 bits correspondiente al numero IP del router-id OSPF): Assigned number subfield (32 bits). Ejemplo 192.168.0.1:10

Usualmente el primer método es el mas utilizado.

Route Target (RT)

El route target (RT) indica los miembros de una VPN y permite que rutas de una VPN se importen o exporten dentro o fuera de nuestras VRFs. El RT funciona como una política de encaminamiento, ya que determina como se distribuyen las rutas de una VPN particular.

Vemos a continuación las VRF que creamos en nuestra topología para conectar a los routers CE y los Gateways:

```
vrf definition vrf1 → vrf1 es el nombre que le dimos a la vrf
rd 65002:1 → primer método utilizado
!
address-family ipv4 → importación y exportación de rutas ipv4
route-target export 65002:1
route-target import 65002:1
exit-address-family
!
address-family ipv6 → importación y exportación de rutas ipv6
```

```
route-target export 65002:1
route-target import 65002:1
exit-address-family
```

Para chequear nuestra configuración, podemos utilizar las herramientas `ping vrf, traceroute`:

```
router# ping vrf vrf-name IP-address
```

Podemos verificar también la tabla de encaminamiento virtual (virtual routing table):

```
router# show ip route vrf vrf-name
```

MPLS Multi-VRF : Configuración de MPLS en GNS3

Requisitos previos para la implementación de IPv6 sobre MPLS

Un requisito previo a la implementación del protocolo 6PE, es que el núcleo de red IPv4 debe estar ejecutando MPLS. Si se utilizan routers Cisco, Cisco Express Forwarding o distributed Cisco Express Forwarding debe estar habilitado para los protocolos IPv4 e IPv6. (Utilizando los comandos ip cef y su análogo ipv6 cef).

Beneficios de la Implementación de IPv6 sobre backbone MPLS

La inclusión del protocolo IPv6 sobre redes troncales MPLS permite que dominios IPv6 aislados se comuniquen entre si a través de un núcleo de red MPLS IPv4. Esta aplicación no requiere re-configuración de los routers del núcleo dado que el reenvío (forwarding) se basa en las etiquetas MPLS en lugar de la cabecera IP, proporcionando una estrategia muy rentable para el despliegue de IPv6.

MPLS VPN: Selección de VRF basada en la dirección IP origen

VPN Routing and Forwarding (VRF) permite a una interfaz específica en un provider edge (PE) router encaminar paquetes a las diferentes redes privadas virtuales (VPN) basadas en la dirección IP de origen del paquete. Esta característica es una mejora sobre el uso de un router basado en políticas para encaminar los paquetes a distintas VPNs.

Descripción general

La función Selección de VRF permite que los paquetes que llegan a una interfaz se conecten a la tabla VRF apropiada basada en la dirección IP de origen de los paquetes. Una vez que los paquetes han sido "seleccionados" en la tabla correcta de encaminamiento VRF, se procesan normalmente en base a la dirección destino y se reenvían a través de MPLS-VPN.

En la mayoría de los casos, la selección de VRF es una característica "one way", ya que funciona en los paquetes que provienen de los usuarios finales al router PE. Se describe a continuación como es el proceso de selección de tablas vrf para el encaminamiento de los paquetes.

VRF: Proceso de Selección

La función selección de VRF utiliza el siguiente proceso para encaminar los paquetes de las redes de los clientes en el router PE y en la red de proveedores. Un mecanismo de búsqueda de dos tabla se utiliza en la interfaz de entrada del router PE para determinar el encaminamiento y el reenvío de los paquetes procedentes de las redes de clientes, que utilizan protocolos IP, a la redes MPLS VPN, que utilizan protocolos de MPLS.

• La primera tabla, la tabla de selección VRF, se utiliza para comparar la dirección IP de origen del paquete con una lista de direcciones IP en la tabla. Cada dirección IP de la tabla está asociada con una VPN MPLS. Si se encuentra una coincidencia entre la dirección IP de origen del paquete y una dirección IP en la tabla de selección VRF, el paquete se encamina a la segunda tabla (la tabla VRF) o la tabla de encaminamiento de la VPN apropiado. Si no hay coincidencias en la tabla para la dirección IP de origen del paquete, el paquete o bien se encamina a través de la tabla de encaminamiento global utilizada por el router PE (este es el comportamiento por defecto), o es descartado.

• La segunda tabla, la tabla VRF (también conocida como la tabla de encaminamiento de VPN), contiene el encaminamiento virtual y la transmisión de información para la VPN especificada y se utiliza para reenviar el tráfico de la VPN seleccionada para la etiqueta MPLS Switched Path (LSP) en base a la dirección IP de destino del paquete.

El proceso de selección VRF elimina la asociación entre la VPN y la interfaz y permite más de una VPN de MPLS para ser asociado con la interfaz.

La agregación de rutas por defecto en cada vrf puede realizarse estáticamente (con el comando ip route vrf) o dinámicamente con eBGP (agregando default information originate) . En nuestro ejemplo utilizaremos eBGP dado que las VRF están en diferentes sistemas autónomos (para simplificar la configuración y tener escalabilidad).

Las VRF las crearemos para conectar al router 7 (Cliente) y para conectar al router 5 (Gateway).

7.5 Solución Propuesta: IPv6 sobre MPLS (Cisco 6PE)

Son múltiples las técnicas disponibles para integrar servicios IPv6 en redes: podría ser una red puramente IPv6, una red doble pila IPv4-IPv6 ejecutándose en paralelo, o aprovechar un backbone MPLS existente (como es el caso de la Empresa Aguas del Colorado).

Estas soluciones, (despliegue de IPv6) son viables cuando la cantidad de tráfico IPv6 y los ingresos generados están emparejados con las inversiones y los riesgos asumidos.

En el caso de la Empresa ADC, ya se tiene en servicio una infraestructura MPLS/IPv4, y como se informó en el capítulo 4, donde se hizo el relevamiento de tecnologías, la mayor parte de su equipamiento corresponde a la marca Cisco Systems, por lo tanto es una buena opción analizar que alternativas tenemos con esta marca.

De lo investigado, tenemos que: Cisco Systems desarrolló 6PE [16] para cumplir con todos estos requisitos. Proveedores de Servicios que ya despliegan MPLS, o planean hacerlo, pueden aprovechar los siguientes beneficios de Cisco 6PE :

- Mínimo costo de riesgos y operaciones: permite implementar IPv6 sin impacto en los servicios existentes de IPv4 y MPLS, es decir sin interrupciones ya que un router 6PE puede agregarse en cualquier momento.
- Mejoras en Provider Edge routers solamente: un router 6PE puede ser un router PE ya existente o uno nuevo dedicado al tráfico IPv6.
- Sin impacto en los Customer Edge routers IPv6: El ISP (Internet Service Provider) puede conectar a cualquier Customer CE corriendo IGP o EGP.
- Permite aprovechar la velocidad máxima de la línea, ya que al utilizar MPLS, no se examina el paquete IP, solo las etiquetas (en los routers intermedios).

Ver anexo 26: IPv6 over MPLS (Cisco 6PE)

Características de 6PE

La implementación de Cisco IPv6 Provider Edge router sobre MPLS se llama 6PE, y permite a sitios IPv6 comunicarse entre sí a través de una red MPLS IPv4 utilizando MPLS Label Switched Paths (LSPs): esta función se basa en una extensión del multiprotocolo Border Gateway Protocol (BGP), y requiere una configuración de red IPv4 en el provider edge router (PE) para intercambiar información de alcanzabilidad IPv6, adicionando una etiqueta MPLS para cada address prefix IPv6 que se anuncia.

Esto es: los routers multiprotocolo 6PE utilizan BGP para intercambiar información de accesibilidad con otros dispositivos 6PE dentro del dominio MPLS y para distribuir etiquetas IPv6 entre ellos.

Todos los routers 6PE y de núcleo dentro del dominio MPLS IPv4 comparten un protocolo de borde interno IPv4 (Internal Gateway Protocol - IGP), tales como Open Shortest Path First (OSPF) o Integrated Intermediate System-to-Intermediate System (IS-IS).

Los routers de borde están configurados para ser de doble pila (ejecutar IPv4 e IPv6), y utilizar la dirección IPv4 mapeada a IPv6 para el intercambio de prefijos IPv6.

En la figura 7.8, los routers 6PE están configurados como doble pila capaz de encaminar el tráfico IPv4 e IPv6. Cada router 6PE esta configurado para ejecutar LDP (Label Distribution Protocol), TDP (Tag Distribution Protocol), o RSVP (Resource Reservation Protocol); este último para el caso que se haya configurado la ingeniería de tráfico para vincular etiquetas IPv4.

La figura 7.8 ilustra el funcionamiento de 6PE:

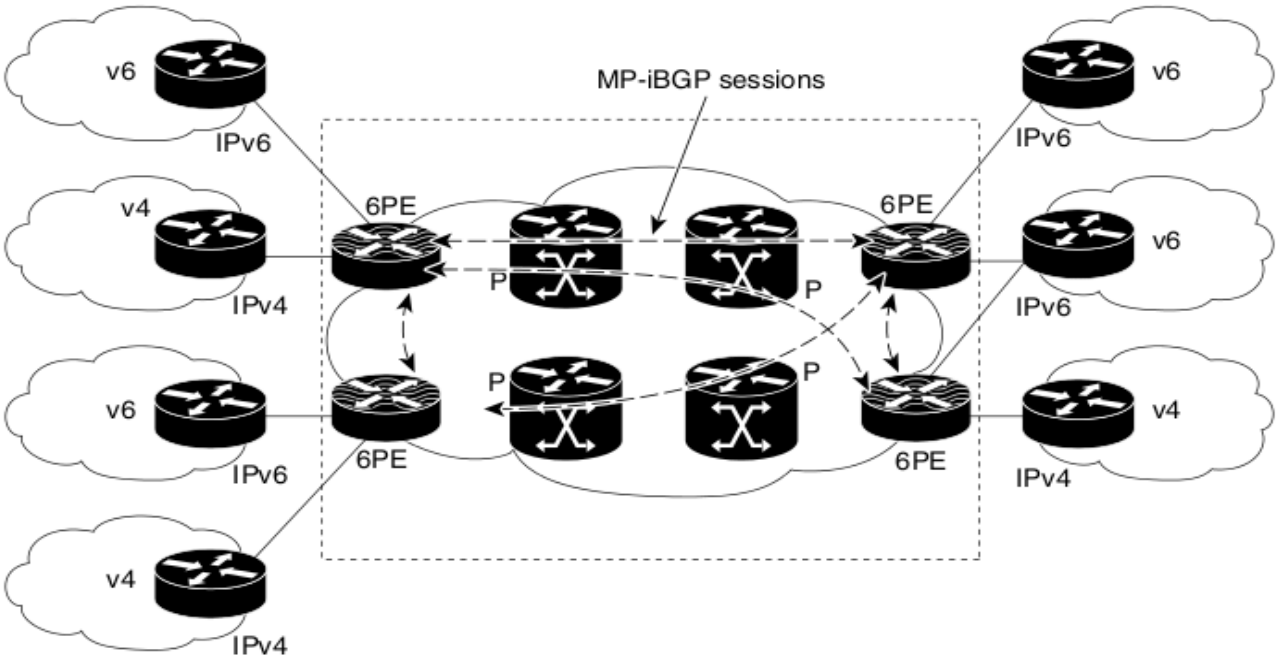


Figura 7.8: 6PE - IGP

Las interfaces de los routers 6PE conectadas al router CE pueden ser configuradas para reenviar el tráfico IPv6, IPv4, o ambos tipos de tráfico en función de los requisitos del cliente.

Los routers 6PE IPv6 anuncian información de accesibilidad aprendida de sus compañeros 6PE sobre la nube MPLS. Los proveedores de servicios pueden delegar un prefijo IPv6 a través de la infraestructura 6PE, de esta manera, no hay impacto en un router CE.

Los routers P en el núcleo de la red no son conscientes de que se están cambiando los paquetes IPv6. Los routers de núcleo están configurados para soportar MPLS y el mismo IGP IPv4 como los routers PE para establecer accesibilidad interna en el interior de la nube MPLS. Los routers del núcleo también utilizan LDP, TDP, o RSVP para la unión de etiquetas IPv4.

Implementar la funcionalidad Cisco 6PE, no tendrá ningún impacto en los dispositivos del núcleo MPLS, dado que dentro de la red MPLS, el tráfico IPv6 se reenvía mediante la conmutación de etiquetas, haciendo que el tráfico IPv6 sea transparente para el núcleo. No se requieren métodos de túneles IPv6 sobre IPv4 o encapsulación de capa 2.

6PE: procesamiento de TTL (Time to life o Tiempo de Vida)

6PE soporta las mismas opciones de procesamiento TTL para IPv6 como para IPv4. Podemos habilitar o no la propagación, esto es :

- Propagate: IP TTL. Se utiliza para establecer el TTL inicial MPLS
- Do not propagate: MPLS TTL se setea en 255. Nótese que es la misma configuración de un solo mando que controla la opción tanto para IPv4 como para IPv6 6PE.

Los comandos para habilitar y deshabilitar la propagación son:

```
router(config)# mpls ip propagate-ttl → habilita la propagación
```

En la mayoría de los casos, desactivar la propagación TTL hace que el núcleo de red IPv4 sea completamente transparente.

```
router(config)#no mpls ip propagate-ttl → deshabilita la propagación
```

7.6 Archivos de Configuración y pruebas funcionales en topología Piloto:

Dado que en nuestra topología ya tenemos el protocolo OSPF ejecutándose, a continuación tenemos que iniciar el protocolo 6PE en los routers de borde del backbone. El proceso es muy sencillo: los routers 6PE (R1 y R4) se configuran para el tráfico IPv4 e IPv6.

Entonces, los routers 6PE tienen que:

1. Participar en el protocolo de pasarela interior IPv4 para establecer la accesibilidad interna dentro de la nube MPLS: en el ejemplo que usaremos, tenemos declaradas las interfaces IPv4 con OSPFv2 como IGP.

2. Participar en LDP o TDP para la unión de etiquetas IPv4: usaremos LDP.

3. Ejecutar Multi-Protocol iBGP (MP-iBGP) para anunciar disponibilidad de IPv6 y distribuir aggregate-labels IPv6.

4. Ejecutar MP-eBGP, un IGP IPv6 o encaminamiento estático en routers CE para anunciar prefijos IPv6 aprendidos de sus peers sobre la nube MPLS.

Cisco esta trabajando en la IETF (Internet Engineering Task Force - http://www.ietf.org) para asegurar el progreso de la normalización correspondiente. En particular, el esquema Cisco 6PE es compatible con las versiones mas recientes del proyecto de IETF sobre "Conexión de dominios IPv6 a través de Nubes IPv4 con BGP ".

A continuación presentaremos, como parte de la solución propuesta, los archivos de configuración (running-config) 6PE de los routers de borde R1 y R4, y de los routers Cliente R7 correspondientes a la topología presentada en la figura 7.1.

Router 1 (6PE-1)

```
vrf definition vrf1 → VRF doble pila ipv4/ipv6
rd 65002:1
!
address-family ipv4
route-target export 65002:1
route-target import 65002:1
exit-address-family
!
address-family ipv6
route-target export 65002:1
route-target import 65002:1
exit-address-family
!
ip cef → comandos de cisco para habilitar Cisco Express Forwarding ipv4
```

```
ipv6 unicast-routing → habilita el reenvío de paquetes ipv6 entre interfaces
ipv6 cef → comandos de cisco para habilitar Cisco Express Forwarding ipv6
interface Loopback0
ip address 1.1.1.1 255.255.255.255
ipv6 address cafe:1::1/128
!
interface GigabitEthernet1/0
ip address 192.168.1.1 255.255.255.0
mpls ip → habilitamos etiquetado mpls
!
interface GigabitEthernet2/0
ip address 192.168.3.1 255.255.255.0
!
interface GigabitEthernet3/0
description LINK_R5
vrf forwarding vrf1 → asociamos la VRF a la interfaz
no ip address
ipv6 address 2001:1111:1111::1/64
!
interface GigabitEthernet4/0
no ip address
ipv6 address 2001:1111:2222::1/64
!
router ospf 1
router-id 1.1.1.1
log-adjacency-changes
redistribute connected
network 1.1.1.1 0.0.0.0 area 0
network 192.168.1.0 0.0.0.255 area 0
network 192.168.3.0 0.0.0.255 area 0
!
router bgp 65000
no synchronization
bgp log-neighbor-changes
neighbor 2.2.2.2 remote-as 65000
neighbor 2.2.2.2 description RR_iBGP → conexión con Route Reflector por iBGP
neighbor 2.2.2.2 update-source Loopback0
no auto-summary
!
address-family ipv6
redistribute connected
default-information originate
no synchronization
neighbor 2.2.2.2 activate
neighbor 2.2.2.2 send-label
exit-address-family
!
address-family vpnv6
neighbor 2.2.2.2 activate
neighbor 2.2.2.2 send-community both
neighbor 2.2.2.2 next-hop-self
exit-address-family
!
```

```
address-family ipv4 vrf vrf1 → extensión de BGP para vrf ipv4
no synchronization
exit-address-family
!
address-family ipv6 vrf vrf1 → extensión de BGP para vrf ipv6
redistribute connected
no synchronization
neighbor 2001:1111:1111::2 remote-as 65001
neighbor 2001:1111:1111::2 description ENLACE_R5
neighbor 2001:1111:1111::2 activate
neighbor 2001:1111:1111::2 next-hop-self
exit-address-family
!
```

Router 4 (6PE-2)

```
vrf definition vrf1 → vrf que conecta a R7 (mismo nombre que en R1)
rd 65002:1
!
address-family ipv4
route-target export 65002:1
route-target import 65002:1
exit-address-family
!
address-family ipv6
route-target export 65002:1
route-target import 65002:1
exit-address-family
!
ip cef
ipv6 unicast-routing
ipv6 cef
!
interface Loopback0
ip address 4.4.4.4 255.255.255.255
ipv6 address cafe:4::1/128
!
interface GigabitEthernet1/0
description R2
ip address 192.168.2.1 255.255.255.0
mpls ip
!
interface GigabitEthernet2/0
description R3
ip address 192.168.4.1 255.255.255.0
mpls ip
!
interface GigabitEthernet3/0
description CLIENTE_R7
vrf forwarding vrf1
no ip address
ipv6 address 2001:DB8:CE::2/64
!
interface GigabitEthernet4/0
```

```
ip address 192.168.8.2 255.255.255.0
shutdown → por ahora no usamos esta interfaz, la deshabilitamos
router ospf 1
router-id 4.4.4.4
log-adjacency-changes
network 4.4.4.4 0.0.0.0 area 0
network 192.168.2.0 0.0.0.255 area 0
network 192.168.4.0 0.0.0.255 area 0
!
router bgp 65000
bgp log-neighbor-changes
neighbor 2.2.2.2 remote-as 65000
neighbor 2.2.2.2 description RR_iBGP
neighbor 2.2.2.2 update-source Loopback0
!
address-family ipv4
no synchronization
redistribute connected
neighbor 2.2.2.2 activate
no auto-summary
exit-address-family
!
address-family ipv6
redistribute connected
no synchronization
neighbor 2.2.2.2 activate
neighbor 2.2.2.2 send-label
exit-address-family
!
address-family vpnv6 → creamos la vpn a la cual se conectara la vrf
neighbor 2.2.2.2 activate
neighbor 2.2.2.2 send-community both
neighbor 2.2.2.2 next-hop-self
exit-address-family
!
address-family ipv6 vrf vrf1
redistribute connected
no synchronization
exit-address-family
```

Router 7 (Cliente)

```
ip cef
ipv6 unicast-routing
ipv6 cef
interface Loopback0
ip address 7.7.7.7 255.255.255.255
ipv6 address CAFE:7::1/128
!
interface GigabitEthernet1/0
no ip address
ipv6 address 2001:DB8:CE::1/64
!
ipv6 route ::/0 2001:DB8:CE::2 → ruta por defecto al router 4
```

Router 5 (Gateway)

```
ip cef
ipv6 unicast-routing
ipv6 cef
!
interface Loopback0
ip address 5.5.5.5 255.255.255.255
ipv6 address CAFE:5::1/128
!
interface GigabitEthernet1/0
no ip address
negotiation auto
ipv6 address 2001:1111:1111::2/64
!
router bgp 65001
bgp log-neighbor-changes
neighbor 2001:1111:1111::1 remote-as 65000
neighbor 2001:1111:1111::1 description 6PE1_neighbor
neighbor 2001:1111:1111::1 update-source GigabitEthernet1/0
!
address-family ipv4
no synchronization
neighbor 2001:1111:1111::1 activate
no auto-summary
exit-address-family
!
address-family ipv6
no synchronization
network CAFE:5::1/128
neighbor 2001:1111:1111::1 activate
neighbor 2001:1111:1111::1 send-community both
neighbor 2001:1111:1111::1 next-hop-self
neighbor 2001:1111:1111::1 default-originate
neighbor 2001:1111:1111::1 soft-reconfiguration inbound
exit-address-family
```

Se presentan a continuación, una serie de capturas de consola que visualizan detalles de funcionamiento, y archivos de configuración (llamadas "running-config" en los routers cisco).

