TECNOLOGÍA MULTICAST: FUNDAMENTOS, ENRUTAMIENTO Y SIMULACIÓN EN ENTORNOS REALES

MARILYN RAMOS HERNÁNDEZ
ANDREA PAOLA SÁNCHEZ PÉREZ

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS FÍSICO-MECÁNICAS
ESCUELA DE INGENIERÍA ELÉCTRICA ELECTRÓNICA Y DE TELECOMUNICACIONES
BUCARAMANGA
2010

TECNOLOGÍA MULTICAST: FUNDAMENTOS, ENRUTAMIENTO Y SIMULACIÓN EN ENTORNOS REALES.

MARILYN RAMOS HERNÁNDEZ
ANDREA PAOLA SÁNCHEZ PÉREZ

Monografía para optar al título de
Especialista en Telecomunicaciones

Director
Ing. RAÚL BAREÑO GUTIERREZ
Ingeniero de Sistemas

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS FÍSICO-MECÁNICAS
ESCUELA DE INGENIERÍA ELÉCTRICA ELECTRÓNICA Y DE TELECOMUNICACIONES
BUCARAMANGA
2010

DEDICATORIA

A Dios, por ofrecerme cada día la oportunidad de alcanzar mis sueños.

A Nati, la luz que ilumina mi vida.

A Javier, por su amor y apoyo incondicional.

A mi madre por su apoyo y motivación constante.

ANDREA PAOLA

A Dios y a la Virgen, por guiarme y darme fortaleza para seguir adelante con mis propósitos.

A mi familia, por enseñarme a ser fuerte y a enfrentar cada obstáculo.

A Luis Fernando por su paciencia y comprensión en esta etapa de mi vida.

MARILYN

AGRADECIMIENTOS

Las autoras expresan sus agradecimientos a:

La **UNIVERSIDAD INDUSTRIAL DE SANTANDER**, por ser una entidad forjadora de nuestro saber y por apoyar nuestro proceso de formación personal y profesional.

El ingeniero **RAÚL BAREÑO GUTIERREZ**, por su orientación y colaboración como director de esta monografía.

Todos nuestros profesores, quienes nos compartieron sus conocimientos y experiencias profesionales y nos impulsan a seguir adelante en nuestro camino.

Elbert, Hector, Manuel E. y Manuel A., excelentes compañeros e invaluables amigos, quienes nos acompañaron en esta etapa de nuestra vida y compartieron con nosotras experiencias inolvidables.

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE ANEXOS

RESUMEN

TÍTULO: TECNOLOGÍA MULTICAST: FUNDAMENTOS, ENRUTAMIENTO Y SIMULACIÓN EN ENTORNOS REALES[*]

AUTORAS: MARILYN RAMOS HERNÁNDEZ
ANDREA PAOLA SÁNCHEZ PÉREZ [**]

PALABRAS CLAVES: Multicast, Enrutamiento, OSPF, EIGRP, PIM, PIM-DM, PIM-SM

DESCRIPCIÓN

La continua evolución en las redes de comunicación, ha generado un incremento tanto en los volúmenes de información que viajan a través de la red como en el número de usuarios de ésta. Como consecuencia se obtiene un aumento significativo en el tráfico de red, lo cual demanda el desarrollo de técnicas que permitan un uso eficiente de recursos que garanticen el buen funcionamiento de la red.

IP Multicast es una tecnología que promueve la disminución de tráfico en la red permitiendo el envío simultáneo de información a múltiples destinos (interesados en recibir el tráfico). Multicast se basa en el concepto de grupo multicast, el cual está formado por usuarios (receptores) interesados en recibir el tráfico de la red. El protocolo IGMP es el encargado de gestionar la suscripción de usuarios al grupo multicast. Para determinar la mejor ruta hacia los receptores, se han definido protocolos y algoritmos de enrutamiento muticast. Entre los algoritmos de enrutamiento multicast se destacan: inundación, spanning tree y las variaciones de spanning tree: RPB, TRPB y RPB.

Los protocolos de enrutamiento EIGRP y OSPF proporcionan mecanismos para elaborar y mantener tablas de enrutamiento de los routers en la red y para determinar la mejor ruta para llegar a un destino. Los protocolos de enrutamiento multicast PIM-DM y PIM-SM usan esas tablas de enrutamiento para obtener información de las rutas para el envío de información a grupos multicast.

En este documento se hace una revisión de los fundamentos de IP multicast donde se mencionan conceptos básicos así como los algoritmos y protocolos de enrutamiento utilizados en este tipo de difusión, adicionalmente se desarrollan algunas prácticas en los software simuladores de redes Packet Tracer y GNS3, donde se realiza la configuración de protocolos de enrutamiento, prestando especial atención a los protocolos de enrutamiento EIGRP, OSPF y PIM.

[*] Monografía.

[**] Facultad de Ingenierías Físico-Mecánicas. Escuela de Ingeniería Eléctrica, Electrónica y Telecomunicaciones. Director: Ing.Rául Bareño Gutiérrez.

ABSTRACT

TITLE: MULTICAST TECHNOLOGY: FUNDAMENTALS, ROUTING AND SIMULATION IN REAL ENVIRONMENTS*

AUTORS: MARILYN RAMOS HERNÁNDEZ
ANDREA PAOLA SÁNCHEZ PÉREZ **

KEY WORDS: Multicast, Routing, OSPF, EIGRP, PIM, DM, PIM-SM

DESCRIPTION

The continuing evolution in communications networks, due to advances in Information and Communications Technology (ICT), has caused an increase in the volumes of information traveling through the network and the number of users of it. As a result, a significant increase in network traffic is derived, which requires the development of techniques for efficient use of resources to ensure efficient performance of the network.

IP Multicast is a technology that promotes the reduction of network traffic as it allows the simultaneous transmission of information to multiple destinations (interested in receiving traffic). Typical multicast applications include video conference, e-learning and data distribution. Multicast is based on the concept of multicast group, which consists of users (receivers) interested in receiving the network traffic. The IGMP (Internet Group Management Protocol) protocol is responsible for managing users' subscription to the multicast group. To determine the best route to the receivers, some protocols and routing algorithms muticast have been defined. Some of the multicast routing algorithms are: flooding, spanning tree and the spanning tree modifications: RPB and RPB TRPB.

EIGRP (Enhanced Interior Gateway Routing Protocol) and OSPF (Open Shortest Path First) routing protocols provide mechanisms to develop and maintain routing tables of routers in the network and to determine the best route to a destination. Multicast routing protocols PIM-DM and PIM-SM use these routing tables for route information to send information to multicast groups.

In this paper we review the IP multicast fundamentals, where basic concepts are mentioned as well as routing algorithms and protocols used in this type of delivery, additionally there were developed some practices in network simulator software (Packet Tracer and GNS3) where the configuration of routing protocols, with particular attention to routing protocols EIGRP, OSPF and PIM were performed.

* Monograph.

** Physique-Mechanics Enginnering Department, Specialization in Telecommunications. Director: Eng. Rául Bareño Gutiérrez.

INTRODUCCIÓN

El constante avance en tecnologías de la información y la comunicación ha provocado cambios en las redes de comunicaciones, produciendo un incremento tanto en los volúmenes de información (voz, datos y video) que se transmiten, como en el número de destinatarios de esta información.

Este crecimiento del tráfico en redes exige el desarrollo de técnicas que permitan un consumo de menor cantidad de recursos, aumentando la velocidad, capacidad, rendimiento y tasa de envío de paquetes. Las aplicaciones modernas y servicios de comunicaciones exigen funcionalidades mayores y más versátiles en las redes, y los usuarios día a día son más exigentes en cuanto a servicios de comunicación interactiva.

Las tecnologías basadas en multicast ofrecen una opción viable para la difusión masiva, ya que promueven la disminución del tráfico en la red en la medida que permiten el envío de la información a múltiples destinos simultáneamente (realizando la transmisión una sola vez), de esta forma se reduce sustancialmente el consumo de recursos de ancho de banda y se emplea un menor tiempo para hacer llegar los contenidos a todas las ubicaciones.

En este documento se hace una revisión de los fundamentos de IP multicast donde se mencionan conceptos básicos así como los algoritmos y protocolos de enrutamiento utilizados en este tipo de difusión, adicionalmente se desarrollan algunas prácticas en los software simuladores de redes Packet Tracer y GNS3 donde se realiza la configuración de protocolos de enrutamiento, prestando especial atención a los protocolos de enrutamiento EIGRP y OSPF y al protocolo de enrutamiento multicast PIM.

El primer capítulo contiene una descripción general de la tecnología multicast, donde se presenta su filosofía de transmisión, algunas de sus aplicaciones, ventajas y desventajas de su aplicación en redes de comunicación. Adicionalmente se esboza el direccionamiento multicast y se describe el protocolo de administración de grupos multicast IGMP. Finalmente se mencionan algunos algoritmos de enrutamiento que han sido desarrollados para la transmisión de información a grupos multicast.

El capítulo dos presenta una introducción a los protocolos de enrutamiento y su clasificación. Se profundiza específicamente en los protocolos EIGRP (*Enhanced Interior Gateway Protocol)* y OSPF (*Open Shortest Path First*), en cuanto a sus características, modo de operación y configuración básica.

El capítulo tres presenta una introducción a los protocolos de enrutamiento multicast y su clasificación, prestando especial atención al Protocolo Independiente Multicast (PIM) en sus dos modos de operación: modo denso (Dense Mode - DM) y modo esparcido (Sparse Mode - SM).

El capítulo cuatro contiene una descripción general y un breve tutorial sobre el manejo de los dos simuladores de redes Packet Tracer y GNS3, utilizados para realizar las prácticas de simulación.

El capítulo cinco contiene las prácticas realizadas en los simuladores de redes mencionados anteriormente, presentadas paso a paso. Específicamente se trabajaron los protocolos OSPF, EIGRP, PIM-DM, PIM-SM y un híbrido de estos dos últimos denominado PIM-DSM.

Finalmente, se presenta un glosario que incluye algunos de los términos más usados en el ambiente de enrutamiento y multicast.

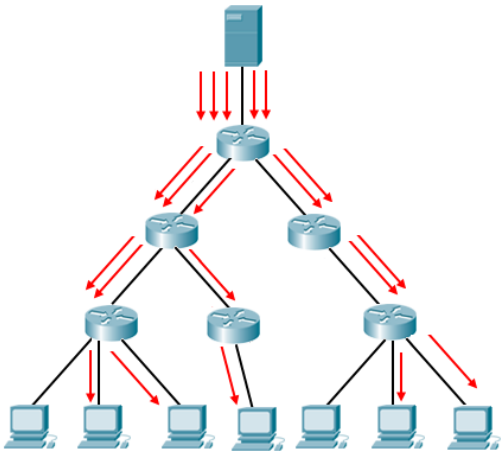
1. CONCEPTOS Y PRINCIPIOS BÁSICOS DE LA TECNOLOGÍA IP MULTICAST

1.1. GENERALIDADES DE IP MULTICAST

El envío de información sobre una red se puede realizar utilizando tres métodos básicos: unicast, broadcast y multicast.

En el primero de los casos, el método de transmisión es uno a uno (one-to-one), aquí el envío de datos se realiza desde un único emisor a un único receptor. En un entorno unicast donde varios usuarios soliciten la misma información al servidor, el servidor responderá a las peticiones de los usuarios enviando la misma información (duplicada) a cada usuario, (como se muestra en la figura 1), provocando a su vez la inundación "*flooding"* de la red por la cantidad de tráfico.

Figura 1. Transmisión Unicast



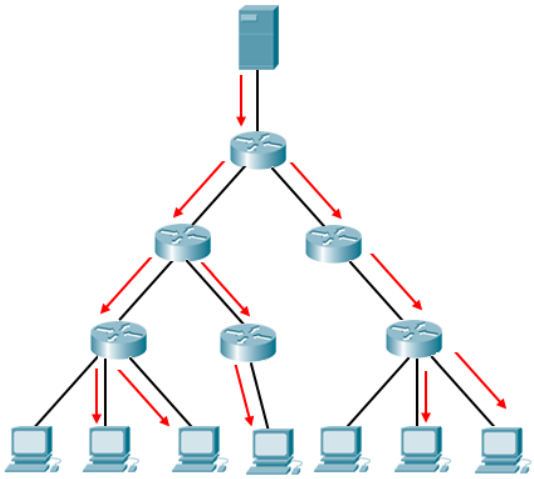
Fuente: Autoras.

El método Broadcast es un método de transmisión de uno-a-todos, en donde se envían los datos a todos los dispositivos al mismo tiempo, sin embargo se genera una sobrecarga debido a que los paquetes se envían

por toda la red sin tener en cuenta a los usuarios que realmente lo requieren. Esto produce carga innecesaria en los vínculos y proceso adicional en los routers y hosts.

El tercer método, denominado multicast, es un método de transmisión de uno-a-muchos que realiza el envío de los datos a múltiples destinos simultáneamente, este método de transmisión es similar al broadcast, excepto que el multicast solo envía la información a un grupo específico y el broadcast envía la información a todos los nodos de la red.

Figura 2. Transmisión Multicast



Fuente: Autoras.

El término IP multicast o multidifusión hace referencia a una tecnología de conservación de ancho de banda que reduce el tráfico en la red, entregando simultáneamente un *único* flujo de información a múltiples receptores. Esta tecnología que se originó a comienzos de la década de los noventa, está tomando importancia en la actualidad debido al incremento de volúmenes de información que se transmiten en la red; aplicaciones como videoconferencia, comunicaciones corporativas, aprendizaje a distancia, distribución de software, actualización de bases

de datos y juegos distribuidos han sido algunos de los objetos de estudio de la utilización de multicast.

El uso de envíos multicast favorece la disminución del tráfico en la red, ya que los datagramas que comparten un grupo de enlaces hasta sus destinos sólo requieren ser transmitidos una vez y sólo se replica el mensaje cuando es necesario. Los paquetes multicast son replicados en los routers habilitados con Protocolo Independiente Multicast (PIM) y otros protocolos multicast de soporte que permiten realizar más eficientemente la entrega de datos a múltiples receptores, de esta forma, la responsabilidad de la duplicación de paquetes recae en los routers (para hacer llegar una copia a cada miembro del grupo), de modo que estos aseguren que los paquetes viajarán una vez por cada enlace como máximo (basta con asegurar que todos los miembros reciben una copia del paquete).

A continuación se explica brevemente el proceso para la realización de multicast en una red:

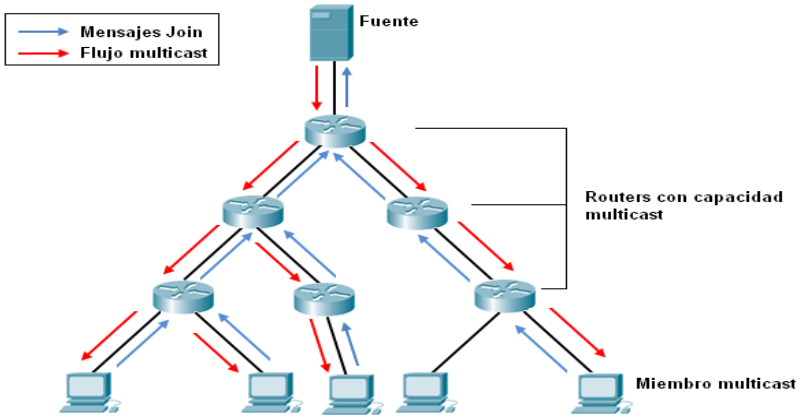
Una fuente se encarga de proveer los flujos de datos para su distribución a los receptores finales. Estos receptores finales que se unen al árbol de distribución se denominan miembros multicast. En la siguiente figura se identifican cinco receptores finales, de los cuales sólo cuatro son miembros multicast.

Cuando un posible miembro multicast desea unirse al árbol de distribución, envía un mensaje *join* (de unión) al router designado de la subred junto con la dirección IP del grupo multicast al cual desea unirse (flechas azules inferiores).

Cuando el mensaje *join* llega al router designado (routers inferiores en la figura) éste busca una correspondencia entre el grupo multicast al que desea unirse el miembro potencial y la dirección IP de alguna fuente que

esté sirviendo al grupo. Si la encuentra, traduce el mensaje *join* del miembro en un mensaje *join* del protocolo de enrutamiento multicast.

Figura 3. Esquema de transmisión multicast



Fuente: Autoras.

Cuando el mensaje *Join* llega a la fuente, ésta comienza a enviar los datos al grupo multicast. Los paquetes IP del flujo multicast que alcanzan cada *router* son inspeccionados por éste, que comprueba la dirección IP de destino. Si es una dirección IP multicast, comprueba si alguna de sus interfaces de salida pertenece a una rama del árbol. Si es así, reenvía una copia del paquete por cada interfaz de salida que pertenezca a una rama (flechas rojas), creándose flujos de datos multicast.

Si no hay coincidencia en las tablas de grupos multicast del *router*, se descarta el paquete multicast. En todo momento y por cada enlace de la red circula como máximo una copia del flujo de datos.

1.2. VENTAJAS Y DESVENTAJAS DE LA APLICACIÓN DE IP MULTICAST EN REDES DE COMUNICACIÓN

El uso de soluciones multicast en redes de internet conlleva beneficios significativos tales como:

- Desempeño optimizado de la red: el uso inteligente de los recursos de red evita duplicaciones innecesarias de flujos de datos. Por un lado, se logra un ahorro en consumo de ancho de banda mediante una estructura mejorada de distribución de datos, por otro lado, se reduce la capacidad de procesamiento consumida en los servidores y equipos de red, aumentando de esta forma la disponibilidad de red y reduciendo los cuellos de botella. Además esta descarga de recursos de red implica una reducción de retardo, lo que conlleva a una mejor calidad de servicio (QoS).

- Soporte a aplicaciones de difusión: la tecnología multicast está orientada a aplicaciones de difusión. Aplicaciones multimedia como educación a distancia, videoconferencia, distribución de video y voz, se pueden usar de forma notablemente eficaz.

- Escalabilidad: el uso eficiente de la red y la reducción de carga en las fuentes de tráfico permite que los servicios y aplicaciones puedan ser accedidos por un mayor número de usuarios. De esta forma, los servicios distribuidos mediante multicast se pueden dimensionar más fácilmente.

Aunque hay un gran número de razones para utilizar IP multicast en redes, se debe reconocer que hay ciertas limitaciones y desventajas de esta tecnología, entre las que se incluyen entrega de paquetes no fiable, duplicación de paquetes y congestión de la red.

- IP multicast, como IP unicast, son inherentemente no confialbles. Sólo con el uso de TCP (en capa 4) los datagramas IP unicast se envían de forma confiable. Sin embargo, debido a que IP multicast asume un modo de comunicación uno-a-muchos no fue diseñado para usar mecanismos inherentes en TCP; los paquetes IP multicast generalmente usan el protocolo UDP (*User Datagram Protocol)* el cual usa el mejor esfuerzo; por lo tanto, en una aplicación que utilice IP multicast se pueden presentar pérdidas ocasionales de paquetes. Según el Dr. Stever Deering[1] "…durante periodos cuando los caminos están siendo actualizados inmediatamente después de un cambio de topología los paquetes multicast tienen una menor probabilidad de alcanzar los destinos que los paquetes unicast., debido a que los mecanismos de envío de IP multicast están basados en la dirección IP de la fuente y para prevenir ciclos el paquete se descarta si no llega a la interfaz que lo regresaría a la fuente."

- En IP multicast puede existir duplicación de paquetes ya que los routers envían intencionalmente copias de paquetes multicast a las interfaces. Esto incrementa la probabilidad de que a un mismo receptor lleguen múltiples copias del paquete. Por ejemplo, en algunas topologías de red redundantes en las cuales existen múltiples caminos para el receptor pueden ocurrir duplicación de paquetes hasta que el protocolo de enrutamiento multicast converja y elimine la ruta redundante. Esto significa que solo se duplicarán paquetes ocasionalmente dentro de la red.

- El protocolo TCP cuenta con un mecanismo de "escalado de ventana" que permite ajustar automáticamente la velocidad de transferencia de datos y de esta forma trata de evitar en cierto grado la congestión en la red; como IP multicast no puede usar TCP, no puede hacer uso de esta función para prevenir la congestión. Sin embargo, cabe aclarar que las transmisiones unicast sobre UDP tienen este mismo problema,

[1] Co-autor investigador de IP multicast.

y gracias al aumento de popularidad de aplicaciones multimedia de audio y video en internet se ha venido incrementando la cantidad de tráfico unicast UDP.

1.3. APLICACIONES DE IP MULTICAST

IP multicast es usado cuando se realiza un envío simultáneo a un grupo de receptores. Existen varios tipos de aplicaciones multicast. Dos de los modelos más comunes son uno-a-muchos y muchos-a-muchos.

En aplicaciones uno-a-muchos, un emisor envía datos a muchos (dos o más) receptores. Este tipo de aplicación puede ser usada para distribución de audio o video, video conferencia, etc. Si una aplicación uno-a-muchos requiere alguna respuesta por parte de los receptores, se convierte en una aplicación muchos-a-muchos.

En las aplicaciones muchos-a-muchos cualquier número de hosts realizan envíos al mismo grupo multicast. Dos o más receptores actúan también como emisores y un host puede enviar y recibir al mismo tiempo. El hecho de recibir datos de muchas fuentes puede incrementar la complejidad de las aplicaciones.

A menudo cuando se habla de IP multicast se relaciona directamente con videoconferencia; sin embargo esta es solo una de las aplicaciones que se podrían mencionar.

- Streaming IP: se trata de una retransmisión tipo “Broadcast” (para todos los terminales conectados) o Multicast mediante protocolo IP, que goza de un determinado caudal asegurado durante un determinado tiempo. Por ello este tipo de aplicación es ideal para transmisión de video y/o de audio donde se requiere una calidad de servicio, para que no se produzcan cortes en la señal.

- Sistemas de Distribución de Contenidos: consiste en el envío de una gran cantidad de información, como pueden ser ficheros, programas, películas, etc. a usuarios determinados. En este caso no se exige un caudal determinado sino que lleguen los datos a tiempo según las necesidades del cliente. Un servicio de gran valor agregado es el envío de actualizaciones de software y su ejecución en acceso remoto o la actualización de antivirus.
- Tele-enseñanza: básicamente la aplicación consiste en emitir un streaming IP con la señal de video y audio del profesor con la calidad requerida por el usuario. Los alumnos visualizarán y escucharán al profesor en su computador o en páneles especiales para ello. La interactividad se logra mediante la implementación de un canal de retorno que puede ser vía terrestre (RTC, RDSI, etc.) o satelital.
- Distribución de canales de televisión en implementaciones IPTV: dentro de las ofertas de servicios triple play de los operadores de red, como cada canal supone un flujo de video similar para todos los abonados que lo estén viendo en un momento dado, la entrega mediante multicast libera significativamente la carga tanto en el núcleo de la red y la sección de distribución como en el borde y a zona de acceso. La distribución multicast genera un "árbol" cuyas ramas se van dividiendo a medida que el flujo atraviesa la red, llegando estas divisiones hasta cada usuario final. De este modo la capacidad consumida en la red, sobre todo en el núcleo, es mucho menor que la capacidad agregada existente cuando el número de usuarios que ven el canal es significativo.
- Otra aplicación importante para justificar el despliegue y soporte de protocolos multicast en los routers de Internet es la retrasmisión a nivel mundial de eventos en directo o en diferido. Acontecimientos como eventos deportivos de interés

general podrían ser difundidos a todos los usuarios con una calidad aceptabe incluso si el número de usuarios se eleva a millones. El motivo es que las partes críticas en la distribución como los backbones internacionales y núcleos de red de los operadores en cada región se verían altamente aliviados de carga, con lo que la disponibilidad de recursos y eficiencia en la distribución se verían altamente mejoradas.

Dos aplicaciones específicas que emplean multicast de red son Conference XP y Mcast6. [2]

Conference XP

Es una plataforma de investigación de código compartido de *Microsoft Research*. Constituye una plataforma para realizar conferencias y trabajos colaborativos que aprovecha las redes de banda ancha y lo entornos inalámbricos. El proyecto da soporte a los investigadores y educadores que deseen implementar aplicaciones para colaboración online en tiempo real y entornos de aprendizaje distribuidos. Conference XP provee la infraestructura que da soporte a estas aplicaciones. Hay tres tipos de escenarios principales: aplicaciones de investigación colaborativa, entornos de aprendizaje distribuidos de alta interactividad y aulas habilitadas para aplicaciones inalámbricas.

En el ambiente multicast resultan interesantes los dos primeros tipos de aplicaciones. Las sesiones colaborativas para investigación usan el cliente de Conference XP, que cuenta con un soporte nativo para multiconferencias de alta calidad sobre redes de banda ancha con capacidad de realizar multicast. Las multiconferencias usan

[2] CACHINERO POZUELO, Juan Angel. Análisis y modelado de “multicast” interdominio para el soporte de servicios de video. Madrid, 2009, 268 p. Trabajo de grado (Ingeniero de Telecomunicación), Universidad Politécnica de Madrid. Escuela superior de ingenieros de telecomunicación.

flujos de video con una resolución de 640x480 puntos y 30 cuadros por segundo, enriquecidas mediante otras aplicaciones colaborativas como chat, presentaciones y ficheros de video compartidos.

MCast6

La aplicación MCast6 está formada por dos componentes principales. Los clientes (reproductores) y los servidores. El cliente es el encargado de la recepción de los flujos multimedia (audio y video) tanto en *unicast* como multicast. El servidor trabaja en un modo interactivo a través de una interfaz basada en web y mantiene un registro con la información de los recursos multimedia disponibles que están accesibles desde su ubicación, enviándolos de acuerdo a las directrices del administrador del sistema o de acuerdo a las peticiones de los clientes finales. Esto último puede considerarse transmisión bajo demanda. La aplicación puede trabajar con IPv4 e IPv6 y en varios sistemas operativos.

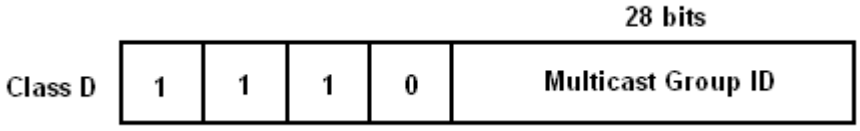
1.4. DIRECCIONAMIENTO MULTICAST

Cuando un origen envía tráfico multicast, la dirección de destino es una dirección del grupo multicast; esta dirección le permite a un dispositivo de origen enviar un paquete a un grupo de dispositivos. Una dirección IP de grupo multicast se asigna a los dispositivos que pertenecen a un grupo multicast.

Para cada dirección multicast puede existir cero o más destinatarios activos, que recibirán una copia del datagrama enviado a dicha dirección. El grupo multicast está formado por los miembros activos, y se mantiene de forma dinámica mediante conexiones y desconexiones de los mismos (orientado al receptor).

Las direcciones de multidifusión IP se reservan y asignan a partir del intervalo de direcciones de la clase D, que va de 224.0.0.0 a 239.255.255.255. Los cuatro bits más significativos de las direcciones de Clase D se fijan a "1110", y los siguientes números de 28- bit reciben la denominación de identificador del grupo multicast, no estando, por lo tanto estructuradas las direcciones como las direcciones IP unicast. Su formato se indica en la figura siguiente:

Figura 4. Dirección IP de clase D



Fuente: http://www.cisco.com/networkers/nw00/pres/2214.pdf.

Debido a que las direcciones multicast representan un grupo de direcciones (a veces denominado un grupo de hosts), sólo pueden utilizarse como el destino de un paquete. El origen siempre tendrá una dirección unicast.

Existen dos tipos de grupos multicast: temporales y permanentes:

- Un grupo temporal se crea dinámicamente (en el momento que se lanza una aplicación multidifusión), y dejará de existir cuando deje de tener miembros activos.

- Un grupo permanente tiene asociada una dirección IP multicast fija, independiente del número de miembros que tenga el grupo. Algunos grupos permanentes han sido predefinidos por la IANA (Internet Assigned Numbers Authority) en el RFC1700 para propósitos especiales. Por ejemplo, la dirección 224.0.0.0 está reservada y el rango de direcciones desde 224.0.0.1 a 224.0.0.255

está reservado para el uso de protocolos de enrutamiento y otros protocolos de descubrimiento y mantenimiento de topologías de bajo nivel.

En la siguiente tabla se incluye una lista parcial de direcciones de la clase D reconocidas que están reservadas para multidifusión IP:

Tabla 1. Algunas direcciones multicast reservadas

Dirección	Descripción
224.0.0.0	Dirección de base (reservada).
224.0.0.1	Grupo de multidifusión Hosts con soporte multicast.
224.0.0.2	Grupo de multidifusión Routers con soporte multicast.
224.0.0.4	Grupo de multidifusión Routers DVMRP (enrutamiento multicast)
224.0.0.5	Dirección AllSPFRouters. Routers OSPF (OSPF, Open Shortest Path First). Se utiliza para enviar información de enrutamiento OSPF a todos los routers OSPF de un segmento de red.
224.0.0.6	La dirección AllDRouters de OSPF. Routers OSPF designados. Se utiliza para enviar información de enrutamiento OSPF a los routers OSPF designados en un segmento de red.
224.0.0.9	La dirección de grupo de la versión 2 de RIP. Se utiliza para enviar información de enrutamiento RIP a todos los routers RIP v2 en un segmento de red.

Fuente: http://www.worldlingo.com/ma/enwiki/es/Multicast_address

El resto de los grupos que van desde 224.0.1.0 a 239.255.255.255 están asignados a diversas aplicaciones multicast o permanecen sin ser asignadas. De este rango, las direcciones que van de 239.0.0.0 a 239.255.255.255 están reservadas para ser utilizadas para aplicaciones locales no extensibles a Internet.

En la página web de la IANA[3] se encuentra el listado completo y actualizado de las asignaciones de direcciones multicast realizado por la IANA.

1.5. IGMP (INTERNET GROUP MANAGEMENT PROTOCOL)

En una transmisión multicast, cuando un receptor está interesado en recibir datos de una fuente se debe suscribir en su router multicast local para que éste le haga llegar los paquetes en los que esta interesado. La fuente emitirá los paquetes dirigidos a una dirección multicast, esta dirección recibe el nombre de grupo multicast. Para que el receptor y el router multicast se puedan comunicar la información sobre las suscripciones se creó el protocolo IGMP.

IGMP es el protocolo de administración del grupo Internet, el cual establece un mecanismo para el intercambio y actualización de información sobre la pertenencia de los equipos o nodos de un segmento a un grupo multicast.

Los nodos que desean recibir datagramas multicast deben informar a los routers vecinos que están interesados en recibir datagramas dirigidos a ciertos grupos multicast. De este modo, cada nodo se convierte en miembro de uno o más grupos multicast y recibe los datagramas dirigidos a dicho grupo.

[3] http://www.iana.org/assignments/multicast-addresses/multicast-addresses.xml

Todos los mensajes IGMP se envían con un valor de TTL igual a 1, por lo que los mensajes IGMP solo pueden ser intercambiados entre equipos directamente conectados entre sí (normalmente entre hosts y routers conectados en una misma LAN).

IGMP ha evolucionado a través de tres versiones que serán revisadas a continuación. (Actualmente los más extendidos son IGMP v2 y v3)

1.5.1. IGMP versión 1

El protocolo IGMPv1 fue definido en el apéndice I del RFC 1112 (*Host Extensions for IP Multicasting*). Con la versión 1 de IGMP los routers envían consultas de miembros periódicamente a la dirección 224.0.0.1. Después, los hosts envían reportes de las direcciones multicast a las cuales desean unirse. Una desventaja de esta versión es que los hosts abandonan silenciosamente el grupo multicast sin notificar que ya no desean recibir el tráfico.

IGMPv1 implementa dos tipos de mensajes:

- *Membership Query:* Consulta de miembros. Son mensajes emitidos por los routers y enviados a la dirección multicast 224.0.0.1 (todos los hosts multicast de la red). Su objetivo es preguntar a los hosts en que grupos multicast están interesados.

- *Membership Report:* Informe de pertenencia. los hosts responden a un *Membership Query* con un mensaje *Membership Report*, en el cual informan a los routers de los grupos en los que están interesados. Este mensaje es enviado a la dirección multicast en la que está interesado el host. Los routers capturan absolutamente todo el tráfico multicast que pasa por sus interfaces, por lo que captarán el mensaje ‘Membership Report’ y podrán por tanto tomar nota del grupo multicast en que está interesado el host.

Ni el '*Membership Query'* ni el '*Membership Report'* salen del ámbito de la LAN pues los mensajes IGMP llevan siempre TTL=1.

IGMP v1 presentaba algunos problemas:

- Ausencia de un mensaje '*Leave'*: que permita a los hosts indicar su abandono de un grupo multicast. Al tener que esperar tres minutos antes de suprimir un grupo determinado se podían producir situaciones poco eficientes.

- Elección del Query router: se delegaba al protocolo de enrutamiento. Esta dependencia no resulta adecuada y en algún caso interesa que el router designado del protocolo de enrutamiento no sea el mismo que el query router de IGMP.

Debido a las limitaciones encontradas en la versión 1, se desarrolló IGMP versión 2.

1.5.2. IGMP versión 2

Con el fin de mejorar los problemas presentados por IGMP v1, se aprobó el RFC 2236 que especifica IGMPv2. Algunas de las mejoras introducidas en esta nueva versión son:

- *Group Specific Query.* Consultas a un grupo específico: Se agregaron las consultas a un grupo específico que permiten al router consultar un solo grupo en lugar de requerir consultas para ir a todos los grupos. Esto optimizó la forma en que un router descubre si queda algún miembro en un grupo en particular sin preguntarle a todos los grupos. La diferencia entre la consulta a un grupo específico y la consulta a los miembros es que la consulta a los miembros es multicast para todas las direcciones de los hosts (224.0.0.1) y una consulta a un grupo particular (por ejemplo

224.1.1.1) es un multicast para ese grupo específico de direcciones multicast.

- Mensaje *Leave Group.* Mensaje de abandono de grupo. Este mensaje permite a los hosts informarle al router que están dejando el grupo, reduciendo así la cantidad de tiempo para un grupo específico del segmento para saber cuando el último miembro deja el grupo.

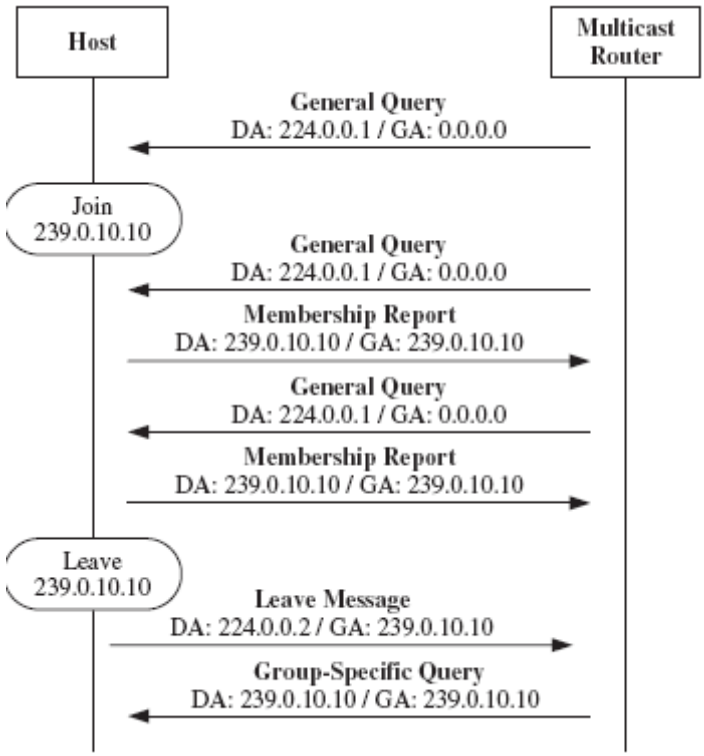
- Mecanismo de elección del router líder (*Query router)*: Este mecanismo permite tener un backup o configuración redundante. Se puede tener más de un router en el segmento, y el router con la IP más baja se convertirá en el router líder designado.

- Tiempo de respuesta de la consulta (*Timeouts)*: Permite controlar la recarga y la puntualidad de los reportes. Este tiempo se establece dentro de las consultas para informar a los miembros cuánto tiempo tienen para responder a una consulta con un informe.

El siguiente ejemplo describe en forma general el funcionamiento de IGMPv2.(Ver figura 5)

El router multicast envía periódicamente mensajes de consulta de miembros, con la dirección de destino (DA) 224.0.0.1 (Todas las direcciones multicast del sistema) y dirección de grupo (GA) 0.0.0.0. Después de algún tiempo, una aplicación se une al grupo multicast 239.0.10.10 por medio de la interfaz. Se envía una un informe de pertenencia al router multicast con la dirección del destino y grupo establecida en 239.0.10.10, la dirección del grupo multicast en cuestión.

Figura 5. Ejemplo de operación de IGMPv2.



Fuente: Multicast in 3rd Generation Mobile Networks, 2009.

El router agrega la dirección del grupo a la lista de grupos interesados para la interfaz y pasa la información a un protocolo de enrutamiento. El router comienza a enviar tráfico para el grupo multicast en la interfaz. El router continúa con sus consultas periódicas durante la sesión multicast, con el host respondiendo con *membership reports*. Cuando la aplicación deja el grupo multicast, por ejemplo como resultado de que el usuario cierre la aplicación, se envía un mensaje al router para informar que el host desea abandonar el grupo. El mensaje *leave* es direccionado a la dirección 224.0.0.2 (Todos los routers multicast) y proporciona la dirección del grupo multicast en el campo “dirección de grupo” del mensaje IGMP. El router entonces envía una consulta *group specific query* para determinar quien está interesado en el grupo multicast previo a la eliminación de la entrada de la lista de la interfaz.

1.5.3. IGMP versión 3

Con IGMP v1 y v2 los routers mantienen una relación de los grupos multicast en los que están interesados los hosts, pero no tienen ninguna información sobre las direcciones de origen de dichos grupos. En ocasiones el receptor está interesado en el tráfico multicast de un grupo, pero solamente cuando la dirección de origen sea una determinada.

IGMP versión 3 es un estándar propuesto que busca que los hosts puedan especificar una fuente en particular de la cual quisieran recibir tráfico en un grupo multicast determinado, y de esta manera proveer un enrutamiento más eficiente.

Para permitir la suscripción selectiva a algunos emisores el comando '*Membership Report*' de IGMP v3, además de indicar el grupo multicast en el que está interesado el receptor, especifica un filtro que puede ser de dos tipos: EXCLUDE (lista) para indicar que se desea recibir el tráfico de todas las fuentes menos las indicadas explícitamente, o INCLUDE (lista) para indicar lo contrario, es decir que se desea recibir solo el tráfico de las fuentes indicadas.

Para completar adecuadamente su funcionalidad IGMP v3 amplía el comando *Query* con un tercer tipo que es el '*Group-and-Source-Specific Query'*, el cual permite a los routers preguntar a los hosts si siguen interesados en recibir el tráfico multicast de un grupo determinado originado por una fuente concreta.

1.5.4. IGMP Snooping (Multicast Capa 2)

En principio cualquier host que desee ser miembro de un grupo multicast debe emitir un mensaje IGMP *Membership Report*. Si los switches pudieran analizar los mensajes IGMP que pasan por ellos podrían averiguar que hosts están interesados en que grupos multicast, y hacer

así la distribución de forma optimizada. En principio esta no debería ser tarea de los switches puesto que son dispositivos capa 2 y los mensajes IGMP son capa 3, pero esto es precisamente lo que hace la técnica denominada IGMP snooping

Con IGMP snooping, un switch debe examinar cada paquete de datos multicast para determinar si contiene alguna información de control pertinente IGMP y después actualiza la tabla MAC de acuerdo a esto.