7.7 Capturas de consola : Tablas IP, OSPF, MPLS, VRF y alcanzabilidad

Veremos las interfaces de los routers 6PE, con direcciones IPv4 (Figura 7.9) e IPv6 (Figura 7.10).

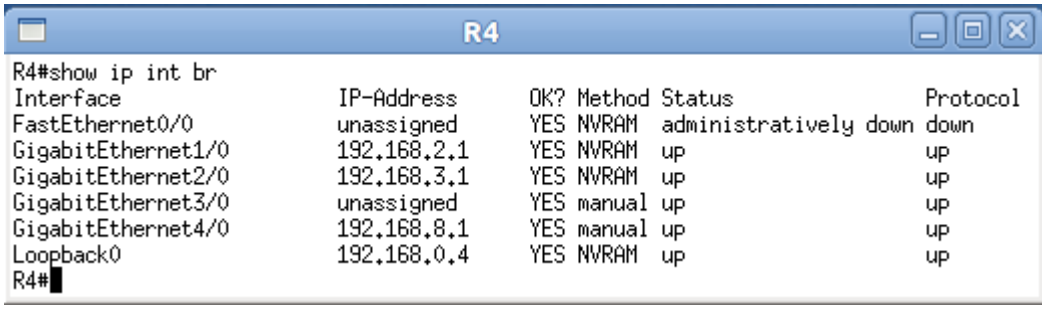


Figura 7.9: interfaces configuradas con IPv4 en R4

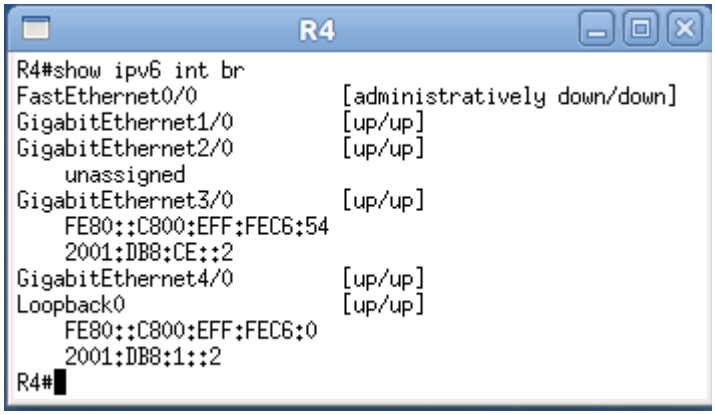


Figura 7.10: interfaces configuradas con IPv6 en R4

Configuramos los routers 6PE con sus interfaces de loopback en IPv6 y sus interfaces punto a punto con conectividad IPv4 (para el etiquetado MPLS). Se utilizó como IGP a OSPF, puede verse en la figura 7.11 la base de datos OSPF en R1:

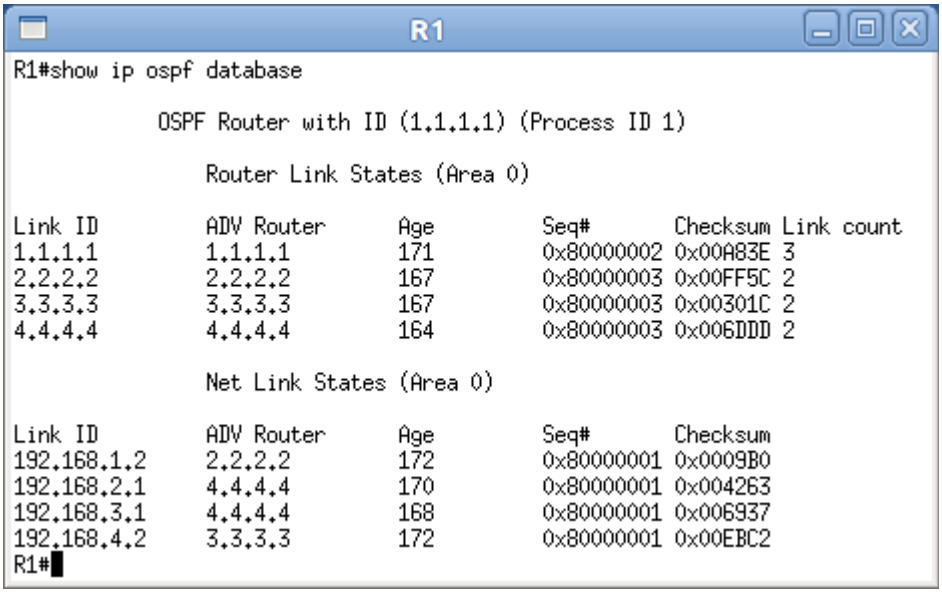


Figura 7.11: Captura de Base de Datos OSPF en R1

Una vez configurado IGP OSPF, pasamos a la configuración MPLS y luego a crear las VRF correspondientes a cada cliente y cada Gateway.

Vemos en la figura 7.12 como se establecen las adyacencias OSPF y BGP:

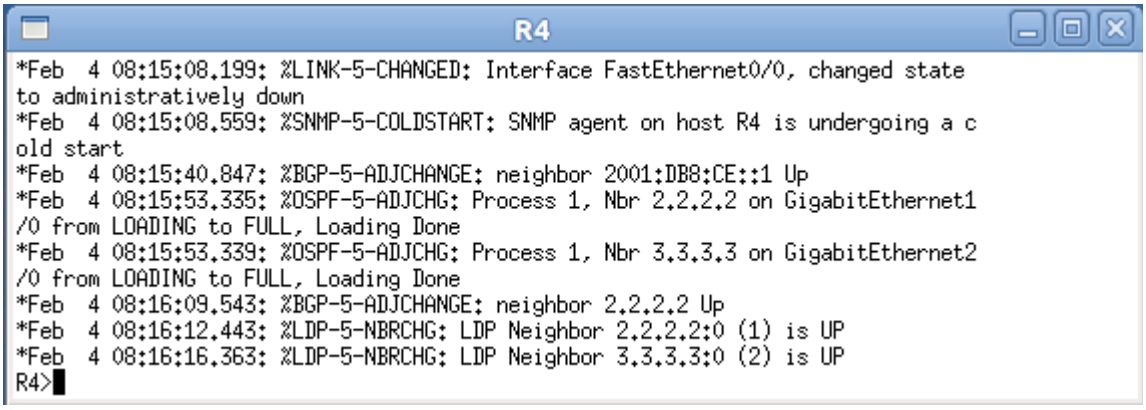


Figura 7.12: Arranque de router 4 (6PE-1) . Vemos la adyacencia de vecinos BGP , LDP y OSPF

Vemos las VRF que hemos creado para conectar R7 y R5 en la figura 7.13:

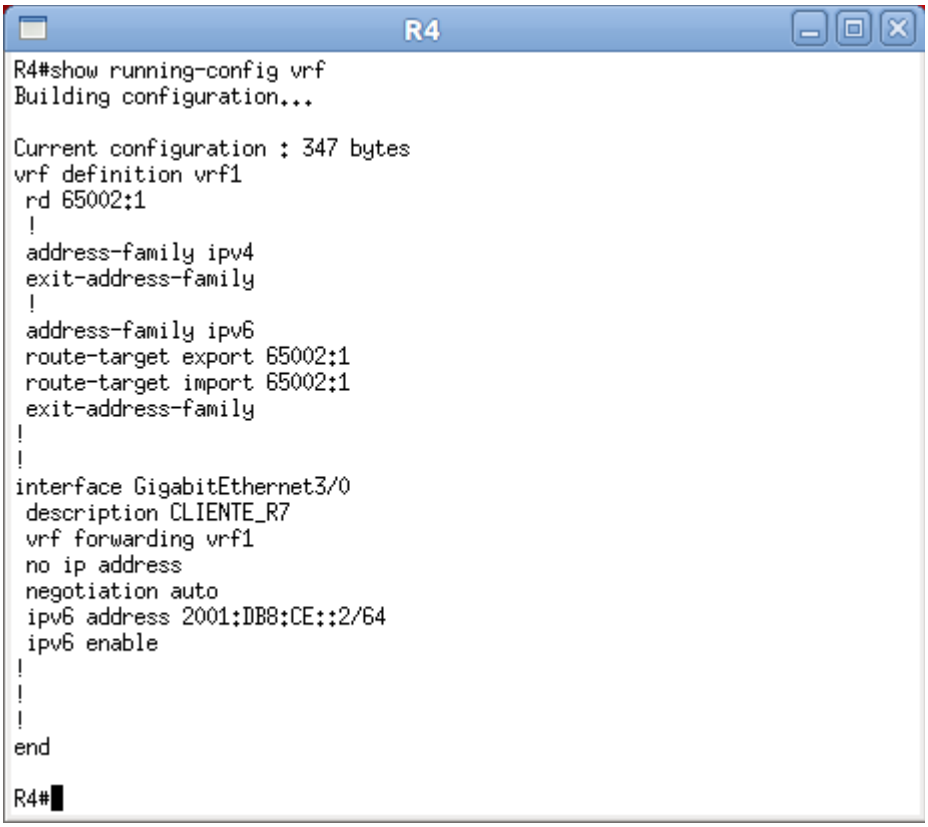


Figura 7.13: VRF creada en el router 4

Es necesario definir un address family tanto para IPv4 como para IPv6, dado que el protocolo 6PE requiere doble pila en los routers de borde.

Verificamos la conectividad desde el router 7 al router 5 en la figura 7.14:

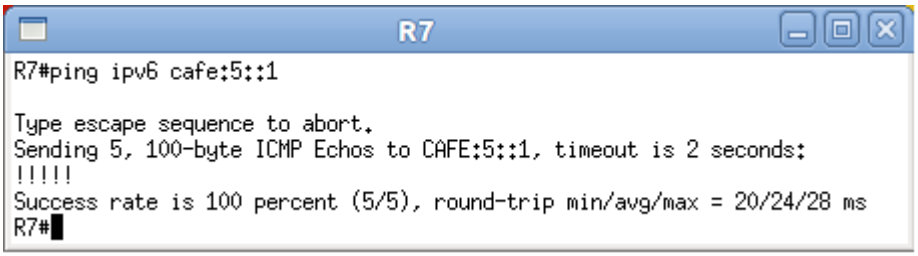


Figura 7.14: ping desde R7 (cliente) a R7 (Gateway)

En la siguiente figura 7.15, puede verse el etiquetado MPLS para IPv6:

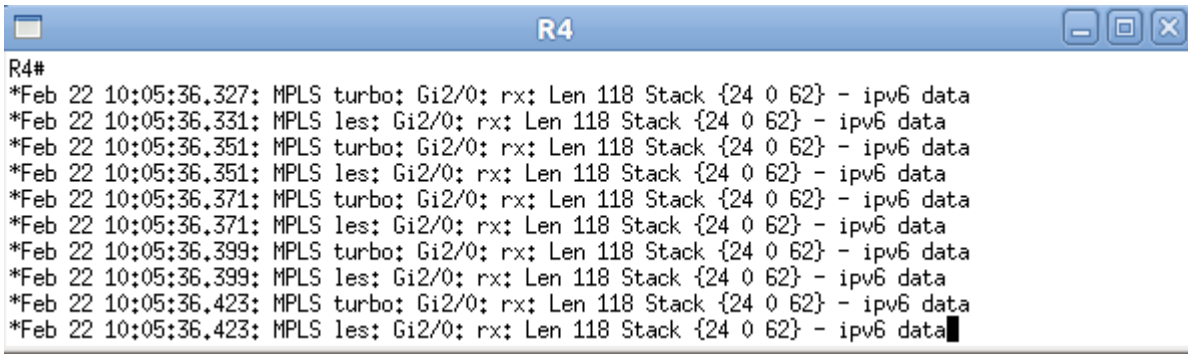


Figura 7.15: debug de paquetes mpls en router 4

La información que se muestra en la figura 7.15 es la siguiente:

```
MPLS turbo: Gi2/0: rx: Len 118 Stack {24 0 62} - ipv6 data
```

- `24 = label (etiqueta nro 24)`
- `0 = EXP VALUE`
- `62 = TTL (Time to Life)`

Para mostrar información sobre los enlaces de etiquetas aprendidas por el Protocolo de distribución de etiquetas (LDP), utilizamos el comando `show mpls ip binding` en el modo EXEC privilegiado.

Para resumir la información sobre los enlaces de etiquetas aprendidas por LDP, utilice el comando `ip binding summary` en el modo EXEC privilegiado.

En la figura 7.16, pueden verse las etiquetas asignadas a cada LSR (Label Switch Router) , en este caso el router-id 2.2.2.2 y el 3.3.3.3:

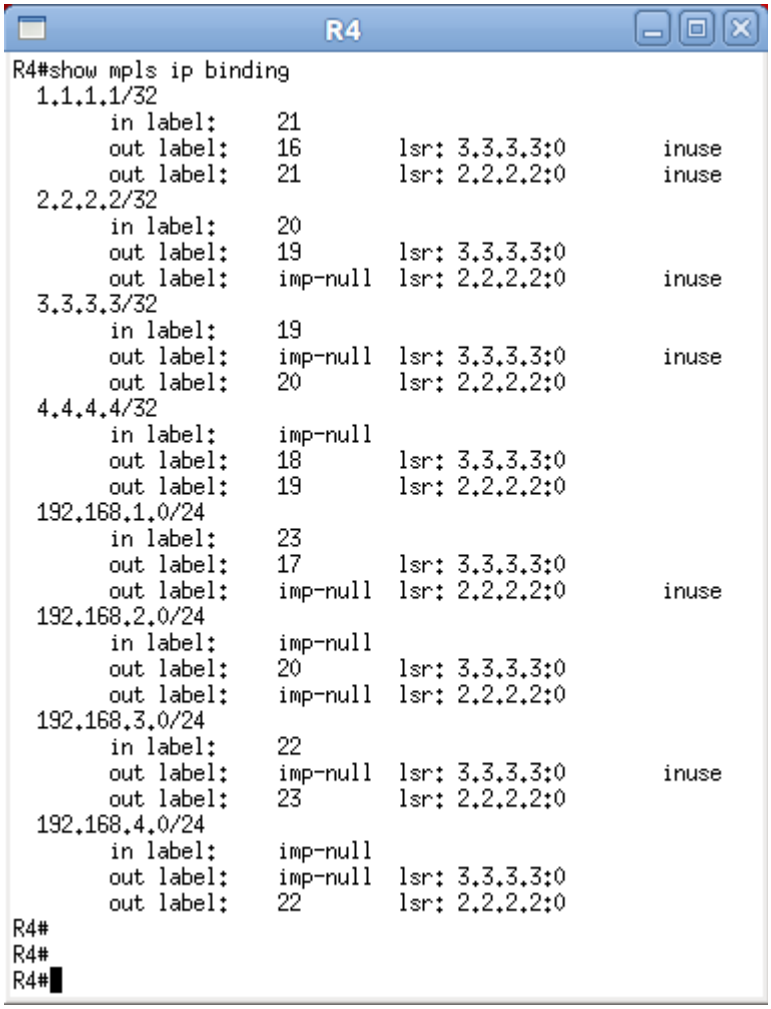


Figura 7.16: salida del comando show mpls ip binding

En la figura 7.17 se ve el camino que toma un paquete para llegar a R5 (cafe:5::1) desde el router cliente R7. Utilizamos el comando traceroute:

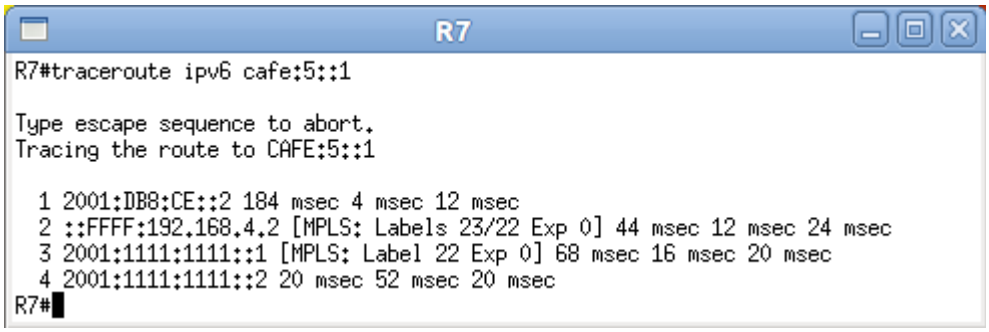


Figura 7.17: salida de comando traceroute al ipv6 cafe:5::1

Como puede verse, en la figura 7.17 , hay una distancia de 4 saltos en el camino:

1. 2001:DB8:CE::2 →es la ruta por defecto

2. ::FFFF:192.168.4.2 [MPLS: Labels 23/22 Exp 0] →camino escogido por MPLS hacia R3 (dirección mapeada de IPv4 a ipv6)

3. 2001:1111:1111::1 [MPLS: Label 22 Exp 0] →interfaz de router 1 conectada a R5

4. 2001:1111:1111::2 20 →router 5 (Destino)

A continuación, en la figura 7.18, veremos como se re-estructura el camino MPLS, dando de baja el enlace R3-R4.

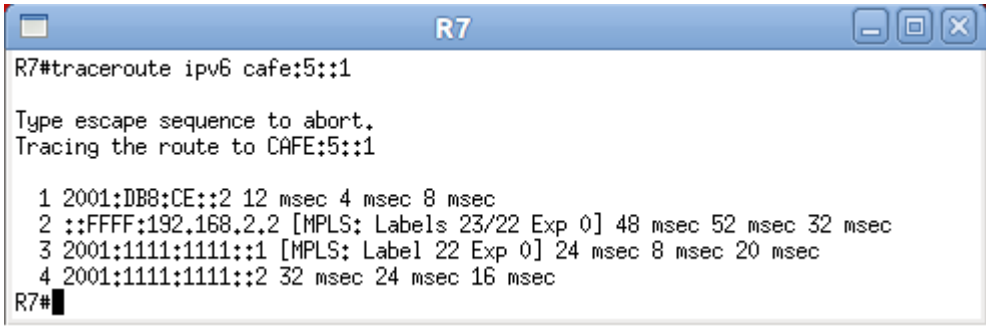


Figura 7.18: salida de comando traceroute ipv6 cafe:5::1 (toma otro camino)

Como puede verse, se estableció el nuevo camino a través de R2 (Route Reflector). Vemos como quedo la tabla de encaminamiento de la VPNv6 en R1 para la vrf1 en la figura 7.19 :

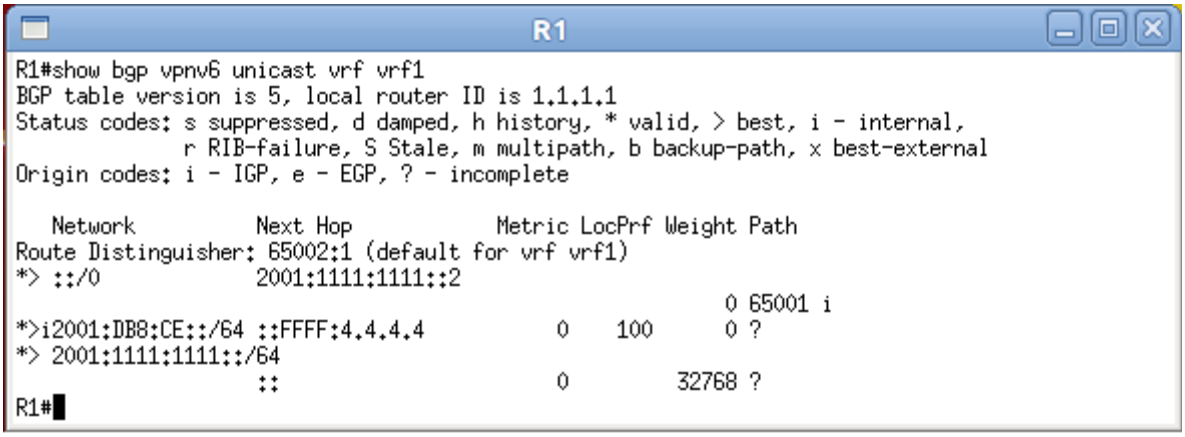


Figura 7.19: tabla de encaminamiento de vpn vrf1

En esta captura, verificamos la tabla de encaminamiento de la vrf1. Puede verse, que tiene como salida por defecto ::/0 el número IPv6 2001:1111:1111::2 que corresponde a la interfaz IPv6 del Router de salida R5 en el sistema autónomo 65001.

Se ve también la ruta interna 2001:DB8:CE::/64 que tiene como siguiente salto la dirección mapeada ::FFFF:4.4.4.4 . Esto es para el retorno de la información desde R1 a R4 hacia los clientes (R7 y R8).

El código de estado asterisco (*) indica que son rutas válidas.

Concluido el capítulo 7, pasamos al capítulo 8, donde finalmente se presentan pruebas reales de laboratorio, alternativas de encaminamiento, y conclusiones finales.

Capítulo 8: Pruebas de Laboratorio

8.0 Introducción

En el presente capítulo, veremos todo lo presentado en los capítulos anteriores, pero esta vez en equipos reales, presentes en el laboratorio de la Empresa Aguas del Colorado SAPEM.

Es el paso previo a una puesta en marcha de la solución propuesta en los equipos presentes en producción. Veremos como se configuran los equipos, los archivos de configuración, el tipo de topología y el modelo de Reflector de Rutas utilizado para el protocolo BGP. Analizaremos e incluiremos en la solución la alternativa del uso de VLANs, y finalmente realizaremos pruebas para verificar el funcionamiento real. Se analizaran diferentes capturas de consola para entender el funcionamiento a nivel general, de forma tal de tener una visión global del trabajo presentado.

La topología que se diseño esta compuesta de los siguientes equipos:

Cisco c2921: R1 y R4 como routers de borde
Cisco c3925: router de núcleo
Cisco c7201: router de núcleo, actúa como Reflector de Rutas (Route Reflector) BGP

Las conexiones punto-a-punto entre los equipos, son a través de cable de cobre RJ45, y configuradas como Gigabit-Ethernet dentro de los routers, con una velocidad de 1 Gigabit por segundo.

Como equipo cliente, se utilizó una computadora portátil (Notebook) con interfaz de red configurada para IPv4 e IPv6, tanto en el Sistema Operativo Linux como en Windows 7.

Presentamos la topología en la figura 8.1:

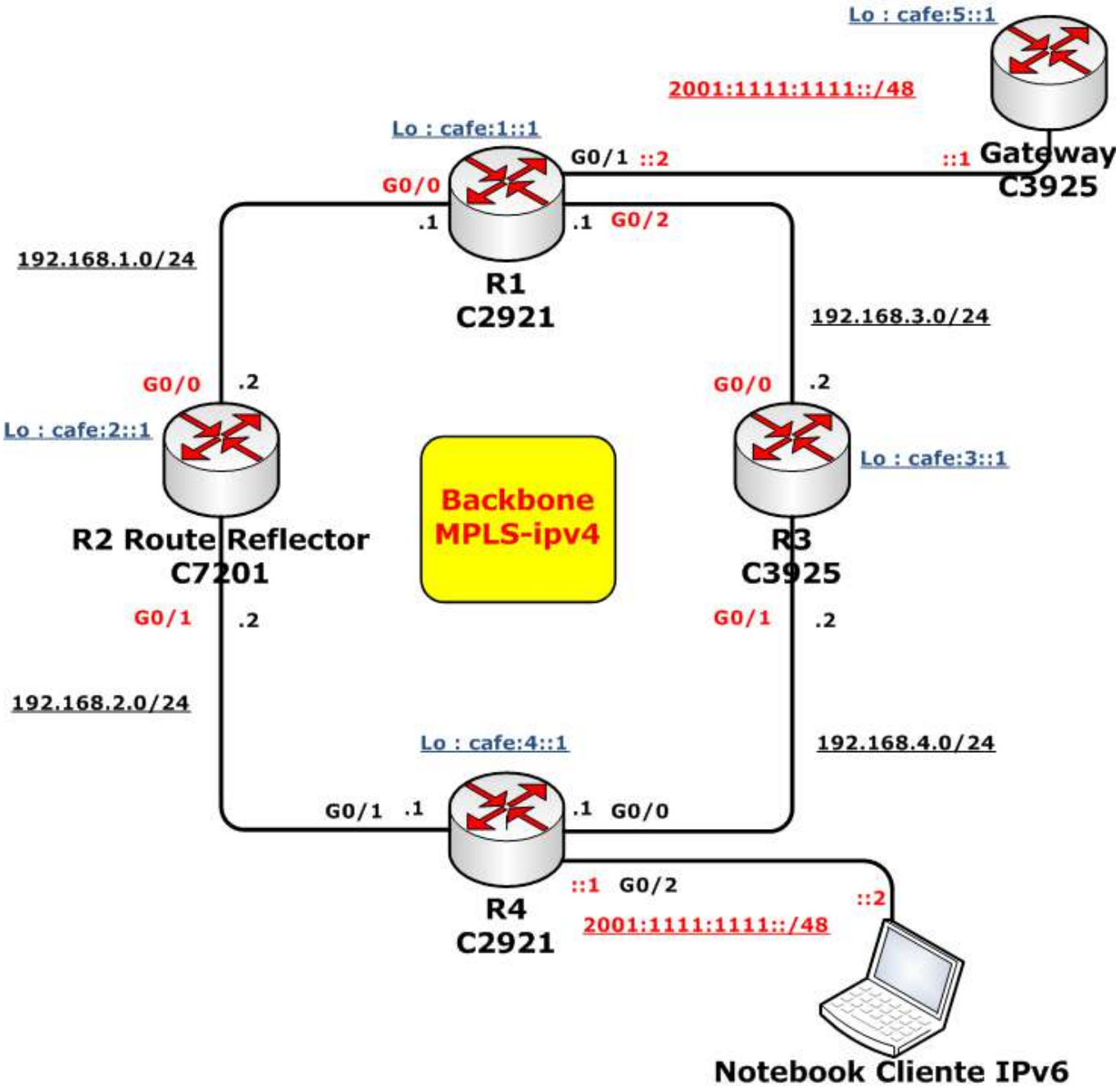


Figura 8.1: Topología Real a utilizar (en equipos de Laboratorio)

8.1 Conexiones

Para realizar las configuraciones de los equipos Cisco, nos conectaremos por el puerto Serial de nuestra PC Notebook al puerto destinado para tal funcionalidad en dichos equipos. Se verán a continuación imágenes de dichos puertos (Figuras 8.2 y 8.3).

Figura 8.2: cable DB9 a RJ45

Cable de consola RJ45 a DB9. Este cable de 182 centímetros de largo de una pieza se utiliza para conectar un ordenador de puerto serie DB9 al puerto RJ45 de la consola en la mayoría de equipos Cisco. La siguiente figura muestra la conexión de la PC al equipo Cisco:

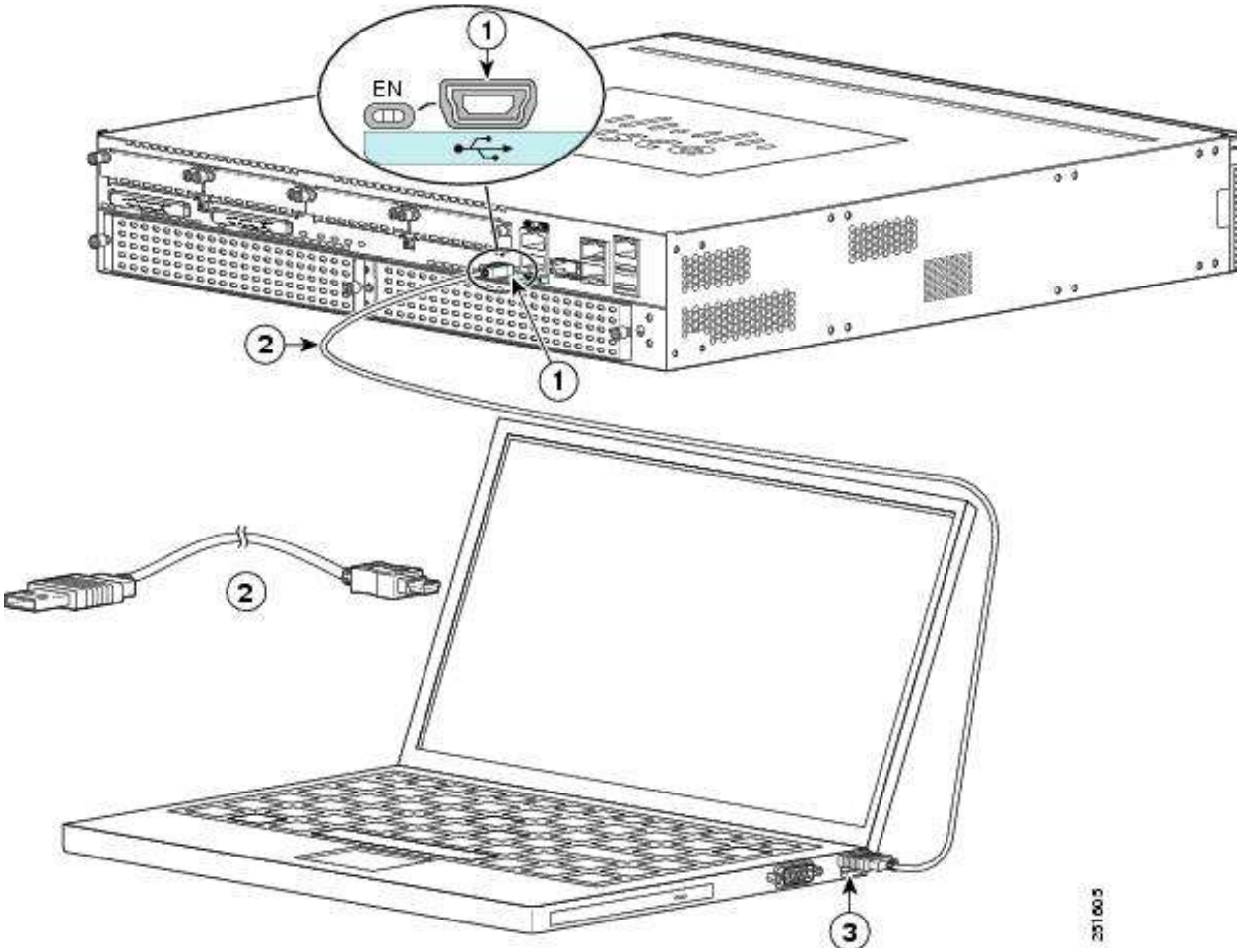


Figura 8.3: conexión Router – PC mediante cable serial/RJ45

Una vez conectados físicamente los equipos procedemos a realizar la conexión por software. Utilizaremos el software libre llamado "Putty" en modo conexión serial:

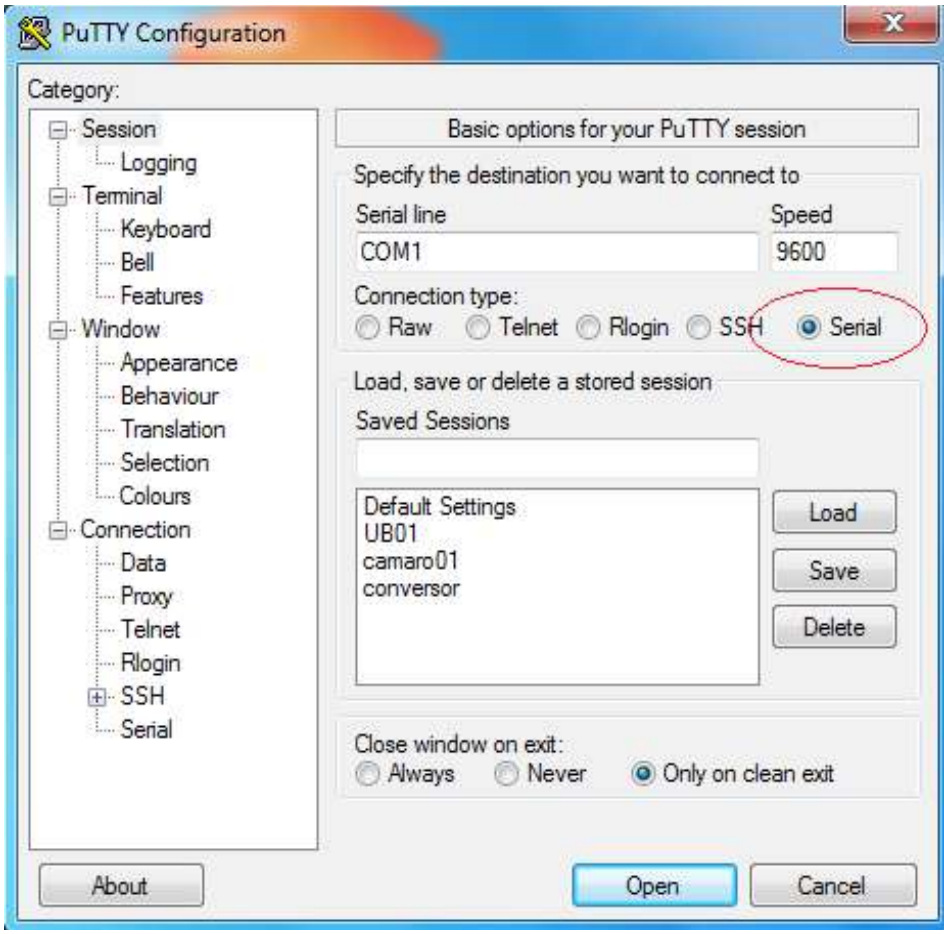


Figura 8.4: software Putty en modo Serial

Al ejecutar la opción open, se abrirá una consola de configuración del router Cisco, la cual utilizaremos para ejecutar todos los comandos de configuración.

8.2 Pruebas de Alcanzabilidad

Como primer paso, se configurarán las interfaces de loopback. A continuación se iniciará el proceso OSPF para el encaminamiento interno. Puede verse en la figura 8.5 , la tabla de encaminamiento OSPF en router 2 (Route Reflector RR).

Vemos que la tabla tiene al router-id 1.1.1.1 que corresponde a R1, a 3.3.3.3 que corresponde a R3 y a 4.4.4.4 que representa a R4.

Las dos entradas restantes, son las conexiones punto-a-punto con R3 y R1.

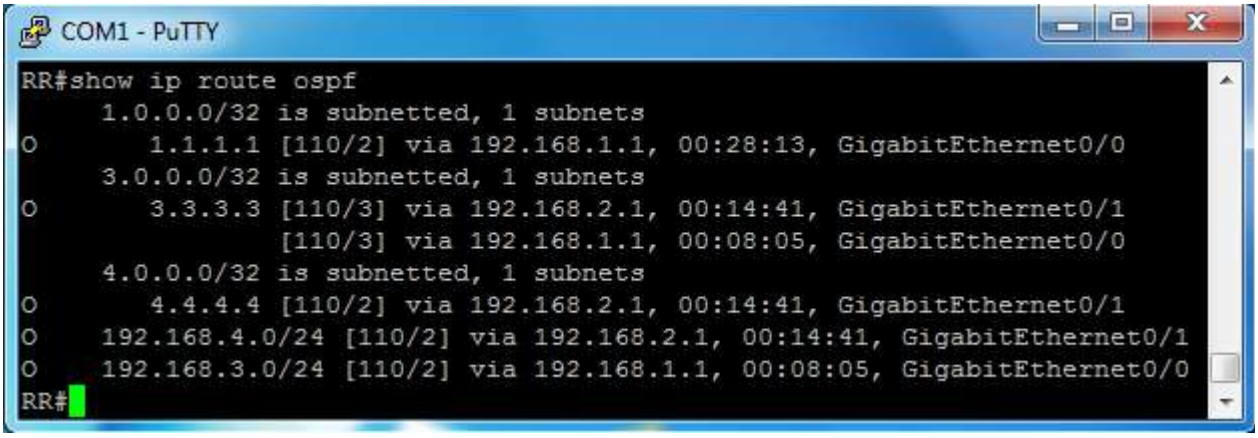


Figura 8.5: salida del comando show ip route ospf (en router 2 RR)

En la figura 8.6 se verifica la conectividad desde RR hacia R1, R3 y R4, y en la Figura 8.7 se verifica la conectividad IPv6 desde R1 hacia el Gateway.