Para implementar el IGMP snooping existen dos opciones:

- Hacerlo por hardware. Esta opción requiere diseñar chips adicionales a medida. Esto aumenta considerablemente el costo del equipo y solo es viable en switches de gama alta.

- Hacerlo por software. En este caso el IGMP snooping requiere la intervención de la CPU del equipo, que tiene una capacidad limitada de proceso de paquetes (mucho menor que la capacidad de los ASICs[4] que conmutan normalmente las tramas unicast). Generalmente esto supone que el rendimiento del switch en tráfico multicast será muy inferior al del mismo equipo con tráfico unicast.

1.6. ALGORITMOS DE ENRUTAMIENTO MULTICAST

Los algoritmos de enrutamiento multicast son los procedimientos que ejecutan los protocolos de enrutamiento para determinar el mejor árbol para transmitir la información a los nodos destinos del grupo multicast. A continuación se describen los algoritmos más comunes en multicast:

[4] ASICs: Aplication Specific Integrated Circuit

1.6.1. Inundación

También conocido como *Flooding*. Este algoritmo ha sido usado en protocolos tales como OSPF, es la técnica más sencilla para enviar los paquetes multicast a los routers de una red. En este algoritmo cuando un router recibe un datagrama multicast, primero comprueba si es la primera vez que llega o si ya ha llegado anteriormente. Si es la primera vez que el paquete ha llegado, entonces el router procederá a reenviarlo por todas las interfaces excepto por la que lo recibió. Si ya lo había recibido anteriormente el paquete será descartado. Con este mecanismo se asegura que un router reciba al menos una copia del paquete multicast.

Es importante resaltar que aunque este algoritmo resulta bastante simple, presenta una desventaja importante en cuanto genera un gran número de paquetes duplicados, desaprovechando de esta forma el ancho de banda. Además, debido a que cada router requiere la información de los datagramas para saber si se ha recibido con anterioridad, debe mantener una entrada diferente en su tabla para cada datagrama recientemente recibido, por lo que este algoritmo conduce a una utilización muy pobre de los recursos de memoria.

1.6.2. Spanning Tree

También conocido como árbol de expansión, es un subgrupo de la red que incluye a todos los routers pero que no contiene ciclos. Si cada router sabe cuáles de sus interfaces pertenecen al árbol de expansión, puede copiar un paquete de entrada difundido en todas las interfaces del árbol de expansión, excepto en aquella por la que llegó. Este método hace un uso eficiente del ancho de banda, generando la cantidad mínima de paquetes necesarios para llevar a cabo el trabajo. El único problema es que cada router debe tener conocimiento de algún árbol de expansión para que pueda funcionar. Algunas veces está disponible esta

información, por ejemplo con el enrutamiento por estado de enlace, pero a veces no, por ejemplo con el enrutamiento por vector distancia.

1.6.3. Reverse Path Broadcasting (RPB)

El algoritmo RPB es una modificación del Spanning Tree. En este caso, en lugar de construir un árbol que atraviesa toda la red, construye un árbol implícitamente por cada origen. En este algoritmo siempre que un router recibe un paquete multicast en un enlace “L” y desde un origen “S”, revisará si el enlace “L” pertenece al camino más corto hacia “S”. Si este es el caso el paquete es reenviado por todos los enlaces excepto “L”. En otro caso el paquete es descartado.

El algoritmo RPB es simple. Para cada pareja (fuente, grupo), cuando llega un paquete a través de un enlace, que el router local considera que está en el camino más corto hacia el emisor del mismo, el router los reencamina por todos las interfaces excepto por el de llegada. En caso contrario, el datagrama es descartado. La interfaz por el que el router espera recibir los datagramas multicast de un emisor determinado se conoce como enlace “padre”. Los enlaces de salida a través de los cuales el router encamina el datagrama multicast se conocen como enlaces “hijos”.

Este algoritmo puede ser mejorado fácilmente para evitar duplicaciones de datagramas teniendo en cuenta el hecho de que si el router local no está en el camino más corto entre el emisor y un vecino, el datagrama será descartado en el router vecino. Por lo tanto, si este es el caso, no sería necesario reenviar el datagrama hacia dicho router vecino. Esta información se obtiene fácilmente si se está utilizando un protocolo de enrutamiento de estado de enlace. Si se emplea un protocolo vector-distancia, un vecino puede bien advertir su próximo salto para el emisor como parte de los mensajes de actualización de rutas o hacer “*poison-reverse*" de la ruta.

Este algoritmo es fácil de implementar. Además, dado que los datagramas se envían a través del camino más corto desde el emisor a los nodos de destino, resulta muy rápido. El algoritmo RPB no necesita ningún mecanismo para detener el proceso de envío. Los routers no necesitan tener conocimiento del árbol de expansión completo y puesto que los datagramas son enviados a través de árboles de expansión diferentes (y no un único árbol) el tráfico se distribuye entre varios árboles, aprovechando mejor la red. Sin embargo, el algoritmo RPB tiene una gran desventaja y es que no tiene en cuenta la información acerca de la pertenencia a grupos multicast para construir los árboles de expansión.

1.6.4. Truncated Reverse Path Broadcasting (TRPB)

El algoritmo TRPB se propuso para solucionar algunas limitaciones del algoritmo RPB. A través del protocolo IGMP, un router puede determinar si los miembros de un grupo multicast están en la subred. Si esta subred es una hoja del árbol el router deshabilitará al *SpanningTree* y por lo tanto no reenviará mensajes al enrutador vecino.

1.6.5. Reverse Path Multicast (RPM)

Este algoritmo también se conoce como RPB con podas, es una mejora a RPB y a TRPB en donde construye el árbol únicamente si: Las subredes y los routers contienen miembros del grupo, en caso de que no presenten miembros de ese grupo emitirán un mensaje de poda (*Prune)*, el cual deshabilita la recepción de mensajes a esa red.

El árbol RPM puede ser podado de forma tal que los paquetes multicast se envíen por enlaces que conducen a los miembros del grupo destino. Para un par dado (fuente, grupo) el primer datagrama multicast se envía basándose en el algoritmo TRPB. Los routers que no tienen ningún router

más abajo en el árbol TRPB se denominan routers hojas. Si un router hoja recibe un datagrama multicast para un (emisor, grupo) dado y no tiene ningún miembro del grupo en sus subredes, enviará un mensaje de “poda” al router del que recibió el paquete multicast. El mensaje de poda indica que los paquetes multicast correspondientes a dicha pareja (emisor, grupo) no deben ser reenviados por el enlace por que el que se recibe un mensaje de poda.

Es importante resaltar que los mensajes de poda sólo se envían un salto hacia atrás en dirección al emisor. Es necesario que el router por encima registre la información de poda en su memoria. Además, si el router por encima no tiene ningún miembro local y recibe mensajes de poda de todos sus “hijos” en el árbol TRPB, enviará a su vez un mensaje de poda a su “padre” en el árbol TRPB indicando que los datagramas multicast correspondientes al par (fuente, grupo) no es necesario que sean reenviados hacia él. Los mensajes de poda en cascada truncarán el árbol original TRPB de modo que los datagramas multicast serán enviados sólo por aquellos enlaces que conduzcan a un nodo de destino (miembro de un grupo).

La pertenencia a grupos y la topología de la red cambia dinámicamente, por que lo que el estado de poda de los árboles debe refrescarse a intervalos regulares. Por lo tanto, la información de poda se elimina periódicamente de los routers y el siguiente paquete se reenviará a todos los routers hoja reiniciándose el proceso. RPM requiere una capacidad de almacenamiento relativamente grande para mantener la información de estado de todos los pares (fuente, grupo), lo que constituye un inconveniente que hace al algoritmo *no* escalable.

1.6.6. Steiner Tree (ST)

También conocido cómo árbol de Steiner. Los algoritmos RPB, TRPB, RPM utilizan el *shortest path* entre el nodo origen y cada nodo destino para enviar paquetes multidifusión garantizando que el envío se hace lo

más pronto posible. Sin embargo, ninguno de estos algoritmos trata de minimizar el uso de los recursos de la red. El objetivo de este algoritmo es el de minimizar el número de enlaces usados para construir el árbol; pero dada la forma en que el ST cambia con la adhesión o abandono de un nodo de un grupo multicast, estos árboles son muy inestables y requieren gran complejidad computacional por lo cual *no* han sido prácticamente implementados.

1.6.7. Core Based Trees (CBT)

Este algoritmo se basa en el enrutamiento a través de un árbol compartido a cuyo nodo central se le llama Core. CBT crea un árbol de distribución para cada grupo, el árbol utilizado para enviar los paquetes multicast de un grupo particular es un árbol independiente de la localización del nodo emisor. Un router, o un conjunto de routers son elegidos para constituir el router núcleo ("core") del árbol de distribución. Los datagramas de un grupo particular son enviados como mensajes unicast al router “core” hasta que alcanzan un router que pertenece al correspondiente árbol de distribución; entonces el datagrama se envía por todas las interfaces que son parte del árbol de distribución excepto por el que llegó.

Debido a que CBT construye un árbol de expansión para cada grupo multicast, los routers multicast requieren almacenar menos información comparado con los requisitos de los algoritmos anteriores. Adicionalmente CBT conserva el ancho de banda de la red debido a que no necesita inundar ningún datagrama multicast. Sin embargo, el hecho de utilizar un árbol por cada grupo puede llevar a una concentración de tráfico y a cuellos de botella cerca del router “core”, además de producir rutas no-óptimas y por lo tanto retraso en el envío de los datagramas

1.7. ÁRBOLES DE DISTRIBUCIÓN MULTICAST

Los routers multicast crean árboles de distribución que definen el camino que toma el tráfico IP multicast a través de la red desde una fuente (*source*) para distribuirlo a todos los receptores. Estos árboles son dinámicos debido a que las fuentes y los participantes varían en el tiempo. Además, permiten técnicas de podado (*prune*) que elimina un receptor del árbol de distribución y de Injerto (*graft*) que añade un receptor al árbol de distribución.

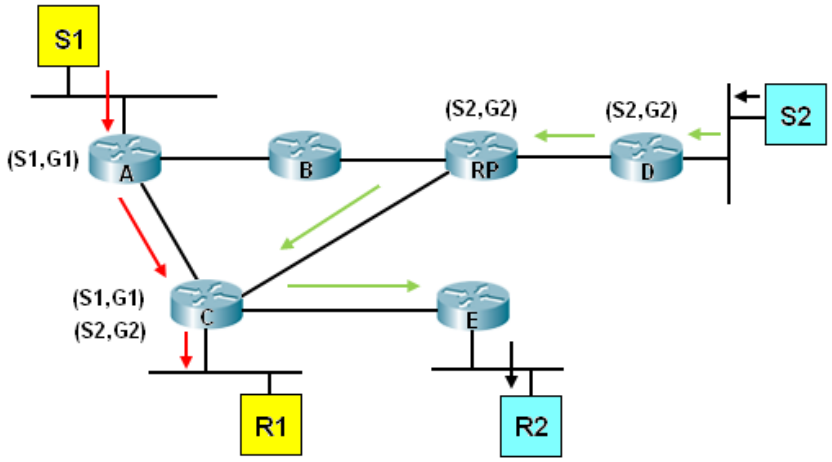
Existen dos tipos básicos de árboles de distribución multicast: árboles basados en el origen *(source based tees)* y árboles compartidos (*shared trees*).

1.7.1. Árboles basados en el origen (*Source Based Trees)*

También conocidos como SPT (*Short Path Trees).* El árbol basado en el origen es la forma más simple de árbol de distribución multicast, es un árbol fuente con su raíz en el origen y sus ramas formando un spanning tree a través de la red y hacia los receptores. Debido a que estos árboles usan el camino más corto, son referenciados como SPT *(shortest path tree*).

La notación especial de (S, G) enumera un SPT donde “S” es la dirección IP de la fuente y “G” la dirección IP del grupo multicast. Usando esta notación, el SPT para el ejemplo de la siguiente figura se muestra que existe un SPT separado para cada fuente individual (S1 y S2) y enviado a cada grupo.

Figura 6. Distribución árboles basados en el origen (SPT)



Fuente: http://www.ccapitalia.net/netica/teleco/multicast-ip-jorgef.pdf.

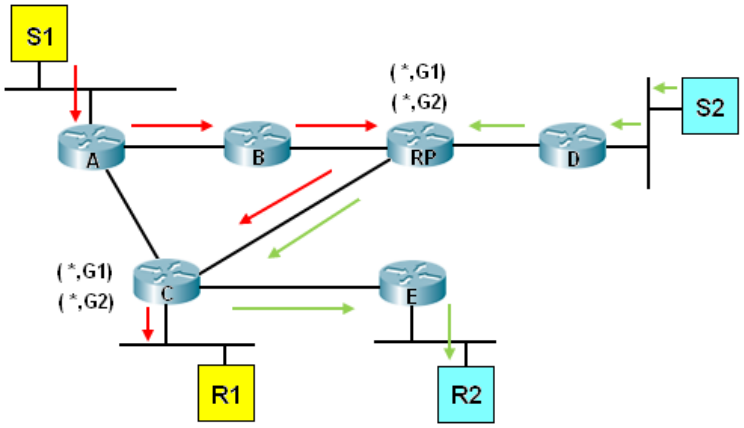
La principal ventaja de SPT es que crea una ruta óptima entre el origen y los participantes y de esta forma garantiza un tiempo mínimo de latencia (retardo). Sin embargo, el hecho que cada router deba mantener una tabla de distribución para cada uno de los grupos multicast que existan en la red puede crear rápidamente un problema de recursos en los routers en redes con muchos orígenes y destinos.

1.7.2. Árboles compartidos (Shared Trees)

También conocidos como RPT *(Rendezvous Point Trees)* o árboles de punto de encuentro. A diferencia de SPT, los árboles compartidos utilizan una única raíz, situada en algún punto de la red. Dependiendo del protocolo IP Multicast utilizado, esta es a menudo denominada *Rendezvous Point*, *RP*, o *Core*. Al utilizar esta topología de distribución, las fuentes envían el tráfico al *RP* definido por el protocolo IP Multicast, y este lo direcciona al grupo IP Multicast destino.

Debido a que todas las fuentes utilizan la misma raíz (RP), la notación utilizada para este caso es (*,G) donde * indica todas las fuentes y G, indica la dirección IP del grupo multicast.

Figura 7. Distribución de árboles compartidos (RPT)



Fuente: http://www.ccapitalia.net/netica/teleco/multicast-ip-jorgef.pdf.

Esta topología de distribución IP Multicast puede dividirse en dos tipos: direccional o bidireccional.

- **Árbol compartido bidireccional:** el tráfico IP Multicast puede ser transmitido en dirección *upstream* o *downstream*, a través del árbol de distribución multicast, para alcanzar los receptores del grupo IP multicast al cual este dirigido.
- **Árbol compartido unidireccional:** sólo permite el flujo de tráfico IP Multicast en sentido *downstream*, desde la raíz hacia los receptores. Las fuentes de tráfico IP Multicast deben utilizar otro medio para enviar primero el tráfico IP Multicast al *RP*, para que luego este envíe el tráfico a los receptores dentro del grupo IP Multicast. Un método para enviar el tráfico desde las fuentes al *RP* puede ser la utilización de *SPT* (este método es utilizado por el protocolo PIM).

La principal ventaja de RPT es que requiere pocos recursos de los routers para mantener las tablas de distribución, debido a que solo se guarda la información de los grupos multicast y no de los orígenes. Sin embargo, el hecho de que todos los datos deban ser enviados a un punto central implica mayor tiempo de latencia, por lo cual la ubicación del RP es importante al realizar el diseño de la red.

2. PROTOCOLOS DE ENRUTAMIENTO

Los protocolos de enrutamiento son el conjunto de reglas utilizadas por un router para comunicarse con otros routers con el fin de compartir información de enrutamiento. Esta información es utilizada para construir y mantener las tablas de enrutamiento así como para determinar la mejor ruta para llegar al destino.

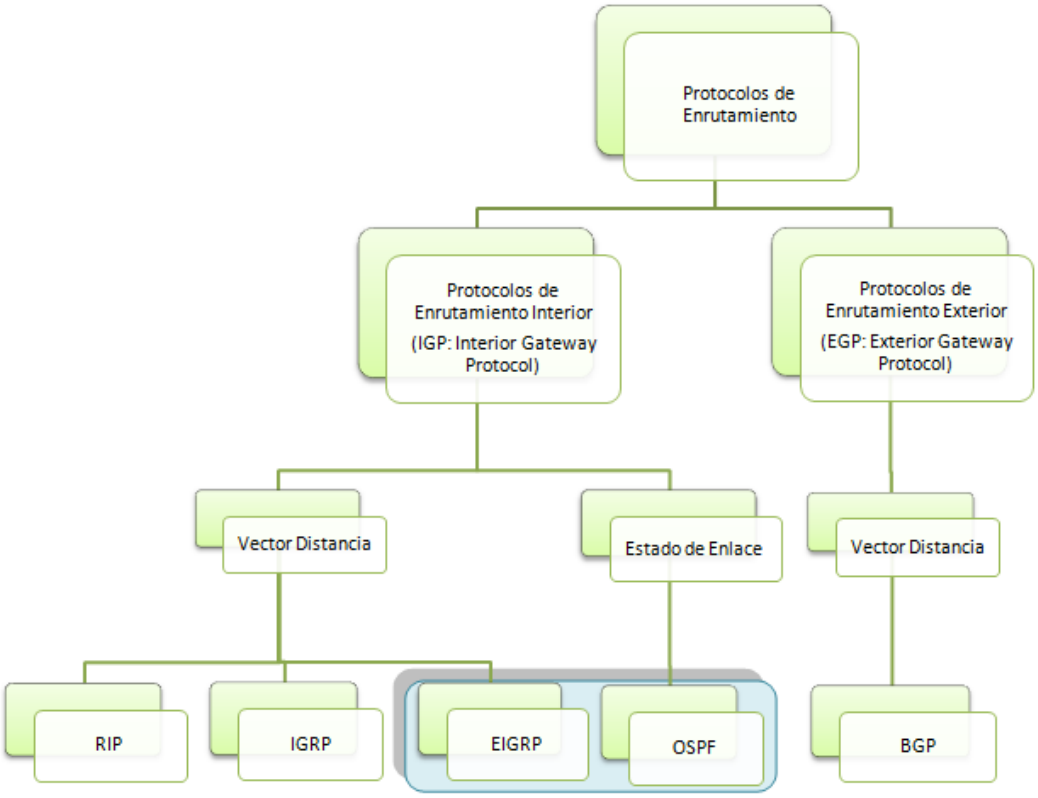
Existen protocolos de enrutamiento estático y dinámicos.

- **Protocolo de Enrutamiento Estático:** Es generado por el administrador, todas las rutas estáticas que se le ingresen son las que el router "conocerá", por lo tanto sabrá enrutar paquetes hacia dichas redes. El principal problema que plantea mantener tablas de enrutamiento estáticas, además de tener que introducir manualmente en los routers toda la información que contienen, es que el router no puede adaptarse por sí solo a los cambios que puedan producirse en la topología de la red.

- **Protocolos de Enrutamiento Dinámico:** Con un protocolo de enrutamiento dinámico, el administrador sólo se encarga de configurar el protocolo de enrutamiento mediante comandos IOS, en todos los routers de la red y estos automáticamente intercambiarán sus tablas de enrutamiento con sus routers vecinos, por lo tanto cada router conoce la red gracias a las publicaciones de las otras redes que recibe de otros routers.

Los protocolos de enrutamiento dinámico utilizan algoritmos de enrutamiento para determinar la mejor forma de transmisión de la información. Básicamente se distinguen dos algoritmos: vector distancia y estado de enlace. (El ANEXO A presenta una explicación más detallada del modo de operación de estos algoritmos).

Figura 8. Clasificación de los protocolos de enrutamiento



Fuente: http://www.slideshare.net/Ingcarlosadarragamejia/act-3-protocolos-de-enrutamiento

Se distinguen dos tipos protocolos de enrutamiento dinámico: protocolos de enrutamiento interior (IGP), que están diseñados para operar dentro de un mismo dominio administrativo o sistema autónomo y los protocolos de enrutamiento exterior (EGP) que son utilizados para administrar el enrutamiento entre dominios diferentes y donde cada dominio es independiente de la implementación de políticas de enrutamiento.

Debido al motivo de estudio de la presente monografía, sólo se hará énfasis en dos protocolos IGP, los cuales administran rutas que interconectan redes dentro de mismo dominio administrativo o sistema autónomo. Específicamente se enfatizará en los protocolos EIGRP y OSPF, con los cuales se trabajarán los protocolos de enrutamiento

multicast PIM modo denso y PIM modo esparcido que se estudiarán en la siguiente sección del documento.

2.1. PROTOCOLO OSPF

El protocolo OSPF (Open Shortest Path First) es un protocolo de enrutamiento de estado de enlace basado en estándares abiertos; lo que hace que esté disponible en múltiples sistemas operativos: Windows, Linux, Cisco IOS, etc.

OSPF fue desarrollado como reemplazo del protocolo de enrutamiento por vector de distancia: RIP. RIP constituyó un protocolo de enrutamiento aceptable en los comienzos del networking y de Internet; sin embargo, su dependencia en el conteo de saltos como la única medida para elegir el mejor camino rápidamente se volvió inaceptable en redes mayores que necesitan una solución de enrutamiento más sólida.

Este protocolo es bastante implementado como protocolo de enrutamiento interior para redes corporativas medianas y grandes, ya que cuenta con opciones y posibilidades de configuración que le permite dar respuesta a los escenarios o requerimientos más diversos. Sin embargo, esa misma potencialidad requiere un conocimiento y destreza superiores por parte del administrador de la red a los que requiere la implementación de protocolos más simples como por ejemplo RIP versión 2.

OSPF implementa el algoritmo de Dijkstra para calcular la ruta más corta a cada red de destino. Su métrica de enrutamiento es el *costo de los enlaces*, el cual se calcula en función del ancho de banda; por esta razón es de gran importancia la configuración del parámetro *bandwidth* en las interfaces que participan de este proceso de enrutamiento.

Este protocolo opera estableciendo relaciones de adyacencia con los dispositivos vecinos, a los que envía periódicamente paquetes *hello*. Adicionalmente, cada vez que un enlace cambia de estado inunda la red

con la notificación de este cambio y cada 30 minutos envía a los dispositivos vecinos (o adyacentes) una actualización que contiene todos los cambios de estado de enlaces de ese período.

OSPF se caracteriza por utilizar el ancho de banda de los enlaces como base de su métrica. Además soporta VLSM (*variable length subnet mask*) y CIDR (*Classless Inter-Domain Routing*).

Tabla 2. Ventajas y desventajas del protocolo OSPF

VENTAJAS	DESVENTAJAS
- Converge con mayor velocidad que los protocolos de vector distancia. - Sus actualizaciones son pequeñas ya que no envía toda la tabla de enrutamiento. - No es propenso a bucles de enrutamiento. - Escala muy bien en redes grandes. - Brinda múltiples opciones de configuración lo que permite adaptarlo a requerimientos muy específicos. - En comparación con RIP v1 y v2, OSPF es el IGP (Interior Gateway Protocol) preferido porque es escalable. RIP se limita a 15 saltos, converge lentamente y a veces elige rutas lentas porque pasa por alto ciertos factores críticos como por ejemplo el ancho de banda a la hora de determinar la ruta. OSPF ha superado estas limitaciones y se ha convertido en un protocolo de enrutamiento	- Las redes OSPF grandes utilizan un diseño jerárquico. - OSPF es un protocolo apto para implementar en redes de todo tipo y tamaño. Sin embargo, su desventaja principal es que requiere una configuración más compleja que otros protocolos, sobre todo para redes pequeñas

sólido y escalable adecuado para las redes modernas. - OSPF se puede usar y configurar en una sola área en las redes pequeñas. También se puede utilizar en las redes grandes.	

Fuente: http://www.slideshare.net/sasuukee/ccn-pm1ch03-v5a

2.1.1. Funcionamiento

Cuando un router inicia un proceso de enrutamiento OSPF en una interfaz, envía un paquete Hello y sigue enviando *Hellos* a intervalos regulares. El conjunto de reglas que rigen el intercambio de paquetes *Hello* de OSPF se denomina protocolo *Hello*. En las redes multiacceso el protocolo *Hello* elige un router designado (DR) y un router designado de respaldo (BDR). *Hello* transmite información que todos los vecinos deberán aceptar para que se pueda formar una adyacencia y para que se pueda intercambiar información del estado de enlace. En las redes multiaceso, el DR y el BDR mantienen adyacencias con todos los demás routers OSPF en la red.

Los routers adyacentes pasan por una secuencia de estados. Los routers adyacentes deben estar en su estado completo antes de crear tablas de enrutamiento y enrutar el tráfico. Cada router envía publicaciones del estado de enlace (LSA) en paquetes de actualización del estado de enlace (LSU). Estas LSA describen todos los enlaces de los routers. Cada router que recibe una LSA de su vecino registra la LSA en la base de datos del estado de enlace. Este proceso se repite para todos los routers de la red OSPF.

Una vez completas las bases de datos, cada router utiliza el algoritmo SPF para calcular una topología lógica sin bucles hacia cada red conocida. Se utiliza la ruta más corta con el menor costo para crear esta topología, por lo tanto, se selecciona la mejor ruta.

La información de enrutamiento ahora se mantiene. Cuando existe un cambio en el estado de un enlace, los routers utilizan un proceso de inundación para notificar a los demás routers en la red acerca del cambio. El intervalo muerto del protocolo Hello ofrece un mecanismo sencillo para determinar que un vecino adyacente está desactivado.

2.1.2. Mensajes OSPF

OSPF maneja cinco tipos de mensajes:

Tabla 3. Tipos de mensajes OSPF

MENSAJE	DESCRIPCIÓN
HELLO (Saludo)	Permite: - Identificar a los vecinos, para crear una base de datos en mapa local. - Enviar señales de <estoy vivo>, al resto de routers para mantener el mapa local. - Publicar parámetros en los que dos routers deben acordar convertirse en vecinos. - Elegir el router designado (DR) y el router designado de respaldo (BDR).
DBD *Database Description*	Incluye una lista abreviada de la base de datos de estado de enlace del router

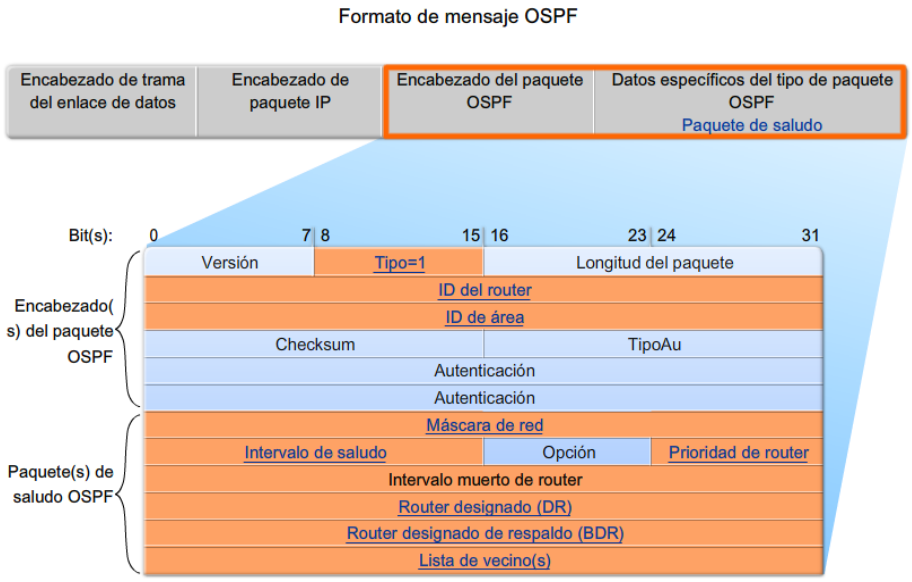
<table>
<tr><td>Packets (Descripción de la base de datos)</td><td>emisor; se usa para intercambiar información para que un router pueda descubrir los datos que le faltan durante la fase de inicialización o sincronización cuando dos nodos han establecido una conectividad.</td></tr>
<tr><td>LSR
Link State Request
(Petición del estado del enlace)</td><td>Se usa para pedir datos que un router receptor se ha dado cuenta que le faltan en su base de datos o que están obsoletos durante la fase de intercambio de información entre dos routers.</td></tr>
<tr><td>LSU
Link State Update
(Actualización del estado del enlace)</td><td>Se usa como respuesta a los mensajes LSR (envía los registros de estado de enlace específicamente solicitados) y también para informar dinámicamente de los cambios en la topología de la red. El emisor retransmitirá hasta que se confirme con un mensaje de ACK.
Un mensaje LSU puede incluir diez tipos diferentes de Notificaciones de estado de enlace (LSA), como se muestra a continuación.
<table><tr><th>Tipo</th><th>Descripción</th></tr><tr><td>1</td><td>LSA de router</td></tr><tr><td>2</td><td>LSA de red</td></tr><tr><td>3 ó 4</td><td>LSA de resumen</td></tr><tr><td>5</td><td>LSA externos del sistema autónomo</td></tr><tr><td>6</td><td>LSA de OSPF multicast</td></tr><tr><td>7</td><td>Definido para áreas no tan llenas</td></tr><tr><td>8</td><td>Atributos externos de LSA</td></tr></table></td></tr>
</table>

	para Border Gateway(BGP) 9,10,11 LSA opacas La diferencia entre los términos actualización de estado de enlace (LSU) y notificación de estado de enlace (LSA) en ocasiones puede ser confusa. A veces, dichos términos pueden utilizarse indistintamente. Una LSU incluye una o varias LSA y cualquiera de los dos términos puede usarse para hacer referencia a la información de estado de enlace propagada por los routers OSPF.
LSACK *Link State ACK* (ACK del estado del enlace)	Se usa para confirmar la recepción de un LSU (acuse de recibo).

Fuente: http://www.slideshare.net/sasuukee/ccn-pm1ch03-v5a

El formato de mensajes OSPF el siguiente:

Figura 9. Formato de mensaje OSPF.



Fuente: Cisco CCNA Exploration.

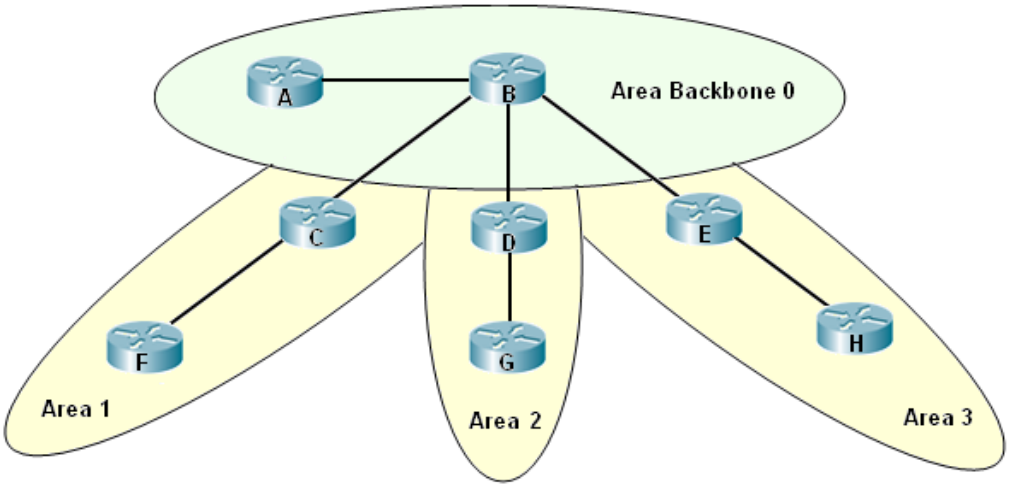
Los campos importantes que se muestran en la figura incluyen:

- Tipo: Tipo de paquete OSPF: Saludo (1), DBD (2), LSR (3), LSU (4), LSACK (5)
- ID del Router: ID del router de origen
- ID del área: área en la que se originó el paquete
- Máscara de red: máscara de subred asociada con la interfaz emisora
- Intervalo de saludo: cantidad de segundos entre los paquetes de saludo del router emisor
- Prioridad del router: utilizado en la elección de DR/BDR (se analizará más adelante)
- Router designado (DR): ID del router del DR, si existe
- Router designado de respaldo (BDR): ID del router del BDR, si existe
- Lista de vecinos: enumera el ID del router OSPF de los routers vecinos

2.1.3. Areas en OSPF

Un área es un conjunto de redes y host contiguos, con sus respectivos routers e interfaces. Un sistema autónomo (SA) que use OSPF está construido por una o más áreas. Cada área tiene asignado un número. El área 0 está conectada al Backbone que enlaza con el resto de áreas y agrupa al resto de sistemas autónomos.

Figura 10. Sistema Autónomo



Fuente: Autoras.

El enrutamiento dentro de un área se basa en un mapa completo del estado de los enlaces del área ya que los routers solo necesitan conocer información del área a la que pertenecen. Eso permite (y es una de las ventajas de OSPF) un fácil crecimiento de la red.

Todos los routers que están implementados con OSPF de una misma área, mantienen una base de datos de las rutas a través de los nodos (routers) de esa área. La base de datos se usa para construir el mapa de esa área y contiene el estado de todas las rutas, interfaces útiles de los routers, las redes conectadas y sus routers adyacentes.

Siempre que ocurre un cambio, la información se propaga por toda el área. De esta forma en un periodo de tiempo muy corto, todos los routers tienen la información actualizada y están en un estado óptimo para cualquier petición. Así, si se produce un problema, por ejemplo que un router tiene demasiada actividad o se bloquea, el router vecino informará a todos los demás routers que ese camino se encuentra inaccesible. Este proceso se repetirá hasta que el router con el problema se recupere.

En estos casos es donde se ve la importancia de una de las características del método: La velocidad en la que se propaga la base de datos. Si el tiempo en que se propaga la información fuese más lento, haría que se perdiera gran cantidad de información ya que hasta que no le llegase el cambio en el estado, daría tiempo a enviar gran cantidad de mensajes que quedarían suspendidos en ese router.

Cuando un router se conecta a la red, obtiene una copia de la base de datos actual, tras esto, solo se comunicarán los cambios. Esto hace más óptimo a OSPF, ya que no tiene que enviar toda la base de datos entera.

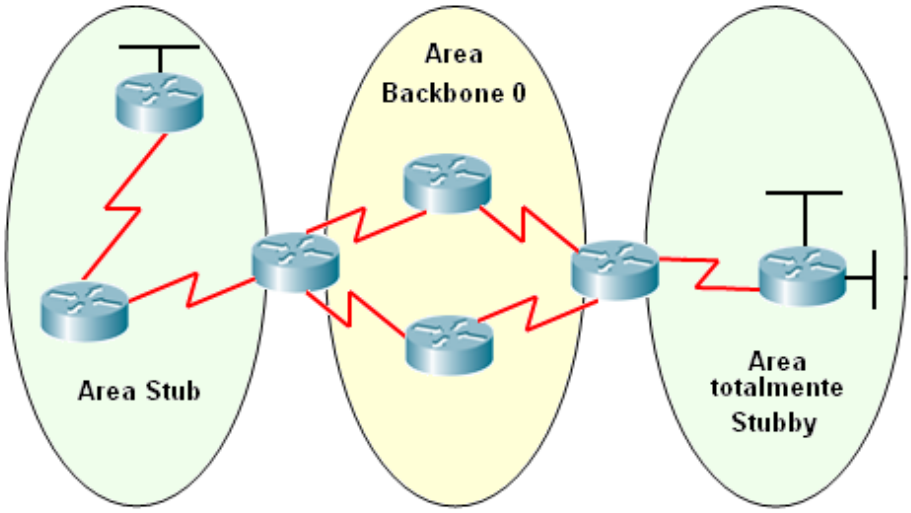
A continuación se presentan los diversos tipos de áreas que distingue OSPF:

- **Standard area:** Área Estándar. Este tipo de área se conecta a la de backbone o Área 0. Todos los routers del área conocen los demás routers del área y tiene la misma base de datos topológica. Sin embargo cada router tiene su propia tabla de routing. Acepta actualizaciones, rutas sumarizadas y rutas externas
- **Backbone area** (área de transito): Conocida como Área 0. Es la unidad central de interconexión entre áreas. No puede propagar LSA de tipo 7, estos son traducidos a LSA de tipo 5 por el ABR
- **Stub area:** No acepta rutas externas al AS (no acepta LSA tipo 5, LSA tipo 4 son innecesarios, por ende son bloqueados). Sólo existe una

forma de ver fuera el AS es mediante una ruta por defecto. El ABR usa la ruta 0.0.0.0 dentro de OSPF para mantener conectividad.

- **Totally stubby area:** No acepta rutas externas ni sumarizadas al AS (no acepta LSA tipo 5, y sumariza LSA tipo 3 & LSA tipo 4), los LSA tipo 3 que contienen información sobre la ruta 0.0.0.0. La única forma de salir del área es mediante una ruta por defecto. Este tipo de área es muy útil para sitios remotos con pocas redes y conectividad limitada con el resto de la empresa. Esta es una solución propietaria de Cisco Systems.

Figura 11. Tipos de áreas OSPF



Fuente: Autoras

- **NSSA (Not-so-stubby area):** Este tipo de áreas se suelen utilizar para conectar a un ISP o cuando se requiere una redistribución. Tiene los beneficios del área Stub y Totally Stub, y además permite actualización de enrutamiento sobre rutas externas al AS, pero que no pueden propagarlas hacía el área de backbone y por tanto al resto del dominio de OSPF. En estas áreas se crean los LSA de tipo 7 que son

transformados a LSA de tipo 5 por el ABR del NSSA, de esta forma se puede propagar al resto del dominio OSPF.

Un área puede ser Stub o Totally stub

- Si existe un único ABR
- Si todos los routers en el área son configurados como routers Stub
- Si no hay ASBR en el área
- Si el área no es área 0
- No hay ¨Virtual Links¨ configurados para pasar a través del área

2.1.4. Tipos de red OSPF

OSPF define cinco tipos de redes:

a. Punto a punto
b. Broadcast multiacceso (BMA)
c. Multiacceso sin broadcast (NBMA)
d. Punto a multipunto
e. Enlaces virtuales

a. Redes punto a punto

En las redes punto a punto solo dos routers pueden estar conectados, por esta razón no necesitan DR ni BDR. Los routers detectan dinámicamente a los vecinos utilizando paquetes multicast (a todos los routers), con dirección 224.0.0.5

Habitualmente cuando un router manda un paquete, la dirección origen es la IP de la interfaz de salida del router, pero cuando se están usando

interfaces sin IP (IP unnumbered), la dirección origen es alguna otra interfaz del router.

El paquete *Hello* y el intervalo *Dead*, en redes punto a punto son de 10 y 40 respectivamente

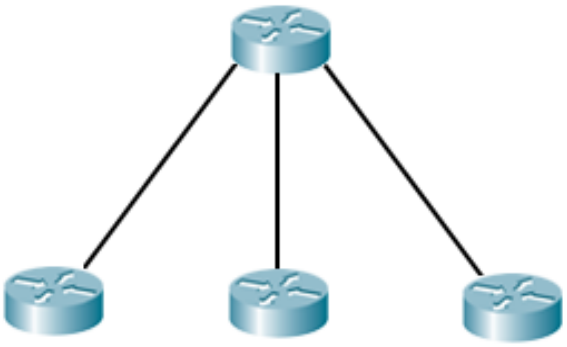
Figura 12. Diagrama de red punto a punto

Fuente: Autoras.

b. Redes punto a multipunto

Las redes punto a multipunto son tratadas como si fueran punto a punto, los routers se detectan mutuamente como vecinos y no eligen ni DR ni BDR.

Figura 13. Diagrama de red punto a multipunto



Fuente: Autoras.