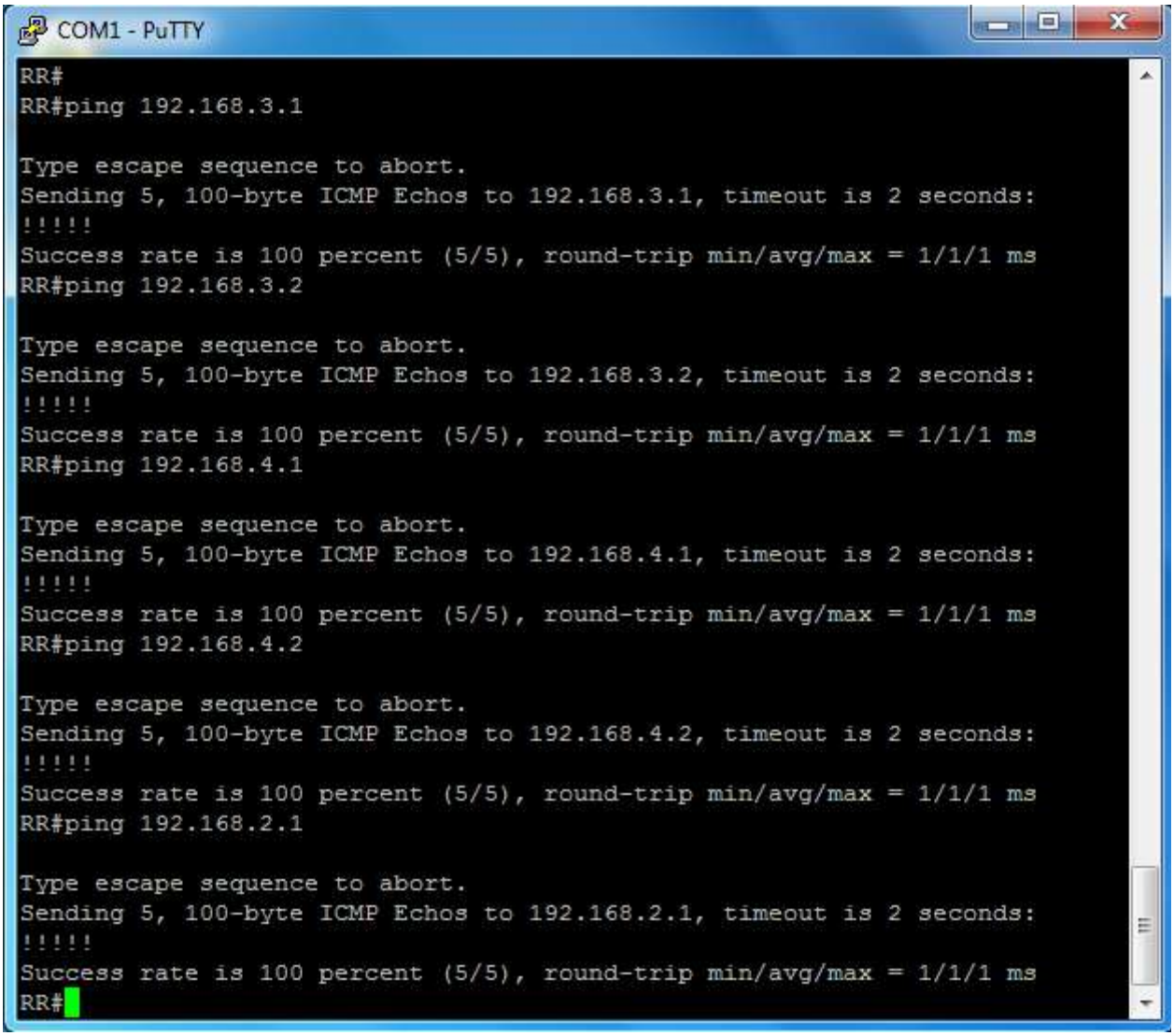


Figura 8.6: verificación de conectividad con router 1 , 3 y 4 con éxito.

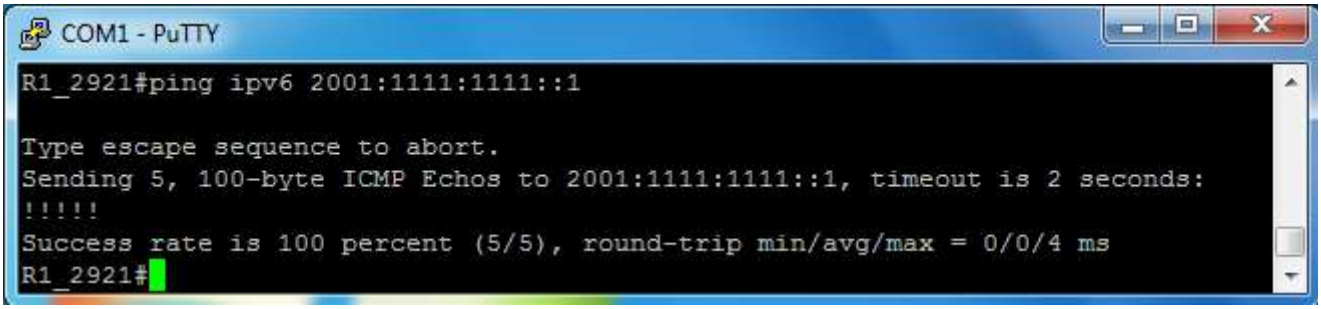


Figura 8.7: prueba de conectividad IPv6

A continuación pasamos a crear la VRF llamada "vrf1" en los routers 1 (Figura 8.8) y 4, en la cual se conectarán al Gateway R5 (en R1) y al cliente (en R4). Vemos la VRF en R1:

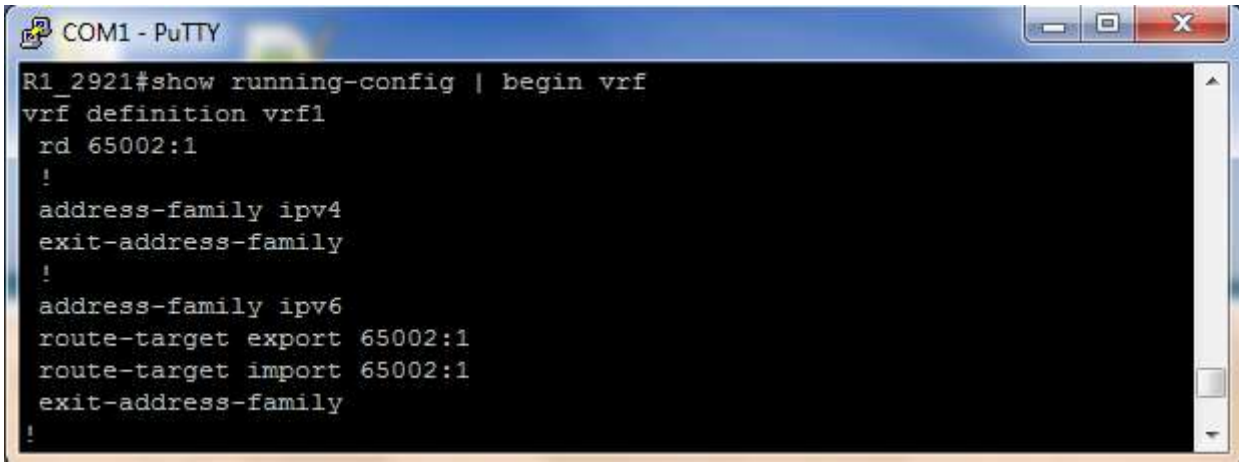


Figura 8.8: definición de VRF en R1 y asociación a interfaz directamente conectada a R5.

Verificamos la conectividad con la VRF en R1 (Figura 8.9):

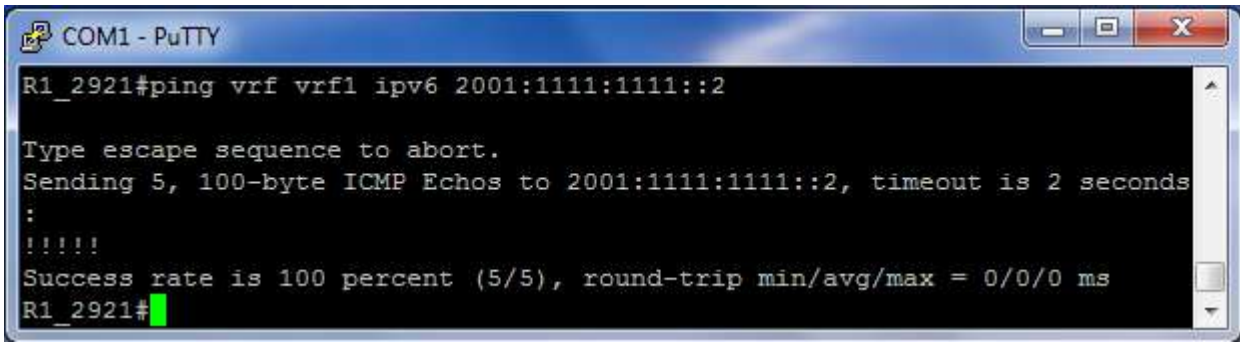


Figura 8.9: salida del comando ping vrf vrf1 ipv6 2001:1111:1111::2

En la figura 8.10, se chequea con ping la VRF "vrf1" con la dirección IPv6 asignada al Gateway.

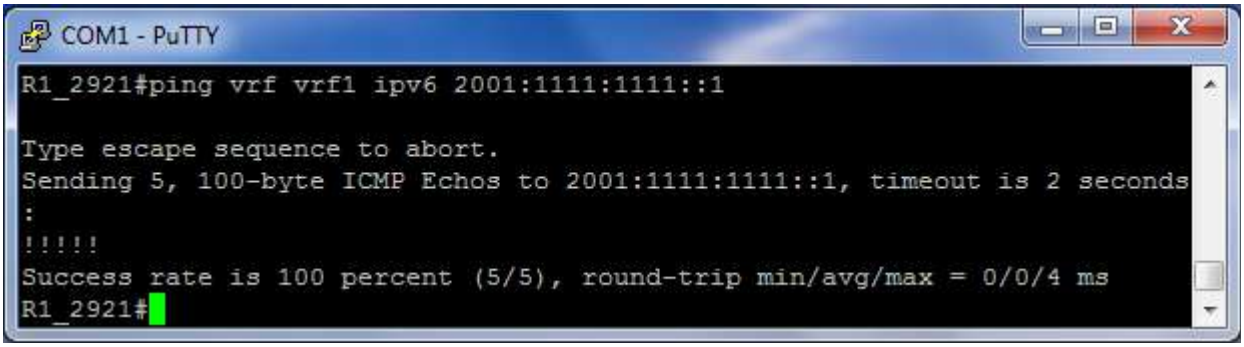


Figura 8.10: salida del comando ping vrf vrf1 ipv6 2001:1111:1111::1 (Ping de R1 a R5)

Y ahora, la conectividad desde el cliente (Notebook) hacia R5 (Figura 8.11):

Figura 8.11: verificación de conectividad desde el cliente al Router 5

8.3 Route Reflector (Reflector de Rutas)

Un reflector de ruta o en inglés Route Reflector (RR) es un componente de encaminamiento de red. Un RR actúa como un punto focal para las sesiones IBGP. El propósito del RR es la concentración. Múltiples routers BGP pueden hacer de peer con un punto central, el RR - que actúa como Route Reflector Server – en lugar de pares con cada otro router en una malla completa. Todos los routers IBGP pasan a ser clientes del Route Reflector Server. Este método, similar a la característica DR/BDR de OSPF, permite configurar grandes redes con escalabilidad IBGP. En una red totalmente mallada IBGP de 10 routers, son necesarios 100 declaraciones individuales (a lo largo de todos los routers en la topología) solo para definir el control remoto-AS de cada par: esto rápidamente se convierte en un dolor de cabeza para administrar. Una topología RR podría reducir estas 100 sentencias a 20, que ofrece una solución viable para las grandes redes administradas por los ISP.

Un reflector de ruta es un punto único de fallo, por lo tanto (al menos) un segundo reflector de ruta debe ser configurado con el fin de proporcionar redundancia.

Reglas: un servidor RR propagará rutas dentro del Sistema Autónomo basado en las siguientes reglas:

- Si una ruta se recibe de pares no cliente (nonclient peer), se reflejará dicha ruta sólo a los clientes.
- Si una ruta se recibe de un par cliente (client peer), se reflejara a todos los nonclient peer y también a los client-peer, excepto al originador de la ruta.
- Si una ruta se recibe de un par EBGP, se reflejará a todos los pares client y noclient.

8.4 Configuración de Cliente

Para este paso, la única tarea a ejecutar, es configurar una interfaz IPv6 y agregar rutas por defecto. Vemos como hacerlo en las diferentes plataformas que utilizamos, estas son: Linux (Ubuntu) y Windows.

Ubuntu: Conexión nativa

1) Asigna una dirección IPv6 desde consola: *ip addr add dirección_ipv6 dev nombre_interfaz*
2) Agrega la ruta por default y el gateway :
   1. route -Ainet6 add red_ipv6/prefijo dev nombre_interfaz
   2. route -Ainet6 add default gw dirección_ipv6

En nuestro caso quedaría entonces:

#ip addr add 2001:db8:ce::2 dev eth0
#route -Ainet6 add 2001:db8:ce::/64 dev eth0
#route -Ainet6 add default gw 2001:db8:ce::1

Para verificar conectividad IPv6: ip -6 address show eth0 .

Para ver la ruta por defecto IPv6: ip -6 route show dev eth0

Microsoft Windows 7: nos dirigimos directamente a:

Inicio → Panel de Control → Redes e Internet → Centro de Redes y recursos compartidos → Cambiar configuración del adaptador.

Una vez allí, hacemos clic derecho en Conexión de Área Local → propiedades . Se nos presentara la siguiente interfaz (Figura 8.12):

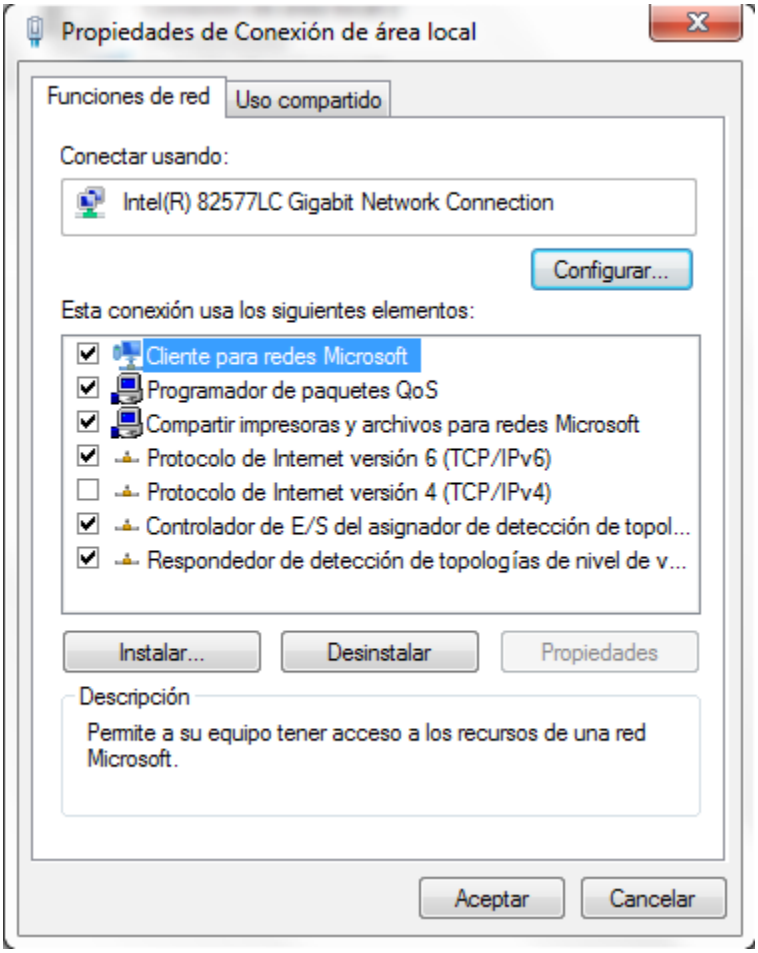


Figura 8.12: Propiedades de Conexión de Área Local

Tenemos que tildar la opción "Protocolo de Internet versión 6 (TCP/IPv6)". Luego pasamos a configurar la dirección IPv6 en propiedades (Figura 8.13):

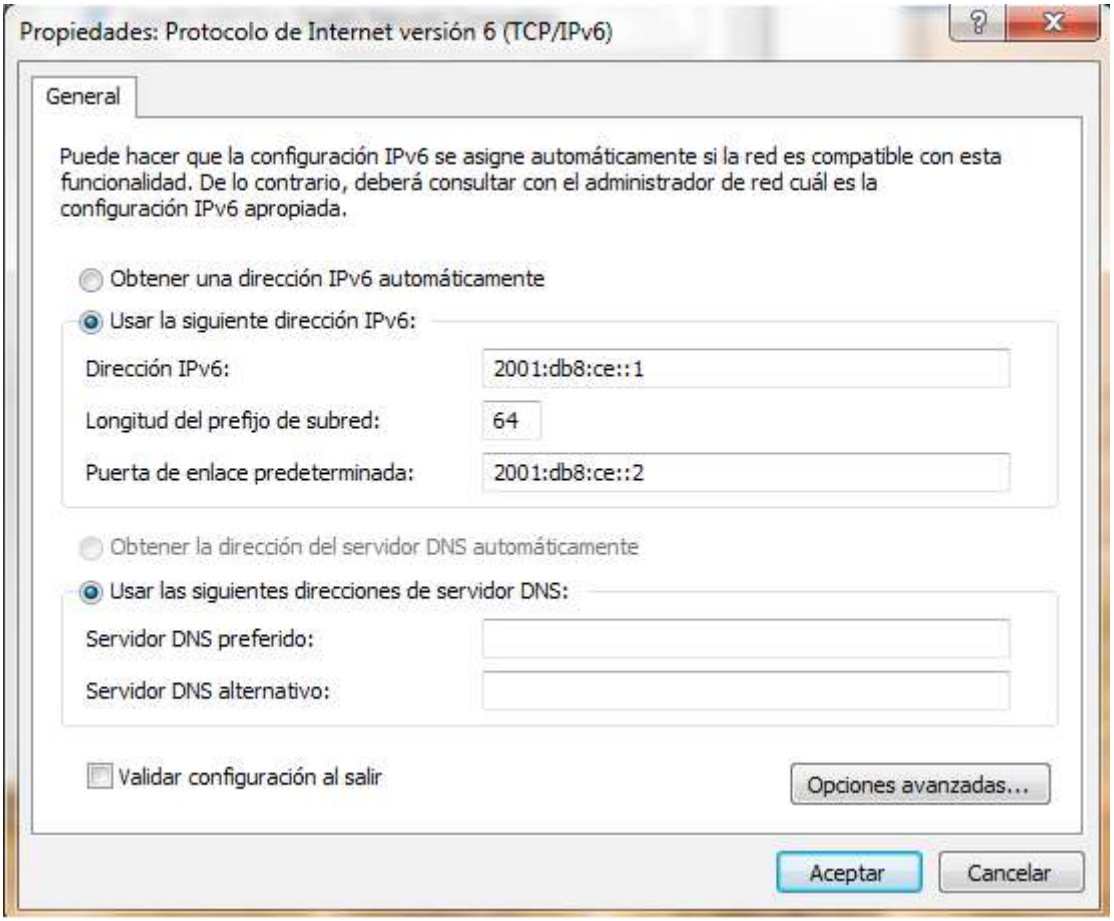


Figura 8.13: asignación de dirección IPv6 en Windows 7

Se debe ingresar una dirección de red IPv6, la longitud del prefijo y la puerta de enlace predeterminada. Las direcciones DNS no son necesarias por el momento. Lo que haremos a continuación, será poner a la VRF1 como doble pila IPv4/IPv6, es decir, al mismo enlace físico R1-R5 y R4-R7 le asignaremos una dirección IPv6 (ya la asignamos previamente) y una dirección IPv4. De esta forma, no cortaremos la conectividad ya establecida con IPv4 en los equipos reales, de forma tal de no perder enlace a los clientes IPv4 de la empresa. Para lograr esto, realizamos las siguientes tareas :

1. En la VRF agregamos la doble pila IPv4/IPv6 (Figura 8.14).

2. Asignamos números IPv4 en los enlaces punto a punto R1-R5 y R4-R7.

3. Agregamos el address family ipv4 vrf y establecemos la adyacencia bgp con el vecino (en el caso de R1, en R4 solo agregamos el address family con redistribute connected). Ver Figura 8.15 y 8.16.

4. Verificamos la conectividad, tanto IPv4 como IPv6 desde R7 hasta el Gateway doble pila R5, ver Figura 8.17.

Tarea Nro 1: Modificamos vrf1 en los routers 1 y 4:

```
vrf definition vrf1
rd 65002:1
address-family ipv4 → habilitamos el forwarding para ipv4
route-target export 65002:1
route-target import 65002:1
exit-address-family
!
address-family ipv6 → ya teníamos la vrf con ipv6
route-target export 65002:1
route-target import 65002:1
exit-address-family
```

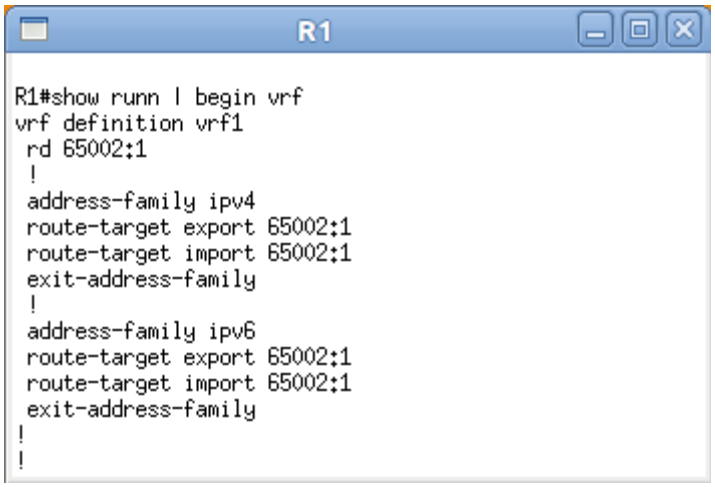


Figura 8.14: VRF creada en el router 1

Tarea Nro 2: En R1 asignamos el ip 192.168.5.2 , y en R5 192.168.5.1 para el enlace punto a punto. Además configuramos la dirección de loopback en R5 como 5.5.5.5.

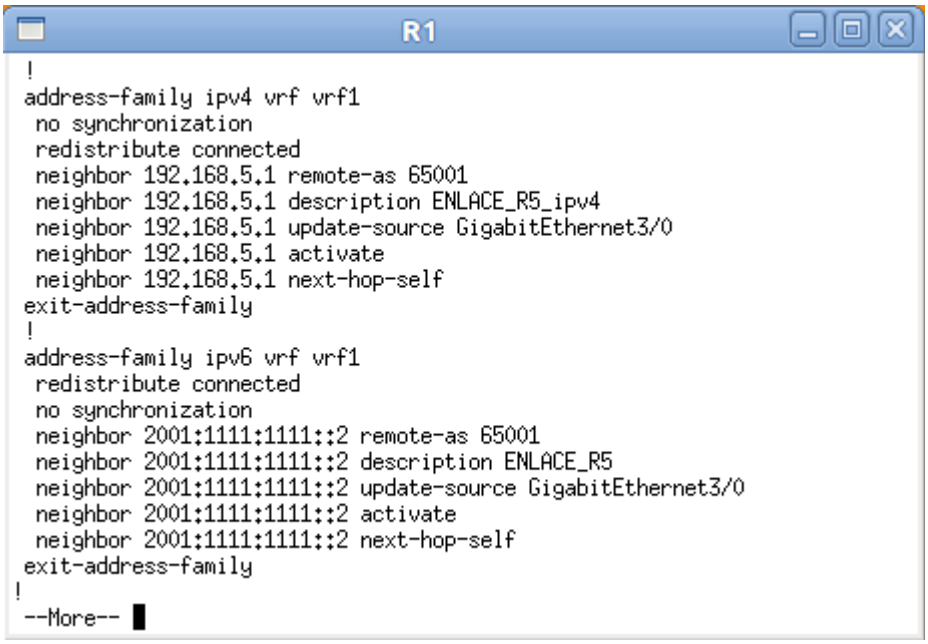


Figura 8.15: address family para la VRF en R1

Debemos definir las familias de direcciones de IPv4 e IPv6 para la adyacencia bgp.

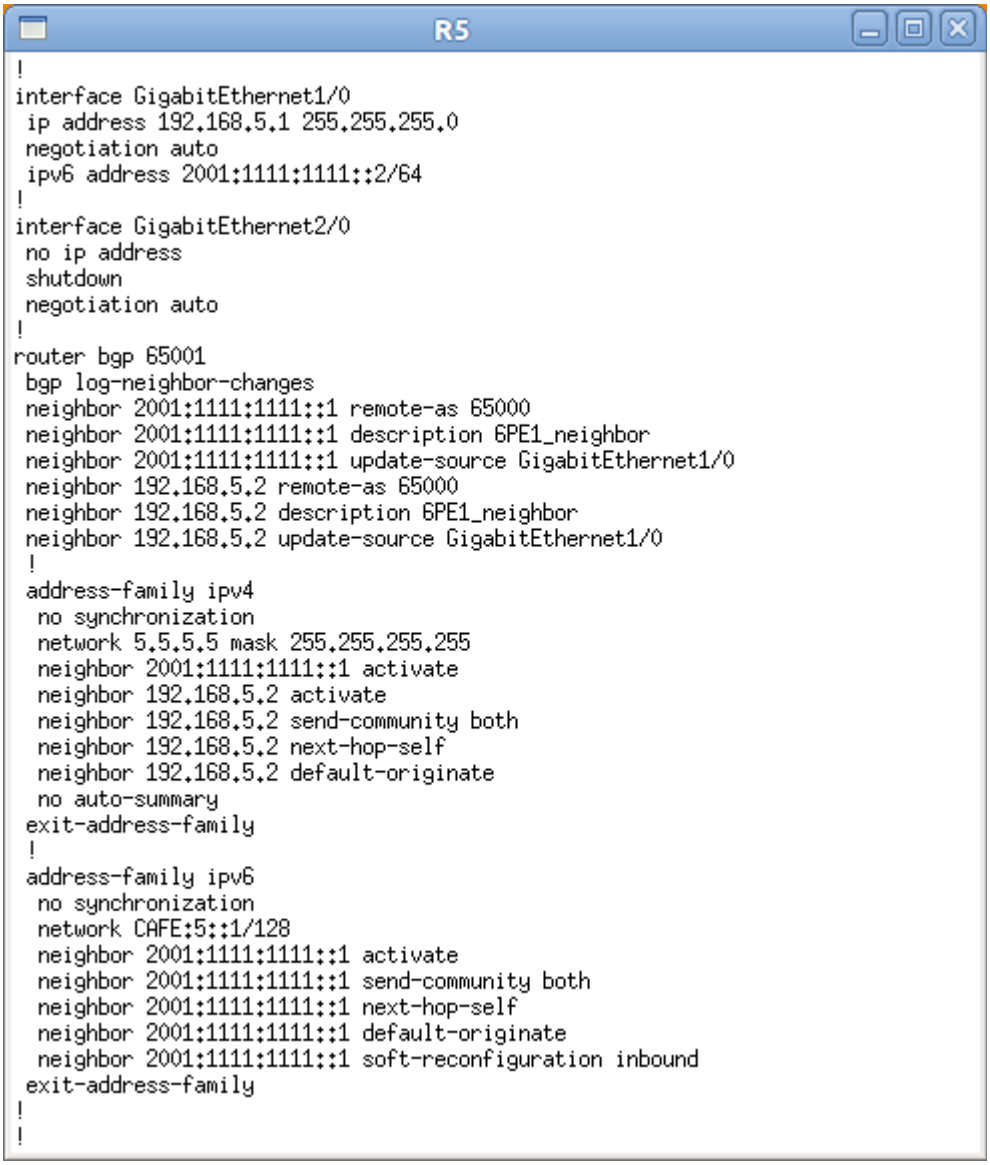


Figura 8.16: adyacencia BGP en R5 con la VRF del router 1

Tarea Nro 4: probamos la conectividad desde el Cliente R7 hasta R5.

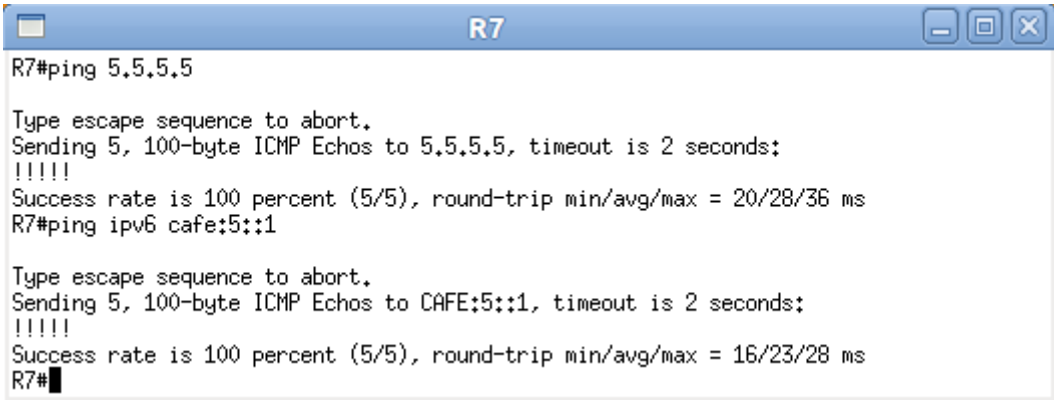


Figura 8.17: ping desde R7 hacia R5 que comprueba la visibilidad

8.5 Alternativa 2 : uso de Sub-Interfaces (o VLANs)

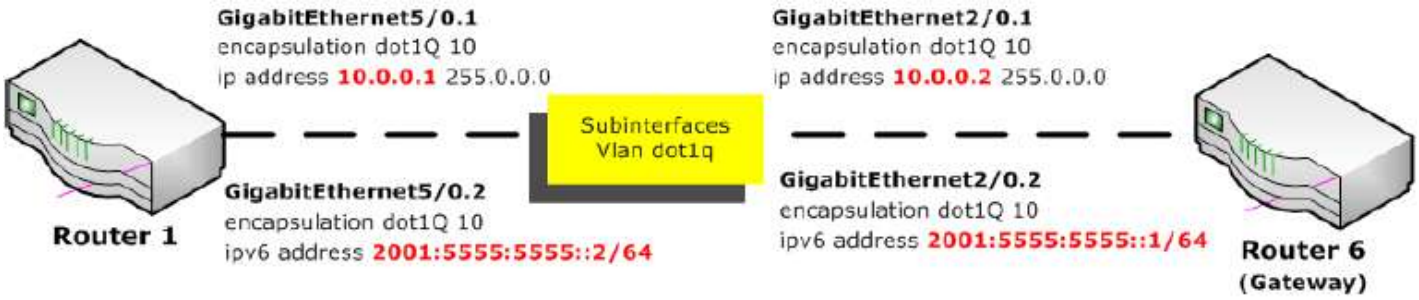


Figura 8.18: sub-interfaces creadas en R1 y R5 para aprovechar un único enlace físico

Interfaces y Sub-Interfaces

El encaminamiento tradicional requiere de routers que tengan interfaces físicas múltiples para facilitar el encaminamiento entre VLAN (como el ejemplo que presentamos con VRF, en el cual tenemos sólo una VRF por interfaz). El router realiza el encaminamiento al conectar cada una de sus interfaces físicas a una VLAN única. Además, cada interfaz está configurada con una dirección IP para la subred asociada con la VLAN conectada a ésta. Al configurar las direcciones IP en las interfaces físicas, los dispositivos de red conectados a cada una de las VLAN pueden comunicarse con el router mediante la interfaz física conectada a la misma VLAN. En esta configuración los dispositivos de red pueden utilizar el router como un gateway para acceder a los dispositivos conectados a las otras VLAN.

Configuración de la sub-interfaz

La configuración de las sub-interfaces del router es similar a la configuración de las interfaces físicas, excepto que es necesario crear la sub-interfaz y asignarla a una VLAN.

La sintaxis para la sub-interfaz es siempre la interfaz física, en este caso G5/0, seguida de un punto y un número de sub-interfaz. El número de la sub-interfaz es configurable, pero generalmente está asociado para reflejar el número de VLAN. Antes de asignar una dirección IP a una sub-interfaz, es necesario configurar la sub-interfaz para que funcione en una VLAN específica mediante el comando encapsulation dot1q id de la VLAN (ver nota 6).

En el ejemplo, la sub-interfaz G5/0.1 está asignada a la VLAN 10. Una vez asignada la VLAN, el comando ip address 10.0.0.1 255.0.0.0 asigna la sub-interfaz a la dirección IP apropiada para esa VLAN.

Nota 6: El protocolo IEEE 802.1Q, también conocido como dot1Q, fue un proyecto del grupo de trabajo 802 de la IEEE para desarrollar un mecanismo que permita a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas (Trunking). Es también el nombre actual del estándar establecido en este proyecto y se usa para definir el protocolo de encapsulamiento usado para implementar este mecanismo en redes Ethernet. Todos los dispositivos de interconexión que soportan VLAN deben seguir la norma IEEE 802.1Q que especifica con detalle el funcionamiento y administración de redes virtuales.

Sub-Interfaces en R1 (Figura 8.19)

```
interface GigabitEthernet5/0 → en la interfaz no hemos configurado números ip
```

```
interface GigabitEthernet5/0.1 → sub-interfaz que usaremos para ipv4
encapsulation dot1Q 10
ip address 10.0.0.1 255.0.0.0 → nro. ip en la misma red que la sub-interfaz de R5
interface GigabitEthernet5/0.2 → sub-interfaz que usaremos para ipv6
encapsulation dot1Q 20
ipv6 address 2001:5555:5555::2/64 → nro. ip en la misma red que la sub-interfaz de R5
```

A diferencia de una interfaz física típica, las sub-interfaces no están habilitadas con el comando no shutdown en el nivel de modo de configuración de la sub-interfaz del software IOS de Cisco. En cambio, cuando la interfaz física esta habilitada con el comando no shutdown, todas las sub-interfaces configuradas están habilitadas. De manera similar, si la interfaz física está deshabilitada, todas las sub-interfaces están deshabilitadas también.

Una ventaja de utilizar un enlace troncal es que se reduce la cantidad de puertos del switch y del router. Esto no solo permite un ahorro de dinero sino también reduce la complejidad de la configuración. Como consecuencia, el enfoque de la sub-interfaz del router puede ampliarse hasta un numero mucho mas alto de VLAN que una configuración con una interfaz física por diseño de VLAN.

A continuación , para tener acceso desde el Cliente R8 hasta R6, estableceremos la adyacencia BGP con estas sub-interfaces, en el enlace R1-R6 (deberemos crear también las sub-interfaces del lado de R6 con sus respectivos números IPv4 e IPv6 en cada caso). Entonces tenemos:

Sub-Interfaces en R6

```
interface GigabitEthernet2/0 → no hace falta asignar ip a la interfaz
no ip address
negotiation auto
!
interface GigabitEthernet2/0.1
encapsulation dot1Q 10
ip address 10.0.0.2 255.0.0.0
!
interface GigabitEthernet2/0.2
encapsulation dot1Q 20
ipv6 address 2001:5555:5555::1/64
```

A continuación, la Figura 8.19 nos muestra las sub-interfaces que se crearon en el Router 1, estas son: Interface GigabitEthernet5/0.1 para IPv4 , y Interface GigabitEthernet5/0.2 para IPv6.

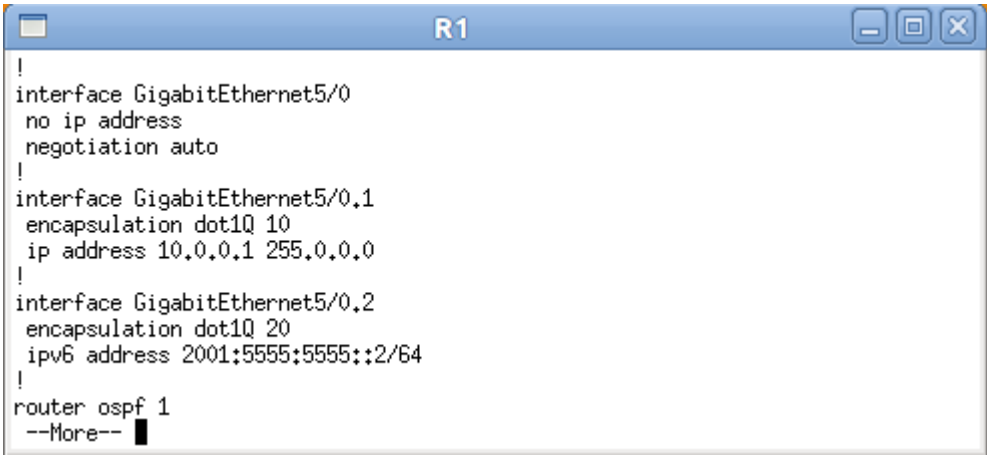


Figura 8.19: sub-interfaces creadas en router 1

Una vez creadas y verificadas las conexiones de estas sub-interfaces, lo único que falta hacer es crear la vecindad BGP entre las mismas. Entonces nos queda la configuración completa de BGP en R1:

```
router bgp 65000
bgp log-neighbor-changes
neighbor 2.2.2.2 remote-as 65000 → enlace con el Route Reflector R2
neighbor 2.2.2.2 description RR_iBGP
neighbor 2.2.2.2 update-source Loopback0
neighbor 10.0.0.2 remote-as 65006 → conexión con R6 (a la vlan 10)
neighbor 10.0.0.2 description enlace_vlan_ipv4
neighbor 10.0.0.2 update-source GigabitEthernet5/0.1
neighbor 2001:5555:5555::1 remote-as 65006 → conexión con R6 (a la vlan 20)
neighbor 2001:5555:5555::1 description enlace_R6
neighbor 2001:5555:5555::1 update-source GigabitEthernet5/0.2
!
address-family ipv4
no synchronization
redistribute connected
neighbor 2.2.2.2 activate → adyacencia con Route Reflector
neighbor 2.2.2.2 soft-reconfiguration inbound
neighbor 10.0.0.2 activate → adyacencia con la vlan 10
default-information originate
no auto-summary
exit-address-family
!
address-family vpnv4
neighbor 2.2.2.2 activate
neighbor 2.2.2.2 send-community both
```

```
neighbor 2.2.2.2 next-hop-self
exit-address-family
!
address-family ipv6
redistribute connected
default-information originate
no synchronization
neighbor 2.2.2.2 activate
neighbor 2.2.2.2 send-label
neighbor 2001:5555:5555::1 activate → adyacencia con R6 (vlan 20)
exit-address-family
!
address-family vpnv6
neighbor 2.2.2.2 activate
neighbor 2.2.2.2 send-community both
neighbor 2.2.2.2 next-hop-self
exit-address-family
!
address-family ipv4 vrf vrf1 → vrf que conecta con R5 para ipv4
no synchronization
redistribute connected
neighbor 192.168.5.1 remote-as 65001
neighbor 192.168.5.1 description ENLACE_R5_ipv4
neighbor 192.168.5.1 update-source GigabitEthernet3/0
neighbor 192.168.5.1 activate
neighbor 192.168.5.1 next-hop-self
exit-address-family
!
address-family ipv6 vrf vrf1 → conexión VRF con R5 para la interfaz ipv6
redistribute connected
no synchronization
neighbor 2001:1111:1111::2 remote-as 65001
neighbor 2001:1111:1111::2 description ENLACE_R5
neighbor 2001:1111:1111::2 update-source GigabitEthernet3/0
neighbor 2001:1111:1111::2 activate
neighbor 2001:1111:1111::2 next-hop-self
exit-address-family
```

Configuraciones en R4: Vemos primero la configuración ip de las interfaces que conectaran a los routers cliente R7 y R8 :

```
interface GigabitEthernet3/0
description CLIENTE_R7
vrf forwarding vrf1
ip address 192.168.7.2 255.255.255.0
ipv6 address 2001:DB8:CE::2/64

interface GigabitEthernet4/0
description CLIENTE_R8
ip address 192.168.8.2 255.255.255.0
ipv6 address 2001:DB8:1111::1/64
```

Ahora vemos la configuración del router BGP en R4 completa (Figura 8.20), definimos la VPNv4 y la VPNv6, para luego definir el address family de la VRF para IPv4 e IPv6.