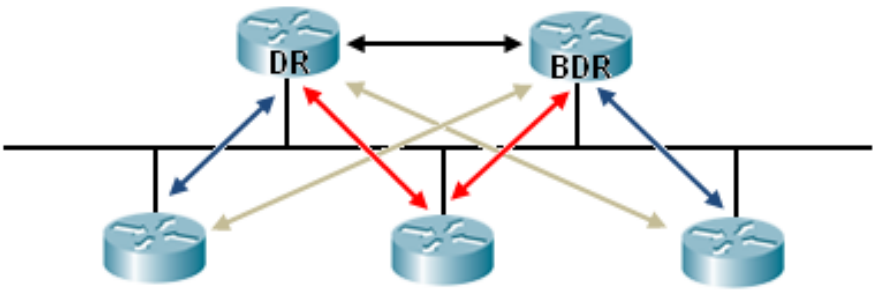
c. Redes Broadcast Multiacceso (BMA)

En este tipo de redes el número de routers conectados es desconocido.

Si cada router tuviera que establecer adyacencia completa con cada uno de los otros routers e intercambiar información del estado de enlace con cada vecino, el procesamiento tendría un gasto demasiado grande. Por lo general, para **n** routers, se necesitan **n*(n-1)/2** adyacencias. La solución para este gasto es elegir un router designado (DR). Este router se hace adyacente a todos los demás routers del segmento de broadcast. Todos los demás routers del segmento envían su información del estado de enlace al DR.

Los routers en un segmento deben elegir un DR y un BDR. El BDR no ejecuta funciones del DR cuando el DR está en estado operacional, en cambio, el BDR recibe toda la información, pero solo el DR se encarga de mandar los LSA y ejecutar las tareas de sincronización. Si el DR falla, el BDR asume el rol de DR y se genera una nueva elección de DR. Los paquetes hacia el DR y BDR utilizan la dirección 224.0.0.6 y los paquetes desde el DR a todos los routers utilizan la dirección 224.0.0.5. Un ejemplo de este tipo de redes pueden ser las redes Ethernet.

Figura 14. Diagrama de red Broadcast Multiacceso



Fuente: Autoras.

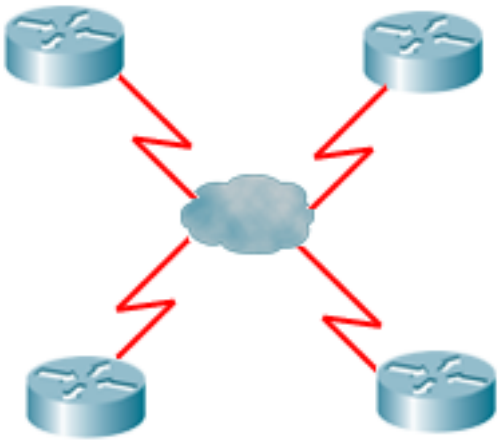
d. Redes Multiacceso sin Broadcast (NBMA)

OSPF considera una red NBMA similar a una red BMA. Cuando una interfaz del router interconecta múltiples interfaces, puede que existan problemas de interconectividad. Para implementar broadcast o multicast en redes NBMA, el router replica los paquetes que serán broadcast o multicast y los manda individualmente en cada circuito permanente virtual (PVC) a todos los destinos.

El intervalo Hello es de 30 y el intervalo Dead es de 120 en redes NBMA con OSPF.

OSPF no puede construir de forma automática las adyacencias con los routers vecinos sobre interfaces NBMA, por lo tanto se deben configurar manualmente los vecinos; además NBMA requiere elección de DR y BDR. Elegir un DR puede ser un factor clave en esta topología debido a que el DR y el BDR deben tener conectividad física completa con todos los routers. Ejemplo: Frame relay

Figura 15. Diagrama de red Multiacceso sin Broadcast



Fuente: Autoras.

2.1.5. Configuración del protocolo OSPF

Aunque la implementación de características avanzadas del protocolo puede ser compleja, su configuración inicial para entornos pequeños no es tan compleja como pudiera creerse.

2.1.5.1. Configuración de interfaces loopback en OSPF

Al iniciar el proceso OSPF, Cisco IOS utiliza la dirección IP activa local más alta como su ID de router OSPF. Si no existe ninguna interfaz activa, el proceso OSPF no se iniciará. Si la interfaz activa se desactiva, el proceso OSPF se queda sin ID de router y por lo tanto deja de funcionar hasta que la interfaz vuelva a activarse.

Para asegurar la estabilidad de OSPF, debe existir una interfaz activa en todo momento para el proceso OSPF. Para lograr esto, se configura una interfaz de loopback y OSPF utiliza esta dirección como ID del router, sin importar el valor. En un router que tiene más de una interfaz loopback, OSPF toma la dirección IP de loopback más alta como su ID de router.

Para crear y asignar una dirección IP a una interfaz de loopback se usan los siguientes comandos:

Router(config)#**interface loopback** *number*

Router(config-if)#**ip address** *ip-address subnet-mask*

Se recomienda usar interfaces loopback para todos los routers que ejecutan OSPF.

2.1.5.2. Activación del protocolo OSPF

Como en todos los protocolos, el inicio es la activación del protocolo. OSPF se habilita con el comando de configuración global router ospf *process-id* como se muestra a continuación.

Router(config)#**router ospf [proceso]**
Router(config-router)#_

El ID de proceso es un número entre 1 y 65535 elegido por el administrador de red. Es un identificador de carácter exclusivamente local del dispositivo en el que se está ejecutando, lo que implica que no necesita coincidir con otros routers OSPF para establecer adyacencias con dichos vecinos. Esto difiere de EIGRP. El ID del proceso EIGRP o el número de sistema autónomo sí necesita coincidir con dos vecinos EIGRP para volverse adyacente. El uso habitual es utilizar el mismo ID en todos los dispositivos solamente por una cuestión de orden y sencillez.

2.1.5.3. Identificación de las redes

A continuación, como en otros protocolos de enrutamiento interior, se identifican las redes directamente conectadas que deben ser publicadas por el protocolo:

Router(config-router)#**network [red] [wildcard] area [ID]**

Se indica la dirección de red y a continuación la máscara de wildcard (inversa a la máscara de subred). La máscara le indica a OSPF, tomando como base la dirección de red, el rango de interfaces que deben considerarse: con una sola sentencia network se puede identificar a un conjunto de interfaces.

También es necesario especificar un ID de área. El área es el modo en que OSPF organiza la red. Una red puede estar dividida en múltiples

áreas y la información de enrutamiento se comparte entre los enlaces que constituyen una misma área. Si es necesario pasar información de enrutamiento de un área hacia otra, esto se hace a través de un router de borde.

Por lo tanto es necesario que los enlaces que participan de un intercambio de información de enrutamiento pertenezcan a la misma área OSPF. En redes pequeñas se opera con una única área OSPF y se suele utilizar para esto el área 0, que es el área de backbone.

Una vez que se han configurado ambos extremos de un enlace, los routers comienzan el intercambio de información para lo cual comienzan por generar las adyacencias. Este proceso se puede monitorear a partir de los mensajes de logging que Cisco IOS envía a la consola de configuración. Un ejemplo de estos mensajes es el siguiente:

***Nov 5 12:23:33.370: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.1.1 on Ethernet0/0 from LOADING to FULL, Loading Done**

Para asegurarse de que estos mensajes sean enviados a la consola y almacenados en un archivo log, se utiliza el comando:

Router(config-router)#log-adjacency-changes

De este modo se asegura tener un registro en un archivo log de los cambios de adyacencias, lo que permite verificar lo ocurrido, por ejemplo, en el caso de la pérdida de conectividad con un dispositivo vecino.

2.1.5.4. Monitoreo de OSPF

Existen una serie de comandos que permiten monitorear y verificar la operación del protocolo en el dispositivo:

- show ip ospf

- show ip ospf neighbor
- show ip ospf interface
- show ip ospf database
- show ip protocols
- show ip route

Comando "show ip ospf "

Descripción: Muestra las estadísticas y la información del estado de los procesos OSPF en ejecución.

Modo: Router#

Sintaxis: **show ip ospf { [***process-id***] | border-routers | database | interface | virtual-links }**

Descripción de la sintaxis:

Tabla 4. Descripción de la sintaxis del comando show ip ospf

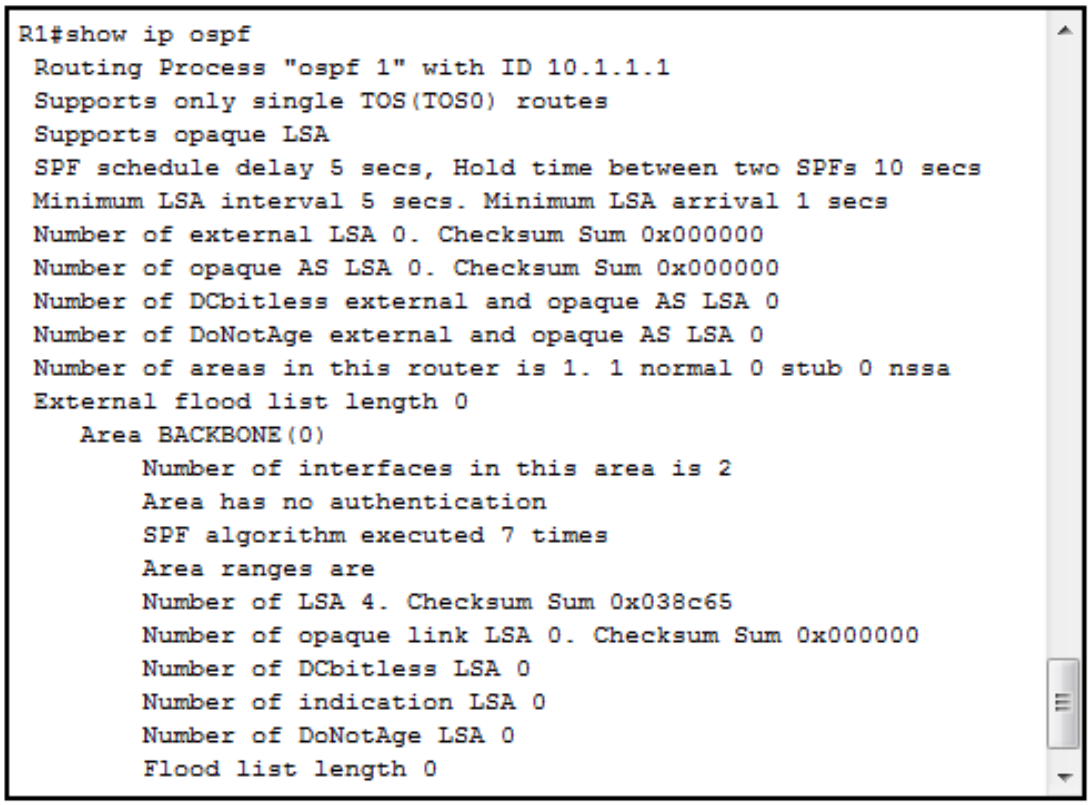
Campo	Descripción
process-id	Muestra la información sobre un caso especifico de OSPF, es el mismo valor especificado por el comando router ospf.
border-routers	Muestra el interior de las entradas de la tabla de enrutamiento OSPF a un router ABR (Area Border Router) y router ASBR(autonomous system boundary router).
database	Muestra las listas de información relacionada con la Base de datos OSPF para un router específico.

interface	Muestra la información de la interfaz relacionada OSPF, incluyendo temporizadores, Id de los vecinos, tipo de red y detalles del área.
virtual-links	Muestra los parámetros y el estado actual de los enlaces virtuales OSPF, incluyendo temporizadores, y el estado de las adyacencias

Fuente: Aplicación Ciscopedia v.3.0.

Ejemplo:

Figura 16. Ejemplo del comando show ip ospf



Fuente: Software Packet Tracer 5.2.

Comando “show ip ospf neighbor”

Descripción: Muestra información de los vecinos OSPF sobre una interface base.

Modo: Router>

Sintaxis: **show ip ospf neighbor** [*interface-type interface-number*] [*neighbor-id*] [detail]

Descripción de la sintaxis:

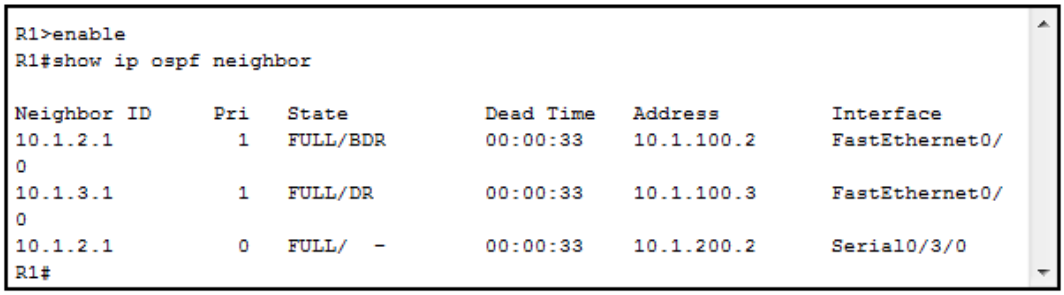
Tabla 5. Descripción de la sintaxis del comando show ip ospf neighbor

Campo	Descripción
interface-type	Tipo de interfaz (Opcional).
interface-number	Número de la interfaz (Opcional).
neighbor-id	ID del router vecino (Opcional).
detail	Muestra todos los vecinos dados en detalle (lista de todos los vecinos) (Opcional).

Fuente: Aplicación Ciscopedia v.3.0.

Ejemplo:

Figura 17. Ejemplo del comando show ip ospf neighbor



Fuente: Software Packet Tracer 5.2.

Descripción de los campos:

Tabla 6. Descripción de los campos de show ip ospf neighbor

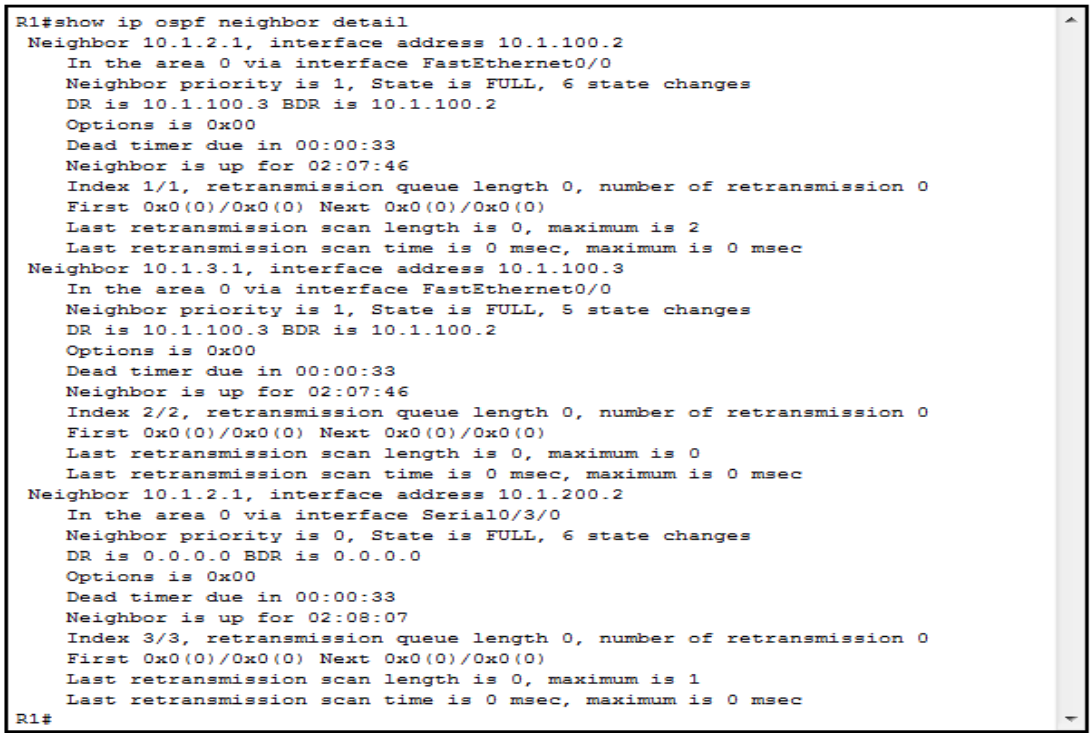
Campo	Descripción
Neighbor ID	ID del router vecino.
Pri	La prioridad OSPF de la interfaz
State	Estado OSPF de la interfaz. El estado FULL significa que el router y su vecino poseen bases de datos de estado de enlace de OSPF idénticas.
Dead Time	Tiempo muerto. Es la cantidad de tiempo restante que el router esperará para recibir un paquete de saludo OSPF por parte del vecino antes de declararlo desactivado. Este valor se reestablece cuando la interfaz recibe un paquete de saludo.
Address	La dirección IP de la interfaz del vecino a la que está conectada directamente el router.

Interface	La interfaz donde este router formó adyacencia con el vecino.

Fuente: Cisco IOS Cookbook.

Para visualizar información más detallada sobre los vecinos, se utiliza el comando **show ip ospf neighbor detail.** A continuación se presenta un ejemplo de la salida del comando:

Figura 18. Ejemplo del comando show ip ospf neighbor detail



Fuente: Software Packet Tracer 5.2.

Descripción de los campos (adicionales al comando **show ip ospf neighbor**)

Tabla 7. Descripción de campos adicionales de show ip ospf neighbor

Campo	Descripción
In the area	Area e interfaz a través de la cual se conoce el vecino OSPF.
state changes	Número de cambios de estado desde que el vecino fue creado. Este valor puede ser reiniciado usando el comando **clear ip ospf counters neighbor.**
DR is	ID del router designado (DR) para la interfaz.
BDR is	ID del router de respaldo designado (BDR) para la interfaz.
Options	Valores posibles: 0 y 2. 2 indica que el area no es stub, 0 indica que el área es stub.
Neighbor is up for	Número de horas:minutos:segundos desde que el vecino pasó a un estado two-way.
retransmission queue length	Número de elementos en la cola de retransmisión.
number of retransmission	Número de veces que los paquetes update han sido retransmitidos durante la inundación (flooding).
First	Localización en memoria de los detalles del *flooding.*
Next	Localización en memoria de los detalles del *flooding*
Last retransmission scan	Número de LSAs en el último paquete de

length	retransmisión.
maximum	Máximo número de LSAs enviados en un paquete de retransmisión.
Last retransmission scan time	Tiempo tomado para construir el último paquete de retransmisión
maximum	Máximo tiempo tomado para construir el último paquete de retransmisión.

Fuente: Cisco IOS Cookbook.

Comando "show ip ospf interface"

Descripción: Muestra la información del protocolo OSPF de una interfaz determinada.

Modo: Router>

Sintaxis: **show ip ospf interface [*interface-type interface-number*]**

Descripción de la sintaxis:

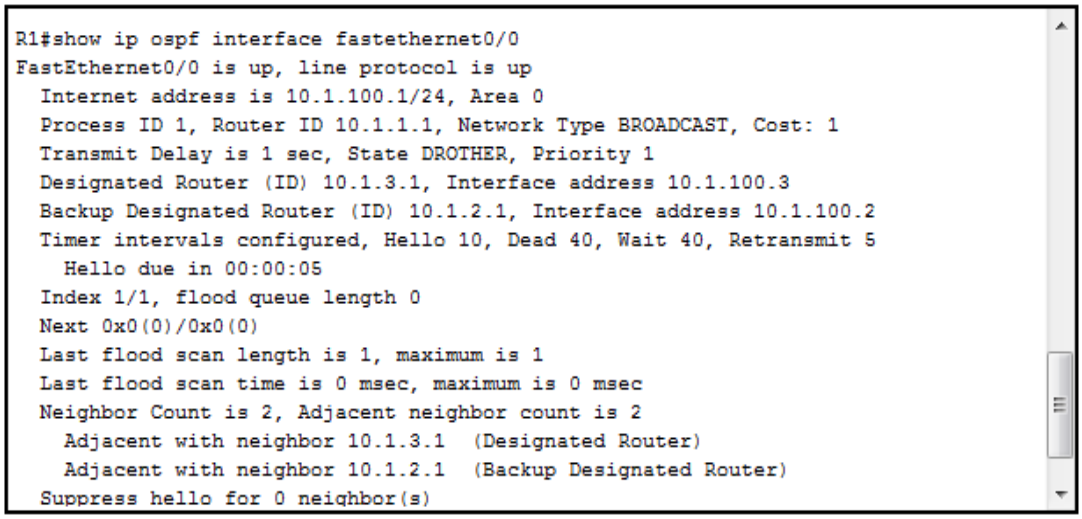
Tabla 8. Descripción de la sintaxis del comando show ip ospf interface

Campo	Descripción
interface-type	Tipo de Interfaz (Opcional).
interface-number	Número de la interfaz (Opcional)

Fuente: Cisco IOS Cookbook.

Ejemplo:

Figura 19. Ejemplo del comando show ip ospf interface



Fuente: Software Packet Tracer 5.2.

Comando "show ip protocols"

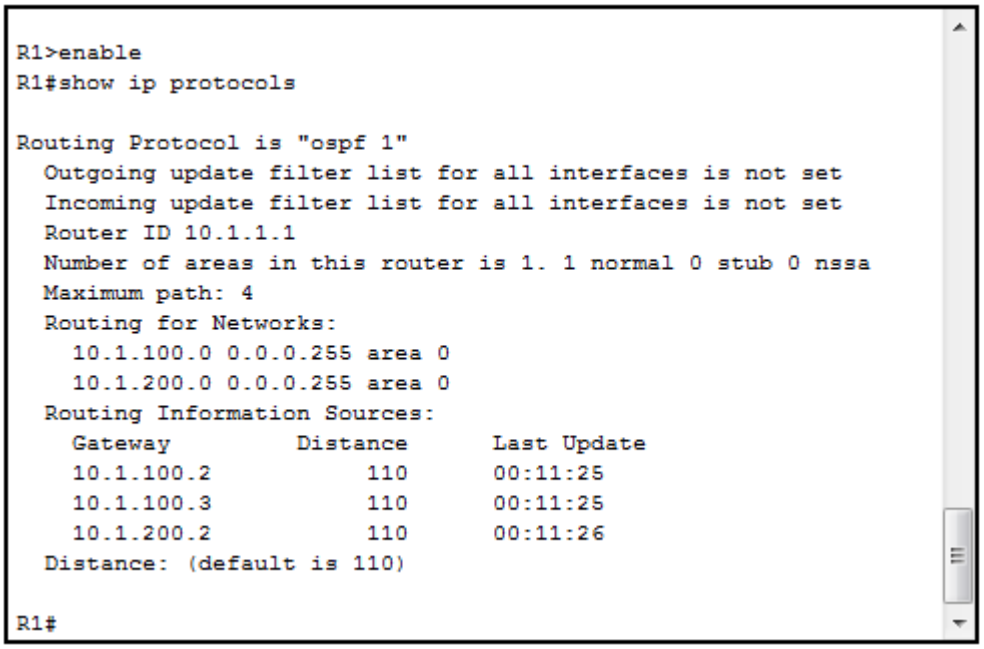
Descripción: Permite verificar información de configuración vital de OSPF, como el ID del proceso OSPF, el ID del router, las redes que el router publica, los vecinos de quienes el router recibe actualizaciones y la distancia administrativa predeterminada, que es de 110 para OSPF.

Modo: Router>

Sintaxis: **show ip protocols**

Ejemplo:

Figura 20. Ejemplo del comando show ip protocols



Fuente: Software Packet Tracer 5.2.

Comando "show ip route"

Descripción: Muestra el estado actual de la tabla de enrutamiento.

Modo: Router#

Sintaxis: **show ip route** [*address* [*mask*] [**longer-prefixes**]] | [*protocol* [*process-id*]] | [**list** *access-list-number* | *access-list-name*]

Descripción de la sintaxis:

Tabla 9. Tabla. Descripción de la sintaxis del comando show ip route

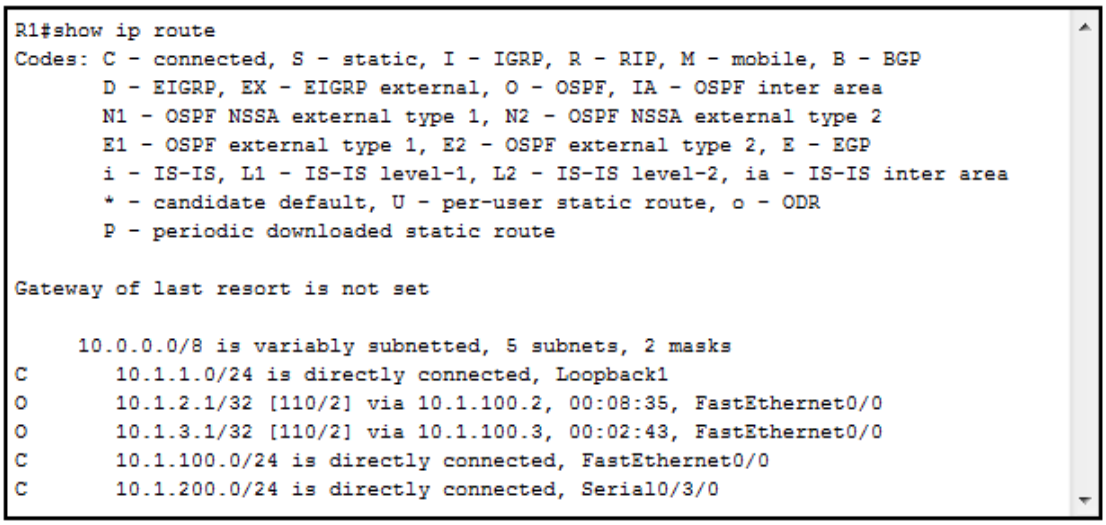
Campo	Descripción
Address	Dirección sobre la cual se debe mostrar la

	información del enrutamiento. (Opcional)
mask	Mascara de subred. (Opcional)
longer-prefixes	La pareja dirección y máscara se convierte en un prefijo y las rutas que coincidan con ese prefijo son mostradas. (Opcional)
protocol	Nombre de un protocol de enrutamiento (bgp, egp, eigrp, hello, igrp, isis, ospf, o rip). (Opcional)
process-id	Número que identifica un proceso del protocol especificado (Opcional)
list	La lista de palabras clave es requerida para filtrar una salida por medio de una lista de acceso. (Opcional)
access-list-name	Filtra la salida de la table de enrutamiento basada en el nombre de la lista de acceso especificada. (Opcional)
access-list-number	Filtra la salida de la table de enrutamiento basada en el número de la lista de acceso especificada (Opcional)

Fuente: Aplicación Ciscopedia v.3.0.

Ejemplo:

Figura 21. Ejemplo del comando show ip route



Fuente: Software Packet Tracer 5.2.

Comando “show ip ospf database”

Descripción: Muestra listados de información relacionada con la base de datos de un router específico. Adicionalmente ofrece información adicional sobre las diferentes LSAs.

Modo: Router>

Sintaxis: **show ip ospf [***process-id* **[***area-id***]] database**

show ip ospf [*process-id* **[***area-id***]] database [***adv-router* **[***ip-address***]]**

show ip ospf [*process-id* **[***area-id***]] database [asbr-summary] [***link-state-id***]**

show ip ospf [*process-id* **[***area-id***]] database [asbr-summary] [***link-state-id***] [adv-router [***ip-address***]]**

show ip ospf [*process-id* **[***area-id***]] database [asbr-summary] [***link-state-id***] [self-originate] [***link-state-id***]**

show ip ospf [*process-id* **[***area-id***]] database [***database-summary***]**

show ip ospf [*process-id* **[***area-id***]] database [external] [***link-state-id***]**

show ip ospf [*process-id* [area-id]] **database [external] [***link-state-id***] [adv-router [***ip-address***]]**

show ip ospf [*process-id* **[***area-id***]] database [external] [***link-state-id***] [self-originate] [***link-state-id***]**

show ip ospf [*process-id* **[***area-id***]] database [network] [***link-state-id***]**

show ip ospf [*process-id* **[***area-id***]] database [network] [***link-state-id***] [adv-router [***ip-address***]]**

show ip ospf [*process-id* **[***area-id***]] database [network] [***link-state-id***] [self-originate] [***link-state-id***]**

show ip ospf [*process-id* **[***area-id***]] database [***nssa-external***] [***link-state-id***]**

show ip ospf [*process-id* **[***area-id***]] database [nssa-external] [***link-state-id***] [adv-router [***ip-address***]]**

show ip ospf [*process-id* **[***area-id***]] database [nssa-external] [***link-state-id***] [self-originate] [***link-state-id***]**

show ip ospf [*process-id* **[***area-id***]] database [opaque-area] [***link-state-id***]**

show ip ospf [*process-id* **[***area-id***]] database [opaque-area] [***link-state-id***] [adv-router [*ip-address*]]**

show ip ospf [*process-id* **[***area-id***]] database [opaque-area] [***link-state-id***] [self-originate] [***link-state-id***]**

show ip ospf [*process-id* **[***area-id***]] database [opaque-as] [***link-state-id***]**

show ip ospf [*process-id* **[***area-id***]] database [opaque-as] [***link-state-id***] [adv-router [***ip-address***]]**

show ip ospf [*process-id* **[***area-id***]] database [opaque-as] [***link-state-id***] [self-originate] [***link-state-id***]**

show ip ospf [*process-id* **[***area-id***]] database [opaque-link] [***link-state-id***]**

show ip ospf [*process-id* **[***area-id***]] database [opaque-link] [***link-state-id***] [adv-router [***ip-address***]]**

show ip ospf [*process-id* **[***area-id***]] database [opaque-link] [***link-state-id***] [self-originate] [***link-state-id***]**

show ip ospf [*process-id* **[***area-id***]] database [router] [***link-state-id***]**

show ip ospf [*process-id* **[***area-id***]] database [router] [adv-router [***ip-address***]]**

show ip ospf [*process-id* **[***area-id***]] database [router] [self-originate] [***link-state-id***]**

show ip ospf [*process-id* **[***area-id***]] database [self-originate] [***link-state-id***]**

show ip ospf [*process-id* **[***area-id***]] database [summary] [***link-state-id***]**

show ip ospf [*process-id* **[***area-id***]] database [summary] [***link-state-id***] [adv-router [***ip-address***]]**

show ip ospf [*process-id* **[***area-id***]] database [summary] [***link-state-id***] [self-originate] [***link-state-id***]**

Descripción de la sintaxis:

Tabla 10. Descripción de la sintaxis de show ip ospf database

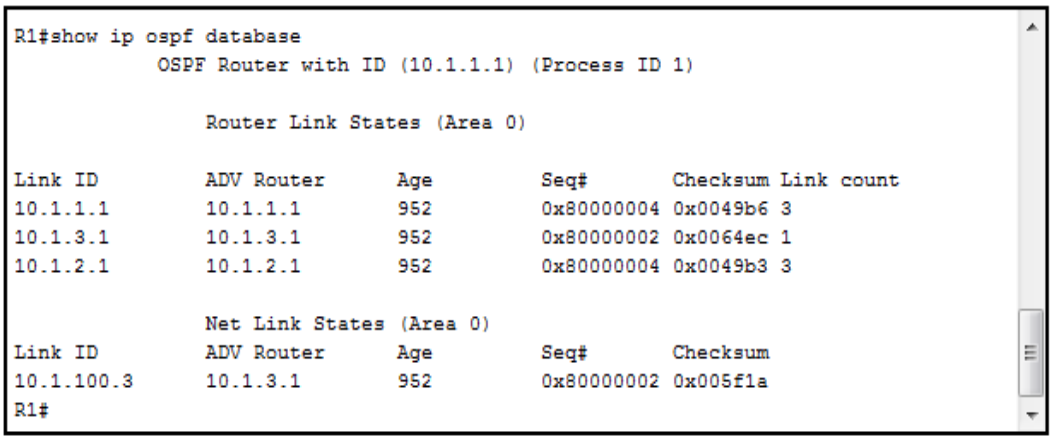
Campo	Descripción
process-id	Identificación interna (opcional). Es localmente asignada y puede ser un entero positivo. El número usado aquí es el número asignado administrativamente cuando se habilita el proceso de enrutamiento OSPF.
area-id	Número de área asociado con el rango de direcciones OSPF definidos en el comando de configuración de la red del router usado para definir el área particular. (opcional)
adv-router [ip-address]	Muestra todas las LSAs del router señalado. Si no se incluye la dirección IP, la información mostrada se refiere al mismo router local. (Opcional)
asbr-summary	Muestra la información del Router ASBR (Opcional).
link-state-id	Id del estado del enlace. El valor introducido depende del tipo de LSA. El valor debe ser introducido en forma de una dirección IP. (Opcional).
database-summary	Muestra cuántas LSA de cada tipo hay para cada área en la base de datos, y el total. (Opcional)
external	Muestra información acerca de las LSAs externas. (Opcional)

network	Muestra información acerca de las LSAs de la red. (Opcional)
nssa-external	Muestra información sobre las *not so stubby area* (NSSA) de las *LSAs externas*. (Opcional)
opaque-area	Muestra la información acerca de las LSAs tipo 10 (Opcional).
opaque-as	Muestra la información acerca de las LSAs tipo 11 (Opcional).
opaque-link	Muestra la información acerca de las LSAs tipo 9 (Opcional).
router	Muestra información sobre el router LSA. (Opcional)
self-originate	Muestra información sobre las LSAs self-originated (del router local). (Opcional)
summary	Muestra información sobre el resumen de LSAs. (Opcional)

Fuente: Aplicación Ciscopedia v.3.0.

Ejemplo:

Figura 22. Ejemplo del comando show ip ospf database



```
R1#show ip ospf database
            OSPF Router with ID (10.1.1.1) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
10.1.1.1        10.1.1.1        952         0x80000004 0x0049b6 3
10.1.3.1        10.1.3.1        952         0x80000002 0x0064ec 1
10.1.2.1        10.1.2.1        952         0x80000004 0x0049b3 3

                Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
10.1.100.3      10.1.3.1        952         0x80000002 0x005f1a
R1#
```

Fuente: Software Packet Tracer 5.2.

Descripción de los campos:

Tabla 11. Descripción de los campos de show ip ospf database

Campo	Descripción
Link ID	ID del router. Verificación OSPF Multiárea.
ADV Router	ID del router que anuncia la ruta.
Age	Edad del estado del enlace.
Seq#	Número de secuencia del LSA, para detectar LSAs antiguos.
Checksum	Suma de comprobación del LSA.
Link count	Número de interfaces detectados por router.

Fuente: Aplicación Ciscopedia v.3.0.

2.1.5.5. Comandos útiles en la configuración de OSPF

Comando "debug ip ospf adj / undebug all"

Descripción: Depura el proceso de establecimiento de vecinos OSPF. Para deshabilitar la depuración se utiliza la palabra **no** con este mismo comando.

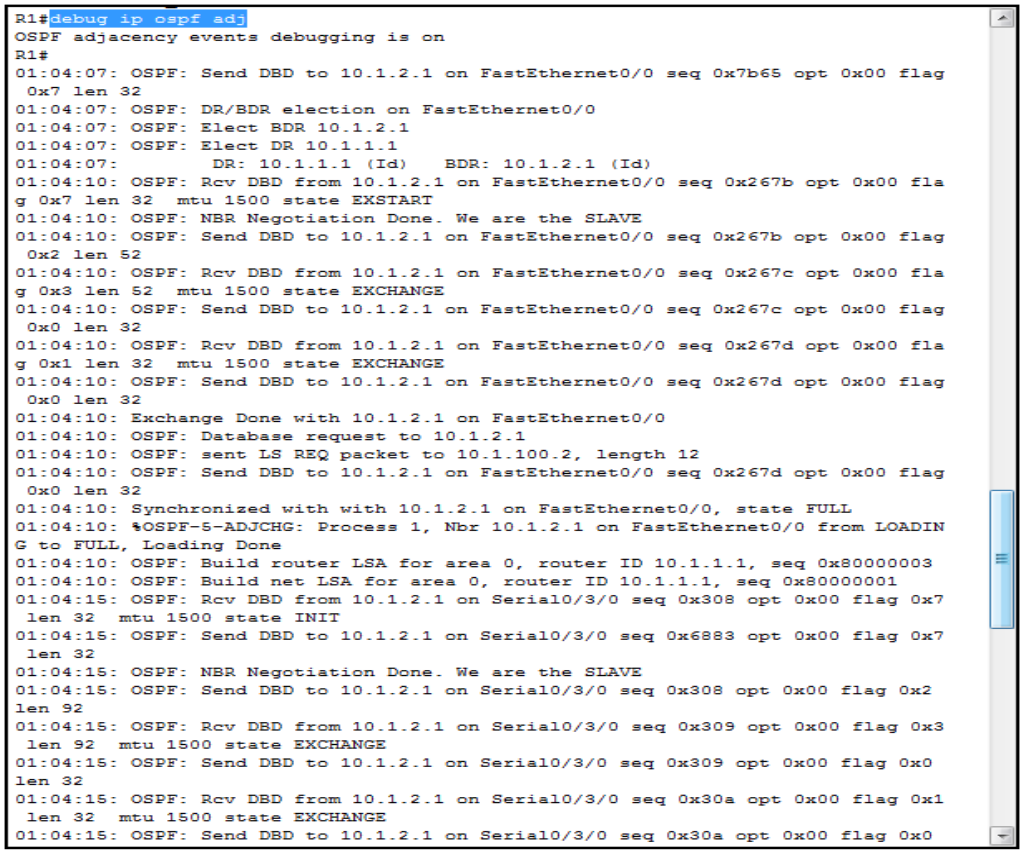
Modo: Router#

Sintaxis: Debug ip sopf adj

No debug ip ospf adj

Ejemplo:

Figura 23. Ejemplo del comando debug ip ospf adj



```
R1#debug ip ospf adj
OSPF adjacency events debugging is on
R1#
01:04:07: OSPF: Send DBD to 10.1.2.1 on FastEthernet0/0 seq 0x7b65 opt 0x00 flag
 0x7 len 32
01:04:07: OSPF: DR/BDR election on FastEthernet0/0
01:04:07: OSPF: Elect BDR 10.1.2.1
01:04:07: OSPF: Elect DR 10.1.1.1
01:04:07:         DR: 10.1.1.1 (Id)   BDR: 10.1.2.1 (Id)
01:04:10: OSPF: Rcv DBD from 10.1.2.1 on FastEthernet0/0 seq 0x267b opt 0x00 fla
g 0x7 len 32  mtu 1500 state EXSTART
01:04:10: OSPF: NBR Negotiation Done. We are the SLAVE
01:04:10: OSPF: Send DBD to 10.1.2.1 on FastEthernet0/0 seq 0x267b opt 0x00 flag
 0x2 len 52
01:04:10: OSPF: Rcv DBD from 10.1.2.1 on FastEthernet0/0 seq 0x267c opt 0x00 fla
g 0x3 len 52  mtu 1500 state EXCHANGE
01:04:10: OSPF: Send DBD to 10.1.2.1 on FastEthernet0/0 seq 0x267c opt 0x00 flag
 0x0 len 32
01:04:10: OSPF: Rcv DBD from 10.1.2.1 on FastEthernet0/0 seq 0x267d opt 0x00 fla
g 0x1 len 32  mtu 1500 state EXCHANGE
01:04:10: OSPF: Send DBD to 10.1.2.1 on FastEthernet0/0 seq 0x267d opt 0x00 flag
 0x0 len 32
01:04:10: Exchange Done with 10.1.2.1 on FastEthernet0/0
01:04:10: OSPF: Database request to 10.1.2.1
01:04:10: OSPF: sent LS REQ packet to 10.1.100.2, length 12
01:04:10: OSPF: Send DBD to 10.1.2.1 on FastEthernet0/0 seq 0x267d opt 0x00 flag
 0x0 len 32
01:04:10: Synchronized with with 10.1.2.1 on FastEthernet0/0, state FULL
01:04:10: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.2.1 on FastEthernet0/0 from LOADIN
G to FULL, Loading Done
01:04:10: OSPF: Build router LSA for area 0, router ID 10.1.1.1, seq 0x80000003
01:04:10: OSPF: Build net LSA for area 0, router ID 10.1.1.1, seq 0x80000001
01:04:15: OSPF: Rcv DBD from 10.1.2.1 on Serial0/3/0 seq 0x308 opt 0x00 flag 0x7
 len 32  mtu 1500 state INIT
01:04:15: OSPF: Send DBD to 10.1.2.1 on Serial0/3/0 seq 0x6883 opt 0x00 flag 0x7
 len 32
01:04:15: OSPF: NBR Negotiation Done. We are the SLAVE
01:04:15: OSPF: Send DBD to 10.1.2.1 on Serial0/3/0 seq 0x308 opt 0x00 flag 0x2
len 92
01:04:15: OSPF: Rcv DBD from 10.1.2.1 on Serial0/3/0 seq 0x309 opt 0x00 flag 0x3
 len 92  mtu 1500 state EXCHANGE
01:04:15: OSPF: Send DBD to 10.1.2.1 on Serial0/3/0 seq 0x309 opt 0x00 flag 0x0
len 32
01:04:15: OSPF: Rcv DBD from 10.1.2.1 on Serial0/3/0 seq 0x30a opt 0x00 flag 0x1
 len 32  mtu 1500 state EXCHANGE
01:04:15: OSPF: Send DBD to 10.1.2.1 on Serial0/3/0 seq 0x30a opt 0x00 flag 0x0
```

Fuente: Software Packet Tracer 5.2.