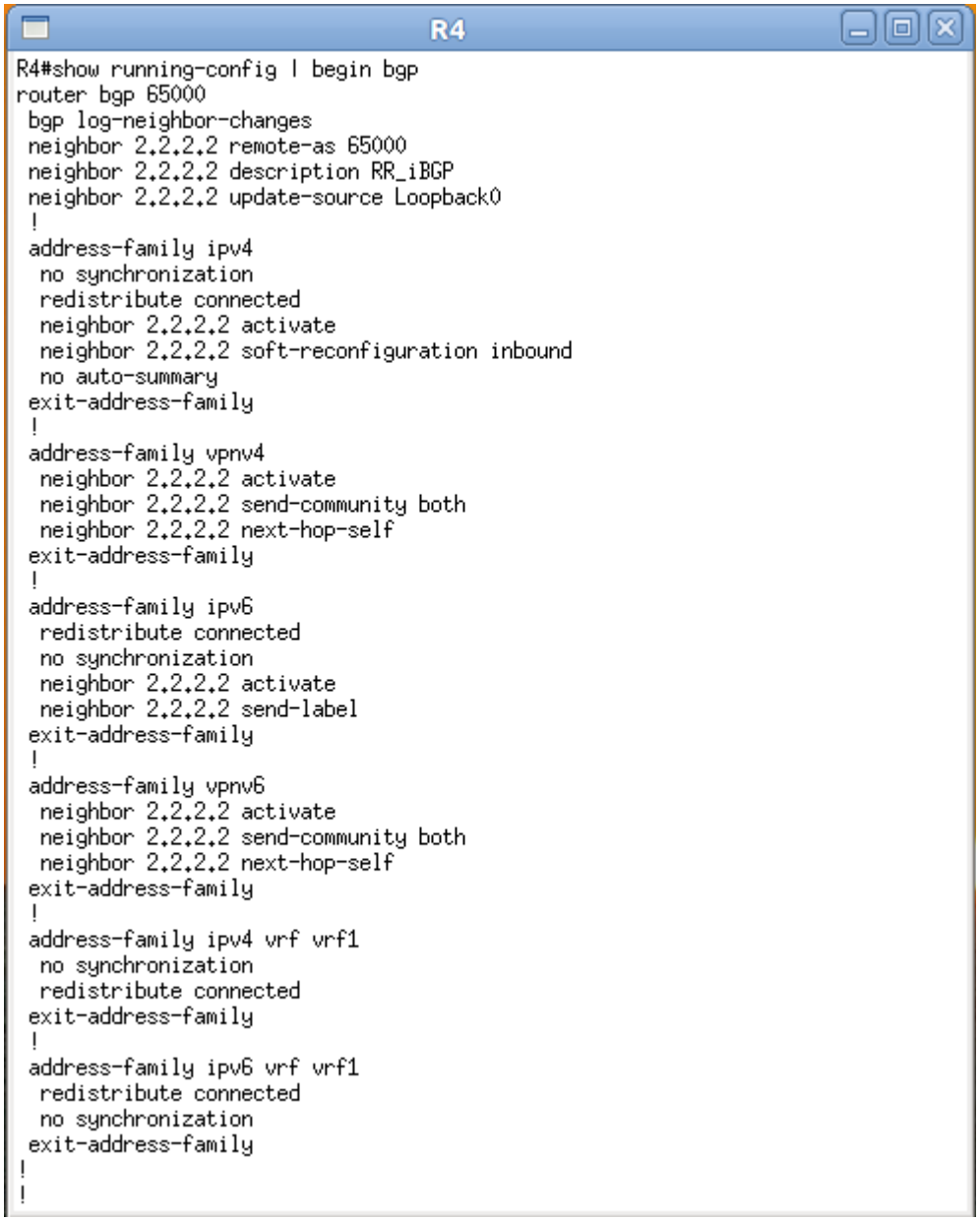


Figura 8.20: configuración BGP en router 4

Como puede apreciarse en la figura, tenemos en R4 la conexión con R7 a través de la VRF *vrf1*

```
vrf definition vrf1 → mismo nombre de la vrf del enlace R1-R5
rd 65002:1
!
address-family ipv4
route-target export 65002:1
route-target import 65002:1
exit-address-family
!
address-family ipv6
```

```
route-target export 65002:1
route-target import 65002:1
exit-address-family
!
interface GigabitEthernet3/0 → interfaz directamente conectada a R7
description CLIENTE_R7
vrf forwarding vrf1 → la conectamos a la VRF vrf1
ip address 192.168.7.2 255.255.255.0 → asignamos dirección ipv4
ipv6 address 2001:DB8:CE::2/64 → asignamos dirección ipv6
```

Como puede verse, al Router 7 se lo conecta al Backbone a través de la VRF vfr1 (misma VRF que conectamos R1 con R5) sin necesidad de establecer la vecindad ip; de esta forma el cliente R7 podrá salir del Backbone al exterior a través de R5.

Entonces en R7, solo debemos definir los números ip de la interfaz, y las rutas por defecto. Lo vemos a continuación:

```
interface GigabitEthernet1/0
ip address 192.168.7.1 255.255.255.0
ipv6 address 2001:DB8:CE::1/64
!
ip route 0.0.0.0 0.0.0.0 192.168.7.2 → ruta por defecto para tráfico ipv4 (número IPv4 del router 4)
ipv6 route ::/0 2001:DB8:CE::2 → ruta por defecto para tráfico ipv6 (número IPv6 del router 4)
```

Al router 8 solo se lo conecta físicamente, y se le configuran las direcciones IPv4 e IPv6 correspondientes, en la interfaz directamente conectada a R4, ya que este cliente saldrá del Backbone hacia el exterior a través del Gateway R6 (recordemos que R6 se conecta a R1 a través de sub-interfaces y BGP).

Configuración de R8: configuramos las direcciones IPv4 e IPv6, y las rutas por defecto.

```
interface GigabitEthernet1/0
ip address 192.168.8.1 255.255.255.0
ipv6 address 2001:DB8:1111::2/64
ip route 0.0.0.0 0.0.0.0 192.168.8.2 → ruta por defecto para tráfico ipv4 (numero IPv4 del router 4)
ipv6 route ::/0 2001:DB8:1111::1 → ruta por defecto para tráfico ipv6 (numero IPv6 del router 4)
```

8.6 Pruebas de conectividad: ping y traceroute

A continuación, realizaremos pruebas de conectividad, con los comandos ***ping*** y ***traceroute***, para ver como se resuelve el camino desde los routers cliente, pasando por el backbone MPLS y llegando a los routers Gateway (R5 y R6. Ver Figuras 8.21, 8.22, 8.23). Luego veremos las tablas de MPLS (Figuras 8.24, 8.25, 8.34 y 8.35), las tablas IP (Figura 8.26 y 8.27), y las tablas de BGP en los routers R4 y R2 (Figuras 8.28, 8.29, 8.30, 8.31, 8.32 y 8.33).

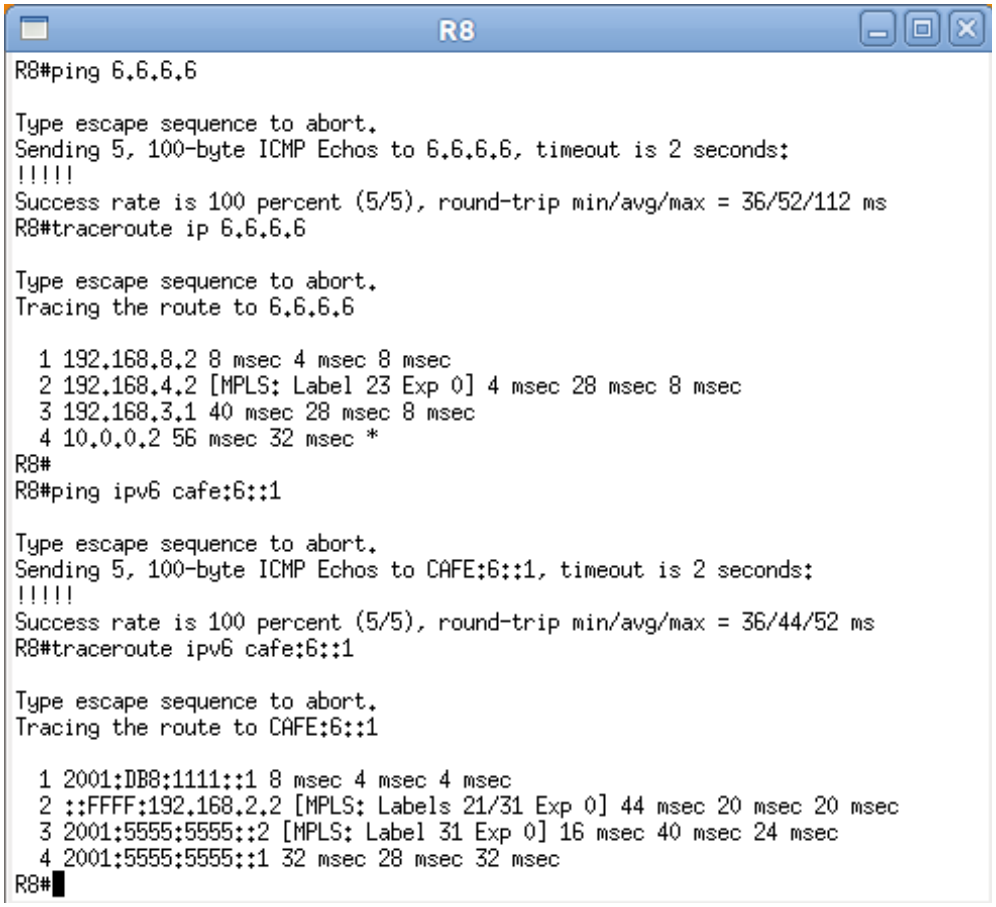


Figura 8.21: prueba de conectividad R8 – R6 con comando ping y traceroute

Verificamos con el comando ping llegar hasta las direcciones de loopback IPv4 e IPv6 del router 6. Vemos también con el comando traceroute el camino que se ha utilizado para llegar hasta el destino. Para llegar al destino de red 6.6.6.6 (loopback0 de R6) se armó el camino:

R8(192.168.8.1)→R4(192.168.8.2)→R3(192.168.4.2)→R1(192.168.3.1)→R6(10.0.0.2)

Y para llegar al destino cafe:6::1 (loopback IPv6 de R6) :

2001:db8:1111::2(R8) →

2001:db8:1111::1(R4) →

::FFFF:192.168.2.2(R2 dirección mapeada IPv4-IPv6 y etiqueta MPLS 21/31) →

2001:5555:5555::2(R1 etiqueta mpls 31) →

2001:5555:5555::1(R6 destino final , con loopback cafe:6::1)

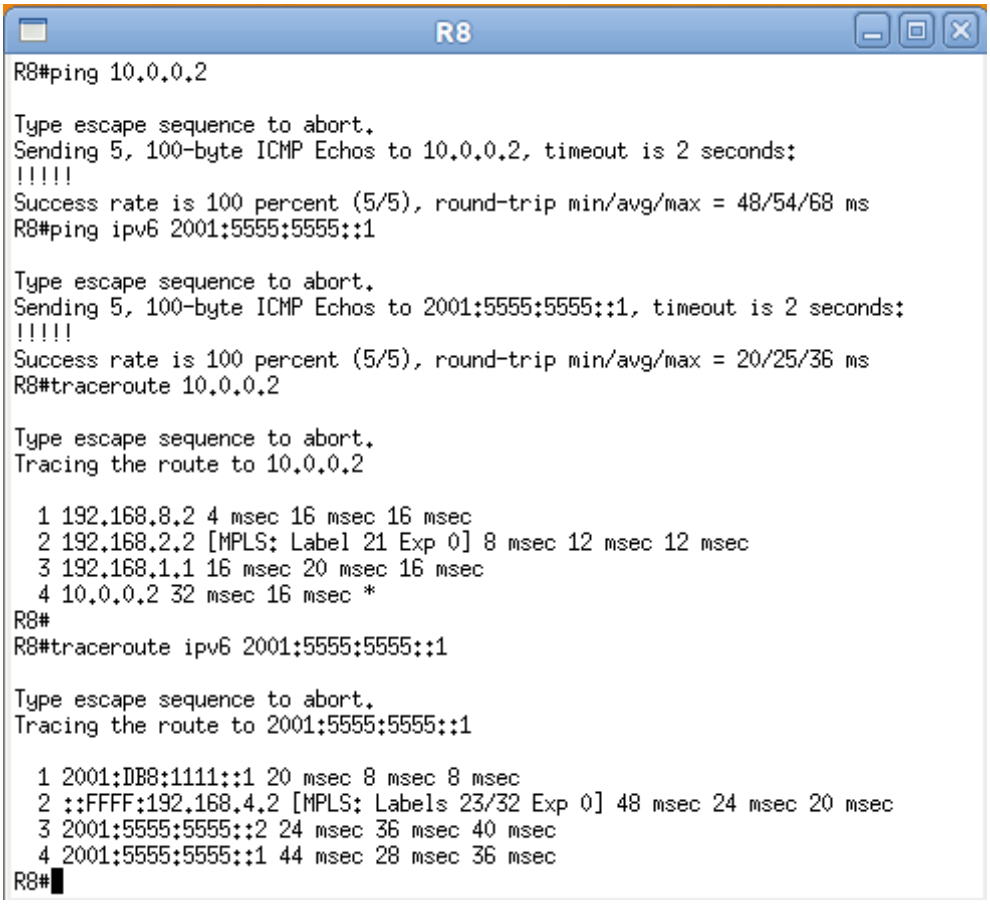


Figura 8.22: prueba de conectividad R8 – R6 con comando ping y traceroute hacia las ip de las VLAN

Podemos ver en la figura 8.23 el uso de las direcciones mapeadas IPv4 a IPv6, en el traceroute a 2001:5555:5555::1, el salto nro 2 utiliza la dirección ::FFFF:192.168.4.2

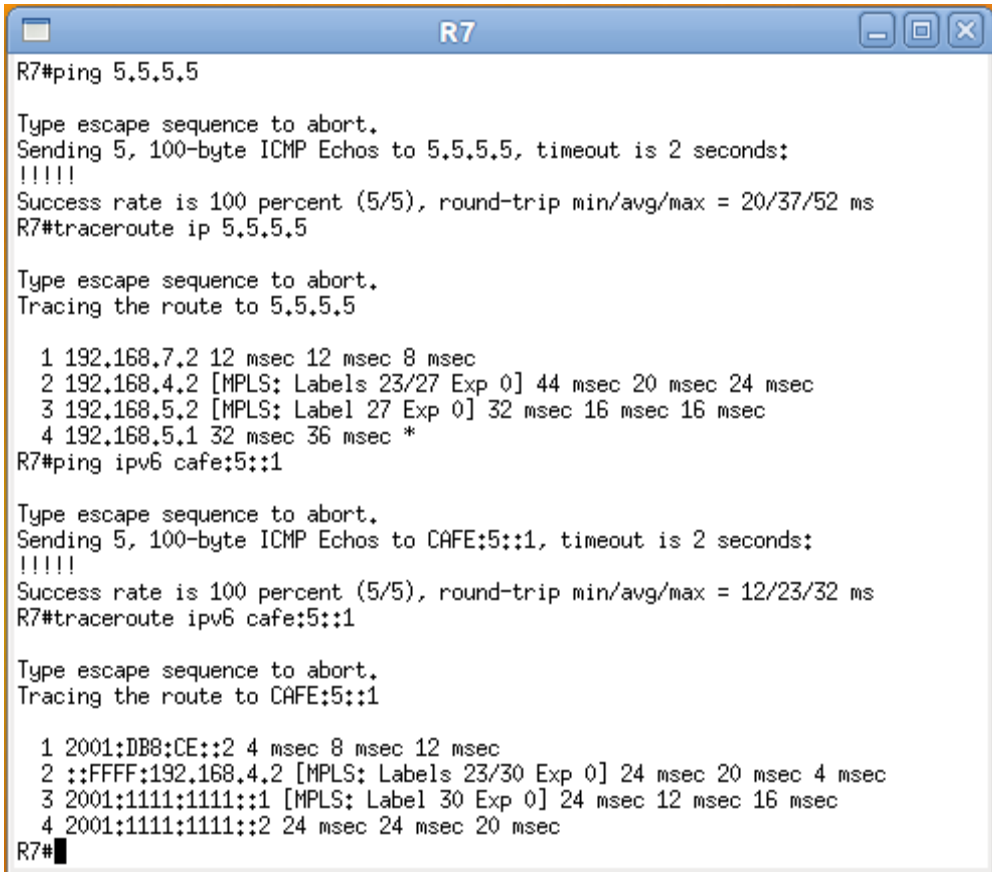


Figura 8.23: prueba de conectividad R7 – R5

En la captura vemos el camino de R5 a R7, recordemos que la conexión es a través de VRF (que se encuentra definida en R4 y en R1 que son los nodos borde).

Realizamos el ping hacia la dirección de loopback IPv4 de R5 y a la de loopback IPv6 del mismo.

8.7 Capturas de tablas de encaminamiento

Veremos diferentes tablas de encaminamiento, realizando capturas de consola las cuales presentaremos como figuras para entender el funcionamiento general del encaminamiento.

Capturas de tablas MPLS : vemos en la figura 8.25 una tabla mpls para ver las etiquetas asignadas:

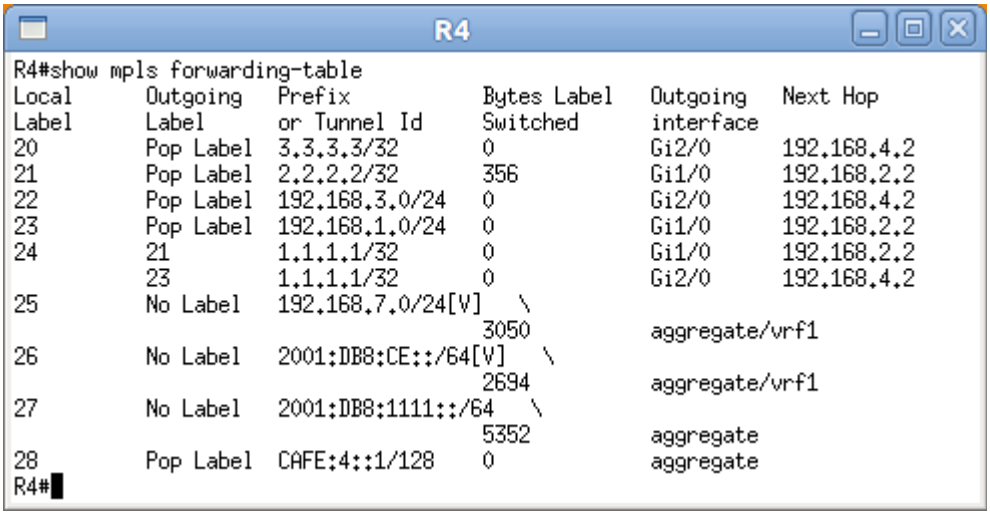


Figura 8.24: salida del comando show mpls forwarding-table

La "Local Label" (o tag) es la etiqueta que este LSR asigna y distribuye a los demas LSRs. Como tal, este LSR espera paquetes etiquetados para llegar a ella con las etiquetas que están en el tope de la pila de etiquetas.