Comando “ip ospf cost”

Descripción: Se utiliza para especificar explícitamente el costo de enviar un paquete en una interfaz. Para restablecer el costo de la ruta en el valor predeterminado, se utiliza el comando **no ip ospf cost cost .**

Modo: Router(config-if)#

Sintaxis: **ip ospf cost** *cost*

no ip ospf cost

Descripción de la sintaxis:

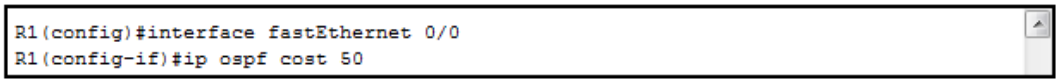
Tabla 12. Descripción de la sintaxis del comando show ip ospf cost

Campo	Descripción
cost	Valor entero expresado como la métrica de estado de enlace. Puede ser un valor en el rango de 1 a 65535

Fuente: Cisco IOS Cookbook.

Ejemplo:

Figura 24. Ejemplo del comando ip ospf cost



Fuente: Software Packet Tracer 5.2.

Comando “ip ospf priority”

Descripción: Establece la prioridad del router, la cual permite determinar el router designado (DR) para la red.

Modo: Router(config-if)#

Sintaxis: **ip ospf priority** *number*

Descripción de la sintaxis:

Tabla 13. Descripción de los campos del comando show ip ospf cost

Campo	Descripción
number	Número entero que especifica la prioridad. El rango es de 0 a 255.

Fuente: Aplicación Ciscopedia v.3.0.

Ejemplo:

Figura 25. Ejemplo del comando ip ospf priority

```
R1>enable
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface fastethernet 0/0
R1(config-if)#ip ospf priority 10
R1(config-if)#
```

Fuente: Software Packet Tracer 5.2.

2.1.5.6. Diagnóstico de fallas de la configuración

La mayoría de los problemas que se producen en OSPF se relacionan con la formación de adyacencias y la sincronización de las bases de datos del estado de enlace.

Un router OSPF debe establecer una relación de vecino o de adyacencia con otro router OSPF para intercambiar la información de enrutamiento. A continuación se presentan las razones por las cuales no se establece esta relación de vecino:

- Los *Hellos* no se envían desde ambos vecinos.
- Los temporizadores de los intervalos *hello* y "muertos" no son iguales.
- Las interfaces se encuentran en tipos de red distintos.
- Las contraseñas o claves de autenticación son distintas.

En el enrutamiento OSPF también es importante asegurar lo siguiente:

- Todas las interfaces tienen las direcciones y la máscara de subred correctas.
- Las sentencias **network area** tienen las máscaras wildcard correctas.
- Las sentencias **network area** colocan a las interfaces en el área correcta.

Los comandos **show** (explicados anteriormente en *Monitoreo de OSPF*) permiten verificar la configuración de OSPF y de esta manera permiten realizar el diagnóstico de fallas de OSPF.

Adicionalmente, existen otros comandos que resultan útiles para el diagnóstico de fallas de OSPF:

Tabla 14. Descripción de comandos útiles para el diagnostico de fallas

Comando	Descripción
Clear ip route *	Despeja todas las rutas en la tabla de enrutamiento.
Clear ip route a.b.c.d.	Despeja la ruta a a.b.c.d en la tabla de enrutamiento.
Debug ip ospf events	Informa todos los eventos OSPF
Debug ip ospf adj	Informa los eventos de adyacencia OSPF

Fuente: Cisco IOS Cookbook.

2.2. PROTOCOLO EIGRP

El protocolo EIGRP (Enhanced Interior Gateway Routing Protocol) es una versión avanzada de IGRP. IGRP es un protocolo de enrutamiento por vector-distancia desarrollado por Cisco.

Algunas de las características de diseño claves de IGRP enfatizan lo siguiente:

- Versatilidad que permite manejar automáticamente topologías indefinidas y complejas

- Flexibilidad para segmentos con distintas características de ancho de banda y de retardo

- Escalabilidad para operar en redes de gran envergadura

El propósito principal en el desarrollo de EIGRP de Cisco fue crear una versión con clase de IGRP. EIGRP incluye muchas características que no se encuentran comúnmente en otros protocolos de enrutamiento vector distancia como RIP (RIPv1 y RIPv2) e IGRP.

Estas características incluyen:

- Reliable Transport Protocol (RTP)

- Actualizaciones limitadas

- Algoritmo de actualización por difusión (DUAL)

- Establecimiento de adyacencias

- Tablas de topología y de vecinos

Específicamente, EIGRP suministra una eficiencia de operación superior y combina las ventajas de los protocolos de estado de enlace con las de los protocolos de vector distancia.

A diferencia de los tradicionales protocolos de vector distancia como RIP e IGRP, EIGRP no se apoya en las actualizaciones periódicas: las actualizaciones se envían sólo cuando se produce un cambio. El enfoque de EIGRP tiene la ventaja que los recursos de la red no son consumidos por las actualizaciones periódicas.

A continuación se presenta una tabla con las ventajas y desventajas de EIGRP:

Tabla 15. Ventajas y desventajas del protocolo EIGRP

VENTAJAS	DESVENTAJAS
- Rápida convergencia: Un router que corra sobre EIGRP almacena las tablas de enrutamiento de todos sus vecinos, y de esta forma puede adaptarse rápidamente a una ruta alterna si el router principal falla. - Uso eficiente del ancho de banda, compatibilidad con VLSM y CIDR. - Soporta que la máscara de subred sea variable. Esto permite una mayor eficiencia en el uso del espacio de direcciones, comunicación entre redes con distinta configuración... - Compatibilidad para múltiples capas de red e independencia de los protocolos de enrutamiento. - No envía actualizaciones periódicas, en cambio envía actualizaciones parciales cuando el camino o la métrica cambian para una ruta; estas actualizaciones solo contienen información acerca de las rutas modificadas. - Fácil configuración.	- El protocolo EIGRP exige altos requisitos de memoria, debido a que se almacenan las tablas de topología y de enrutamiento de los vecinos, por lo que es necesaria una gran cantidad de memoria. - El algoritmo DUAL es complejo, y de un alto costo de CPU.

Fuente: http://www.slideshare.net/ecollado/bscitomo2

Los routers EIGRP mantienen información de ruta y topología a disposición en la RAM, para que puedan reaccionar rápidamente ante los

cambios. EIGRP guarda esta información en varias tablas y bases de datos.

- Tabla de vecinos
- Tabla de topología
- Tabla de enrutamiento

1. Tabla de vecinos

Cada router EIGRP mantiene una tabla de vecinos que enumera a los routers adyacentes. Esta tabla puede compararse con la base de datos de adyacencia utilizada por OSPF. Cuando se identifica un nuevo vecino se registra su dirección e interfaz y se guarda en la estructura de datos.

Cuando un vecino envía un paquete hello, publica un tiempo de espera, que es el tiempo durante el cual un router considera que un vecino se puede alcanzar y que funciona. Si un paquete hello no se recibe dentro del tiempo de espera, entonces se vence este tiempo y se informa al Algoritmo de Actualización Difusa (DUAL), que es el algoritmo de vector-distancia de EIGRP, acerca del cambio en la topología para que recalcule la nueva topología.

2. Tabla de topología

La tabla de topología está compuesta por todas las tablas de enrutamiento EIGRP en el sistema autónomo.

DUAL toma la información proporcionada en la tabla de vecinos y la tabla de topología y calcula las rutas de menor costo hacia cada

destino. EIGRP utiliza esta información para que los routers EIGRP puedan identificar y conmutar a rutas alternativas rápidamente.

La información que el router recibe de DUAL se utiliza para determinar la ruta del sucesor, que permite identificar la ruta principal o la mejor. Esta información también se introduce a la tabla de topología.

3. Tabla de enrutamiento

La tabla de enrutamiento contiene las mejores rutas hacia un destino, las cuales se aprenden de forma dinámica. Esta información se recupera de la tabla de topología.

Los campos que conforman la tabla de enrutamiento son:

- **Distancia factible (FD):** Métrica calculada más baja hacia cada destino.
- **Origen de la ruta:** Número de identificación del router que publicó esa ruta en primer lugar. Este campo se llena sólo para las rutas que se aprenden de una fuente externa a la red EIGRP.
- **Distancia informada de la ruta (RD):** Distancia informada por un vecino adyacente hacia un destino específico.
- **Información de interfaz:** Interfaz a través de la cual se puede alcanzar el destino.
- **Estado de ruta:** Una ruta puede ser pasiva (estable y lista para usar) o activa (se encuentra en el proceso de recálculo por parte de DUAL).

EIGRP maneja el concepto de sucesor, que es una ruta seleccionada como la ruta principal para alcanzar un destino. DUAL identifica esta ruta basado en la información que contienen las tablas de vecinos y de topología y la coloca en la tabla de enrutamiento.

Puede haber hasta cuatro rutas de sucesor para cada destino en particular. Éstas pueden ser de costo igual o diferente y se identifican como las mejores rutas sin bucles hacia un destino determinado. Un sucesor factible (FS) es una ruta de respaldo. Estas rutas se identifican al mismo tiempo que los sucesores, pero sólo se mantienen en la tabla de topología. Los múltiples sucesores factibles para un destino se pueden mantener en la tabla de topología, aunque no es obligatorio

2.2.1. Funcionamiento

La operación de EIGRP es completada en cinco etapas:

1. **Construir relaciones con vecinos**

   Al igual que en OSPF, las relaciones de vecinos son establecidas a través del uso de paquetes *Hello*. Un nuevo router configurado con EIGRP enviará multicast de paquetes *hello* a los routers directamente conectados. Los routers receptores responderán si el router nuevo:

   - Es configurado con EIGRP
   - Está en el mismo AS
   - Usa los mismos pesos de métrica

2. **Descubrir rutas**

Mientras se establecen las relaciones de vecinos, se presentan las siguientes acciones:

- El router nuevo envía *hellos* multicast a 224.0.0.10.
- Los routers EIGRP directamente conectados responden con un mensaje de actualización unicast que contiene todas las rutas en su tabla de enrutamiento.
- El router nuevo responde a todos los vecinos con un mensaje unicast *Ack* y coloca el contenido de las actualizaciones en su tabla topológica.
- El nuevo router envía paquetes unicast de actualización a todos los vecinos con el contenido de su tabla topológica.
- Los vecinos responden a la nueva actualización del router con un paquete Ack.

De esta forma, sus vecinos aprenden acerca de las únicas redes configuradas tales como una nueva LAN.

3. Seleccionar las mejores rutas

Después que un nuevo router ha recibido todas las actualizaciones de sus vecinos directamente conectados, éste puede calcular su DUAL -*Diffusing Update Algorithm*- el cual es un algoritmo que garantiza una operación sin bucles durante todo el cálculo de rutas, lo que permite la sincronización simultánea de todos los routers involucrados en cambio de topología. (Este algoritmo se encuentra detallado en el ANEXO B).

- La métrica para cada ruta en la tabla topológica es calculada usando la siguiente fórmula:

  *Metrica = 256[(10,000,000/min. * ancho de banda) + suma de retrasos]*

- La ruta con el más bajo costo es designada como sucesor y es ubicada en la tabla de enrutamiento.

4. Mantener las rutas

A medida que las nuevas rutas se activan o rutas antiguas se caen, EIGRP maneja rápida y eficientemente estas situaciones con poco o nada *downtime*.

Cuando se activan nuevos routers, sus paquetes hello y el proceso de actualización tiene un “efecto dominó” en la red. Todos los routers en el AS casi instantáneamente convergen en las nuevas redes del router.

Mantener rutas también significa informar a los vecinos directamente conectados cuando otro vecino deja de enviar paquetes *hello* en el intervalo requerido.

5. Eliminar las rutas

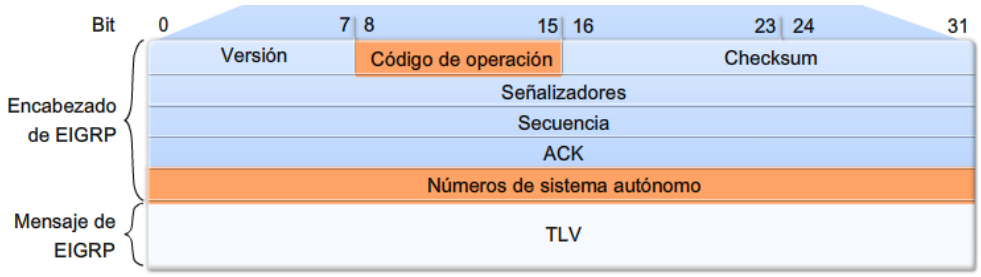
Cuando una ruta falla (un vecino directamente conectado no envía más *hellos*), entra la fase de evaluación de ruta. ¿Hay un *feasible successor* en la tabla topológica? Si es así, inmediatamente la instala, empieza el enrutamiento para la ruta alterna y actualiza los vecinos acerca de esta alternativa. Si no existe un sucesor factible, entra la fase de recálculo de ruta. Pregunta a los vecinos por una ruta alterna.

Una vez que el router ha recibido respuestas de todos los vecinos cuestionados, entonces éste puede recalcular la mejor ruta. Si una nueva alternativa es encontrada, ésta será instalada en la tabla de enrutamiento. Si no hay alternativas encontradas, la ruta antigua es eliminada.

2.2.2. Mensajes EIGRP

El formato de mensaje EIGRP incluye el encabezado y el paquete EIGRP.

Figura 26. Formatos de mensajes EIGRP.



Fuente: Aplicación Cisco CCNA Exploration 4.0

A continuación se presenta una descripción de los campos del mensaje:

- Versión: Versión del proceso EIGRP (Solo ha habido una versión)
- Código de operación: especifica el tipo de mensaje EIGRP: update, query, hello, reply
- Checksum: se aplica a todo el mensaje EIGRP, excluyendo la cabecera IP
- Señalizadores: el bit de más a la derecha es el bit de inicialización, usado en el establecimiento de relación con los vecinos.
- Secuencia: usado para enviar mensajes de manera fiable.
- ACK: usado para enviar mensajes de manera fiable.
- Número de sistema autónomo: identifica el proceso de enrutamiento EIGRP emitido en el paquete
- TLV (Tipo / Longitud / Valor): Los paquetes TLV son responsables de las futuras extensiones del protocolo EIGRP. Se destacan 3 TLVs:

- TLV Parámetros de EIGRP: Los mensajes de los parámetros EIGRP incluyen la ponderación que EIGRP utiliza para su métrica compuesta. Solo el ancho de banda y el retraso se ponderan de manera predeterminada.

- TLV IP interna: El mensaje IP interno se utiliza para publicar rutas EIGRP dentro de un sistema autónomo.

- TLV IP externa: El mensaje IP externo se utiliza cuando las rutas externas se importan en el proceso de enrutamiento EIGRP.

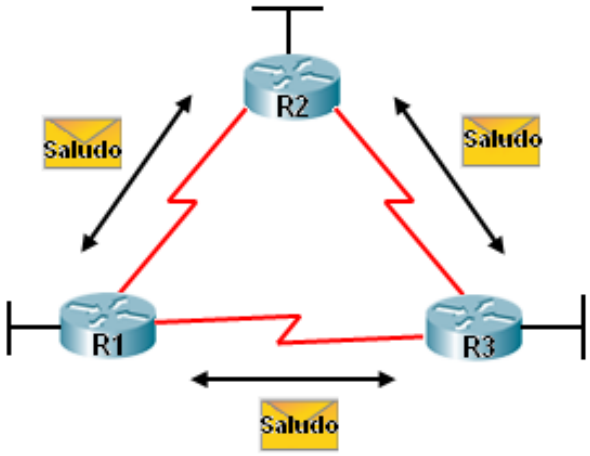
Para mantener las tablas y establecer relaciones con los routers vecinos, EIGRP maneja 5 tipos de mensajes:

1. Mensajes *"Hello"*

EIGRP utiliza los mensajes de saludo para descubrir vecinos y para formar adyacencias con ellos. Los mensajes de saludo EIGRP son multicast y utilizan una entrega no confiable.

En la mayoría de las redes, los mensajes de saludo EIGRP se envían cada 5 segundos (ancho de banda > 1.544 Mbps). En las redes de accesos múltiples sin broadcast (NBMA) y de multipunto, como X.25, Frame Relay, los Hello son unicast cada 60 segundos (ancho de banda ≤ 1.544 Mbps). Un router EIGRP supone que mientras reciba los paquetes de saludo de un vecino, el vecino y sus rutas permanecen viables.

Figura 27. Diagrama de tipo de mensaje EIGRP Hello



Fuente: Aplicación Cisco CCNA Exploration 4.0

El tiempo de espera le indica al router el tiempo máximo que debe esperar para recibir el próximo *Hello* antes de declarar al vecino como inalcanzable. De manera predeterminada, el tiempo de espera es tres veces el intervalo de saludo, o 15 segundos en la mayoría de las redes, y 180 segundos en las redes NBMA de velocidad baja. Si el tiempo de espera expira, EIGRP declarará la ruta como desactivada y DUAL buscará una nueva ruta mediante el envío de consultas.

OSPF requiere que los routers vecinos tengan los mismos intervalos *hello* e intervalos “muertos” para comunicarse. EIGRP no posee este tipo de restricción. Los routers vecinos conocen el valor de cada uno de los temporizadores respectivos de los demás mediante el intercambio de paquetes *hello*. Entonces, usan la información para forjar una relación estable aunque los temporizadores no sean iguales. Como los paquetes *hello* siempre se envían de forma no confiable no se transmite un acuse de recibo.

En las redes IP, los routers EIGRP envían *hellos* a la dirección IP multicast 224.0.0.10.

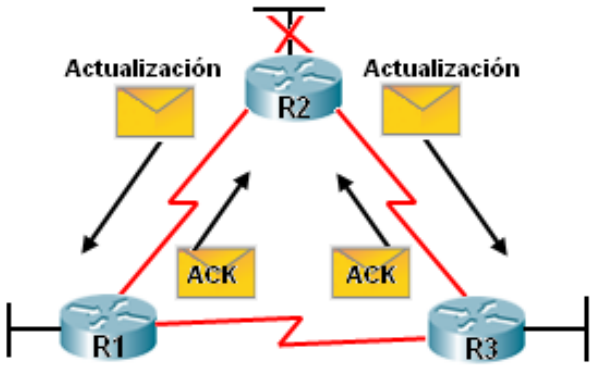
2. Mensajes Ack (Acuse de recibo) y Update (Actualización)

Los mensajes de acuse de recibo (Ack) se envían a través de EIGRP cuando se utiliza una entrega confiable. RTP utiliza una entrega confiable para los mensajes EIGRP de actualización, consulta y respuesta. Los mensajes de acuse de recibo EIGRP siempre se envían como unicast no confiable.

Los mensajes de actualización (Update) se utilizan para propagar la información de enrutamiento. Los mensajes de actualización se envían sólo cuando es necesario. Las actualizaciones de EIGRP sólo contienen la información de enrutamiento necesaria y sólo se envían a los routers que la requieren. Los mensajes de actualización EIGRP utilizan una entrega confiable. Los mensajes de actualización se envían como multicast cuando son requeridos por múltiples routers, o como unicast cuando son requeridos por sólo un router. En la figura anterior, debido a que los enlaces son punto a punto, las actualizaciones se envían como unicast.

De acuerdo a la figura anterior, R2 ha perdido la conectividad con la LAN conectada a su interfaz FastEthernet. R2 envía inmediatamente una actualización a R1 y R3 cuando determina que la ruta se encuentra caída. R1 y R3 responden con un acuse de recibo

Figura 28. Diagrama de tipo de mensaje EIGRP Ack y Update



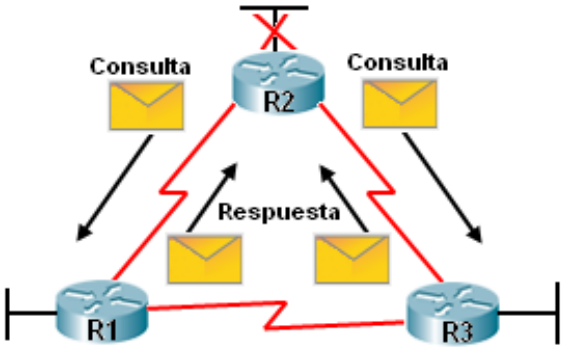
Fuente: Aplicación Cisco CCNA Exploration 4.0.

3. Mensajes Query (Consulta) y Reply (Respuesta)

Los mensajes de consulta (Query) y respuesta (Reply) son utilizados por DUAL cuando busca redes y otras tareas. Los paquetes de consulta y respuesta utilizan una entrega confiable. Las consultas utilizan multicast o unicast, mientras que las respuestas se envían siempre como unicast.

Los mensajes de actualización se utilizan cuando un router detecta un nuevo vecino. Los routers EIGRP envían paquetes de actualización en unicast a ese nuevo vecino para que pueda aumentar su tabla de topología. Es posible que se necesite más de un mensaje de actualización para transmitir toda la información de topología al vecino recientemente detectado. Los mensajes de actualización también se utilizan cuando un router detecta un cambio en la topología. En este caso, el router EIGRP envía un mensaje de actualización en multicast a todos los vecinos, avisándolos del cambio.

Figura 29. Diagrama de tipo de mensaje EIGRP Query y reply



Fuente: Aplicación Cisco CCNA Exploration 4.0.

Un router EIGRP usa mensajes de consulta siempre que necesite información específica de uno o de todos sus vecinos. Se usa un mensaje de respuesta para contestar a una consulta.

En la figura anterior, R2 ha perdido la conectividad con LAN y envía consultas a todos los vecinos EIGRP y busca cualquier ruta posible hacia la LAN. Como las consultas utilizan una entrega confiable, el router receptor debe devolver un acuse de recibo EIGRP. (Para que el ejemplo sea simple, se omitieron los acuses de recibo en el gráfico.)

Todos los vecinos deben enviar una respuesta sin importar si tienen o no una ruta hacia la red caída. Como las respuestas también utilizan una entrega confiable, los routers como R2, deben enviar un acuse de recibo.

2.2.3. Configuración del protocolo EIGRP

Los comandos de configuración de EIGRP varían según el protocolo que debe enrutarse. Algunos de estos protocolos son IP, IPX y AppleTalk. A continuación se describe la configuración de EIGRP para el protocolo IP.

2.2.3.1. Activación del protocolo EIGRP

Habilitar el protocolo de enrutamiento EIGRP, definiendo el sistema autónomo al cual pertenece. El comando para habilitarlo es:

Router (Config)# **Router EIGRP** autonomous system number

Donde Autonomous system number corresponde al sistema autónomo en el cual trabajará EIGRP, el sistema autónomo indica cuales son los routers que trabajan bajo una misma administración y dentro de éste se encuentran los protocolos de gateway interior.

2.2.3.2. Asignación de redes para EIGRP

Indicar cuáles son las redes que trabajan en el sistema autónomo definido para EIGRP. El comando para habilitarlo es:

Router (Config-Router)# **Network** network number

Donde Network number es el número de red que determina cuáles son las interfaces del router que participan en EIGRP y cuáles son las redes publicadas por el router. El comando **network** configura sólo las redes conectadas.

Es necesario considerar la interfaz a utilizar para interconectar los routers y de esta forma poder seleccionar el bandwidth (ancho de banda) idóneo para su óptimo funcionamiento, puesto que si el ancho de banda de estas interfaces no se modifica, EIGRP supone el ancho de banda por defecto en el enlace en lugar del verdadero ancho de banda, lo que puede traer como consecuencia que:

- Si el enlace es más lento, el router puede no ser capaz de converger.
- Las actualizaciones de enrutamiento se pueden perder.

- se produzca una selección de rutas por debajo de la óptima.

2.2.3.3. Definición de ancho de banda para las interfaces

Definir un ancho de banda para el enlace con el propósito de enviar tráfico de actualización de enrutamiento sobre el enlace. El comando para habilitarlo es el siguiente:

Router (config-if)# **bandwidth** kilobits

Donde kilobits corresponde al ancho de banda deseado en kilobits por segundo. En el caso de disponer de una interfaz serial (ya sea PPP o HDLC) seleccionar el ancho de banda especificado para la línea.

2.2.3.4. Activación del registro de cambios

Habilitar el registro de los cambios de adyacencia de vecinos para monitorear la estabilidad del sistema de enrutamiento y para ayudar a detectar problemas (opcional, recomendado por Cisco para todas las configuraciones EIGRP):

router(config-router)#**eigrp log-neighbor-changes**

2.2.4. Monitoreo de EIGRP

Los comandos show y debug a menudo son utilizados para analizar la configuración de EIGRP y monitorear su desempeño.

Comando "show ip eigrp neighbors"

Descripción: Muestra los vecinos detectados por EIGRP e identifica la última vez que se reinició un vecino. También es útil para depurar ciertos tipos de problemas de tráfico.

Modo: Router>

Sintaxis: **show ip eigrp neighbors** [interface-type|as-number|static]

Descripción de la Sintaxis:

Tabla 16. Descripción de la sintaxis de show ip eigrp neighbors

Campo	Descripción
interface-type	Tipo de interfaz (Opcional)
as-number	Número del sistema autónomo (Opcional)
static	Rutas estáticas(Opcional)

Fuente: Aplicación Ciscopedia v.3.0.

Ejemplo:

Figura 30. Ejemplo del comando show ip eigrp neighbors

```
R1#
R1#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address         Interface       Hold Uptime    SRTT   RTO   Q   Seq
                                    (sec)          (ms)       Cnt Num
0   10.1.100.2      Fa0/0           11   01:18:26  40     1000  0   6
1   10.1.100.3      Fa0/0           11   00:06:56  40     1000  0   6
```

Fuente: Software Packet Tracer 5.2.

Descripción de los campos:

Tabla 17. Descripción de los campos de show ip eigrp neighbors

Campo	Descripción
process 1	Número del sistema autónomo especificado en la configuración del router (este valor puede variar de 1 a 65535).
Address	Dirección IP del vecino EIGRP directamente conectado.
Interface	Interfaz en la cual el router está recibiendo paquetes hello del vecino EIGRP.
Holdtime	Longitud de tiempo (en segundos) que el software Cisco IOS (Internetwork Operating System) esperará para escuchar del vecino EIGRP antes de declararlo “abajo” (down). Si el vecino EIGRP está usando holdtime por defecto, este número será menor de15. Si por el contrario configura un holdtime con un valor diferente, éste valor se mostrará en pantalla.
Uptime	Tiempo que ha transcurrido (en horas: minutos: segundos) desde que el router local escuchó a su vecino.
SRTT	Smooth Round-Trip Time. Tiempo requerido (en milisegundos) para que un paquete EIGRP sea enviado a un

	vecino y reciba una respuesta de éste.
RTO	Retransmission TimeOut: Tiempo de espera de retransmisión (en milisegundos), es la cantidad de tiempo que espera el software antes de reenviar un paquete desde la cola de retransmisión a un vecino.
Q Count	Número de paquetes EIGRP (Update, Query, y Reply) que el software espera enviar.
Seq Num	Número de secuencia del último paquete Update, Query o Reply que fue recibido por su vecino.

Fuente: Aplicación Ciscopedia v.3.0.

Comando "show ip eigrp topology"

Descripción: Muestra la tabla de topología, el estado de las rutas (activo o pasivo), la cantidad de sucesores y la distancia factible al destino.

Modo: Router#

Sintaxis: **show ip eigrp topology** [*autonomous-system-number* | [[*ip-address*] *mask*]]

Descripción de la Sintaxis:

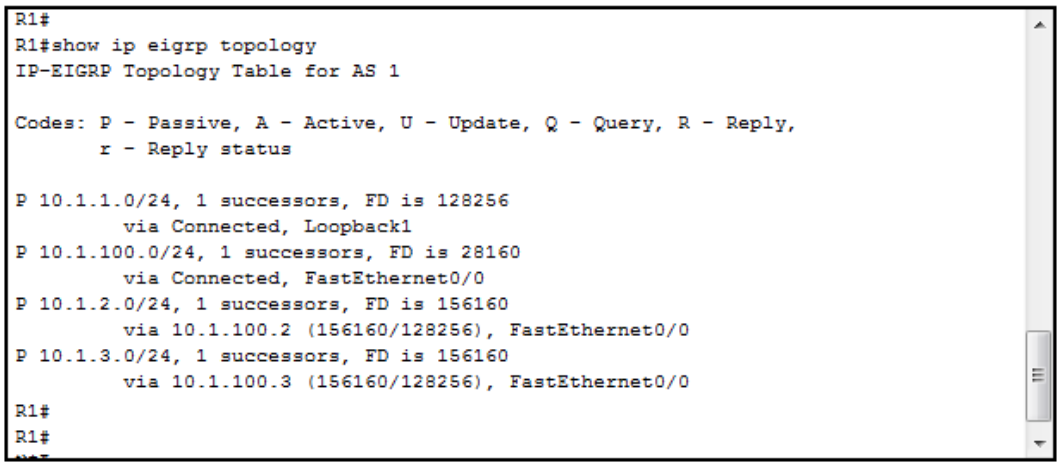
Tabla 18. Descripción de la sintaxis de show ip eigrp topology

Campo	Descripción
Autonomous-system-number	Número de sistema autónomo (Opcional).
ip-address	Dirección IP. Cuando se especifica una máscara se provee una descripción detallada de la entrada. (Opcional)
mask	Máscara de subred (Opcional) .
active	Muestra solo las entradas activas en la tabla de topología EIGRP (Opcional).
All-links	Muestra todas las entradas en la tabla de topología EIGRP (Opcional).
pending	Muestra todas las entradas en la tabla de topología que están esperando a ser actualizadas por un vecino o para responderle a éste.(Opcional).
summary	Muestra un resumen de la tabla de topología EIGRP (Opcional).
zero-successors	Muestra las rutas disponibles en la tabla de topología EIGRP.

Fuente: Aplicación Ciscopedia v.3.0.

Ejemplo:

Figura 31. Ejemplo del comando show ip eigrp topology



Fuente: Software Packet Tracer 5.2.

Descripción de los campos:

Tabla 19. Descripción de los campo de show ip eigrp topology

Campo	Descripción
Codes	Estado de la entrada en la tabla de topología. *Passive* y *Active* hacen referencia al estado EIGRP respecto al destino. *Update, Query* y *Reply* se refiere al tipo de paquetes que están siendo enviados.
P - Passive	No se están realizando cálculos EIGRP para el destino.
A - Active	Se están realizando cálculos EIGRP para el destino.

U - Update	Indica que un paquete Update fue enviado al destino.
Q - Query	Indica que un paquete Query fue enviado al destino..
R - Reply	Indica que un paquete Reply fue enviado al destino.
r - Reply status	Bandera que se establece después de que el software ha enviado una consulta y está esperando una respuesta.
10.1.1.0/24	Número IP de la red destino
successors	Número de sucesores en la tabla de direccionamiento IP. Si la palabra “successors” aparece en mayúscula, entonces la ruta o el siguiente salto está en un estado de transición.
FD	Feasible Distance. La distancia factible es la métrica más baja para alcanzar el destino o la mejor métrica conocida cuando la ruta se puso activa. Este valor es usado en el chequeo de la condición de factibilidad.
via	Dirección IP del vecino EIGRP directamente conectado que informó al software acerca del destino. Pueden existir varias *via* a la misma red destino.
(156160/128256)	El primer número es la métrica EIGRP que representa el costo al destino. El Segundo número es la métrica EIGRP que el vecino EIGRP directamente conectado publicó.

Ethernet0	Interfaz desde la cual se obtuvo esta información.

Fuente: Aplicación Ciscopedia v.3.0.

Comando "show ip route EIGRP"

Descripción: Muestra las entradas EIGRP actuales en la tabla de enrutamiento

Modo: router#

Sintaxis: **show ip route** [*address* [*mask*] [**longer-prefixes**]] | [*protocol* [*process-id*]] | [**list** *access-list-number* | *access-list-name*]

Descripción de la Sintaxis:

Tabla 20. Descripción de la sintaxis del comando show ip route eigrp

Campo	Descripción
address	Dirección de enrutamiento que debe mostrar(Opcional)
mask	Mascara de red(Opcional)
longer-prefixes	La dirección y la mascara se convierten en un prefijo y cualquiera de las rutas que coinciden con el prefijo son desplegadas (opcional).
protocol	Nombre del protocolo de enrutamiento, palabra clave o resumen. Si se especifica un protocolo de enrutamiento utilice una de las siguientes palabras clave: bgp, egp, eigrp, hello, igrp, isis, ospf, or rip. (opcional).

process-id	Número utilizado para identificar un proceso de un protocolo especifico (opcional).
list	La palabra clave de la lista que es requerida para filtrar una salida Para acceder a un nombre o número de la lista (opcional)
access-list-name	Filtra la salida desplegada por la tabla de enrutamiento basado en el nombre de la lista de acceso específicada (opcional).
access-list-number	Filtra la salida desplegada por la tabla de enrutamiento basado en el número de la lista acceso específicada (opcional).

Fuente: Cisco IOS Cookbook.

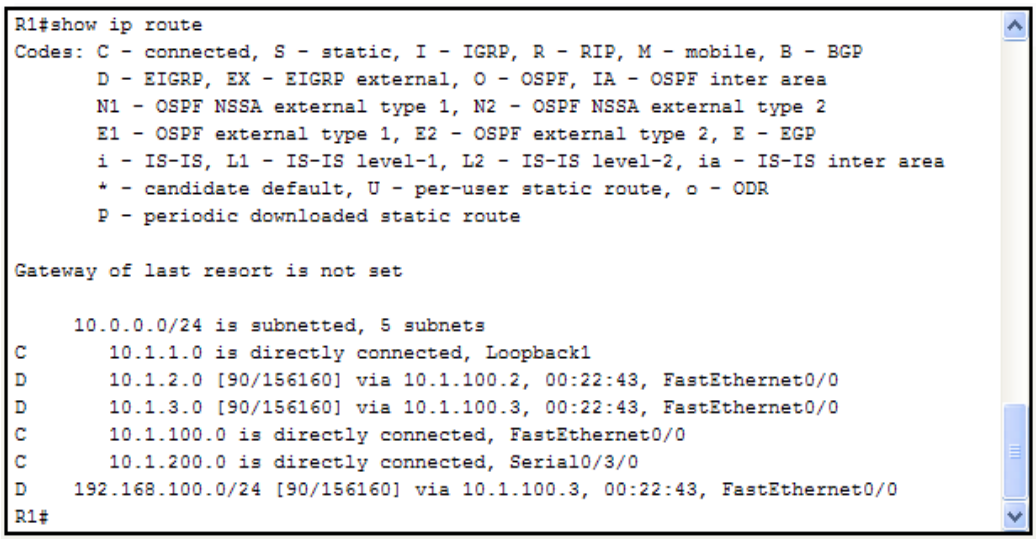
Ejemplos:

Figura 32. Ejemplo del comando show ip route eigrp

```
R1#show ip route eigrp
     10.0.0.0/24 is subnetted, 5 subnets
D       10.1.2.0 [90/156160] via 10.1.100.2, 00:15:21, FastEthernet0/0
D       10.1.3.0 [90/156160] via 10.1.100.3, 00:15:21, FastEthernet0/0
D    192.168.100.0/24 [90/156160] via 10.1.100.3, 00:15:21, FastEthernet0/0
R1#
```

Fuente: Software Packet Tracer 5.2.

Figura 33. Ejemplo del comando show ip route



Fuente: Software Packet Tracer 5.2.

show ip eigrp traffic

Descripción: Muestra el número de paquetes EIGRP enviados y recibidos, así como las estadísticas de *Hello*, actualizaciones, consultas respuestas y acuses de recibo.

Modo: router#

Sintaxis: **show ip eigrp traffic** [*as-number*]

Descripción de la Sintaxis:

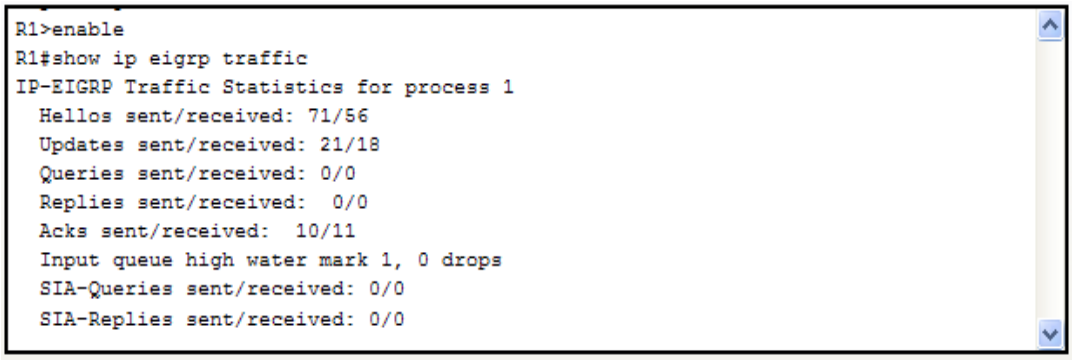
Tabla 21. Descripción de la sintaxis del comando show ip eigrp traffic

Campo	Descripción
as-number	Número del sistema Autónomo (Opcional).

Fuente: Cisco IOS Cookbook.

Ejemplo:

Figura 34. Ejemplo del comando show ip eigrp traffic



Fuente: Software Packet Tracer 5.2.

Descripción de los campos:

Tabla 22. Descripción de los campos del comando show ip eigrp traffic

Campo	Descripción
process 1	Número del sistema autónomo especificado en la configuración del router (este valor puede variar de 1 a 65535).
Hellos sent/received	Número de paquetes Hello enviados y recibidos.
Updates sent/received	Número de paquetes Update enviados y recibidos.
Queries sent/received	Número de paquetes Query enviados y recibidos.
Replies sent/received	Número de paquetes Reply enviados y recibidos.

Acks sent/received	Número de paquetes Ack enviados y recibidos.

Fuente: Aplicación Ciscopedia v.3.0.

Comando "Debug eigrp "

Descripción: Muestra información sobre los paquetes de protocolo EIGRP ampliado, permite analizar los paquetes enviados y recibidos en una interfaz. Este comando sólo debe usarse cuando el tráfico de red es liviano, debido a la magnitud del resultado que genera. Este comando también puede usarse para solucionar problemas o supervisar los procesos Eigrp activos.

Modo: Router#

Sintaxis: **debug ip eigrp** {fsm | neighbors | packet}

no debug eigrp {fsm | neighbors [static] | packet}

Descripción de la Sintaxis:

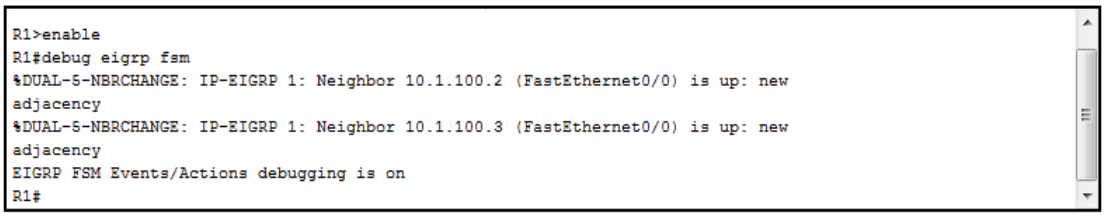
Tabla 23. Descripción de la sintaxis del comando debug eigrp

Campo	Descripción
fsm	Muestra la información EIGRP de depuración sobre la métrica del sucesor factible (FSM).
neighbors	Muestra los vecinos descubiertos por EIGRP.
packet	Muestra la información general de depuración, incluyendo los paquetes transmitidos y recibidos.

Fuente: Aplicación Ciscopedia v.3.0.

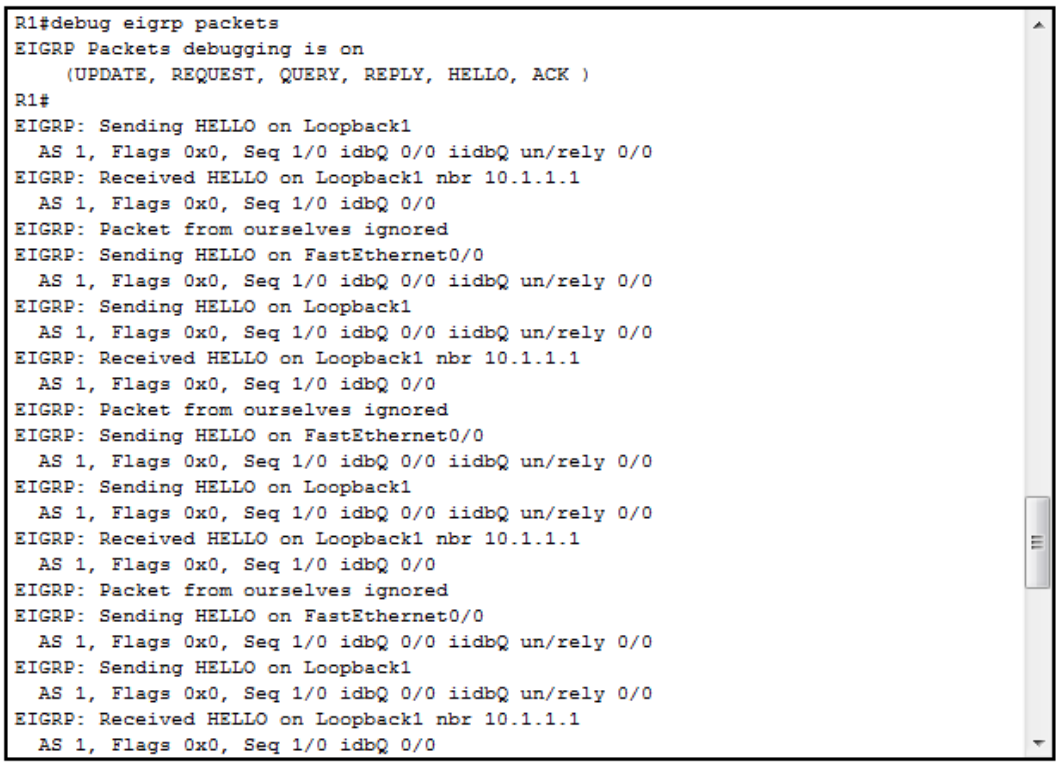
Ejemplos:

Figura 35. Ejemplo del comando debug ip eigrp fsm



Fuente: Software Packet Tracer 5.2.

Figura 36. Ejemplo del comando debug eigrp packets



Fuente: Software Packet Tracer 5.2.

Comando "Show ip interface brief"

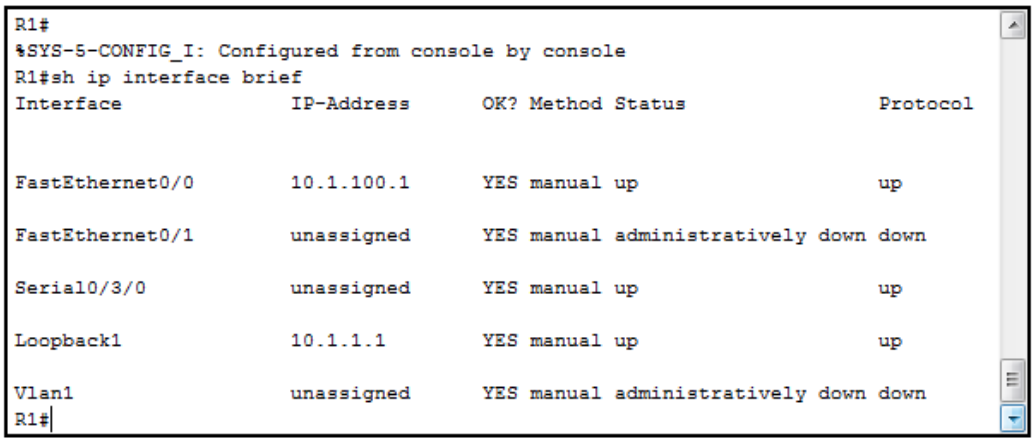
Descripción: Muestra un breve resumen de la información y el estado de una dirección IP.

Modo: Router>

Sintaxis: **show ip interface brief**

Ejemplo:

Figura 37. Ejemplo del comando show ip interface brief



Fuente: Software Packet Tracer 5.2.

Descripción de los campos:

Tabla 24. Descripción de los campos de show ip interface brief

Campo	Descripción
Interface	Tipo de interface.
Ip-Address	Dirección IP asignada a la interfaz
OK?	"YES" significa que la dirección IP es actualmente válida. "NO" significa que la dirección IP no es

	actualmente válida.
Method	Este campo puede tener los siguientes valores: • RARP o SLARP – Reverse Address Resolution Protocol o Serial Line Address Resolution protocol • BOOTP: Protocolo Bootstrap • TFTP: Archivo de configuración obtenido desde el servidor TFTP. • Manual: Manualmente cambiado con el CLI (Command Line Interface). • NVRAM: Configuración de archivo en NVRAM. • IPCP: Internet Protocol Control Protocol • DHCP: Comando dedirección IP DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol) • Unassigned: No tiene dirección IP asignada • Unset • Other – Desconocido
Status	Indica el estado de la interfaz. Puede tomar los siguientes valores: • Up : La interfaz está arriba • Down: La interfaz está abajo • Administratively down: La interfaz
Protocol	Indica el estado operacional del protocol de enrutamiento en la interfaz.

Fuente: Aplicación Ciscopedia v.3.0.

Comando "Show ip eigrp interfaces"

Descripción: Muestra información sobre las interfaces configuradas por EIGRP, estadísticas e información de estado.

Modo: Router>

Sintaxis: **show ip eigrp interfaces** [interface-type interface-number] [as-number]

Descripción de la Sintaxis:

Tabla 25. Descripción de la sintaxis de show ip eigrp interfaces

Campo	Descripción
interface-type:	Tipo de interfaz (Opcional)
interface-number	Muestra la tabla de topología EIGRP
as-number	Número de la interfaz (Opcional)

Fuente: Aplicación Ciscopedia v.3.0.

Ejemplo:

Figura 38. Ejemplo del comando show ip eigrp interfaces

```
R1#show ip eigrp interfaces
IP-EIGRP interfaces for process 1

                      Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface        Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Fa0/0              0        0/0      1236       0/10          0           0
Lo1                0        0/0      1236       0/10          0           0
R1#
```

Fuente: Software Packet Tracer 5.2.

Descripción de los campos:

Tabla 26. Descripción de los campos de show ip eigrp interfaces

Campo	Descripción
Interface	Interfaz sobre la cual se configuró EIGRP.
Peers	Número de vecinos directamente conectados
Xmit Queue Un/Reliable	Número de paquetes restantes en las colas de transmisión confiables y no confiables.
Mean SRTT	Intervalo (en milisegundos) Mean Smooth Round-Trip Time (SRTT)
Pacing Time Un/Reliable	Sincronización utilizada para determinar cuando los paquetes EIGRP deberían ser enviados a la interfaz (paquetes confiables y no confiables).
Multicast Flow Timer	Número máximo de segundos en los cuales el router enviará paquetes EIGRP multicast.
Pending Routes	Número de rutas en los paquetes situados en la cola de transmisión que esperan ser enviados.

Fuente: Aplicación Ciscopedia v.3.0.

Comando "Show interfaces"

Descripción: Muestra estadísticas para todas las interfaces configuradas en el router o servidor de acceso. La salida que se obtiene depende de la red para la cual se ha configurado la interfaz.

Para limitar la cantidad de información que se presenta se usa la opción **summary.**

Modo: Router>
Router#

Sintaxis: **show interfaces** {*type number*}

Descripción de la Sintaxis:

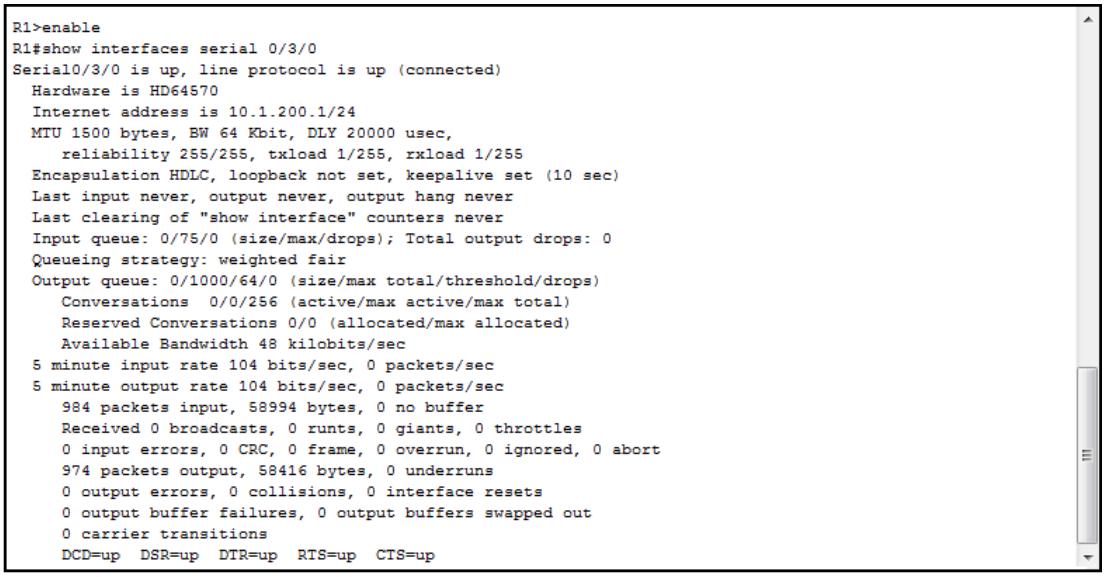
Tabla 27. Descripción de la sintaxis del comando show interfaces

Campo	Descripción
type	Tipo de interfaz a ser configurada
number	Representa un Puerto, conector o número de la interfaz.

Fuente: Aplicación Ciscopedia v.3.0.

Ejemplo:

Figura 39. Ejemplo del comando show interfaces



Fuente: Software Packet Tracer 5.2.

Descripción de los campos:

Tabla 28. Descripción de los campos del comando show interfaces

Campo	Descripción
Serial... is {up | down} ...is administratively down	Indica si la Interfaz hardware está actualmente activa o si ha sido bajada por un administrador.
line protocol is {up | down}	Indica si los procesos software que manejan la línea de protocolos esta activa o ha sido bajada por un administrador.
Hardware is	Especifica el tipo de hardware.

Internet address is	Especifica la dirección de internet y la máscara de subred de la interfaz actual.
MTU	Unidad máxima de transmisión de la interfaz.
BW	Indica el valor del parámetro del ancho de banda que ha sido configurado para la interfaz(en Kilobits/Segundos). El parámetro de ancho de banda es usado para calcular la métrica EIGRP.
DLY	Retardo de la interfaz(en microsegundos).
rely	Fiabilidad de la interfaz, se expresa como una fracción de 255(255/255 es 100 % fiable).
load	Carga de la interfaz, se expresa como una fracción de 255(255/255 está completamente saturada).
Encapsulation	Método de encapsulación asignado a la interfaz.
loopback	Indica si el loopback se estableció o no.
keepalive	Indica si el keepalive se estableció o no.
Last input	Número de horas, minutos y segundos desde que el último paquete se recibió satisfactoriamente por una interfaz.
output	Número de horas, minutos y segundos desde que el último paquete se transmitió satisfactoriamente por una interfaz.
output hang	Número de horas, minutos y segundos desde que

	la interfaz fue reseteada por última vez debido a una transmisión que tomó demasiado tiempo.Cuando el número de horas es mayor de 24, no se muestran las horas, minutos, sino días, si el contador se desborda se muestran asteriscos(*).
Output queue, drops input queue, drops	Número de paquetes en la cola de salida y de entrada. Cada número es seguido por un "/", el tamaño máximo de la cola y el número de paquetes perdidos debido a que la cola está *Full.*
5 minute input rate 5 minute output rate	Promedio de bits y paquetes transmitidos por Segundo en los últimos 5 minutos. Las tasas de de entrada y salida de 5 minutos debería ser usadas sólo como una aproximación del tráfico por segundo durante un periodo dado de 5 minutos.
packets input	Número total de paquetes libres de errores recibidos por el sistema.
bytes	Número total de bytes, incluyendo datos y encapsulación MAC en los paquetes libres de errores recibidos por el sistema.
no buffer	Número de paquetes recibidos descartados debido a la falta de espacio en el buffer en el sistema principal.
Received... broadcasts	Número total de paquetes broadcast o multicast recibidos por la interfaz.

runts	Número de paquetes que son descartados debido a que son más pequeños que el tamaño mínimo establecido de un paquete.
giants	Número de paquetes que son descartados debido a que exceden al tamaño máximo establecido de un paquete.
input errors	Número total de: *no buffer, runts, giants, CRCs, frame, overrun*, *ignored,* y *abort counts*. Otras entradas relacionadas con errors pueden incrementar este contador. Por esta razón la suma podría diferir con los otros contadores.
CRC	*Cyclic redundancy checksum:* Suma de control de redundancia ciclica generada por la estación origen o el dispositivo final cuando la suma de comprobación calculada no coincide con los datos recibidos. En un enlace serial, CRC usualmente indica ruido, u otros problemas de transmisión en el enlace de datos.
frame	Número de paquetes recibidos incorrectamente que tienen un error CRC y un número no entero de octetos. En una línea serial este número sería el resultado de ruido u otros problemas de transmisión.
overrun	Número de veces que el equipo receptor no pudo entregar los datos recibidos a un búfer de hardware porque la tasa de entrada supera la capacidad del receptor para manejar los datos.

ignored	Número de paquetes recibidos ignorados por la interfaz. Algunos factores como el ruido pueden incrementar este contador.
abort	Secuencia de bits en una interfaz serial que usualmente indica un problema de temporización entre la interfaz serial y el enlace de datos.
carrier transitions	Número de veces que la portadora detecta que una interfaz serial ha cambiado de estado. Si el DCD(Data Carrier Detect) se baja y luego se sube el contador de la portadora se incrementará dos veces. Si DCD cambia a menudo indica que puede haber problemas de modem o de línea.
packets output	Número total de mensajes transmitidos por el sistema.
bytes output	Número total de bytes transmitidos por el sistema.
underruns	Número de veces en las que el transmisor trabajó a una velocidad mayor de la que el router podía manejar.
output errors	Suma de todos los errores que impidieron la ultima transmisión de datagramas de la interfaz examinada. En algunas ocasiones esta suma no va a coincidir con la suma de errores de salida enumerados, ya que algunos datagramas pueden tener más de un error, y otros pueden tener errores que no se encuentran en ninguna de las categorías especificadas.

collisions	Número de mensajes retransmitidos debido a una colisión de Ethernet. Algunas colisiones son normales. Sin embargo si la tasa de colisión aumenta en un 4 o 5%, se debe verificar que el equipo no este defectuoso. Un paquete que colisiona se cuenta sólo una vez en los paquetes de salida.
interface resets	Número de veces que una interfaz ha sido completamente reiniciada. Esto ocurre si los paquetes en la cola de transmisión no fueron enviados en un plazo de varios segundos. En una línea serial puede ser causado por un mal funcionamiento del MODEM que no suministra la transmisión de la señal de reloj o por un problema de cable. Si el sistema notifica que la portadora detectada en una interfaz serial esta arriba, pero la línea de protocolo esta abajo, se resetea periódicamente la interfaz en un esfuerzo por reiniciarla.
restarts	Número de veces que el controlador de reinició debido a los errores.
alarm indications, remote alarms, rx LOF, rx LOS	Número de alarmas CSU/DSU, y número de ocurrencias de pérdidas en la recepción de frames y pérdida de la señal recibida.

Fuente: Aplicación Ciscopedia v.3.0.

Comando "Traceroute"

Descripción: Este comando registra la fuente de cada *mensaje ICMP Time Exceeded*, con el fin de proporcionar una ruta sobre el camino que el paquete tomó para alcanzar el destino.

Modo: Router#

Sintaxis: traceroute

Descripción de la Sintaxis:

Tabla 29. Descripción de la sintaxis del comando traceroute

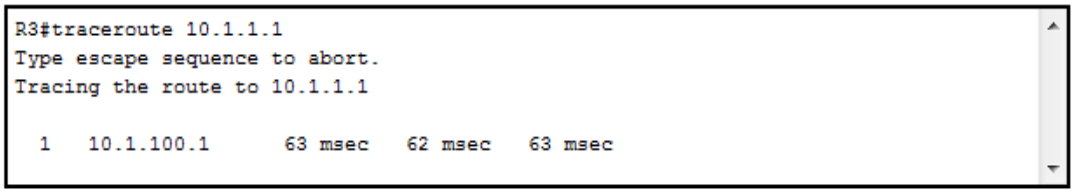
Campo	Descripción
Protocol [ip]:	Protocolo soportado. Se puede elegir entre appletalk, clns, ip, novell, apollo, vines, decnet, or xns. El protocolo por defecto es IP.
Target IP address:	Se debe ingresar un nombre de host o una dirección IP. No hay ningún valor por defecto.
Source address:	La interfaz o dirección IP del router utilizada como la dirección fuente a examinar. El router normalmente escoge la dirección IP de la interfaz de salida.
Numeric display [n]:	Por defecto muestra ambos valores simbólico y numérico; sin embargo se puede suprimir el valor simbólico.
Timeout in	Número de segundos que espera para una respuesta

seconds [3]:	a un paquete examinado. El valor por defecto es de 3 segundos.
Probe count [3]:	El número de sondeos que son enviados para cada nivel TTL. El valor por defecto es de 3.
Minimum Time to Live [1]:	El mínimo valor TTL para los primeros sondeos. El valor por defecto es 1, pero se puede fijar un valor más alto para suprimir el despliegue de saltos conocidos.
Maximum Time to Live [30]:	El máximo valor TTL que puede ser usado. Su valor por defecto es de 30. El comando **traceroute** termina cuando el destino es alcanzado o cuando se alcanza este valor**.**
Port Number [33434]:	El puerto de destino usado por los mensajes UDP examinados, el valor por defecto es 33434.
Loose, Strict, Record, Timestamp, Verbose[none]:	Opciones de la cabecera IP. Se puede especificar cualquier combinación. El comando **traceroute** muestra los campos requeridos y coloca las opciones requeridas para cada sondeo; sin embargo no hay garantía que todos los routers (o nodos finales) procesarán estas opciones.

Fuente: Aplicación Ciscopedia v.3.0.

Ejemplo:

Figura 40. Ejemplo del comando traceroute



Fuente: Software Packet Tracer 5.2.

Comando "Ping"

Descripción: el comando **ping** (packet internet groper) es usado para diagnosticar conectividad en una red básica en Apollo, AppleTalk, CLNS(Connectionless Network Service),DECnet, IP, Novell, IPX, VINES o redes XNS. El argumento opcional del protocolo puede ser cualquiera de los siguientes: Apollo, AppleTalk, CLNS, DECnet, IP, IPX, VINES, or XNS. Para ejecutar un **ping** extendido, ingrese el comando **ping** sin los argumentos.

Modo: Router>
Router#

Sintaxis: **ping** [*protocol*] {*ip-address* | *hostname*}

Descripción de la Sintaxis:

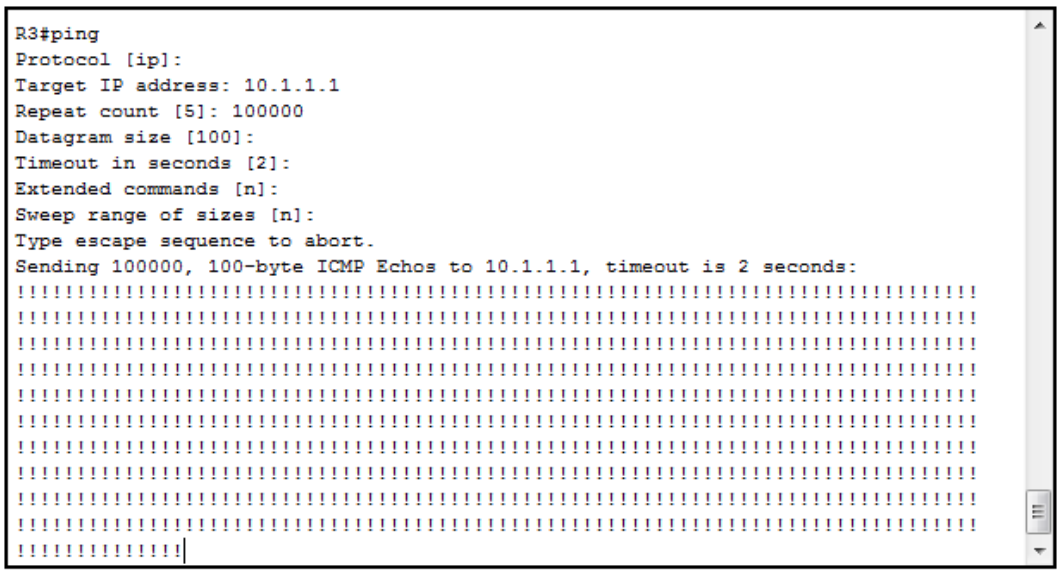
Tabla 30. Descripción de la sintaxis del comando ping

Campo	Descripción
protocol	El protocolo puede ser cualquiera de los siguientes: Apollo, AppleTalk, CLNS, DECnet, IP, IPX, VINES, or XNS. Su protocolo por defecto es IP.
Ip-address | *hostname*	Dirección de la red a la cual se desea comprobar si tiene conectividad.

Fuente: Aplicación Ciscopedia v.3.0.

Ejemplo:

Figura 41. Ejemplo del comando ping



Fuente: Software Packet Tracer 5.2.

2.2.5. Comandos útiles en la configuración de EIGRP

Comando "router eigrp"

Descripción: Se utiliza para configurar el proceso de enrutamiento EIGRP. Para bajar (shutdown) un proceso de enrutamiento se usa el comando **no router eigrp.**

Modo: Router(config)#

Sintaxis: **router eigrp** *autonomous-system*

no router eigrp *autonomous-system*

Descripción de la Sintaxis:

Tabla 31. Descripción de la sintaxis del comando router eigrp

Campo	Descripción
autonomous-system	Número de sistema autónomo que identifica las rutas a los otros routers EIGRP. También es usado para etiquetar la información de enrutamiento.

Fuente: Cisco IOS Cookbook.

Ejemplo:

R1(config)#router eigrp 1

Comando "Network (EIGRP)"

Descripción: Indica las redes que pertenecen al sistema autónomo EIGRP en el router local. El comando **network** configura sólo las redes conectadas.

Modo: Router(config-router)#

Sintaxis: **network** *network-number* [*network-mask*]

no network *network-number* [*network-mask*]

Descripción de la Sintaxis:

Tabla 32. Descripción de la sintaxis del comando network

Campo	Descripción
network-number	Número de red que determina cuáles son las interfaces del router que participan en EIGRP y cuáles son las redes publicadas por el router.
network-mask	Máscara de red (Opcional)

Fuente: Cisco IOS Cookbook.

Ejemplo:

El siguiente ejemplo configura un router para EIGRP y aisgna 1 como número de sistema autónomo. El comando **network** indica la red que está directamente conectada al router:

Router(config)#**router eigrp** *1*

Router(config-router)#**network** *10.0.0.0*

Comando "Bandwidth"

Descripción: Se utiliza para establecer el ancho de banda de una interfaz.

Modo: Router(config-if)#

Sintaxis: **bandwidth** *kilobits*

no bandwidth

Descripción de la Sintaxis:

Tabla 33. Descripción de la sintaxis del comando bandwith

Campo	Descripción
kilobits	Ancho de banda en kilobits/segundo

Fuente: Cisco IOS Cookbook.

Ejemplo:

Router(config)#**interface serial** *0/3/0*

Router(config-if)#**bandwidth** *64*

2.2.6. Diagnóstico de fallas de la configuración

Para el diagnóstico de fallas de EIGRP se debe tener en cuenta:

1. Habilitar el proceso de enrutamiento EIGRP. Para intercambiar actualizaciones de enrutamiento, cada router en la red EIGRP se debe configurar con el mismo número de sistema autónomo:

   router(config)#**router eigrp** *autonomous-system-number*

2. Habilitar las interfaces para que participen en el proceso de actualización de EIGRP:

   router(config-router)#**network** *network-number*

3. Verificar la configuración de EIGRP con los comandos:

   router# **show running-configuration**

   router# **show ip protocols**

El funcionamiento incorrecto de EIGRP puede ser causado por:

- Problemas de conectividad de Capa 1 o Capa 2.
- Los números de sistema autónomo en los routers EIGRP no coinciden.
- El enlace está congestionado o inhabilitado.
- La interfaz de salida está desactivada.
- La interfaz de red publicada está desactivada.
- El autoresumen está habilitado en routers con subredes que no son contiguas. Para desactivarlo se utiliza el comando **no auto-summary**

Para controlar y diagnosticar las fallas de una red EIGRP, se utilizan los siguientes comandos:

- router# **show ip eigrp neighbors**: Muestra los vecinos detectados por EIGRP e identifica la última vez que se reinició un vecino.

- router# **show ip eigrp topology** : Muestra la tabla de topología, el estado de las rutas (activo o pasivo), la cantidad de sucesores y la distancia factible al destino.

- router# **show ip route eigrp**: Muestra las entradas EIGRP actuales en la tabla de enrutamiento

- router# **show ip protocols**: Muestra los parámetros y el estado actual del proceso de protocolo de enrutamiento activo adicionalmente muestra el número de sistema autonómo EIGRP, el filtrado, los números de redistribución, los vecinos y la información de distancia.

- router# **show ip eigrp traffic**: Muestra el número de paquetes EIGRP enviados y recibidos, así como las estadísticas de Hello, actualizaciones, consultas respuestas y acuses de recibo.

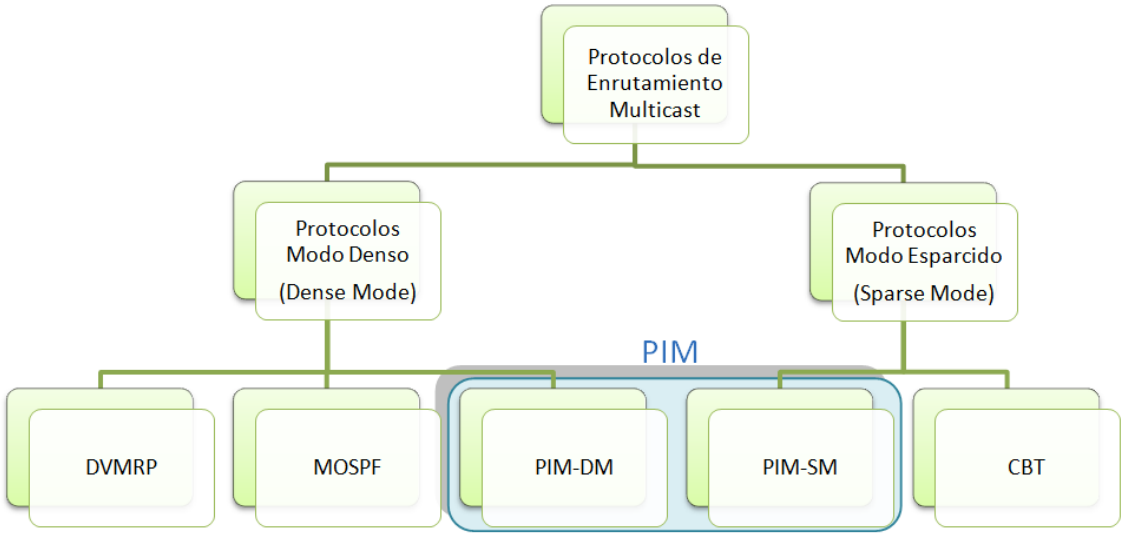
- router(config-router)# **eigrp log-neighbor-changes**: Muestra un historial de reconfiguración de vecinos.

- **Debug eigrp fsm**: Muestra información sobre los paquetes de protocolo EIGRP ampliado, permite analizar los paquetes enviados y recibidos en una interfaz. Este comando sólo debe usarse cuando el tráfico de red es liviano, debido a la magnitud del resultado que genera.

3. PROTOCOLOS DE ENRUTAMIENTO IP MULTICAST

Los protocolos de enrutamiento IP multicast permiten que el tráfico fluya a través de la red para que los routers emisores sepan a dónde enviar los datagramas multicast y los receptores interesados en una emisión puedan recibirla en todo momento. Los protocolos de enrutamiento IP Multicast se pueden clasificar en dos grupos según el modo de operación: protocolos modo denso y protocolos modo esparcido.

Figura 42. Clasificación de los protocolos de enrutamiento multicast



Fuente: Autoras.

3.1. PROTOCOLOS MODO DENSO

Los protocolos modo denso se caracterizan por utilizar para la construcción de los árboles de distribución multicast inundaciones periódicas y podas, árboles basados en el origen. Para cada origen se crea un árbol mediante el algoritmo de mínimo árbol de expansión (Spanning Tree).

El comportamiento de inundación y poda se repite aproximadamente cada 2 o 3 minutos dependiendo del protocolo, por esta razón protocolos del modo denso son mayormente empleados en ambientes LAN, donde el número de receptores usualmente es alto comparado con el de las fuentes y donde el ancho de banda no es un factor restrictivo. Si el número de miembros es minoritario, el protocolo no es eficiente.

Estos protocolos muestran un mejor *delay* debido a la existencia de un árbol por cada origen, pero tienen el inconveniente de consumir mayor memoria en los routers pues para cada origen registran en sus tablas todas las rutas existentes a los destinos.

Entre los protocolos modo denso se pueden mencionar: DVMRP, MOSPF y **PIM-DM**.

- DVMRP[5] - *Distance Vector Multicast Routing Protocol*. Protocolo de enrutamiento Multicast basado en Vector Distancias. Fue el primer protocolo diseñado para realizar enrutamiento multicast. Actualmente sólo se usa en la periferia de redes de operador que contienen sistemas heredados como cortafuegos que no soportan otros protocolos más eficientes.

- MOSPF[6] - *Multicast Open Shortest Path First*. Protocolo de enrutamiento multicast basado en el camino más corto. Es una extensión de OSPF para el soporte al enrutamiento multicast. Funciona bien en redes pequeñas y medianas pero no escala a un ámbito inter-dominio.

[5] CACHINERO POZUELO, Juan Angel. Análisis y modelado de “multicast” interdominio para el soporte de servicios de video. Madrid, 2009, 268 p. Trabajo de grado (Ingeniero de Telecomunicación), Universidad Politécnica de Madrid. Escuela superior de ingenieros de telecomunicación. P. 60.

[6] Ibíd., P. 61.

- **PIM-DM** – *Protocol Independent Multicast Dense Mode.* Protocolo independiente multicast modo denso. (Se profundizará en la sección 3.3).

3.2. PROTOCOLOS MODO DISPERSO

Los protocolos *sparse-mode* se caracterizan por usar árboles compartidos a través de un nodo llamado RP (Rendezvous point) que tiene la función de recibir toda la información de los nodos orígenes y retransmitirla a través del árbol compartido de este grupo multicast a los nodos destinos de ese grupo. Cada nodo origen está conectado al RP mediante una conexión unicast.

Estos protocolos muestran un peor delay porque la existencia de un árbol compartido no garantiza la mejor ruta a todos los destinos. Presentan la ventaja de usar menos memoria en los routers pues solo tienen que registrar el RP para cada árbol compartido y a través del nodo RP deben enviar la información con destino al grupo multicast. Están diseñados para situaciones en las que el ancho de banda es una situación crítica así como el tiempo de distribución.

En los protocolos *sparse-mode* los miembros del grupo están ampliamente dispersos a través de la red. Algunos protocolos *parse-mode son:* **PIM-SM** y CBT (Core Based Trees)

- CBT[7] - *Core Based Trees.* CBT es un protocolo concebido para grupos dispersos sobre grandes áreas. Está basado en árboles compartidos y en mecanismos explícitos de solicitud de pertenencia a un grupo. Al diseñar CBT, se dió gran importancia a la escalabilidad del protocolo, teniendo en cuenta escenarios

[7] RIGOTTI, Guillermo. Implementación y Análisis de CBTv2 en el medioambiente Ns. Argentina, 1998, 195 p. Trabajo de grado (Magíster en redes de datos), Universidad Nacional de la Plata. Facultad de Ciencias Exactas. p.10.

compuestos de miles de routers con capacidad multicast.. (También aparece como algoritmo de enrutamiento multicast).

- **PIM-SM** – *Protocol Independent Multicast Sparse Mode.* Protocolo independiente multicast modo esparcido. (Se profundizará en la sección 3.3).

3.3. PIM (PROTOCOLO INDEPENDIENTE MULTICAST)

PIM es un protocolo de enrutamiento IP independiente. Aunque es un protocolo de enrutamiento multicast, utiliza la tabla de enrutamiento unicast para implementar la función Reverse Path Forwarding (RPF). RPF permite a los routers reenviar correctamente el tráfico multicast hacia la las ramas del árbol de distribución (downstream). RPF hace uso de la tabla de enrutamiento unicast existente para determinar los vecinos downstream. Un router reenviará un paquete multicast solamente si éste es recibido sobre la interfaz “upstream”. Este chequeo RPF ayuda a garantizar que la distribución del árbol esté libre de bucles. Cuando un paquete multicast llega a un router, éste desarrolla un chequeo RPF. Si este chequeo es exitoso, el paquete es reenviado; de lo contrario se descarta.

El procedimiento es el siguiente:

1. El router busca la dirección de la fuente en la tabla de enrutamiento unicast para determinar si el paquete ha llegado a la interfaz, esto es, sobre el camino de reversa a la fuente.
2. Si el paquete ha llegado a la interfaz volviendo desde la fuente, el chequeo RPF es exitoso y el paquete es reenviado.

PIM es usado por routers que están enviando paquetes multicast. El nombre “protocolo independiente” indica que PIM es independiente del

protocolo de enrutamiento unicast (como EIGRP y OSPF) que corra en la red.

PIM usa la tabla de enrutamiento normal poblada por el protocolo de enrutamiento unicast, para sus cálculos de enrutamiento multicast. A diferencia de otros protocolos de enrutamiento, no se envían actualizaciones de enrutamiento entre routers PIM.

Protocolos como EIGRP y OSPF son llamados protocolos de enrutamiento unicast debido a que ellos son usados para crear y mantener información de enrutamiento unicast en la tabla de enrutamiento. Sin embargo, cabe anotar que estos protocolos de enrutamiento unicast utilizan paquetes multicast para enviar su tráfico de actualizaciones de enrutamiento.

Terminología PIM

Cuando un router está enviando un paquete unicast, este busca la dirección destino en su tabla de enrutamiento y envía el paquete hacia la interfaz adecuada. Sin embargo, cuando se envía un paquete multicast, el router tendría que enviar el paquete a múltiples interfaces hacia todos los hosts receptores.

El enrutamiento multicast es orientado a conexión: El tráfico multicast no fluye a los destinos hasta que no se envíen mensajes de conexión hacia la fuente para establecer los caminos para que fluya el tráfico. Los routers habilitados multicast usan PIM para crear dinámicamente árboles de distribución que controlen el camino que toma el tráfico IP multicast a través de la red para distribuir tráfico a todos los receptores.

La construcción de árboles de distribución multicast por medio de la conexión de mensajes es un proceso dinámico; cuando ocurre el cambio

de la topología de la red, los árboles de distribución se reconstruyen alrededor de los enlaces caidos.

3.3.1. PIM Dense Mode (PIM-DM)

También denominado *PIM en modo denso o PIM-DM*. En PIM-DM modo se asume que la mayoría de los routers de la red estarán interesados en la emisión en curso. Es adecuado para redes pequeñas con una gran capacidad sobrante, pero no para grandes redes como es el caso de Internet o cuando el ancho de banda es reducido. No es escalable a redes con muchos routers o con muchos grupos multicast pues requiere que cada router mantenga información de estado sobre las emisiones que no quiere recibir.

El modo denso es el más sencillo de implementar; fue el primero que se utilizó en Internet y el primero que se estandarizó.

PIM en modo denso se maneja a través de los datos y es similar a los protocolos de enrutamiento de multicast típicos. Los paquetes se envían a través de todas las interfaces emisoras hasta que se produce la poda y el truncamiento. En el modo denso, los receptores están densamente poblados y se supone que las redes ubicadas *downstream* desean recibir y que probablemente utilizan los datagramas que se les envían. El costo de usar el modo denso es su forma de inundar las redes por defecto.

Si un router no desea recibir tráfico envía un mensaje de supresión (prune). Como resultado se tiene que el tráfico de multicast sólo es enviado a los routers que tienen miembros de grupos de multicast. Este comportamiento de "Flood" y "Prune" se repite aproximadamente cada 2 o 3 minutos dependiendo del protocolo, por esta razón protocolos del tipo denso son mayormente empleados en ambientes LAN y donde el número de receptores usualmente es alto comparado con el de las fuentes y

donde el ancho de banda no es un factor restrictivo. La estrategia que se sigue es partir de un árbol muy denso (por ejemplo, un árbol de difusión que conecte todas las subredes) e ir podándolo al recibirse notificaciones explícitas por parte de los routers de que no hay actividad en una rama concreta.

El protocolo PIM-DM utiliza una tabla de enrutamiento de difusión única existente y un mecanismo de unión, poda e injerto para crear un árbol. PIM-DM crea árboles de distribución de la ruta de acceso más corta basados en el origen que utilizan el reenvío de ruta inversa (RPF).

3.3.1.1. Características generales

- En el protocolo PIM DM se supone que todos los receptores desean recibir los datos a no ser que lo especifique, por lo tanto puede ocurrir que la información llegue a nodos que no la hayan solicitado.

- Todos los routers pueden tener almacenadas tablas con el estado del resto de los routers, información que en WAN muchas veces es imposible de tener y además es superflua.

- Utiliza la técnica de “broadcast and prune” ideal para grupos densos.

- Los arboles son creados bajo demanda basados en la técnica RPF.

- Si alguna fuente se vuelve inactiva, el árbol es desactivado.

- Utiliza SPT para la distribución de tramas de multicast.

- PIM-DM es un protocolo muy simple de implementar. Su enfoque denso lo hace adecuado para entornos en que hay pocos grupos y muchos receptores en los mismos, poca distancia entre emisores y receptores, y alto volumen de tráfico multicast.