Si este LSR recibe un paquete etiquetado con la etiqueta superior 24, se cambiaría (swap) la etiqueta con etiqueta 21 y se reenviaría a la interfaz Gi1/0. Este es un ejemplo de procedimiento de reenvío de etiqueta a etiqueta (label-to-label forwarding).

Si tenemos por ejemplo una entrada con Local Label 25, y con Outgoing Label "Untagged" o "No Label", si el LSR recibe un paquete con top top label 25, este removerá todas las etiquetas y enviará el paquete como un paquete IP, debido a que el Outgoing Label es "Untagged/No Label". Este seria un caso llamado label-to-IP case.

Si el LSR recibe un paquete con top label 20, este removerá el top label (pop one label) y enviará el paquete como un paquete etiquetado o como un paquete ip.

Recordemos las operaciones de etiquetas :

Pop: La etiqueta superior (top label) es removida. El paquete es enviado con el restante de la pila de etiquetas o como un paquete sin etiquetar (unlabeled packet).

Swap: La etiqueta superior (top label) es removida y reemplazada con una nueva etiqueta.

Push: La etiqueta superior (top label) es reemplazada con una nueva etiqueta (swapped),y una o mas etiquetas son agregadas (pushed) al tope de la etiqueta reemplazada (swapped label).

Untagged/No Label: La etiqueta es removida y el paquete es enviado sin etiqueta (unlabeled).

Aggregate: la pila de etiquetas es removida y una búsqueda IP se efectúa con el IP del paquete.

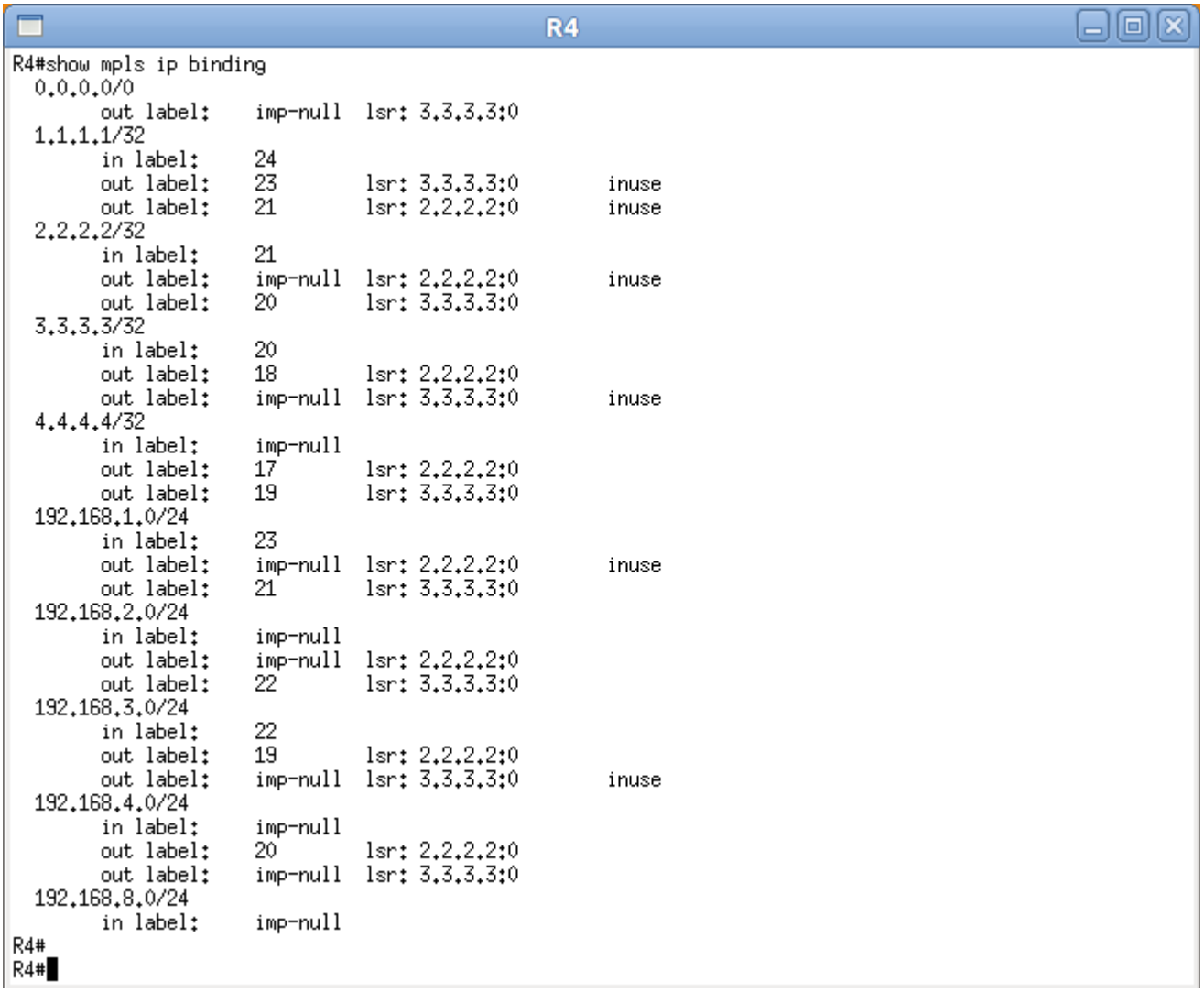


Figura 8.25: salida del comando `show mpls ip binding`

El comando `show mpls ip binding` lo usamos para mostrar las etiquetas MPLS asignadas por el LSR y como sus vecinos identifican las rutas con sus propias etiquetas. Por ejemplo, para el vecino 1.1.1.1/32 (router 1) tenemos:

```
1.1.1.1/32

      in label: 24

      out label: 23 lsr: 3.3.3.3:0 inuse

      out label: 21 lsr: 2.2.2.2:0 inuse
```

Lo que nos esta indicando que tiene 2 posibles caminos para llegar al router 1, a través del router 3, con etiqueta de salida 23, y a través del router 2 con etiqueta de salida 21, actualmente los 2 caminos están en uso.
La etiqueta imp-null (implicit NULL label - Label 3) es para los routers directamente conectados y sumarizados, el único router que no tiene esta etiqueta es el router 1, ya que el resto de las

entradas de la tabla son destinos directamente conectados. Y finalmente, veremos las tablas de encaminamiento IPv4 e IPv6 (Figura 8.27 y 8.28).

Tablas de encaminamiento IPv4 e IPv6

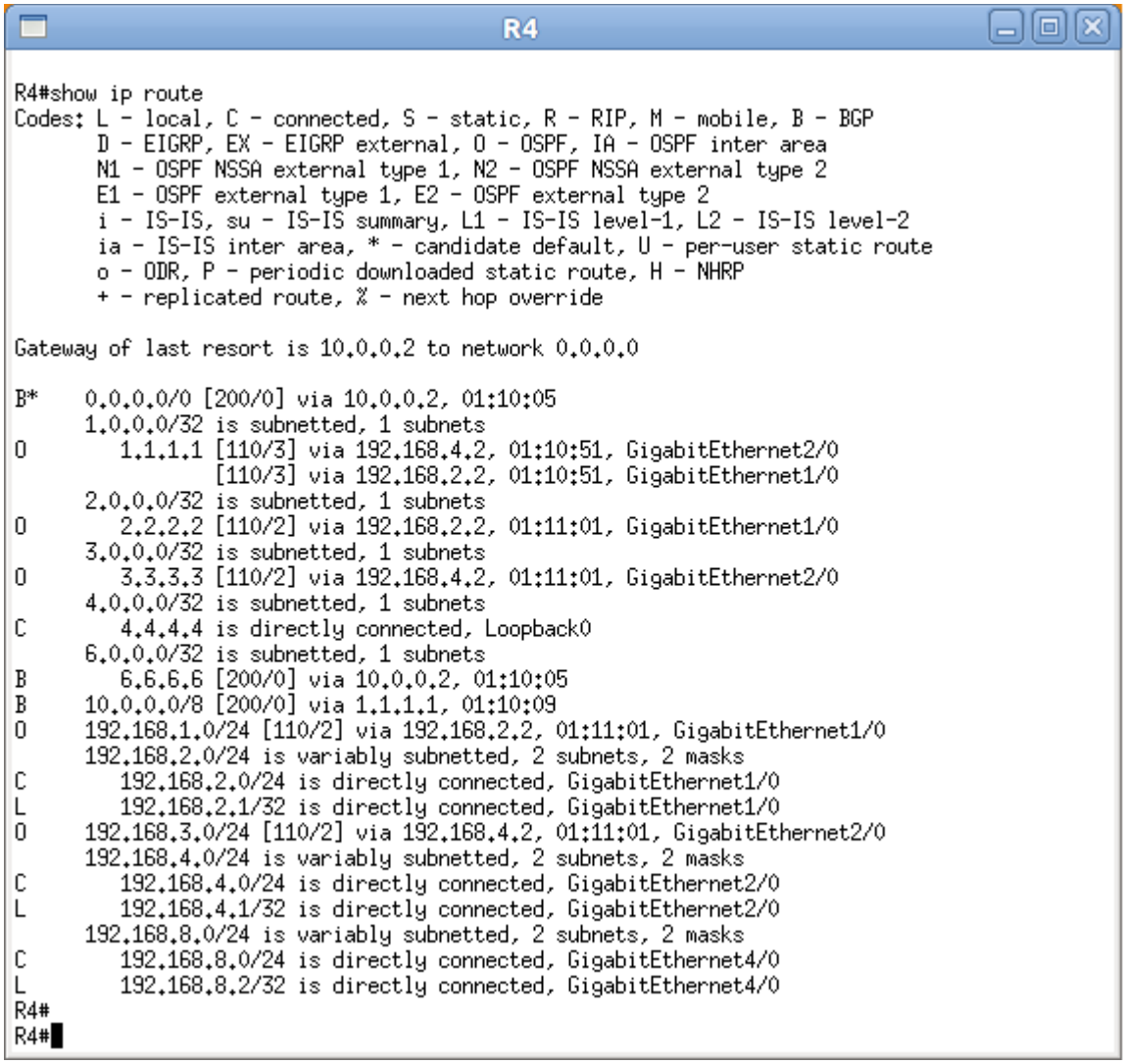


Figura 8.26: salida del comando show ip route en R4

En esta tabla, se ven todas las direcciones de red IPv4, discriminadas por protocolo. Tenemos B (de BGP), O (de OSPF) y L (de enlace local).

Se ve también la primer entrada con un asterisco (*) la ruta recibida por BGP, esto quiere decir, que es la ruta seleccionada como candidata a ser ruta por defecto.

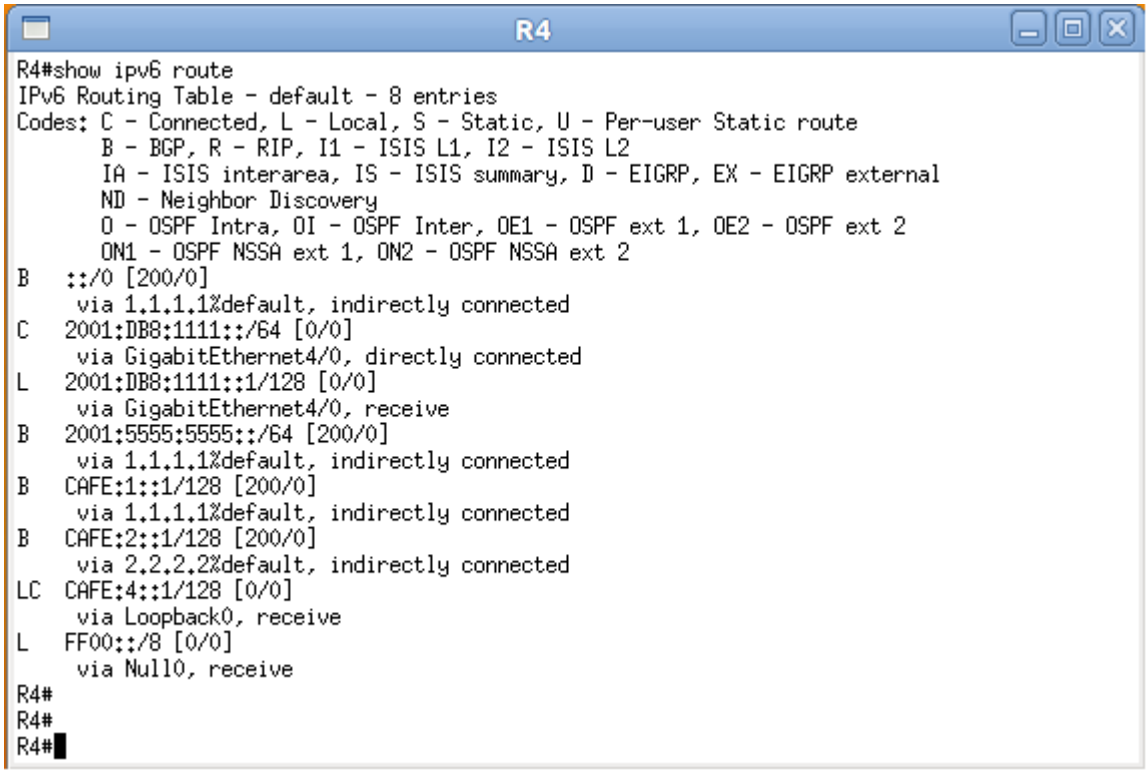


Figura 8.27: salida del comando show ipv6 route

En esta tabla visualizamos las rutas recibidas también por BGP (B), Local (L) , Connected (C) Local Connected (LC). La ruta por defecto de salida IPv6 se indica como ::/0, y el siguiente salto es la dirección de loopback del Router 1 (1.1.1.1), lo cual resulta lógico ya que R1 es quien está conectado a los Gateways R5 y R6.

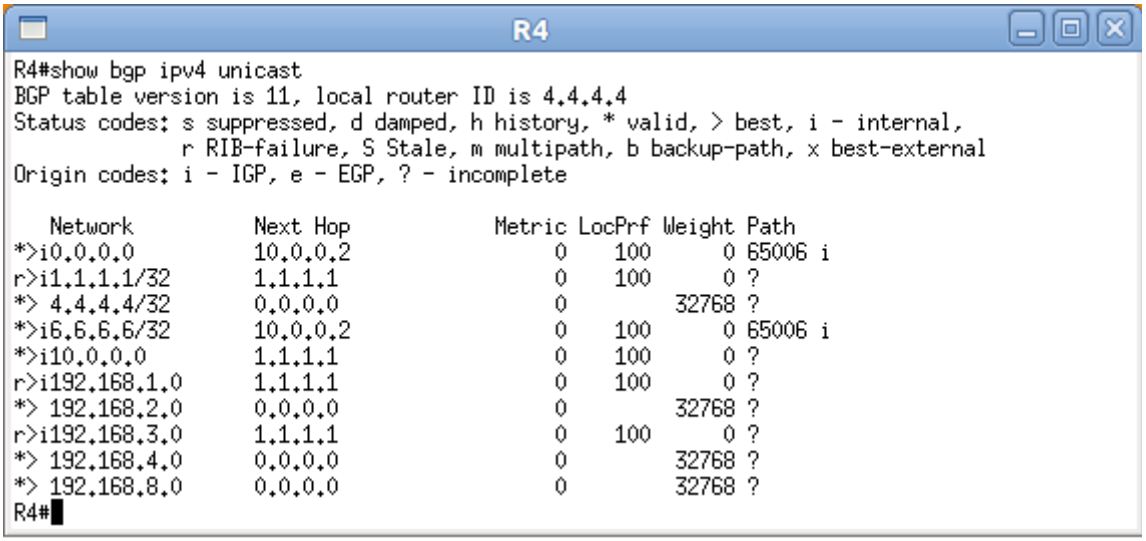


Figura 8.28: salida del comando show bgp ipv4 unicast

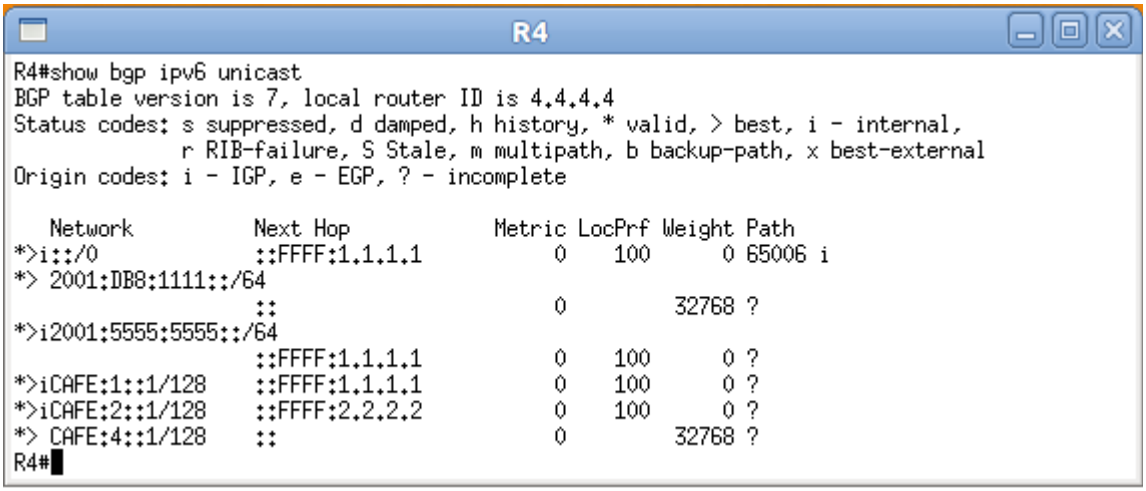


Figura 8.29: salida del comando show bgp ipv6 unicast

Vemos las rutas que R4 recibió del Route Reflector a través de BGP:

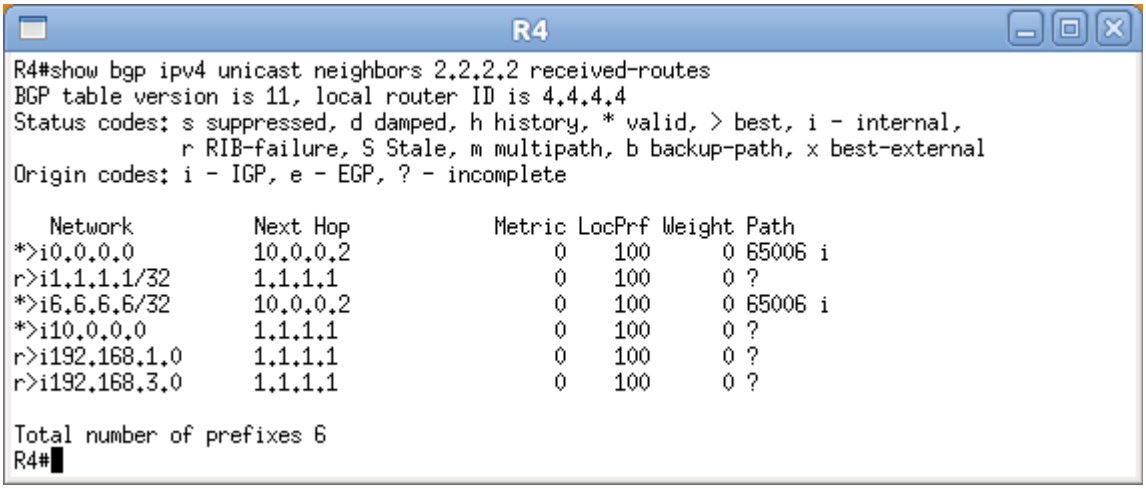


Figura 8.30: rutas recibidas ipv4 en R4 de R2 mediante BGP

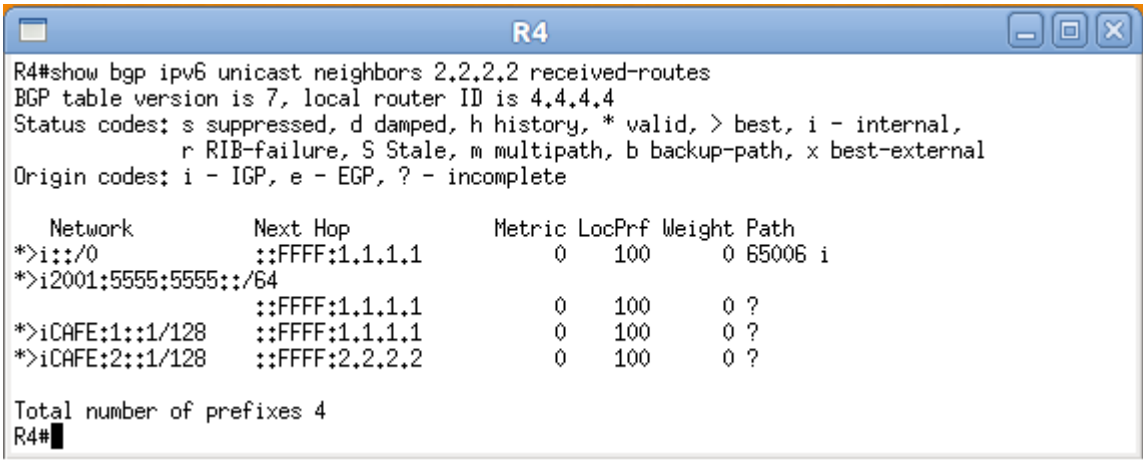


Figura 8.31: rutas recibidas ipv6 en R4 de R2 mediante BGP

Ahora vemos las rutas que recibió R2 de R1 y R4 (Figura 8.32):