- Para calcular las rutas óptimas utiliza la tabla de enrutamiento unicast, independientemente del protocolo utilizado para obtenerla (de ahí lo de ‘protocol independent’). Puede usar OSPF, IS-IS, EIGRP e incluso rutas estáticas

- Puede utilizar OSPF, RIPv2, etc., incluso rutas estáticas. No se construye árbol broadcast, el tráfico se transmite inicialmente por inundación. Los routers no interesados en recibir tráfico multicast pueden enviar comandos *Prune*, y posteriormente podrán ser añadidos enviando comandos *Graft*, (mensajes de conexión).

- Este protocolo remite los paquetes recibidos de cada pareja (S, G), a todas las interfaces de red, excepto a aquella por la que se ha recibido el paquete multicast, y sólo son eliminados aquellos caminos por los que se han recibido explícitamente mensajes de poda (*pruning*). Esto hace que se aproveche el trabajo realizado por los protocolos unicast. Este protocolo no posee límite de saltos mientras que en el DVMRP se fija en 32 saltos.

- Este tipo de protocolo se caracteriza por utilizar inundaciones periódicas y podas para la construcción de los árboles de distribución multicast; a estos árboles se les conoce con el nombre de árboles basados en el origen, y existe uno de ellos por cada origen mediante el algoritmo de Mínimo Árbol de Expansión (Spanning Tree).

- PIM-DM implementa el algoritmo RPF (Propagación por la Trayectoria Inversa). Para determinar si un datagrama multicast ha entrado por la ruta correcta se utiliza la información disponible: la tabla de encaminamiento mantenida con el protocolo unienvío adoptado en el sistema. De manera similar a la del protocolo DVMRP, PIM-DM construye inicialmente un árbol de difusión que lleva desde el origen a todos los routers multicast, y posteriormente se utiliza la información recolectada a través de IGMP y difundida desde los miembros del grupo hacia el origen para podar las ramas inactivas. Debe

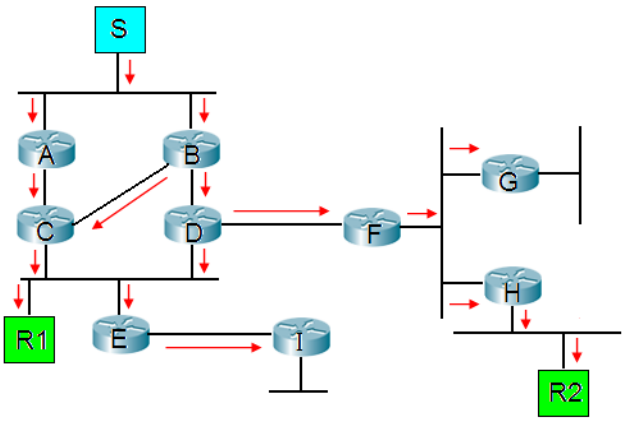
mantenerse información sobre las ramas podadas para un grupo, por si hay que volver a reactivarlas (grafts).

3.3.1.2. Funcionamiento

El protocolo PIM-DM funciona de la siguiente manera:

1. La distribución de las primeras tramas de multicast se efectúa por todas las interfaces excepto por el que ha llegado.

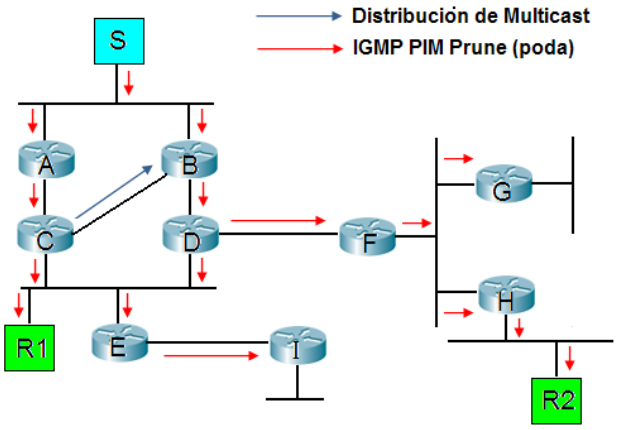
Figura 43. Distribución de primeras tramas PIM-DM



Fuente: http://www.ccapitalia.net/netica/teleco/multicast-ip-jorgef.pdf.

2. Se eliminan las rutas que no corresponden con la ideología de RPF utilizando con el envió de las tramas de PIM-prune para realizar la poda.

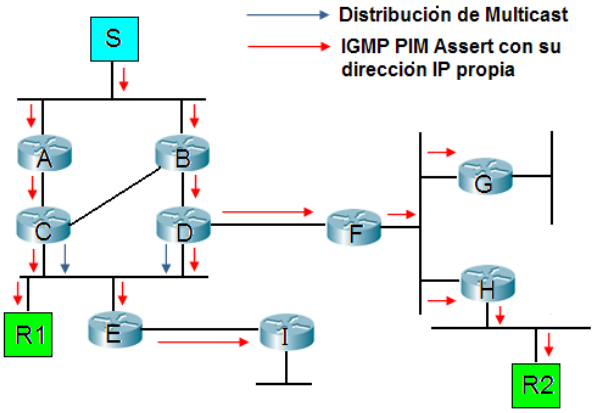
Figura 44. Eliminación de rutas



Fuente: http://www.ccapitalia.net/netica/teleco/multicast-ip-jorgef.pdf.

3. Se envían tramas de asert (aserción) para decidir cual es el router designado (DR) para acceder a esa red. En el esquema C y D son caminos hacia la misma red.

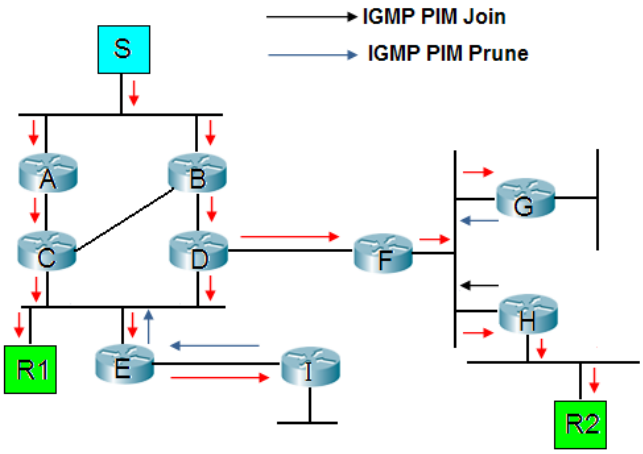
Figura 45. Envio de tramas asert para decidir el DR



Fuente: http://www.ccapitalia.net/netica/teleco/multicast-ip-jorgef.pdf.

4. I, E y G envían una solicitud de poda (prune). H envía un mensaje de Unión (join) para que F ignore el mensaje de poda que envía G.

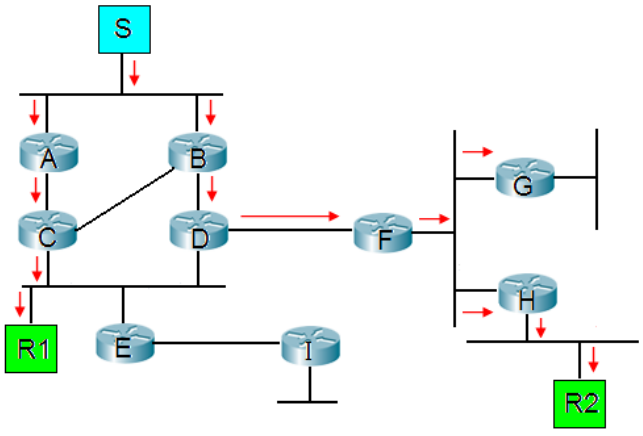
Figura 46. Envio de una solicitud de poda



Fuente: http://www.ccapitalia.net/netica/teleco/multicast-ip-jorgef.pdf.

5. I es “podado”, la petición de poda de E es ignorada, y la petición de “poda” de G es sobrescrita.

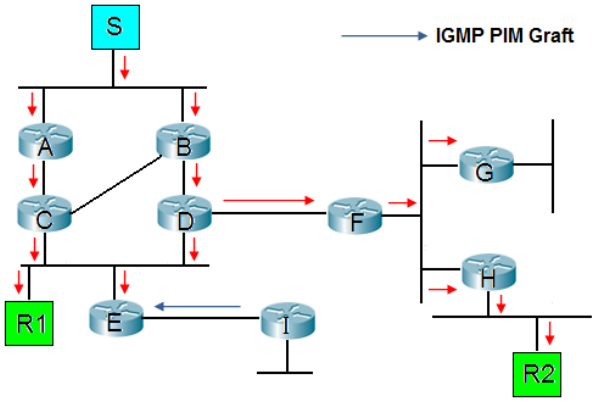
Figura 47. Petición de poda ignorada



Fuente: http://www.ccapitalia.net/netica/teleco/multicast-ip-jorgef.pdf.

6. En I aparece un nuevo receptor que cuelga de el, entonces I envía un mensaje de Injerto o conexión (graft).

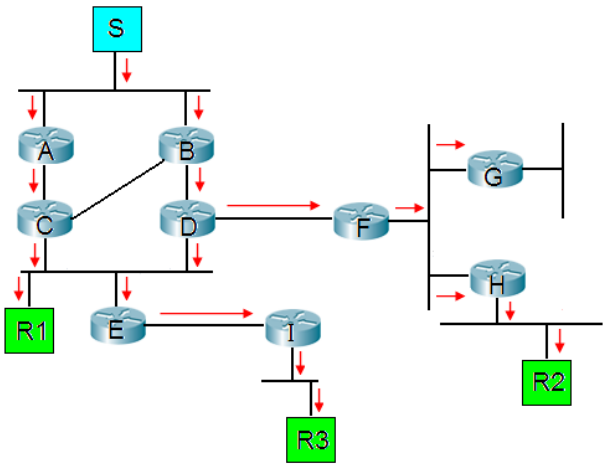
Figura 48. Aparición de un nuevo receptor



Fuente: http://www.ccapitalia.net/netica/teleco/multicast-ip-jorgef.pdf.

7. Se realiza la distribución de la información al nuevo integrante.

Figura 49. Distribución de información al nuevo integrante



Fuente: http://www.ccapitalia.net/netica/teleco/multicast-ip-jorgef.pdf.

3.3.1.3. Ventajas y desventajas

- Es el protocolo de enrutamiento multicast más antiguo y el más sencillo de configurar.
- Se utiliza cuando hay un gran ancho de banda o cuando una mayoría de los routers quieren recibir el grupo multicast
- Es más escalable que el DVMRP.
- El protocolo PIM-DM utiliza la tabla de routing unicast, independientemente del protocolo utilizado.
- Utilizan árboles del tipo “Source Path Tree” (SPT), que representan el camino más corto hacia la fuente.
- Muestran un mejor retardo porque existe un árbol por cada origen.
- No es eficiente cuando el número de receptores es minoritario
- No es escalable.
- La gran cantidad de información de estado hace difícil establecer un servicio multicast en una red grande para un número elevado de emisores y grupos.
- Para construir el SPT inicial se procede por inundación. Para adaptarse a cambios en la red el proceso se repite cada 2-3 minutos, lo cual genera mucho tráfico.
- No es apto para grandes redes por la cantidad de tráfico generado y de información de estado almacenada.
- No se recomienda por su comportamiento de "flood"

- Tienen el inconveniente de consumir mayor memoria en los routers porque tienen que registrar en sus tablas todas las rutas existentes a los destinos.

3.3.2. PIM Sparse Mode (SM)

También conocido como Pim modo disperso. PIM-SM trata de limitar la distribución de datos de manera que una cantidad mínima de routers de la red los reciban. Los paquetes se envían sólo si se lo solicita de forma explicita en los RP (punto de encuentro). En el modo disperso, los receptores están ampliamente distribuidos, y se supone que las redes *downstream* no necesariamente utilizarán los datagramas que se les envían. El costo del uso del modo disperso es su dependencia de la actualización periódica de los mensajes de unión explícitos y su necesidad de los RP. Este modo es a veces denominado como *modo disperso de PIM o PIM-SM.*

PIM-SM se utiliza para direccionar de manera eficaz el tráfico de multidifusión a grupos de multidifusión que pueden abarcar redes de área amplia y en casos en que la amplitud del ancho de banda es una limitación. Utiliza árboles compartidos de manera predeterminada e implementa árboles basados en el origen para obtener mayor eficacia. Y por cada grupo multicast existe un árbol de este tipo en el cual los receptores escuchan al router origen y mantienen el estado del árbol multicast.

3.3.2.1. Características generales

- Los protocolos multicast de modo esparcido como PIM-SM están pensados para situaciones en las que el ancho de banda es una

situación crítica así como el tiempo de distribución o cuando se tienen más fuentes que destinos.

- Este tipo de protocolo se caracteriza por usar árboles compartidos, donde los receptores escuchan al router origen y mantienen el estado del árbol multicast.

- Para construir el árbol compartido el router receptor envía a la raíz un mensaje de solicitud de unión al árbol (*Join message*), éste mensaje viaja de router a router hasta llegar a la raíz construyendo así el camino hacia la misma. Al igual que los DM, en el SM si un receptor no desea recibir tráfico envía un mensaje de supresión (*Prune*).

- Los árboles compartidos minimizan la cantidad de información de estado en los routers. Los árboles SPT optimizan el tráfico.

- Por cada grupo multicast existe un árbol compartido.

- Se supone que solo quieren los datos aquellos receptores que lo soliciten.

- Se suele fijar un umbral de tráfico a partir del cual los routers conmutan de árbol compartido a SPT. Si umbral=0 se conmuta con el primer paquete, si umbral=∞ siempre se usa el árbol compartido.

- Este modo del protocolo utiliza la filosofía de árbol basado en centros.

- Pueden existir uno o más nodos “centrales” llamados RP (Rendezvous Point).

- Cada nodo que quiera recibir mensajes multicast de un cierto grupo necesita enviar un mensaje de unión al RP de ese grupo.

- Los destinos pueden solicitar a cada fuente usar un árbol del tipo *SBT* en vez de utilizar el RP. De esta manera, pueden coexistir las filosofías SBT y CBT en el mismo protocolo.

- Es un protocolo para crear arboles de distribución de multicast.

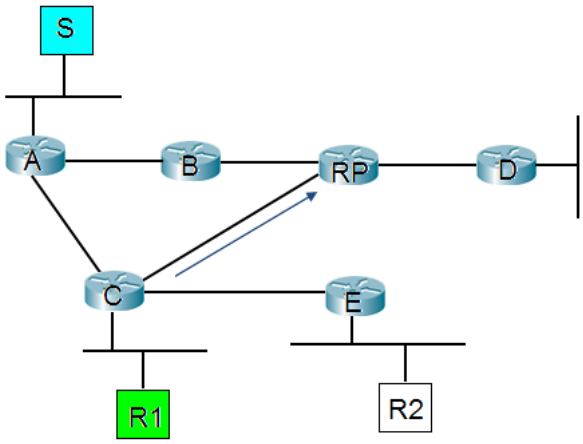
- Está optimizado para entornos WAN aunque funciona también bien en LAN.

3.3.2.2. Funcionamiento

El protocolo PIM-SM funciona de la siguiente manera:

1. El Receptor R1 decide participar del grupo de multicast llamado G. El Router C crea el estado (*, G) y manda una señal de participación al RP.

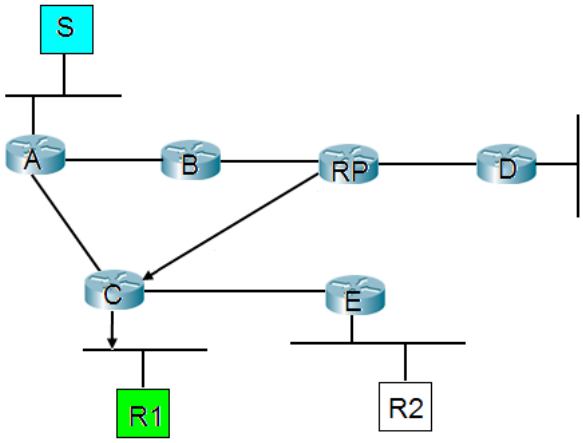
Figura 50. Participación de un receptor al grupo multicast



Fuente: http://www.ccapitalia.net/netica/teleco/multicast-ip-jorgef.pdf.

2. El RP crea un nuevo estado de distribución (*, G) a través de la interfaz que lleva al router C.

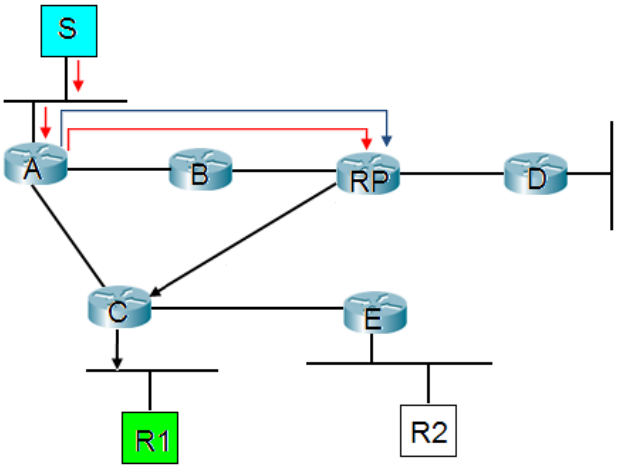
Figura 51. Estado de distribución (*, G) de RP



Fuente: http://www.ccapitalia.net/netica/teleco/multicast-ip-jorgef.pdf.

3. La fuente S comienza a enviar datos hacia el RP. El router A encapsula estos paquetes de datos en paquetes de Registro.

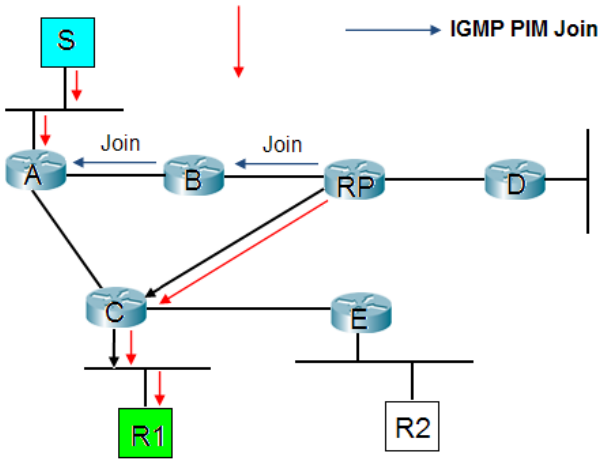
Figura 52. Envio de datos hacia el RP



Fuente: http://www.ccapitalia.net/netica/teleco/multicast-ip-jorgef.pdf.

4. El RP desencapsula estos paquetes de registro y envía la trama original de multicast a través de los puertos que tiene registrados para ese grupo de multicast (*,G). Además manda mensajes *Join* hacia la fuente.

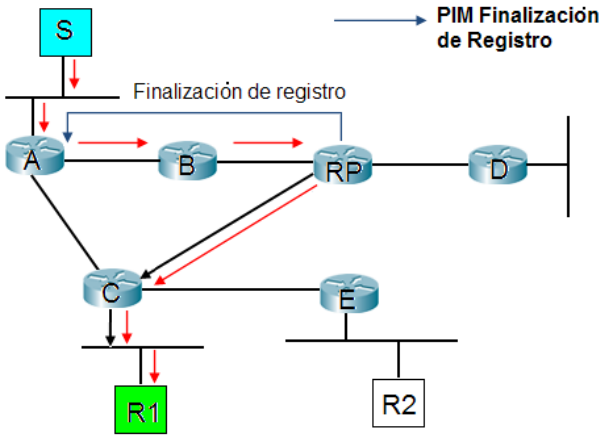
Figura 53. RP desencapsula los paquetes de registro



Fuente: http://www.ccapitalia.net/netica/teleco/multicast-ip-jorgef.pdf.

5. Una vez que el RP recibe los mensajes multicast sin encapsular, a través de los puertos correspondientes, manda un mensaje de finalización de registro hacia A.

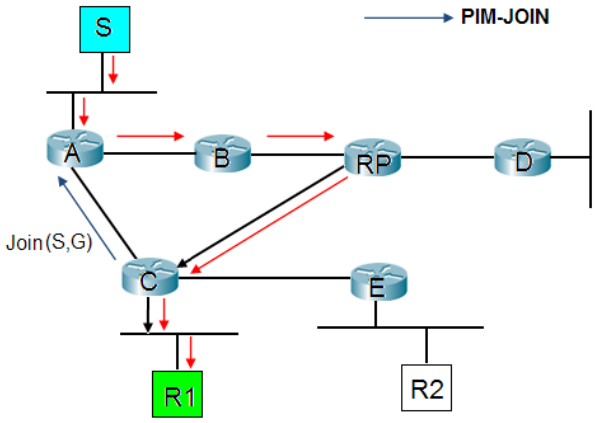
Figura 54. Mensaje de finalización de registro de RP



Fuente: http://www.ccapitalia.net/netica/teleco/multicast-ip-jorgef.pdf.

6. Conmutación de RPT a SPT: Una vez que se ha llegado a un determinado nivel de congestión en el nodo C, decide conmutar a un árbol de ruta de acceso más corta.

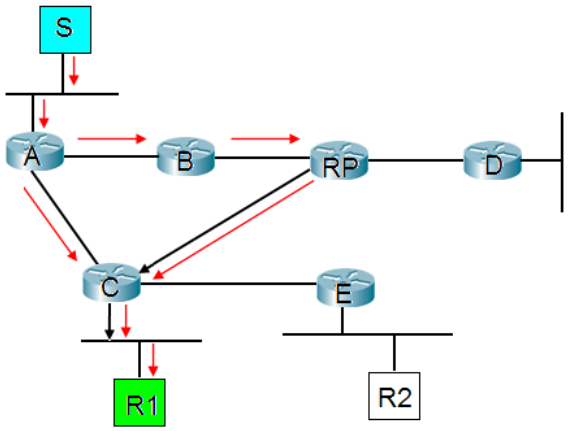
Figura 55. Conmutación de RPT a SPT



Fuente: http://www.ccapitalia.net/netica/teleco/multicast-ip-jorgef.pdf.

7. C comienza a recibir datos nativos de Multicast.

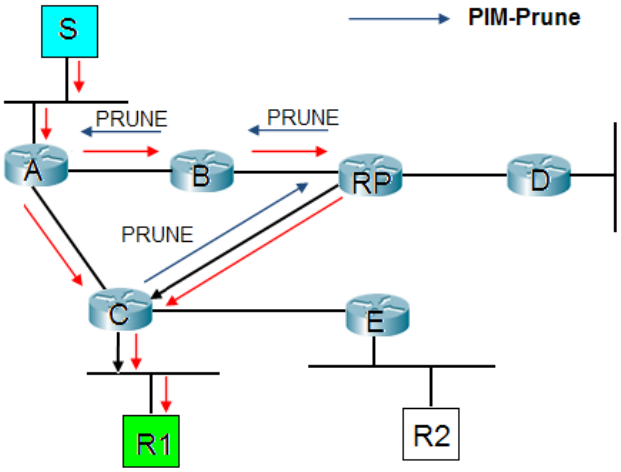
Figura 56. Datos nativos de multicast recibidos



Fuente: http://www.ccapitalia.net/netica/teleco/multicast-ip-jorgef.pdf.

8. C manda mensajes de “poda” hacia el RP. El RP borra la entrada (S, G) que tiene para la interfaz que va a C y manda mensajes de “poda” hacia la fuente.

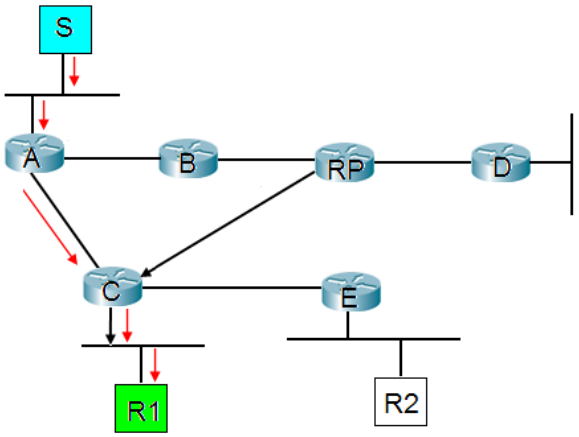
Figura 57. Envio de mensajes de poda hacial el RP



Fuente: http://www.ccapitalia.net/netica/teleco/multicast-ip-jorgef.pdf.

9. La distribución de B y de RP hacia C es “podada”.

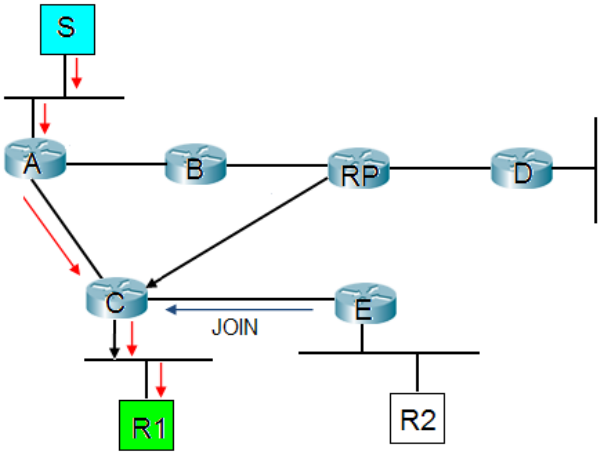
Figura 58. Distribución de B y Rp hacia C podada



Fuente: http://www.ccapitalia.net/netica/teleco/multicast-ip-jorgef.pdf.

10. Inserción de un nuevo participante.

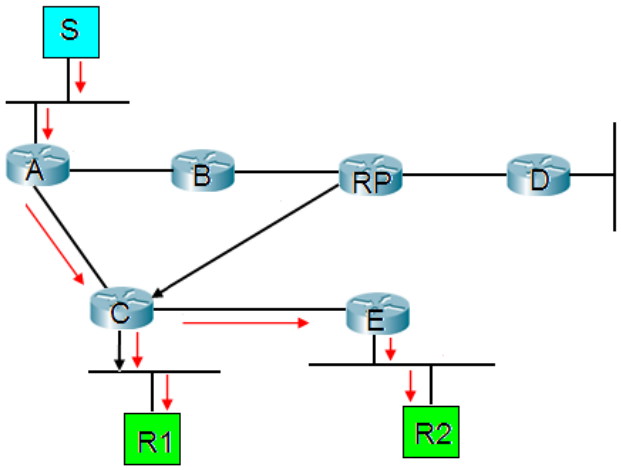
Figura 59. Inserción de un nuevo participante



Fuente: http://www.ccapitalia.net/netica/teleco/multicast-ip-jorgef.pdf.

11. Finalmente, C añade enlaces hacia E, haciendo que lleguen los datos de la fuente.

Figura 60. Fin del proceso PIM-SM



Fuente: http://www.ccapitalia.net/netica/teleco/multicast-ip-jorgef.pdf.

3.3.2.3. Ventajas y desventajas

- Debido a su flexibilidad y escalabilidad PIM-SM es el protocolo que tiene más futuro en Internet.
- Presentan una ventaja en el uso de memoria en los routers, puesto que solo tienen que registrar el RP por cada árbol compartido.
- No genera tráfico a menos que se solicite.
- Se recomienda para ambientes WAN y LAN.
- PIM-SM cuenta con un mecanismo que permite conmutar de árbol compartido a SPT para una fuente en particular.

- Los protocolos esparcidos muestran un peor retardo, debido a que la existencia de un árbol compartido no garantiza la mejor ruta a los destinos.

- Es preferible el modo denso cuando el número de receptores es minoritario.

- Es el más complejo de los protocolos de routing multicast en uso actualmente.

- Si el RP está mal ubicado por el administrador de la red puede ocasionar que el camino fuente-destino no sea el óptimo o que por exceso de tráfico el RP se convierta en un cuello de botella.

3.3.3. PIM Sparse-Dense Mode

Cisco implementó una alternativa para elegir entre *dense mode* y *sparse mode* en la interfaz del router. Esta alternativa surge de la necesidad del cambio de paradigma para el reenvío de tráfico multicast a través de PIM durante su desarrollo.

Así se determinó que, cambiando el modo *sparse* o *dense* sobre la base de un grupo era más eficiente que sobre una base de interfaz de router.

La configuración puede ser realizada por el administrador de la red y permite a grupos individuales correr tanto en modo esparcido como en modo denso, dependiendo de la información disponible sobre el RP del grupo. Si el router “aprende” la información RP para un grupo en particular, éste es tratado como un grupo en *SM*. De lo contrario, es tratado como *DM*. En la práctica PIM-SDM del capítulo 5 se profundizará en el tema.

3.3.4. PIM-DM vs. PIM-SM

A continuación se presenta un comparativo entre los dos modos de operación de PIM.

Tabla 34. PIM-DM vs. PIM-SM

Dense Mode	Sparse Mode
Arbol basado en el origen	Árbol compartido llamado RP (Rendezvous point)
Hay un árbol (TBT) por cada origen	Hay un RP (SPT) por cada grupo multicast
Menor delay porque existe un árbol por cada origen	Delay más alto por tener un árbol compartido, lo que no asegura la mejor ruta a los destinos.
Mayor uso de la memoria del router porque se especifíca una ruta por cada destino	Mejor uso de la memoria del router porque solo registra un RP por cada árbol compartido

Fuente: Autoras.

3.4. COMANDOS ÚTILES EN LA CONFIGURACIÓN DE PIM

A continuación se detallan algunos comandos útiles en la configuración, monitoreo y depuración del protocolo PIM en modo denso y modo esparcido.

Comando "access-list 32 permit 232.32.32.32"

Desripción: Para definir una lista de control de acceso, utilice el comando **access-list**. Para eliminar una lista de acceso estándar, utilice la forma **no** de este comando. Planear las

condiciones de acceso con cuidado y ser conscientes de la declaración implícita "deny all" al final de la lista de acceso. Las listas de acceso se pueden utilizar para controlar la transmisión de paquetes en una interfaz, para control virtual de la línea de acceso terminal, y restringir el contenido de las actualizaciones de enrutamiento.

Modo: Router(config) #

Sintaxis: IP standard access-list: **access-list** *access-list-number* **{deny | permit | remark** *line***}** *source[source-wildcard] [***log***]*

no access-list *access-list-number*

Descripción de la Sintaxis:

Tabla 35. Descripción de la sintaxis del comando access-list

Campo	Descripción
access-list-number	Número de una lista de acceso. Este es un número decimal de 1 a 99 para el IP estándar de 100-199 o de 2000 a 2699 para la IP extendida.
deny	Niega el acceso si las condiciones son compatibles.
permit	Permite el acceso si las condiciones son compatibles.
protocol	Puede ser una de las palabras clave AHP, EIGRP, ESP, GRE, ICMP, IGMP, IGRP, IP,IPINIP,NEP, OSPF, PCP, PIM, TCP o UDP, o un entero en el rango de 0 a 255 lo que representa un número de protocolo IP. Para comparar cualquier protocolo de Internet (incluyendo ICMP, TCP y UDP) utilice la palabra clave **ip**.
source	Número de la red o host desde el cual el paquete es enviado. Hay tres

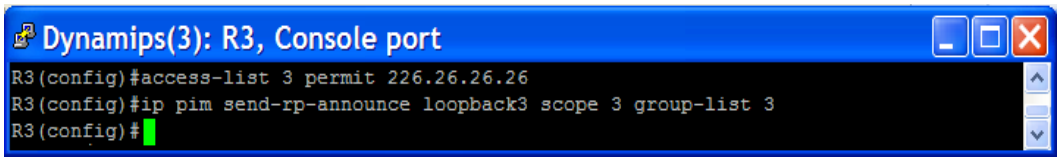
	vías alternativas para indicar la fuente: - Utilizar una cantidad de 32 bits en cuatro fragmentos, en formato decimal con puntos. - Utilizar la palabra clave **any** como una abreviatura para una fuente y fuente wildcard de 0.0.0.0 255.255.255.255. - Utilizar un host de origen como una abreviatura para una fuente y fuente wildcard de procedencia 0.0.0.0
source-wildcard	bits de wildcard para ser aplicado a la fuente. Cada bit wildcard establece un cero indicando que la posición del bit correspondiente en la dirección IP del paquete debe coincidir exactamente con el valor del bit en la posición del bit correspondiente en la fuente. - Hay tres formas alternativas de especificar la fuente Wildcard: Utilizar una cantidad de 32 bits en cuatro segmentos, en formato decimal con puntos. Lugar de las unidades en las posiciones del bit para ser ignorado. Por ejemplo, 0.0.255.255 exigir una coincidencia exacta de sólo los primeros 16 bits de la fuente. - Utilizar la palabra clave **any** como abreviatura de una fuente y la fuente wildcard de 0.0.0.0 255.255.255.255. - Utilizar **host** *source* como abreviatura de una fuente y la fuente wildcard de procedencia 0.0.0.0.
log	(Opcional) Las causas en un mensaje informativo registran sobre el paquete que coincide con la entrada que se enviará a la consola. (El nivel de los mensajes registrados en la consola se controla mediante el comando **logging console**.)

Fuente: Aplicación Ciscopedia v.3.0.

Ejemplo:

En el ejemplo siguiente se crea una lista de acceso 3 en IP estándar, lo que permitirá todo el tráfico desde la red 226.26.26.26:

Figura 61. Ejemplo del comando access-list



Fuente: Software GNS3.

Comando "debug ip pim"

Descripción: Utilice el comando **debug ip pim** para mostrar los paquetes PIM recibidos y transmitidos, así como eventos relacionados con PIM. La forma **no** de este comando desactiva la salida de depuración.

Modo: Router>
Router#

Sintaxis: [no] **debug ip pim** [*group*]

Descripción de la Sintaxis:

Tabla 36. Descripción de la sintaxis del comando debud ip pim

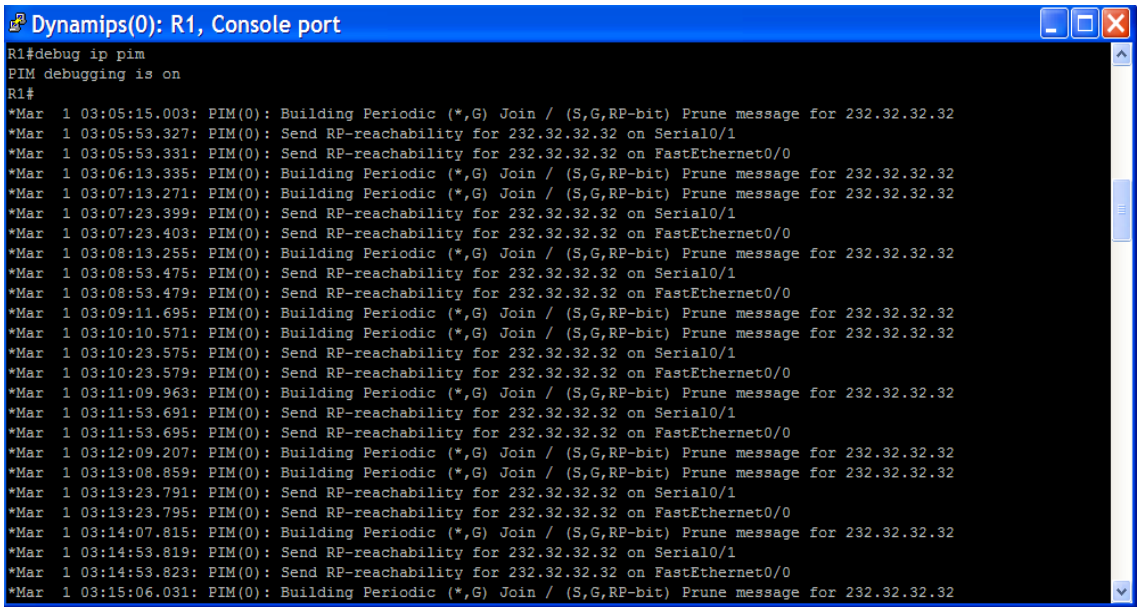
Campo	Descripción
group	(opcional) Nombre del grupo o la dirección para supervisar la actividad de un simple grupo de paquetes.

Fuente: Aplicación Ciscopedia v.3.0.

Ejemplo:

El siguiente es resultado de ejemplo del comando **debug ip pim** sin asignar una dirección en el router R1:

Figura 62.Ejemplo del comando debud ip pim



Fuente: Software GNS3.

El siguiente es resultado de ejemplo del comando **debug ip pim** con dirección. Las siguientes líneas aparecen periódicamente cuando PIM se ejecuta en modo disperso e indica a este router que grupos multicast y otras fuentes de routers multicast están interesados:

PIM: Received Join/Prune on Ethernet1 from 172.24.37.33

PIM: Received Join/Prune on Ethernet1 from 172.24.37.33

Las siguientes líneas aparecen cuando un mensaje del RP(punto de encuentro), es recibido y el temporizador RP se restablece. El temporizador de caducidad establece un punto de comprobación para

asegurarse de que el RP todavía existe, de lo contrario un nuevo RP debe ser descubierto.

PIM: Received RP-Reachable on Ethernet1 from 172.16.20.31
PIM: Update RP expiration timer for 224.2.0.1
PIM: Forward RP-reachability packet for 224.2.0.1 on Tunnel0

El mensaje prune-list en la siguiente línea establece que este router no está interesado en la información de dirección de origen. El mensaje prune (poda) informa a un router ascendente detener el reenvío de paquetes de multidifusión desde esta fuente.

PIM: Prune-list (10.221.196.51/32, 224.2.0.1)

En la siguiente línea, un segundo router de la red quiere reemplazar el mensaje de prune (podar) que el router ascendente acaba de recibir. El temporizador se fija en un valor aleatorio de modo que si hay router adicionales en la red que todavía quieren recibir paquetes de multicast para el grupo, sólo uno realmente enviará el mensaje. Los otros routers recibirán el mensaje join (unir) y después suprimir el envío de su propio mensaje.

PIM: Set join delay timer to 2 seconds for (10.221.0.0/16, 224.2.0.1) on Ethernet1

En la siguiente línea, un mensaje join (unión) es enviado hacia el RP para todas las fuentes

PIM: Join-list: (*, 224.2.0.1) RP 172.16.20.31

En las siguientes líneas, la interfaz está siendo añadido a la interfaz de salida (OIF), de la *, G y S, G de la tabla de enrutamiento multicast de

entrada para que los paquetes desde la fuente puedan ser transmitidos afuera a la interfaz particular:

PIM: Add Tunnel0 to (*, 224.2.0.1), Forward state

PIM: Add Tunnel0 to (10.0.0.0/8, 224.2.0.1), Forward state

En la siguiente línea aparece en modo esparcido solamente. Hay dos árboles en los que los datos pueden ser recibidos: el árbol RP y el árbol fuente. En modo denso no hay RP. Después la fuente y el receptor han descubierto uno a otros el RP, el router del primer salto para el receptor por lo general será la union al árbol fuente en vez del árbol RP.

PIM: Prune-list (172.24.84.16/28, 224.2.0.1) RP-bit set RP 172.24.84.16

El mensaje enviado Prune (podar) en la siguiente linea muestra que un router está enviando un mensaje a un segundo router diciendo que el primer router ya no quiere recibir paquetes de multicast para el S, G. El "RP" al final del mensaje indica que el router es la poda del árbol del RP y es más probable la unión al árbol fuente, aunque el router no puede tener miembros descendentes para el grupo o router descendente con miembros del grupo. La salida muestra que las fuentes específicas de este router ya no desean recibir de multicast.

PIM: Send Prune on Ethernet1 to 172.24.37.6 for (172.24.84.16/28, 224.2.0.1), RP

Las siguientes líneas indican un mensaje de prune (poda) que es enviado hacia el RP a fin de que el router pueda unirse al árbol fuente en lugar del árbol RP

PIM: For RP, Prune-list: 10.9.0.0/16

PIM: For RP, Prune-list: 10.16.0.0/16

PIM: For RP, Prune-list: 10.49.0.0/16

En la línea siguiente, un mensaje se envía periódicamente hacia el RP. El período predeterminado es una vez por minuto. Mensajes de prune (poda) y join (unión) son enviados hacia el RP o la fuente en lugar de directamente al RP o su origen. Es responsabilidad del router del próximo salto emprender las acciones pertinentes, con este mensaje, tales como la continuación de retransmitirlo al siguiente router en el árbol.

PIM: Send periodic Join/Prune to RP via 172.24.37.6 (Ethernet1)

Comando "debug ip igmp"

Descripción: Para mostrar paquetes recibidos y enviados de IGMP , y eventos relacionados con host IGMP, utilice el comando **debug ip igmp**. Para deshabilitar la depuración, utilice la forma **no** de este comando.

Los mensajes mostrados por el comando **debug ip igmp** muestran preguntas e informe de actividades recibidos de otros routers y direcciones de grupo multicast.

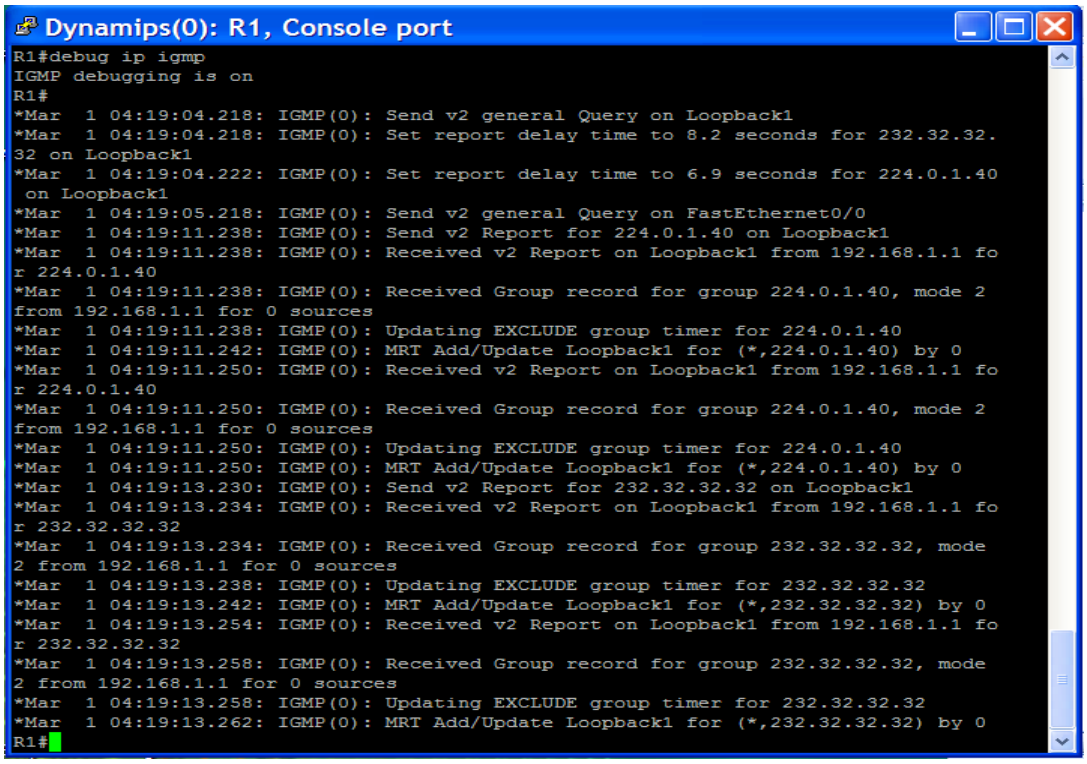
Modo: Router#

Sintaxis: **debug ip igmp**

no debug ip igmp

Ejemplo:

Figura 63. Ejemplo del comando debug ip igmp



Fuente: Software GNS3.

Comando “Switchport Access”

Descripción: Utilice el comando de configuración **switchport access** para establecer un puerto como un acceso estático o puerto con acceso dinámico. Si el modo está configurado para el acceso, el puerto funciona como un miembro configurado de la VLAN. Si se establece en dinámico, el puerto comienza el descubrimiento de su asignación de VLAN basadas en los paquetes entrantes que recibe. Utilice la forma **no** de este comando para restablecer el modo de acceso a la VLAN por defecto para el switch.

Modo: **Switch(config-if)#**

Sintaxis: **switchport access vlan** {*vlan-id* | **dynamic**}

no switchport access

Descripción de la Sintaxis:

Tabla 37. Descripción de la sintaxis del comando Switchport access

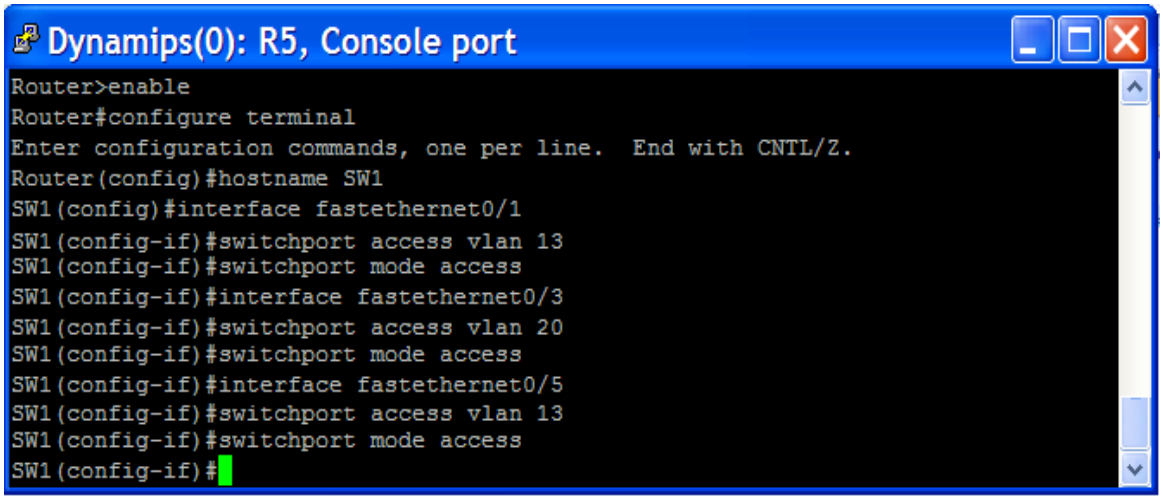
Campo	Descripción
access vlan *vlan-id*	Configura la interfaz como un puerto de acceso estático; los valores válidos son de 1 a 1005.
access vlan dynamic	Especifica que la VLAN de modo de acceso depende de VMPS (the VLAN Membership Policy Server protocol). El puerto está asignado a una VLAN basada en el origen de la dirección MAC de un host (o hosts) conectado al puerto. El switch envía cada nueva dirección MAC recibido al servidor VMPS para obtener el nombre de VLAN a la que el puerto de acceso dinámico debe ser asignado. Si el puerto ya tiene una VLAN asignado y la fuente ya ha sido aprobado por la VMPS, el switch adelanta el paquete a la VLAN.

Fuente: Aplicación Ciscopedia v.3.0.

Ejemplo:

Este ejemplo muestra cómo asignar un puerto en modo de acceso a la VLAN 13 y Vlan 20 (en lugar del predeterminado VLAN 1):

Figura 64. Ejemplo del comando Switchport Access



Fuente: Software GNS3.

Comando "Switchport mode"

Descripción: Use el comando **switchport mode** para configurar el modo de pertenencia de un puerto de la VLAN. Utilice la forma **no** de este comando para restablecer el modo en el valor predeterminado adecuado para el dispositivo.

La configuración mediante las palabras clave **access** o **trunk** toma efecto sólo cuando el puerto se cambia al modo correspondiente utilizando el comando **switchport mode**. La configuración **static-acces y trunk** son guardadas, pero sólo una configuración está activa a la vez.

La forma **no switchport mode** restablece el modo de acceso estático.

Modo: Switch(config-if)#

Sintaxis: **switchport mode {access | trunk}**

no switchport mode {access | trunk}

Descripción de la Sintaxis:

Tabla 38. Descripción de la sintaxis del comando Switchport mode

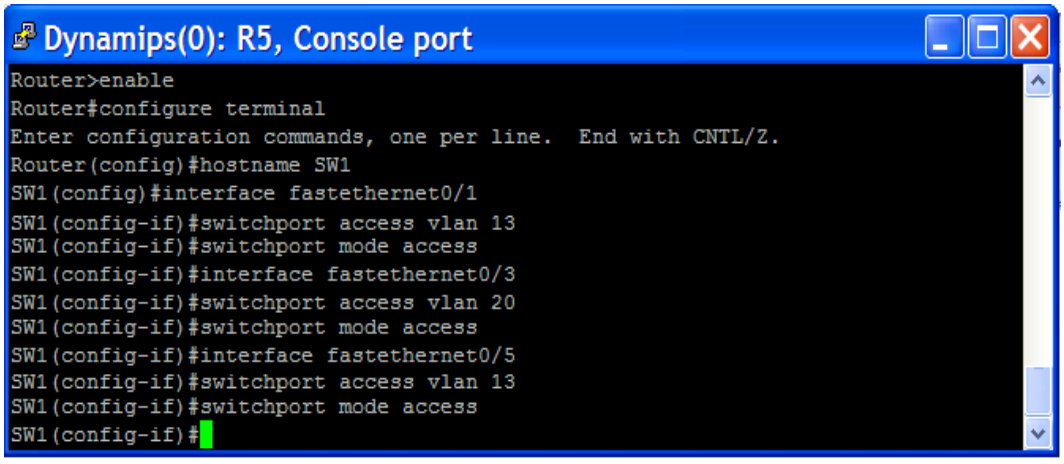
Campo	Descripción
access	Establece el puerto en el modo de acceso (estatic-access). El puerto funciona como un no trunking, única interfaz VLAN que transmite y recibe frames no encapsulados. Un puerto de acceso se puede asignar a una sola VLAN.
trunk	Establece el puerto de la interfaz a una VLAN trunking capa 2. El puerto transmite y recibe frames encapsulados (etiquetados) que identifican la VLAN de origen. Un trunk es un enlace punto a punto entre dos Switch o entre un switch y un router.

Fuente: Aplicación Ciscopedia v.3.0.

Ejemplo:

El siguiente ejemplo muestra cómo configurar un puerto para el modo de acceso de la Vlan 13 y la Vlan 20:

Figura 65. Ejemplo del comando Switchport mode Access



Fuente: Software GNS3.

Comando "Show ip igmp groups"

Descripción: Para mostrar los grupos de multicast con receptores que están directamente conectados al router y que fueron aprendidos a través de IGMP, utilice el comando **show ip igmp-groups**.

Si se omiten todos los argumentos opcionales y las palabras clave, el comando **show ip igmp-groups** muestra por grupo, la dirección, tipo de interfaz, y el número de interfaz de todos los grupos de multicast directamente conectados.

Modo: Router>

Sintaxis: **show ip igmp groups [***group-name* | *group-address* | *type number***]** [detail]

Descripción de la Sintaxis:

Tabla 39. Descripción de la sintaxis del comando show ip igmp groups

Campo	**Descripción**
group-name	(Opcional) Nombre del grupo multicast, como se define en la tabla DNS del host.
group-address	(Opcional) Dirección del grupo multicast. Esta es una dirección IP multicast de cuatro segmentos, con notación de puntos.
type	(Opcional) Tipo de interfaz
number	(Opcional)Número de la Interfaz.

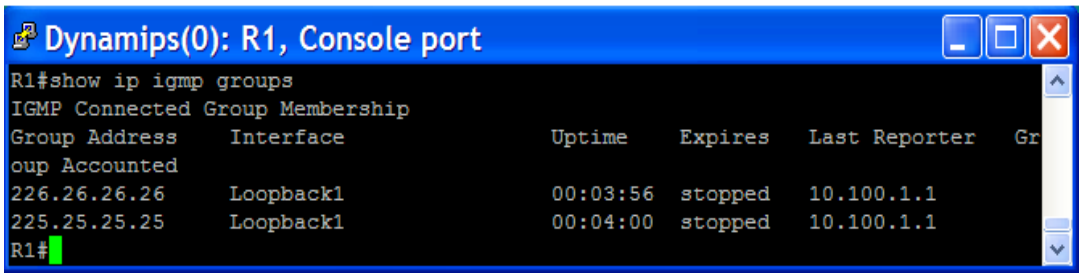
detail	(Opcional) proporciona una descripción detallada de las fuentes conocidas a través de IGMP versión 3 (IGMPv3), IGMP v3 lite.

Fuente: Aplicación Ciscopedia v.3.0.

Ejemplo:

El siguiente es resultado de ejemplo del comando **show ip igmp grupos** en el router R1:

Figura 66. Ejemplo del comando show ip igmp groups



Fuente: Software GNS3.

Descripción de los campos:

Tabla 40.Descripción de la sintaxis del comando show ip igmp groups

Campo	Descripción
Group	Dirección del grupo multicast.

Address	
Interface	Interfaz a través del cual el grupo es accesible.
Uptime	Cuánto tiempo (en semanas, días, horas, minutos y segundos) el grupo multicast se ha conocido.
Expires	Cuánto tiempo (en horas, minutos y segundos) hasta que la entrada caduca. Si una entrada caduca, entonces mostrará (por un corto período de tiempo) la palabra "ahora" antes de ser retirado. La palabra "nunca" indica que la entrada no caduca, porque es un receptor local en este router para esta entrada. La palabra "detenido" indica que el tiempo de espera de esta entrada no esta determinada por el contador expirado. Si el router está en modo INCLUDE por un grupo, entonces todo el grupo entrara en tiempo de espera después de que la última fuente de entrada haya agotado el tiempo (a menos que el modo sea cambiado a modo include antes del tiempo de espera).
Last Reporter	Último host en informar ser un miembro del grupo de multicast.

Fuente: Aplicación Ciscopedia v.3.0.

Comando " Show ip mroute"

Descripción: Se utiliza este comando para mostrar el contenido completo de la tabla de enrutamiento IP multicast. Se usa para verificar:

Las entradas del estado(S, G) y (*, G) de las banderas

La interfaz de entrada es correcta. Si no lo es, compruebe la tabla de enrutamiento unicast.

La interfaz de salida es correcta. Si está mal podado, verificar el estado en el router *downstream*.

Para mostrar el contenido de La tabla de enrutamiento multicast (mroute), utilice el comando **show ip mroute** en modo usuario EXEC o modo de ejecución privilegiado.

Modo: Router>
Router#

Sintaxis: **show ip mroute** [**vrf** *vrf-name*] [[**active** [*kbps*] [**interface** *type number*] | **bidirectional** | **count** [**terse**] | **dense** | **interface** *type number* | **proxy** | **pruned** | **sparse** | **ssm** | **static** | **summary**] | [*group-address* [*source-address*]] [**count** [**terse**] | **interface** *type number* | **proxy** | **pruned** | **summary**] | [*source-address group-address*] [**count** [**terse**] | **interface** *type number* | **proxy** | **pruned** | **summary**] | [*group-address*] **active** [*kbps*] [**interface** *type number*]]

Descripción de la Sintaxis:

Tabla 41. Descripción de la sintaxis del comando show ip mroute

Campo	Descripción
vrf *vrf-name*	(Opcional) Filtra la salida para mostrar sólo el contenido de la tabla de enrutamiento multicast que pertenecen a la red virtual privada de enrutamiento multicast (MVPN) y la instancia de reenvío (MVRF) especificada para el argumento *Vrf-name.*
active *kbps*	(Opcional) Muestra el valor de las fuentes activas que están enviando a grupos de multicast, en kilobits por segundo (kbps).fuentes activas que son aquellos que envían un valor en kbps o superior. El rango es de 1 a 4294967295. El valor por defecto es de 4 kbps.
interface *type number*	(Opcional) Filtra la salida para mostrar solo la información de la tabla de enrutamiento multicast relacionadas con la interfaz especificada para el tipo de número de argumentos.
bidirectional	(Opcional) Filtra la salida para mostrar solo la información acerca de la ruta bidireccional en la tabla de enrutamiento multicast.
count	(Opcional) Muestra las estadísticas sobre el grupo y fuente, incluido el número de paquetes, los paquetes por segundo, tamaño de paquete de promedio, y los bytes por segundo.
terse	(Opcional) Filtros de salida para mostrar una parte de las estadísticas de la tabla de enrutamiento multicast, con exclusión de origen y las estadísticas del grupo para cada entrada en la tabla de enrutamiento multicast.
dense	(Opcional) Filtros de salida para mostrar sólo la información

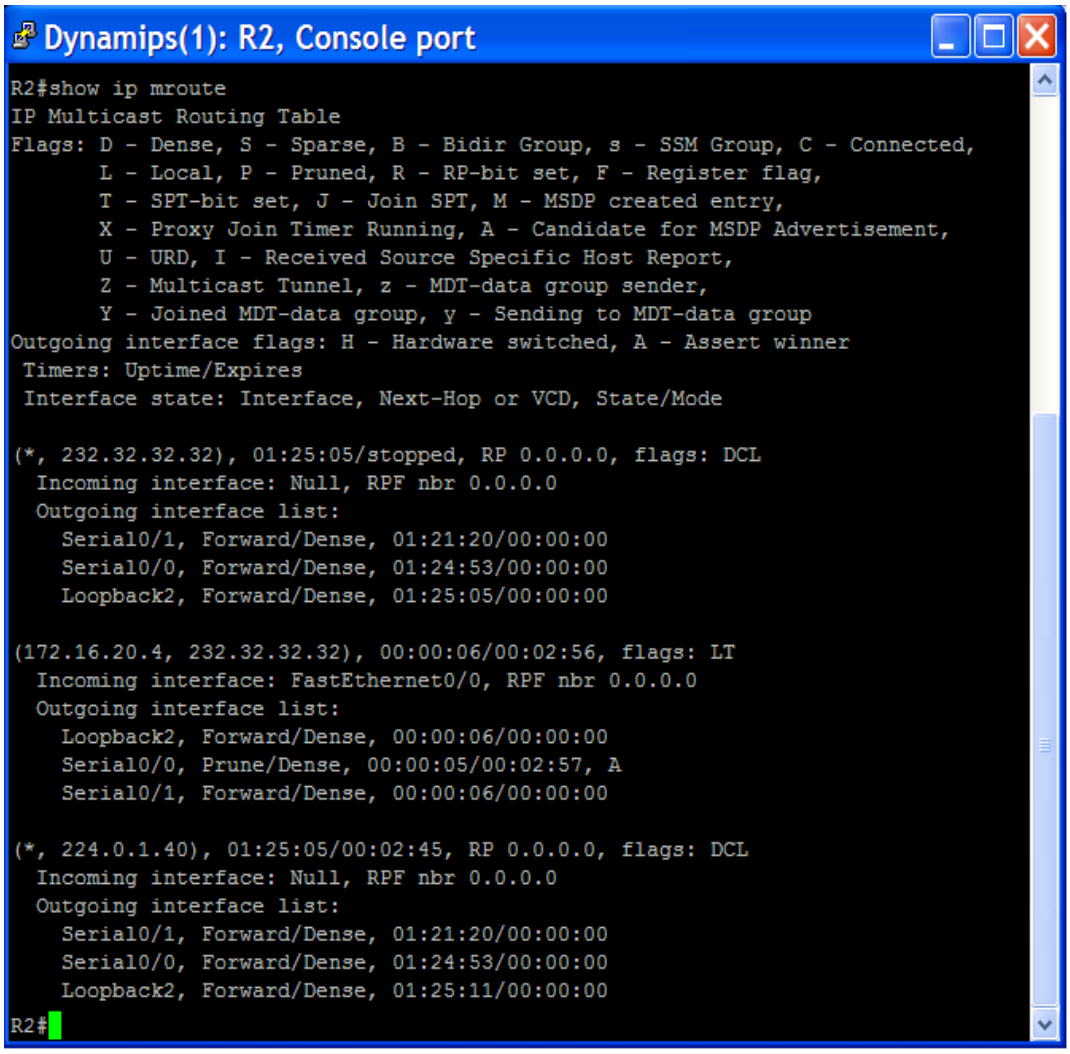
	sobre las rutas de modo denso en la tabla de enrutamiento multicast.
proxy	(Opcional) Muestra información sobre RPF vector proxies recibido en un router multicast.
pruned	(Opcional) Filtros de salida para mostrar la información sólo acerca de poda de rutas en la tabla de enrutamiento multicast.
sparse	(Opcional) Filtros de salida para mostrar solo la información sobre las rutas de modo esparcido en la tabla de enrutamiento multicast.
ssm	(Opcional) Filtra la salida para mostrar sólo las rutas de las fuentes específicas de multicast (SSM) en la tabla de enrutamiento multicast.
static	(Opcional) Filtra la salida para mostrar sólo las rutas estáticas en la tabla de enrutamiento multicast.
summary	(Opcional) Filtra la salida para mostrar una sola línea abreviada de resumen de cada entrada en la tabla de enrutamiento multicast.
group-address	(Opcional) dirección IP o DNS de un grupo de multicast.
source-address	(Opcional) dirección IP o el nombre DNS de una fuente de multicast.

Fuente: Aplicación Ciscopedia v.3.0.

Ejemplo:

El siguiente ejemplo muestra la salida de la tabla de enrutamiento del router R2 que opera en modo Denso:

Figura 67. Ejemplo del comando show ip mroute



Fuente: Software GNS3.

Descripción de los campos:

Tabla 42. Descripción de los campos del comando show ip mroute

Campo	Descripción
Flags:	Proporciona información acerca de la entrada. • D-denso. Indica que está funcionando en modo denso. • S-Sparse. Indica que está funcionando en modo disperso. • Grupo B-bidir. Indica que un grupo de multicast está funcionando en modo bidireccional. • Grupo s-SSM. Indica que un grupo de multicast está dentro del rango de direcciones IP SSM. Esta bandera se restablece si el rango SSM cambia. • C-Conectado. Un miembro del grupo de multicast está presente en la interfaz directamente conectada. • L-Local. El propio router es un miembro del grupo de multicast. Los Grupos se unen a nivel local por el comando **ip IGMP join-group** (por el grupo configurado), el comando **ip sap listen** (para los grupos de sesión de directorio muy conocidos), y punto de encuentro (RP) de asignación (para los grupos conocidos 224,0 .1.39 y 224.0.1.40). A nivel local se unen a los grupos que no conmutan rápido.

	• P-pruned. La ruta ha sido podada. El software IOS de Cisco mantiene la información para que un miembro descendente pueda unirse a la fuente. • R-RP-bit set. Indica que la entrada (S, G) está apuntando hacia el RP. Esta bandera suele indicar un estado de poda a lo largo del árbol compartido, para una fuente particular. • F-Register flag. Indica que el software se está registrando para un origen de multicast. • T-SPT-bit set. Indica que los paquetes se han recibido en el árbol fuente con el camino más corto. • J-Join SPT. Para las entradas (*, G), indica que la tasa de tráfico que fluye por el árbol compartido es superior al umbral SPT establecido para el grupo. (El valor predeterminado del umbral SPT es 0 kbps.) Cuando el J - Join más corto de camino del árbol (SPT) se establece el indicador, el siguiente (S, G) paquete recibido por el árbol para compartir, desencadena una (S, G) se unen en la dirección de la fuente, causando al router la unión al árbol fuente.
Flags: (continued)	Para las entradas (S, G), indica que la entrada se creó debido a que el umbral SPT para el grupo fue superado. Cuando la bandera J- unión STP se establece para las entradas (S, G), los monitores router de la tasa de tráfico en el árbol

	fuente y los intentos de volver a conmutar al árbol compartido, para esta fuente si la tasa de tráfico en el árbol fuente cae por debajo del Umbral SPT del grupo durante más de 1 minuto.
Flags: (continued)	Note Las medidas del router de la porción de tráfico en el árbol compartido, y compara el valor de medida respecto al Umbral SPT del grupo una vez todos los segundos. Si la tasa de tráfico que supera el Umbral SPT, la bandera J – unión STP se establece en la entrada (*, G) hasta la siguiente medición de la tasa de tráfico. La bandera se borra cuando llega el siguiente paquete en el árbol compartido, y un nuevo intervalo de medición se ha iniciado. Si el valor predeterminado del Umbral SPT de 0 kbps se utiliza para el grupo, la bandera J – union STP siempre se establece en entradas (*, G) y nunca se borra. Cuando el valor por defecto del umbral SPT se utiliza, el router inmediatamente conmuta por el camino mas corto al árbol fuente cuando el tráfico de una nueva fuente es recibido. M-MSDP entrada creada. Indica que una entrada (*, G) fue aprendido a través de un par de protocolo MSDP (Multicast Source Discovery Protocol). Este indicador sólo es aplicable a un RP corriendo en MSDP.

Flags: (continued)	Entrada fuente mroute E-Extranet. Indica que una entrada (*, G) o (S, G) en la tabla de enrutamiento VRF es una fuente de multidifusión VRF (MVRF) y tiene las entradas de MVRF de receptor extranet asociadas a ello. X-Proxy Join Timer Running. Indica que el temporizador proxy join está funcionando. Esta bandera sólo se establece para las entradas (S, G) de un RP o "cambio" del router. Un cambio del router se encuentra en la intersección de un camino del árbol compartido (*, G) y el camino más corto desde la fuente hasta el RP. A—Candidate for MSDP Advertisement. Indica que una entrada (S, G) se difundan a través de un par MSDP. Este indicador sólo es aplicable a un RP corriendo en MSDP.
Flags: (continued)	I—Received Source Specific Host Report. Indica que una entrada (S, G) fue creado por un informe (S, G). Este informe (S, G) podría haber sido creado por IGMPv3 (Internet Group Management Protocol Version 3), URD, o IGMP v3lite. Esta bandera sólo se establece en el router designado (DR). Túnel Z-multidifusión. Indica que esta entrada es un grupo de multidifusión IP que pertenece al túnel del árbol de distribución de multidifusión (MDT). Todos los paquetes recibidos para este estado de multidifusión IP se envían al túnel MDT

	para descapsular. Y—Joined MDT-data group. Indica que el tráfico se recibió a través de un túnel de MDT que se creó específicamente para esta fuente y de grupo. Esta bandera se encuentra solo en tablas mroute de la red virtual privada (VPN).
Flags: (continued)	y—Sending to MDT-data group. Indica que el tráfico fue enviado a través de un túnel de MDT que se creó específicamente para esta fuente y grupo. Esta bandera se encuentra solamente en tablas mroute VPN.
Outgoing interface flags:	Proporciona información acerca de la entrada. H—Hardware switched. Indica que una ruta de reenvío de una conmutación multicapa de multidifusión (MMLS) se ha establecido para esta entrada.
Timers:Uptime/Expires	"Uptime" indica por interfaz cuánto tiempo (en horas, minutos y segundos) que la entrada ha estado en la tabla de enrutamiento IP multicast. "Expires" indica por interfaz cuánto tiempo (en horas, minutos y segundos) hasta la entrada seaeliminada de la tabla de enrutamiento IP multicast.
Interface state:	Indica el estado de la interfaz de entrada o salida. Interfaz. Indica el tipo y número de la interfaz que

	figuran en la lista de interfaces de entrada o salida. Next-Hop or VCD. "Next-hop" especifica la dirección IP del vecino descendiente. "VCD" especifica el número de circuito descriptor virtual. State/Mode. "State" indica que los paquetes que serán transferidos podados, o nulos en la interfaz en dependencia de si existen restricciones debido a las listas de acceso o tiempo de vida (TTL) del umbral. "Mode", indica si la interfaz está funcionando en denso, esparcido, o modo disperso-denso.
(*, 224.0.255.1) and (192.168.37.100, 224.0.255.1)	Entrada en la tabla de enrutamiento IP Multicast. La entrada consiste en la dirección IP de la fuente seguido de la dirección IP del grupo de multidifusión. Un asterisco (*) en lugar de router indica la fuente de todas las fuentes. Las entradas en el primer formato se conocen como entradas(*, G). Las entradas en el segundo formato se conocen como entradas (S, G). las entradas (*, G) se utilizan para construir entradas (S, G).
RP	Dirección del router RP. Para los routers y servidores de acceso que funcionan en modo esparcido, esta dirección es siempre 224.0.0.0.

flags:	Información sobre la entrada.
Incoming interface:	Interfaz estimada para un paquete de multidifusión desde la fuente. Si el paquete no se recibe en esta interfaz, se descarta.
RPF neighbor or RPF nbr	Dirección IP del router ascendente a la fuente. *Tunneling* indica que este router está enviando datos al RP encapsulado en paquetes de registro. El número hexadecimal entre paréntesis indica que RP se esta registrando. Cada bit indica un diferente RP si múltiples RP por grupo se utilizan. Si un asterisco (*) aparece después de la dirección IP en este campo, el vecino del FPR se ha aprendido a través de una aserción.
Outgoing interface list:	Interfaces a través del cual los paquetes seran transmitidos. Cuando el comando **Ip pim nba-mode** está activado en la interfaz, la dirección IP vecino del Protocolo Independiente Multicast (PIM) también se muestra.

Fuente: Cisco IOS Cookbook.

Comando "Show ip pim neighbor"

Descripción: Para listar los vecinos PIM descubiertos por el software IOS Cisco, utilice el comando **show ip pim** neighbor.

Se usa para determinar qué router de la red LAN se configuran para PIM

Modo: Router>

Sintaxis: **show ip pim neighbor** [*type number*]

Descripción de la Sintaxis:

Tabla 43. Descripción de la sintaxis de show ip pim neighbor

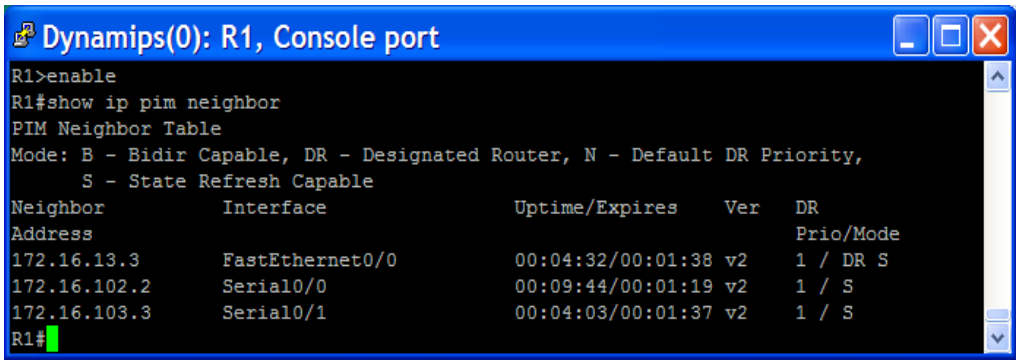
Campo	Descripción
type	(Opcional) tipo de interfaz.
number	(Opcional) número de la interfaz.

Fuente: Cisco IOS Cookbook.

Ejemplo:

El siguiente ejemplo muestra los vecinos del Router R1:

Figura 68. Ejemplo del comando show ip pim neighbor



Fuente: Software GNS3.

Descripción de los campos:

Tabla 44. Descripción de los campos de show ip pim neighbor

Campo	Descripción
Neighbor Address	Dirección IP del vecino PIM
Interface	Tipo y número de interfaz en el que el vecino se puede alcanzar.
Uptime	Cuánto tiempo en horas, minutos y segundos de la entrada ha estado el vecino PIM en la tabla.
Expires	Cuánto tiempo en horas, minutos y segundos hasta que la entrada sea eliminada de la tabla de enrutamiento IP multicast.
Mode	Modo en el que la interfaz está funcionando.
(DR)	Indica que este vecino es un router designado de la LAN.

Fuente: Aplicación Ciscopedia v.3.0.

Comando "Show ip pim interface"

Descripción: Para mostrar información sobre las interfaces configuradas para PIM, utilice el comando **show ip pim interface** en el modo ejecutable.

Este comando sólo funciona en las interfaces que se configuran para el PIM.

Modo: Router>

Sintaxis: **show ip pim interface** [*type number*] [**count**]

Descripción de la Sintaxis:

Tabla 45. Descripción de la sintaxis de show ip pim interface

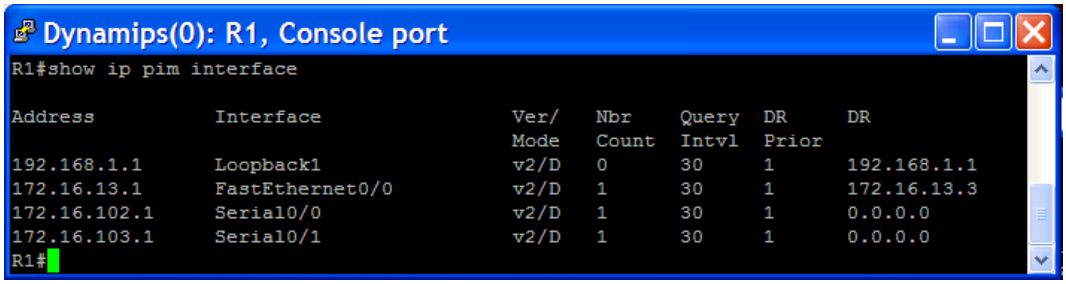
Campo	Descripción
type	(Opcional) Tipo de interfaz
number	(Opcional) Número de la interfaz
count	(Opcional) Número de paquetes recibidos y enviados fuera de la interfaz.

Fuente: Aplicación Ciscopedia v.3.0.

Ejemplo:

El siguiente ejemplo muestra la salida del comando **show ip pim interface** en el Router R1:

Figura 69. Ejemplo del comando show ip pim interface



Fuente: Software GNS3.

Descripción de los campos:

Tabla 46. Descripción de los campos de show ip pim interface

Campo	**Descripción**
Address	Dirección IP del router del siguiente salto.
Interface	Tipo y número de interfaz que está configurado para ejecutar el PIM.
Mode	Modo Multicast en el que el software IOS Cisco está operando. Este puede ser modo denso (dense mode) o modo disperso (sparse mode).

Neighbor Count	Número de vecinos PIM que se han descubierto a través de esta interfaz. Si el Neighbor Count es 1 para un túnel DVMRP, el vecino está activo (recibiendo sondeos y reportes).
Query Interval	Frecuencia, en segundos, de los mensajes PIM del router-query, según lo establecido por el comando **ip pim query-interval** en la configuración de la interfaz. El valor predeterminado es 30 segundos.
DR	Dirección IP del router designado en la LAN. Tenga en cuenta que las líneas del serial no han designado routers, lo que la dirección IP se muestra como 0.0.0.0.
FS	Un asterisco (*) en esta columna indica que la conmutación rápido está habilitada.
Mpackets In/Out	Número de paquetes de entrada y salida de la interfaz.

Fuente: Aplicación Ciscopedia v.3.0.

Comando "Show ip pim rp"

Descripción: Para mostrar los puntos de encuentro (RP) activos que se almacenan en caché asociado con entradas de

enrutamiento multicast, se utiliza el comando **show ip pim rp**.

Modo: Router#
Router>

Sintaxis: **show ip pim** [**vrf** *vrf-name*] **rp** [**mapping** | **metric**] [*rp-address*]

Descripción de la sintaxis:

Tabla 47. Descripción de los campos de show ip pim interface

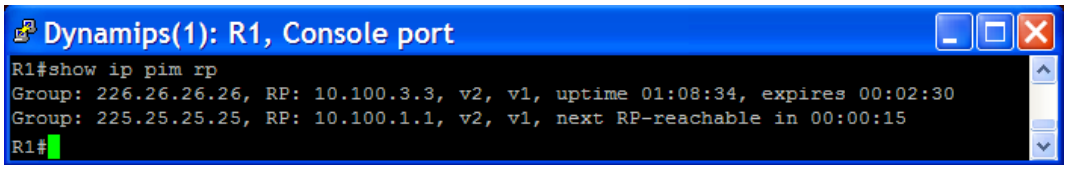
Campo	**Descripción**
vrf	(Opcional) Soporta VPN de enrutamiento multicast y reenvío (VRF).
vrf-name	(Opcional) Nombre asignado a la VRF.
mapping	(Opcional) Muestra todos los grupos para RP asignados el cual el router tiene conocimiento (ya sea configurado o extraídas de Auto-RP).
metric	(Opcional) Muestra la métrica de enrutamiento unicast para los RP configurados de forma estática o aprendido a través de Auto-RP o router bootstrap (BSR).
rp-address	(Opcional) dirección IP del RP.

Fuente: Aplicación Ciscopedia v.3.0.

Ejemplo:

El siguiente es un ejemplo de una salida utilizando el comando **show ip pim rp.**

Figura 70. Ejemplo del comando show ip pim rp



Fuente: Software GNS3.

Descripción de los campos:

Tabla 48. Descripción de los campos de show ip pim rp

Campo	Descripción
Group	Dirección del grupo multicast sobre la cual se mostrará la información del RP.
RP	Dirección del RP para ese grupo.
v2	Indica que el RP está ejecutando PIM versión 2.
v1	Indica que el RP está ejecutando PIM versión 1.

Uptime	Período en que el RP ha sido activado (en días y horas). Si es menos de 1 día,el tiempo es mostrado en horas, minutos y segundos.
expires	Tiempo en (horas, minutos y segundos) en el cual la entrada caducará.

Fuente: Aplicación Ciscopedia v.3.0.

Comando "Show ip pim rp mapping"

Descripción: Para mostrar las asignaciones para el grupo PIM a los puntos de encuentro activos, utilice el comando **show ip pim rp mapping**.

Modo: Router#
Router>

Sintaxis: **show ip pim** [**vrf** *vrf-name*] **rp mapping** [*rp-address*]

Descripción de la sintaxis:

Tabla 49. Descripción de la sintaxis de show ip pim rp mapping

Campo	Descripción
vrf *vrf-*	(Opcional) Nombre asignado a la VPN de enrutamiento

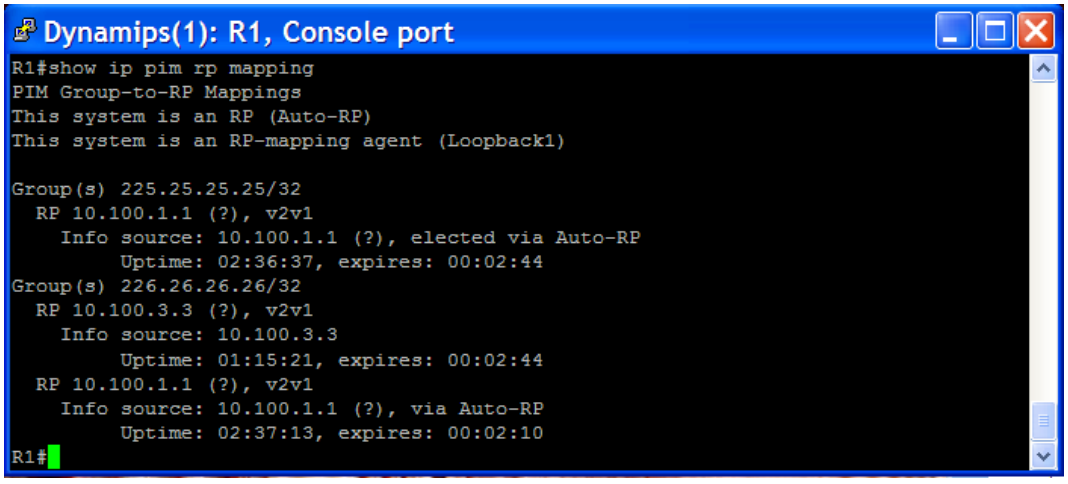
name	multicast y reenvío (VRF).
rp-address	(Opcional) dirección IP del punto de encuentro RP.

Fuente: Aplicación Ciscopedia v.3.0.

Ejemplo:

Este ejemplo indica cómo mostrar las asignaciones para el grupo PIM a los puntos de encuentro RP activos.