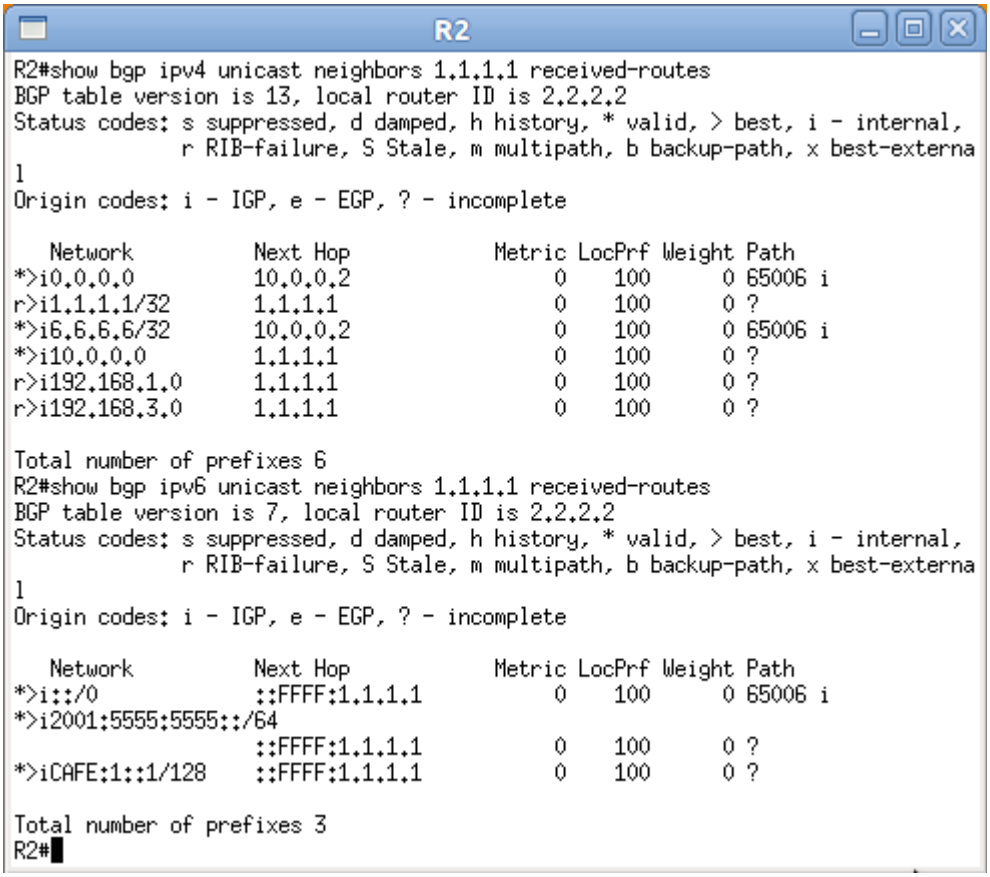


Figura 8.32: rutas ipv4/ipv6 que recibió R2 de R1

De estas capturas de tablas producidas por el uso del comando `show bgp ipv4 unicast neighbors x.x.x.x received routes`, podemos apreciar de esta última tabla, las rutas recibidas por iBGP , con el siguiente salto (Next Hop).

A su vez, también se ven que rutas recibidas corresponden a un sistema autónomo remoto, como la ruta por defecto (i0.0.0.0) que tiene como siguiente salto 10.0.0.2 que corresponde a la conexión de la VLAN 10 de R1 conectada a R6.

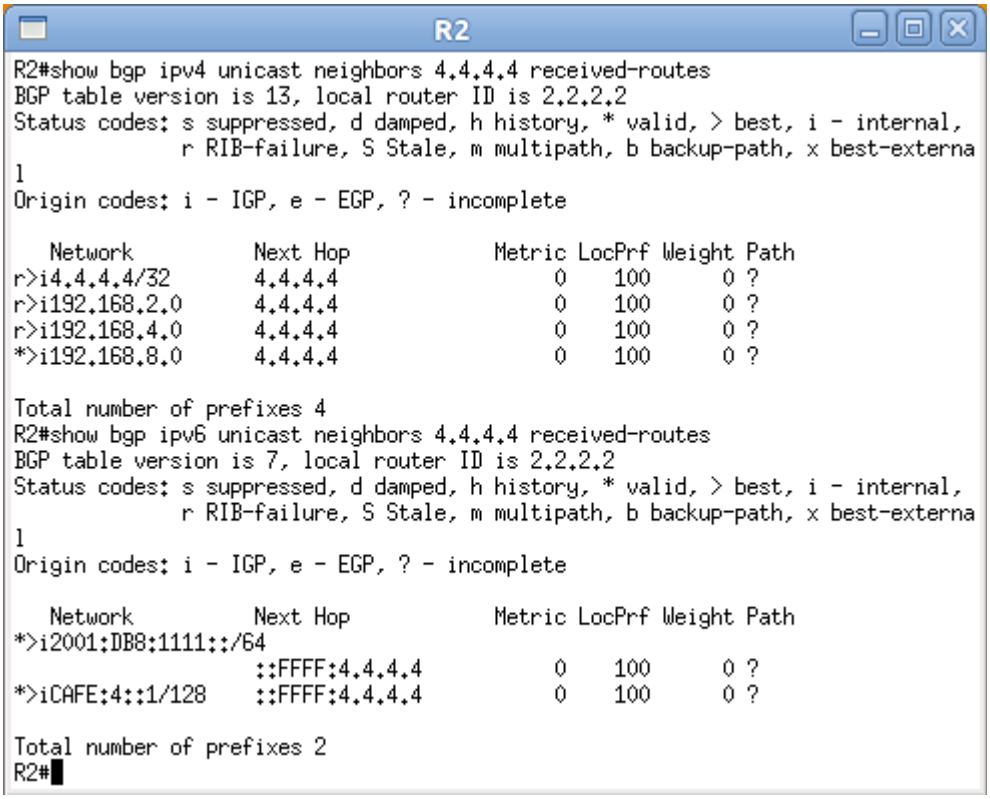


Figura 8.33: rutas ipv4/ipv6 que recibió R2 de R4

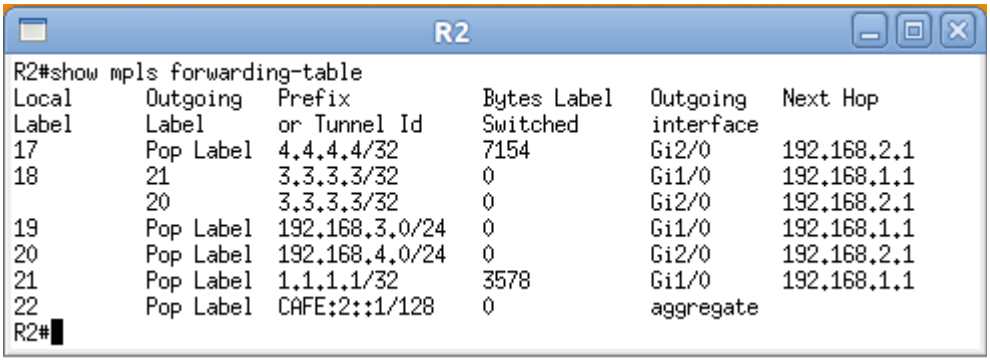


Figura 8.34: tabla de forwarding mpls en R2

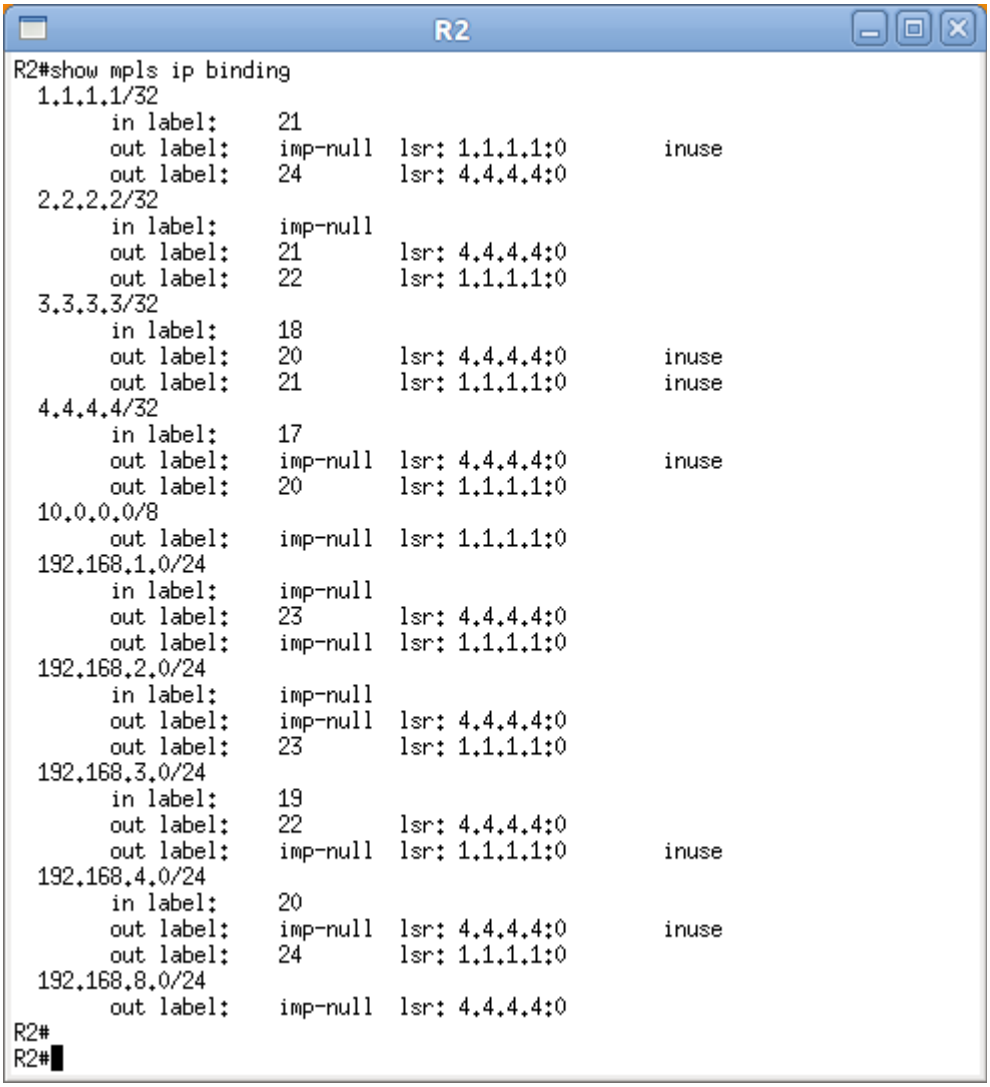


Figura 8.35: mpls ip binding en R2

A modo de resumen, vemos la Tabla 3. Esta nos indica que tabla de encaminamiento ver dependiendo de cada paquete :

Tipo de Paquete	**Tabla para busqueda del paquete**	**Comando para ver esta tabla**
IP to IP	FIB	Show ip cef
IP to MPLS	FIB	Show ip cef
MPLS to MPLS	LFIB	Show mpls forwarding-table
MPLS to ip	LFIB	Show mpls forwarding-table

Tabla 3: tabla de encaminamiento a utilizarse dependiendo del paquete

8.8 Conclusiones finales

En base a la investigación realizada, las pruebas y experimentos en laboratorio, podemos afirmar que es posible incorporar encaminamiento IPv6 en un backbone MPLS IPv4, haciendo algunos ajustes de configuración en los routers (siempre y cuando se disponga del hardware compatible para tal fin) implementando el protocolo 6PE (RFC-4798 anexo 22).

Esta solución resulta útil para delegar prefijos IPv6 a clientes aprovechando de esta manera el bloque disponible, sin necesidad de tener que migrar toda la infraestructura actual del núcleo a IPv6 (opción no soportada dado que no se dispone de un protocolo de distribución de etiquetas en MPLS compatible con IPv6) puede verse en la actualización del RFC-5036 que se publicó el 13 de Octubre de 2010, que se encuentra en el anexo 28 (con el nombre *Updates to LDP for IPv6 draftmanral-mpls-ldp-ipv6-04*).

Vimos diferentes alternativas de conectar clientes, con VRF y con VLAN, resultando ambas soluciones aptas para la problemática planteada. En nuestro caso práctico, optamos por las dos opciones:

- Un gateway con VLAN (el router 6 en la topología presentada), de forma tal de no cortar la conectividad IPv4 y agregar conectividad IPv6 en el mismo enlace físico, (solución temporal dado que se debe mantener el enlace físico con IPv4 hasta que se opte por tener todo en IPv6) dividiendo en subinterfaces la conexión R1-R6, y conectando un cliente al backbone de forma estática.

- Un gateway con VRF (el router 5 en la topología presentada) habilitando IPv4 e IPv6 conjuntamente; y un cliente conectado al backbone en la misma VRF, de esta forma podemos ver las 2 opciones disponibles.

Tanto para VRF como para VLAN, se estableció la adyacencia en el protocolo BGP para el encaminamiento entre diferentes sistemas autónomos; resultando el protocolo BGP de gran utilidad para todo el trabajo realizado.

Una ventaja de usar VLAN es que se puede dividir la interfaz en sub-interfaces, y de esta forma conectarse a diferentes sistemas autónomos, diferentes routers, y/o diferentes sub-interfaces del dispositivo de red análogo.
Como desventaja trivial, sabemos que el ancho de banda que el medio físico nos otorga, es compartido por las n sub-interfaces que definimos en la VLAN (o interfaz física), teniendo la opción por software de asignar el ancho de banda necesario a cada sub-interfaz (con el comando bandwidth en cisco).

Una ventaja de VRF es que tendremos tablas separadas de encaminamiento por cada VRF, y de menor tamaño que una global, ademas de la simplicidad que presenta su creación e inclusión dentro de BGP.

Una desventaja que presenta VRF, es que una interfaz física solo puede estar asociada a una VRF a la vez, limitándonos de esta manera en el número de VRF que podemos tener en un router (tendremos una cantidad máxima de VRF igual a la cantidad de interfaces que posee el dispositivo).

Concluimos de esta forma presentando la solución propuesta y con diferentes opciones según las necesidades o preferencias del organismo en cuestión.

Referencias

[1] Wikipedia (http://es.wikipedia.org/wiki/IPv6)
[2] Number Resource Organization (http://www.nro.net/wp-content/uploads/NRO_Q4_2012.final_.pdf)
[3] Información al 18/04/2013 LACNIC (http://www.lacnic.net/web/lacnic/reporte-direcciones-ipv4)
[4] Agotamiento de IPv4 APNIC (http://www.apnic.net/community/ipv4-exhaustion)
[5] The IPv6 mess (http://cr.yp.to/djbdns/ipv6mess.html)
[6] Wikipedia (http://es.wikipedia.org/wiki/ICMPv6)
[7] Wikipedia (http://es.wikipedia.org/wiki/Backbone)
[8] Wikipedia (http://es.wikipedia.org/wiki/Cisco_IOS)
[9] Sitio Oficial de GNS3 (http://www.gns3.net/)
[10] IOS de Cisco: http://www.cisco.com/cisco/software/navigator.html?mdfid=283887759&i=rm
[11] IANA - Internet Assigned Numbers Authority (http://www.iana.org/)
[12] Wikipedia (http://es.wikipedia.org/wiki/Open_Shortest_Path_First)
[13] Wikipedia (http://es.wikipedia.org/wiki/Border_Gateway_Protocol)
[14] Cisco (cisco.com/en/US/docs/net_mgmt/active_network_abstraction/3.7/reference/guide/vrf.html)
[15] Wikipedia (http://es.wikipedia.org/wiki/Multiprotocol_Label_Switching)
[16] www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_data_sheet09186a008052edd3.html

Anexos

1. RFC 791 Internet Protocol ; September 1981
2. RFC 1550 IPng White Paper Solicitation December 1993
3. RFC 2071 Network Renumbering Overview January 1997
4. RFC 2072 router Renumbering Guide January 1997
5. RFC 2328 OSPF Version 2 April 1998c
6. RFC 2460 IPv6 Specification December 1998
7. RFC 2711 IPv6 router Alert Option October 1999
8. RFC 2766 NAT-PT February 2000
9. RFC 2767 Dual Stack Hosts using BIS February 2000
10.RFC 3031 MPLS Architecture January 2001
11.RFC 3089 SOCKS-based IPv6/IPv4 Gateway Mechanism April 2001
12.RFC 3142 IPv6-to-IPv4 Transport Relay Translator June 2001
13.RFC 3306 Unicast-Prefix-based IPv6 Multicast August 2002
14.RFC 3363 Representation of IPv6 Addresses in DNS August 2002
15.RFC 3364 Tradeoffs in DNS Support for IPv6 August 2002
16.RFC 3338 Dual Stack Hosts Using BIA October 2002
17.RFC 3513 IPv6 Addressing Architecture April 2003
18.RFC 3810 MLDv2 for IPv6 June 2004
19.RFC 3963 NEMO Basic Support Protocol January 2005
20.RFC 4213 Basic IPv6 Transition Mechanisms October 2005
21.RFC 4443 ICMPv6 (ICMP for IPv6) March 2006
22.RFC 4798 6PE February 2007
23.RFC 4861 Neighbor Discovery in IPv6 September 2007
24.RFC 5036 LDP Specification October 2007
25.RFC 5340 OSPF for IPv6 July 2008
26.IPv6 over MPLS (Cisco 6PE) (IPv6 over MPLS (Cisco 6PE).pdf)
27. Cisco 7609 manual (7609.pdf)
28. Updates to LDP for Ipv6 draft-manral-mpls-ldp-ipv6-04
29. Virtual Routing and Forwarding (VRF.pdf)
30.RFC 4364 BGP/MPLS IP VPNs February 2006
31.RFC 4893 BGP Support for Four-octet AS Number Space May 2007