Figura 71. Ejemplo del comando show ip pim rp mapping



Fuente: Software GNS3.

Comando "show ip multicast interface"

Descripción: Para mostrar información sobre los parámetros de configuración de la interfaz IP multicast y contadores de

paquetes, se utiliza el comando **show ip multicast interface.**

Modo: Router>
Router#

Sintaxis: **show ip multicast** [**vrf** *vrf-name*] **interface** [*type number*]

Descripción de la Sintaxis:

Tabla 50. Descripción de la sintaxis de show ip multicast interface

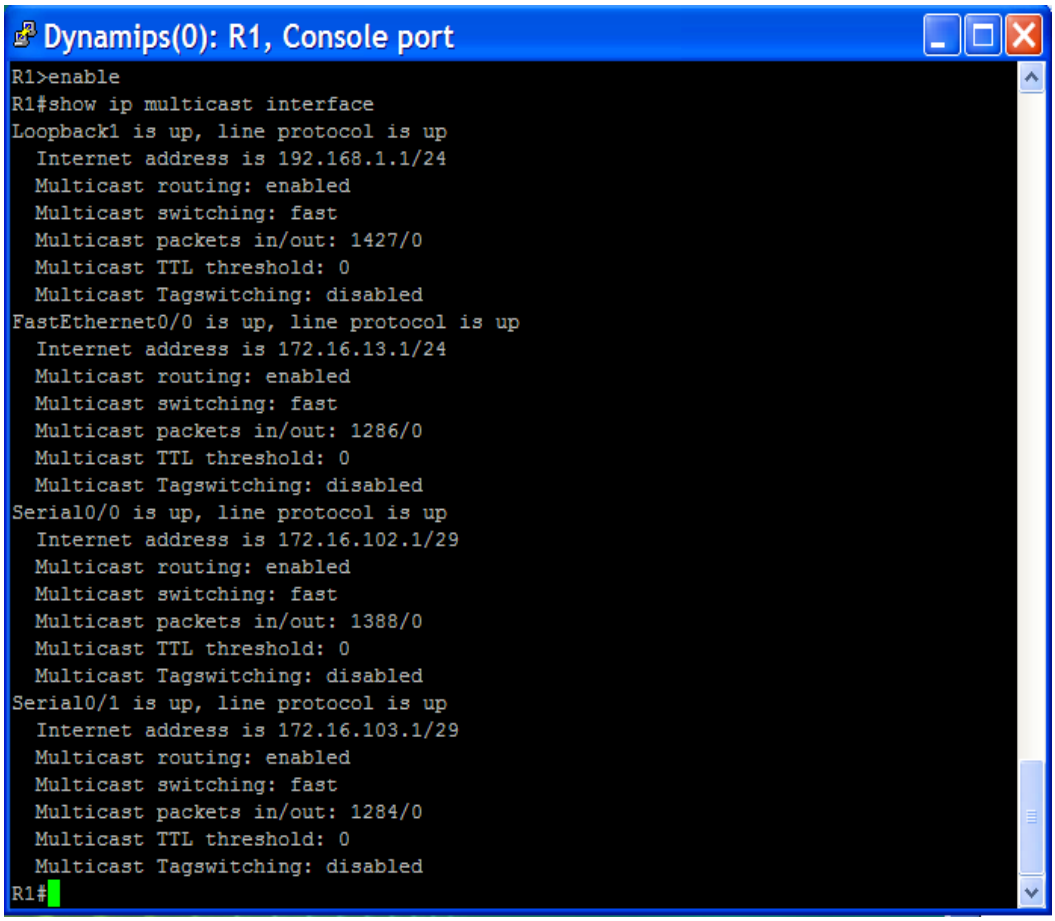
Campo	**Descripción**
vrf *vrf-name*	(Opcional) Restringe la salida para mostrar información sobre las interfaces habilitadas de multicast asociada con la red privada virtual de enrutamiento multicast (MVPN) y la instancia de reenvío (MVRF) especificada por el argumento *vrf-name*.
type number	(Opcional) Tipo de interfaz y el número para los cuales mostrar los parámetros de configuración de la interfaz.

Fuente: Aplicación Ciscopedia v.3.0.

Ejemplo:

El siguiente es el resultado del ejemplo del comando **show ip multicast interface**.

Figura 72. Ejemplo del comando show ip pim multicast interface



Fuente: Software GNS3.

Descripción de los campos:

Tabla 51. Descripción de los campos de show ip multicast interface

Campo	**Descripción**
<interface type> <interface number> is	Indica el estado de la interfaz multicast (up, down).

line protocol is	Indica el estado del funcionamiento del protocolo: - *up*: funcionando correctamente. - *down:* presenta fallas - *administratively down:* retirado manualmente por el administrador.
IP address is	Dirección IP configurada para la interfaz (mediante el comando **IP address**)**.**
Multicast routing:	Indica si enrutamiento multicast (Protocolo Independiente Multicast [PIM]) ha sido activada o desactivada en la interfaz (mediante el comando **ip pim**).
Multicast switching:	Indica el tipo de operación de conmutación multicast en la interfaz (cuando se configura con el comando **ip mroute-cache**).
Multicast packets in/out:	Muestra un contador de paquetes multicast.
Multicast TTL threshold:	Indica el umbral de tiempo de vida (TTL) de paquetes de multicast trasmitidos fuera de la interfaz (como se ha configurado con el comando **IP multicast ttl-threshold**). **Nota:** Este campo es obsoleto en versiones de Cisco

	IOS que soporte la IPv4 MFIB. Para estas versiones, este campo siempre mostrará "0" en la salida.
Multicast Tagswitching:	Este campo es obsoleto. Siempre se mostrará "Disabled" en la salida.

Fuente: Aplicación Ciscopedia v.3.0.

Comando "Show ip route"

Descripción: Utilice el comando **show ip route** en modo ejecución para mostrar el estado actual de la tabla de enrutamiento.

Modo: Router>

Sintaxis: **show ip route** [*address* [*mask*] [longer-prefixes]] | [*protocol* [*process-id*]] | [list *access-list-number* | *access-list-name*]

Descripción de la Sintaxis:

Tabla 52. Descripción de la sintaxis de show ip route address

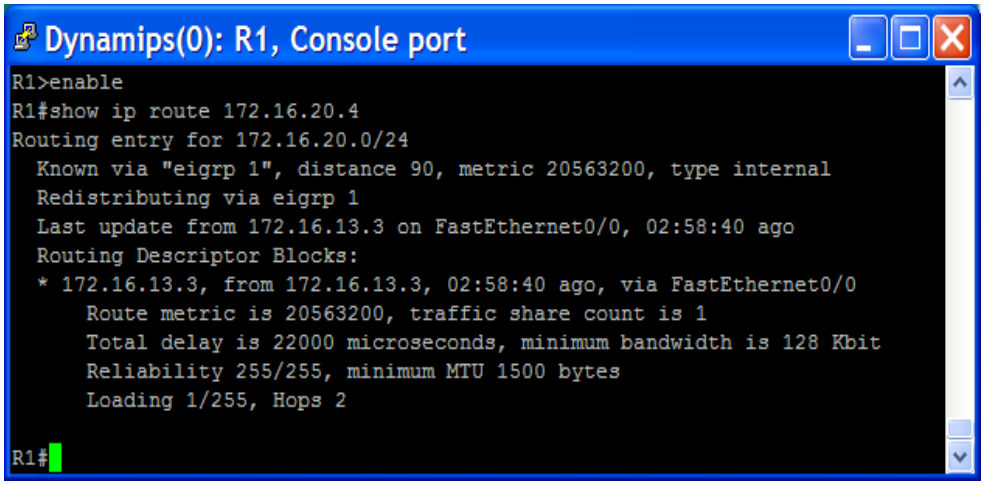
Campo	**Descripción**
address	(Opcional) Dirección de la cual se muestra la información de enrutamiento.
mask	(Opcional) Argumento para una máscara de subred.
longer-prefixes	(Opcional) La pareja dirección y máscara se convierten en un prefijo y cualquier ruta que

	coincidan con ese prefijo es mostrada.
protocol	(Opcional) Nombre de un protocolo de enrutamiento (BGP, EGP, EIGRP, hola, IGRP, isis, OSPF o RIP).
process-id	(Opcional) Número utilizado para identificar un proceso de protocolo especificado.
list	(Opcional) es requerida para filtrar la salida por nombre o número de lista de acceso.
access-list-name	(Opcional) Filtra la salida mostrada de la tabla de enrutamiento basada en el nombre de lista de acceso especificada.
access-list-number	(Opcional) Filtra la salida mostrada de la tabla de enrutamiento basada en el número de lista de acceso especificada.

Fuente: Aplicación Ciscopedia v.3.0.

Ejemplo:

Figura 73. Ejemplo del comando show ip route address



Fuente: Software GNS3.

Descripción de los campos: utilzando el comando **Show ip Route address**

Tabla 53. Descripción de los campos de show ip route address

Campo	Descripción
Routing entry for[ip-address [mask]	Número de red y la máscara.
Known via...	Indica cómo se obtuvo la ruta
Tag	Entero que se utiliza para implementar la ruta.
type	Indica el tipo de ruta IS-IS (Nivel 1 o Nivel 2).
Redistributing via...	Indica el protocolo de redistribución.
Last update from ip-address	Indica la dirección IP de un router que es el próximo salto a la red remota y la interfaz del router a la cual llegó la última actualización.
Routing Descriptor Blocks:	Muestra la dirección ip el siguiente salto seguida por la información de la fuente.

Route metric	Este valor es la mejor métrica para ese bloque de información multicast.
traffic share count	Número de usos para este bloque descriptor de enrutamiento

Fuente: Aplicación Ciscopedia v.3.0.

Comando "Show ip rpf"

Descripción: se utiliza para mostrar cómo el enrutamiento IP multicast realiza el RPF. Útil para verificar que la información de RPF es correcta. Si no lo es, chequea la tabla de enrutamiento de unicast para la dirección de origen.

Modo: Router>
Router#

Sintaxis: **show ip rpf** [vrf *vrf-name*] {*route-distinguisher* | *source-address* [*group-address*]} [metric]

Descripción de la Sintaxis:

Tabla 54. Descripción de la sintaxis de show ip rpf

Campo	Descripción
vrf *vrf-name*	(Opcional) Muestra la información que el enrutamiento IP multicast utiliza para revisar el RPF para una fuente de multicast asociada con la red privada virtual de multidifusión (MVPN) de enrutamiento y reenvío

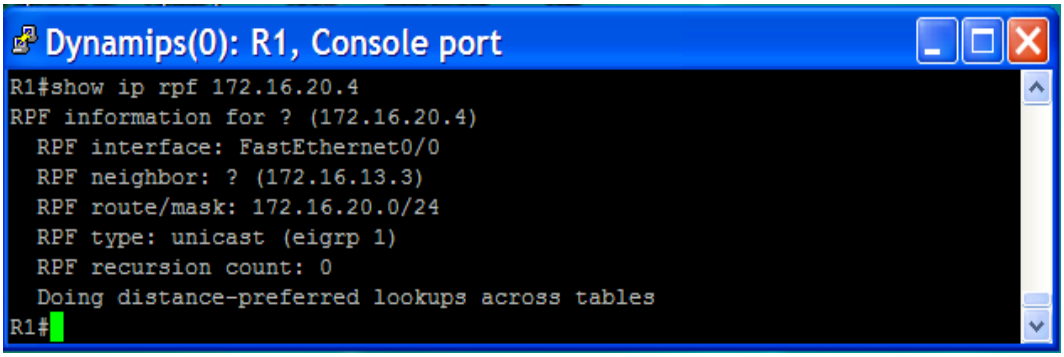
	(MVRF) instancia especificada por el argumento *vrf-name*.
route-distinguisher	Distintivo de ruta (RD) de un prefijo VPNv4. Muestra información RPF relacionada con la ruta VPN especificada.
source-address	Dirección IP o nombre de una fuente multicast para la cual se muestra información RPF.
group-address	(Opcional) dirección IP o nombre de un grupo multicast para el cual se muestra información RPF.
metric	(Opcional) Muestra la métrica del enrutamiento unicast.

Fuente: Aplicación Ciscopedia v.3.0.

Ejemplo:

El siguiente es resultado de ejemplo del comando show ip del RPF asignando una dirección:

Figura 74. Ejemplo del comando show ip rpf



Fuente: Software GNS3.

Descripción de los campos:

Tabla 55. Descripción delos campos del comando show ip rpf

Campo	Descripción
RPF information for	Nombre de host y dirección de origen para los que se muestra la información RPF.
RPF interface	Para la fuente dada, la interfaz desde la cual el router espera para recibir paquetes.
RPF neighbor	Para la fuente dada, el vecino desde el cual el router espera para recibir paquetes.
RPF route/mask	Número de ruta y máscara que coincide con la fuente.
RPF type	Tabla de enrutamiento de la cual se obtuvo esta ruta, ya sea unicast, MBGP, DVMRP, o mroutes estática.
RPF recursion count	El número de veces que la ruta es resuelta recursivamente.
Doing distance-preferred	Si el RPF se determinó basándose en la distancia o longitud de la máscara.
Metric	El valor de preferencia para la selección de la métrica

preference	de enrutamiento unicast al RP anunciado por el promotor designado (DF).
Metric	Métrica de enrutamiento de unicast a la RP anunciado por el DF.

Fuente: Aplicación Ciscopedia v.3.0.

Comando "ip default-gateway"

Descripción: Es usado para definir una puerta de enlace predeterminada cuando el enrutamiento IP está deshabilitado. Para desactivar esta función, utilice la forma **no** de este comando

Modo: Router(config)#

Sintaxis: **ip** *default-gateway ip address*

no ip *default-gateway ip address*

Descripción de la Sintaxis:

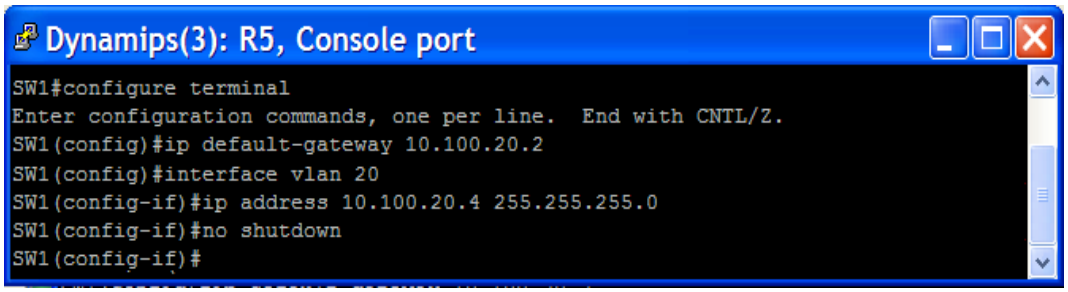
Tabla 56. Descripción de la sintaxis del comando ip default gateway

Campo	Descripción
ip-address	Dirección IP del router

Fuente: Aplicación Ciscopedia v.3.0.

Ejemplo:

Figura 75. Ejemplo del comando show ip default gateway



Fuente: Software GNS3.

Comando "ip igmp join-group"

Descripción: Para unir el router a un grupo multicast se utiliza el comando **ip igmp join-group**. Para cancelar los miembros en un grupo multicast, utilice la forma **no** de este comando.

Modo: Router(config)#

Sintaxis: **ip igmp join-group** *group-address*

no ip igmp join-group *group-address*

Descripción de la Sintaxis:

Tabla 57. Descripción de la sintaxis del comando ip igmp join group

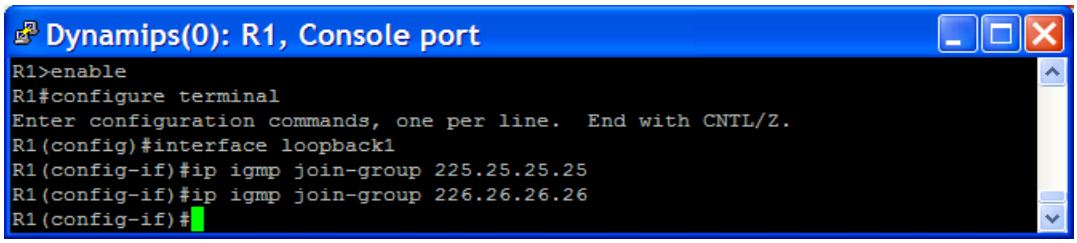
Campo	Descripción
group-address	Dirección del grupo multicast.

Fuente: Aplicación Ciscopedia v.3.0.

Ejemplo:

En el siguiente ejemplo, el router R1 se une al grupo multicast 225.25.25.25 y 226.26.26.26

Figura 76. Ejemplo del comando ip igmp join group



Fuente: Software GNS3.

Comando "ip multicast-routing"

Descripción: Para habilitar el enrutamiento IP multicast, utilice el comando **IP multicast-routing.** Para deshabilitar el enrutamiento IP multicast, utilice la forma **no** de este comando. Cuando el enrutamiento IP multicast está deshabilitado, el software IOS Cisco no transmite ningún paquete multicast.

Modo: Router(config)#

Sintaxis: **ip multicast-routing [distributed]**
no ip multicast-routing

Descripción de la Sintaxis:

Tabla 58. Descripción de la sintaxis del comando ip multicast routing

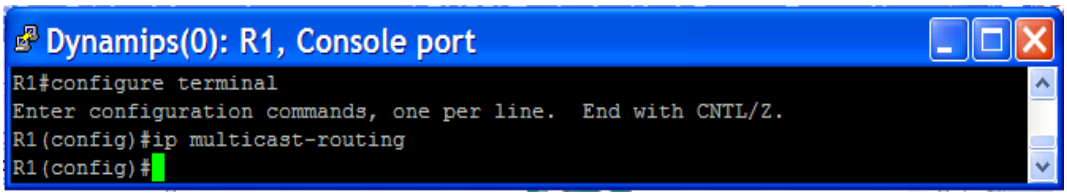
Campo	Descripción
distributed	(Opcional) Permite MDS

Fuente: Aplicación Ciscopedia v.3.0.

Ejemplo:

En el siguiente ejemplo se habilita el enrutamiento IP multicast en el router R1:

Figura 77. Ejemplo del comando ip multicast routing



Fuente: Software GNS3.

Comando "ip pim dense-mode"

Descripción: Para habilitar el Protocolo Independiente Multicast (PIM) en una interfaz, utilice el comando **ip pim** en el modo de configuración de la interfaz. Para deshabilitar PIM en la interfaz, utilice la forma **no** de este comando.

Modo: Router(config-if)#

Sintaxis: **ip pim** {sparse-mode | sparse-dense-mode | dense-mode [proxy-register {list access-list | route-map map-name}]} no ip pim

Descripción de la Sintaxis:

Tabla 59. Descripción de la sintaxis del comando ip pim dense-mode

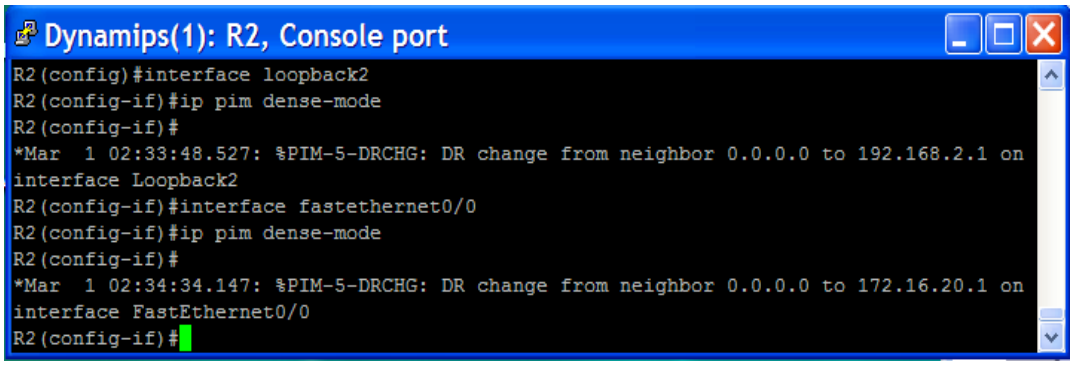
Campo	Descripción
sparse-mode	Habilita el modo de operación disperso (sparse mode).
sparse-dense-mode	La interfaz es tratada en modo de operación disperso (sparse mode) o modo denso (dense mode). Dependiendo en que modo opera el grupo multicast.
dense-mode	Habilita el modo de operación denso (dense mode)
proxy-register	(Opcional) habilita el registro proxy en la interfaz de un router designado (DR) para tráfico multicast a partir de fuentes no conectadas al RD.
list access-list	(Opcional) Define el número o nombre de la lista de acceso.
route-map map-name	(Opcional) Define el mapa de la ruta.

Fuente: Aplicación Ciscopedia v.3.0.

Ejemplo:

El siguiente ejemplo muestra cómo habilitar el modo denso (PIM-SM) en la interfaz loopback 2 y fastethernet 0/0.

Figura 78. Ejemplo del comando ip pim dense-mode



Fuente: Software GNS3.

Comando "ip pim rp-address"

Descripción: Para configurar la dirección de un punto de encuentro PIM (RP) para un grupo en particular, se utiliza el comando **ip pim rp-address** en la configuración global. Para eliminar una dirección RP, utilice la forma **no** de este comando. Debe configurar la dirección IP del RP en todos los routers (incluido en el router RP).

Modo: Router(config)#

Sintaxis: **ip pim rp-address** *ip-address*[*group-access-list-number*] [**override**]

no ip pim rp-address *ip-address* [*group-access-list-number*]

Descripción de la sintaxis:

Tabla 60. Descripción de la sintaxis del comando ip pim rp-address

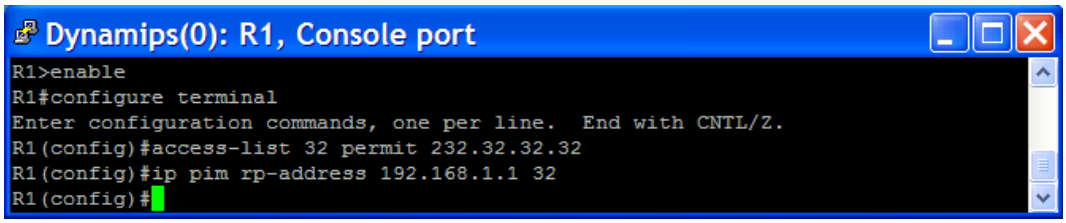
Campo	Descripción
ip-address	Dirección IP del router RP PIM. Esta es una dirección IP unicast.
group-access-list-number	(Opcional) Número de una lista de acceso que define para qué grupos de multicast debe ser utilizado el RP. Esta es una lista de acceso para IP estándar. El número puede ser de 1 a 100.
override	(Opcional) Indica que si hay un conflicto entre el RP configurado.

Fuente: Aplicación Ciscopedia v.3.0.

Ejemplo:

En el ejemplo siguiente se establece la dirección de PIM RP a 192.168.1.1 solo para el grupo multicast 232.32.32.32:

Figura 79. Ejemplo del comando ip pim rp-address



Fuente: Software GNS3.

Comando "ip pim send-rp-announce"

Descripción: Se usa en el router que desea ser un RP. Este comando hace que el router envie un mensaje de anuncio de Auto-RP al grupo mejor conocido **CISCO-RP-announce** (224.0.1.39). Este mensaje anuncia el router como un candidato del RP para los grupos en el rango descrito por la lista de acceso. Para cambiar este router de ser el RP, utilice la forma **no** de este comando.

Modo: Router(config)#

Sintaxis: **ip pim send-rp-announce** *type number* **scope** *ttl* **group-list** *access-list-number*
no ip pim send-rp-announce

Descripción de la sintaxis:

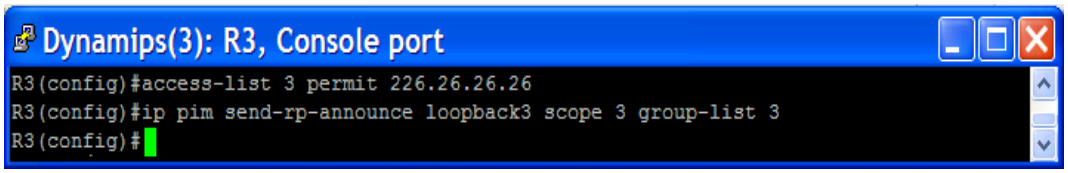
Figura 80. Descripción de la sintaxis del comando send-rp-announce

Campo	Descripción
type number	Tipo y número de Interfaz que identifican la dirección del RP.
scope ttl	Valor del tiempo de vida, que limita los anuncios.
group-list access-list-number	Lista de acceso que descríbe los rangos del grupo para que este router sea el RP.

Fuente: Aplicación Ciscopedia v.3.0.

Ejemplo:

Figura 81. Ejemplo del comando send-rp-announce



Fuente: Software GNS3.

Comando "ip pim send-rp-discovery"

Descripción: Para configurar el router como un agente RP-mapping, se utiliza el comando **ip pim send-rp-discovery.** Para restaurar el valor por defecto, utilice la forma **no** de este comando.

Modo: Router(config)#

Sintaxis: **ip pim send-rp-discovery** [*type number*] **scope** *ttl*

no ip pim send-rp-discovery [*type number*] **scope** *ttl*

Descripción de la sintaxis:

Tabla 61. Sintaxis de ip pim send-rp-discovery

Campo	Descripción
type number	(Opcional) Tipo y número de interfaz que se utiliza para definir la asignación de la dirección del agente de mapeo RP.

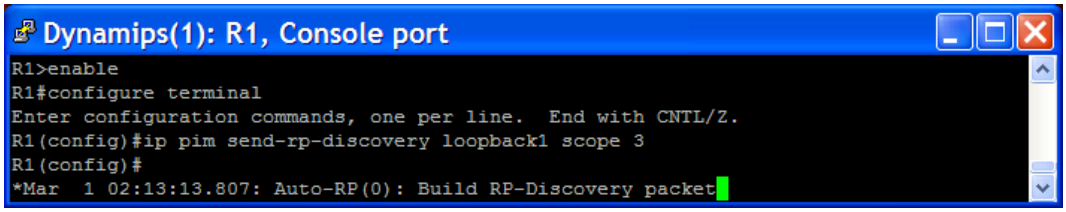
scope ttl	Valor de tiempo de vida en la cabecera IP que mantiene los mensajes de descubrimiento dentro de esta cantidad de saltos.

Fuente: Aplicación Ciscopedia v.3.0.

Ejemplo:

El siguiente ejemplo limita mensajes de descubrimiento RP auto-rp a 3 saltos:

Figura 82. Ejemplo del comando ip pim send-rp-discovery



Fuente: Software GNS3.

Comando "mrinfo"

Descripción: Este comando muestra la información multicast del router vecino, las capacidades del router y la versión, información multicast de la interfaz, los umbrales de TTL, métrica, protocolo, y el estado. Es útil cuando se necesita para verificar vecinos de multicast, confirma que la adyacencia vecina bidireccional existe, y verifica que los túneles son en ambas direcciones.

Modo: Router>

Sintaxis: **mrinfo** [*host-name* | *host-address*] [*source-address*]

no mrinfo

Descripción de la Sintaxis:

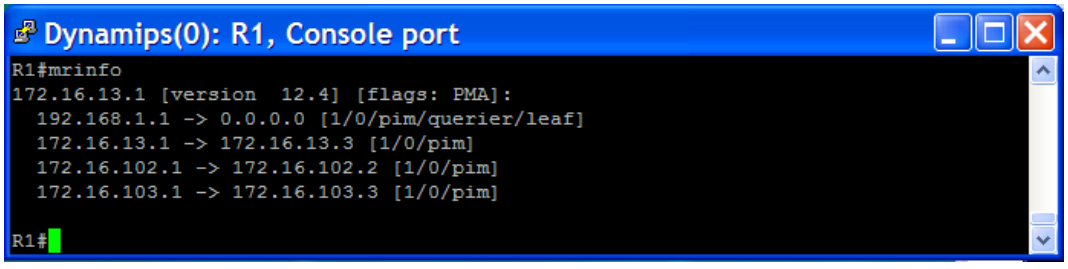
Tabla 62. Descripción de la sintaxis del comando mrinfo

Campo	Descripción
host-name | *host-address*	(Opcional) puede ser uno de los siguientes: • Nombre DNS (Domain Name System • Dirección de IP de un router multicast.
source-address	(Opcional) Dirección de origen utilizados en la solicitud de la información de enrutamiento multicast (mrinfo). Si se omite, la fuente se basa en la interfaz de salida para el destino.

Fuente: Aplicación Ciscopedia v.3.0.

Ejemplo:

Figura 83. Ejemplo del comando mrinfo



Fuente: Software GNS3.

4. SIMULADORES DE REDES

Los simuladores de redes de comunicaciones permiten crear topologías de red mediante la selección de los dispositivos y su respectiva ubicación en un área de trabajo, utilizando una interfaz gráfica. Tienen la característica fundamental de permitir la realización del diseño de topologías, la configuración de dispositivos de red, así como la detección y corrección de errores en sistemas de comunicaciones, razón por la cual se consideran como herramientas de gran ayuda en el estudio y aprendizaje del funcionamiento y configuración de redes de comunicaciones y aplicaciones.

Para los ejercicios de simulación realizados en el presente documento se utilizaron los simuladores de redes Packet Tracer (propietario Cisco) versión 5.2 y GNS3 (libre distribución) versión 0.7.

A continuación se realizará una descripción general de estos simuladores y de su entorno de trabajo.

4.1. PACKET TRACER

4.1.1. Descripción General

El simulador Packet Tracer tiene un ambiente de trabajo basado en ventanas que facilitan la creación, configuración y la simulación de redes. Packet Tracer tiene dos áreas de trabajo:

- Lógica: El espacio de trabajo lógico permite crear topologías de red lógica mediante la distribución, la conexión, y la agrupación de los dispositivos virtuales de la red.

- Física: El espacio de trabajo físico proporciona una dimensión gráfica física de la red lógica, dando un sentido de la escala y la distribución

de cómo los dispositivos de red tales como routers, switches y servidores se verían en un entorno real.

Packet Tracer ofrece dos modos operativos para visualizar el comportamiento de una red:

- En tiempo real: El modo en tiempo real la red se comporta como los teléfonos reales, con respuesta inmediata en tiempo real de todas las actividades de la red.
- En Simulación: En el modo simulación, el usuario puede ver y controlar los intervalos de tiempo, el funcionamiento interno de transferencia de datos, y la propagación de datos a través de una red.

CARACTERÍSTICAS

Packet Tracer posee las siguientes características:

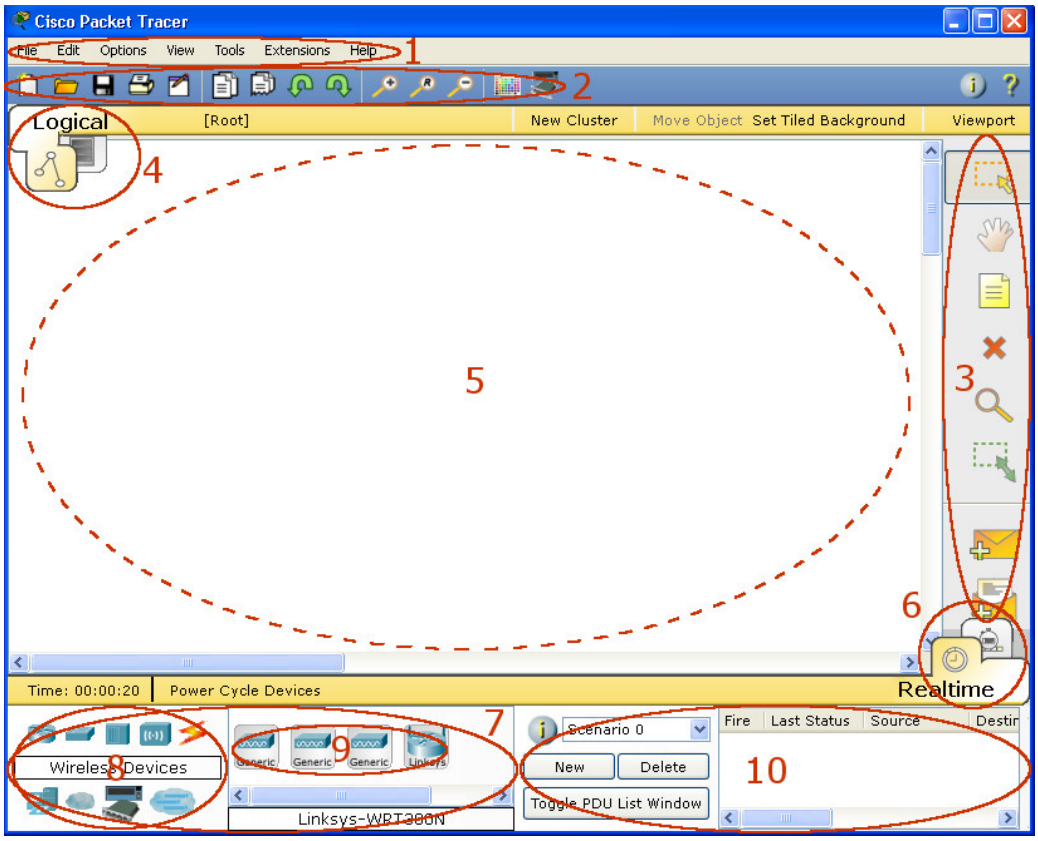
- Utiliza Comandos CLI (command Line Interface).
- Posee una lista de eventos globales (analizador de paquetes).
- Permite LAN, Conmutación, TCP / IP, Enrutamiento, protocolos WAN.
- Funcionalidad Multiusuario.
- Soporte para múltiples plataformas.
- Soporte para múltiples idiomas.
- Ayuda integrada y tutoriales

4.1.2. Entorno de trabajo

A continuación se dará una sencilla introducción del entorno gráfico de packet tracer:

Al iniciar el programa aparece la ventana de inicio, la cual permite el diseño, la interconexión entre los dispositivos, la configuración de los puertos interconectados entre los dispositivos y la edición de los parámetros y características de cada elemento creado en la red como se muestra en la siguiente figura.

Figura 84. Ventana de inicio de Packet Tracer



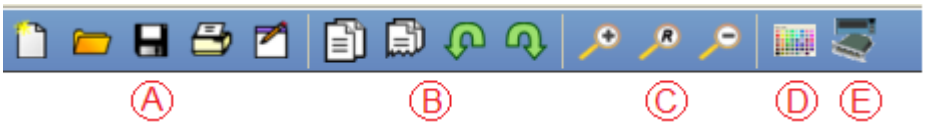
Fuente: Software GNS3.

La herramienta Packet Tracer posee:

1. Barra de menú: cuenta con las opciones de *File, Edit, Options, view, Tools, Extensions* y *Help,* para manejo y edición de archivos de configuración.

2. Barra de uso rápido: Se divide en cinco grupos:

Figura 85. Barra de uso rápido de packet tracer.



Fuente: Software GNS3.

A. Nuevo / Abrir / Guardar / Imprimir / Asistente para actividades.
B. Copiar / Pegar / Deshacer.
C. Aumentar Zoom / Tamaño original / Reducir Zoom.
D. Dibujar figuras (cuadrados, círculos y líneas).
E. Panel de Dispositivos Personalizados: Sirve para agregar o quitar dispositivos personalizados

3. Barra de acceso común: Provee herramientas para la manipulación de los dispositivos

Tabla 63. Herramientas para la manipulación de los dispositivos

	Selección de dispositivos y conexiones, no selecciona conexiones wireless.
	Movimiento de Rejilla, moviliza los dispositivos alrededor del área de trabajo
	Notas, permite agregar notas que enriquecen de conocimiento, del área de trabajo.
	Eliminar, permite eliminar cualquier dispositivo, conexión (excepto wireless) y notas.
	Inspector, permite visualizar la tabla correspondiente al dispositivo seleccionado, entre ellas ARP, MAC y

	ROUTER.
	Permite redimensionar el tamaño del dispositivo
	Mensaje Simple UDP, permite crear paquete del tipo ICMP entre dispositivos
	Mensaje Complejos UDP, permite crear paquetes personalizados entre dispositivos.

Fuente: Autoras.

4. Áreas de trabajo: lógica y física

Figura 86. Áreas de trabajo de packet tracer.

Fuente: Software GNS3.

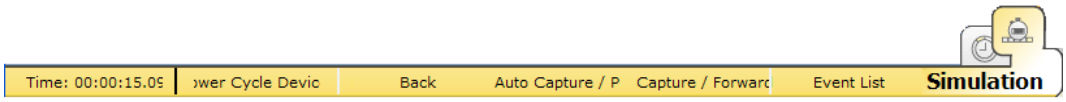
5. Espacio de trabajo: Área donde se crea la topología de la red.

Figura 87. Espacio de trabajo de packet tracer

Fuente: Software GNS3.

6. Modo de trabajo: En tiempo real y Simulación.

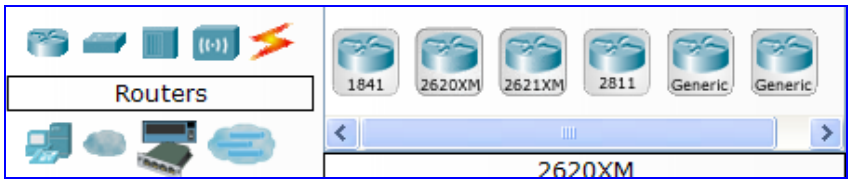
Figura 88. Modos de trabajo de packet tracer



Fuente: Software GNS3.

7. Componentes de la red: Esta sección permite elegir el dispositivo y conexión para llevarlo al área de trabajo.

Figura 89. Componentes de red de packet tracer



Fuente: Software GNS3.

8. Selección de Tipos de dispositivos: Contiene el tipo de dispositivo y de conexión que tiene disponible packet tracer.

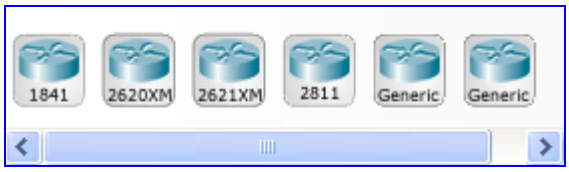
Figura 90. Tipos de dispositivos de packet tracer

Fuente: Software GNS3.

Por ejemplo, al seleccionar un router, a la par aparece una serie de referencias de routers, entre ellos se destacan los específicos de CISCO y un genérico. En el caso de los hubs, solo se dispone de genéricos. Las conexiones tienen todas las conocidas, desde automáticas, que detectan el tipo correcto entre dispositivos, hasta punto a punto (Cooper Straight - through), cruzadas (Cooper Cross - over), consola (console), fibra óptica (fiber), teléfono (telephone), Serial DCE y Serial DTE. Entre los últimos se encuentran los dispositivos (genéricos) que van conectados entre si, es decir PCs, servidores, impresoras.

9. Selección específica del dispositivo: Dispositivo y conexión especifica a elegir para llevarlo al área de trabajo.

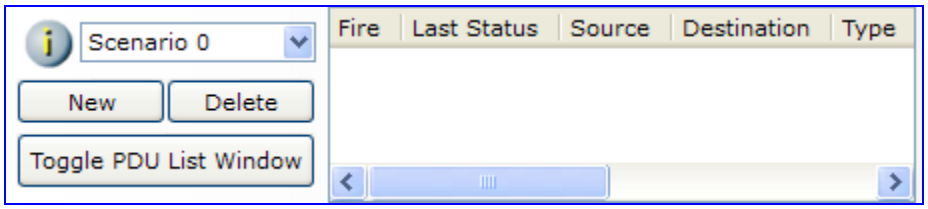
Figura 91. Tipos de router en packet tracer



Fuente: Software GNS3.

10. Ventana de paquetes creados: Esta ventana maneja los paquetes que se han colocado en la red durante la simulación del escenario.

Figura 92. Paquetes creados en la red en la simulación

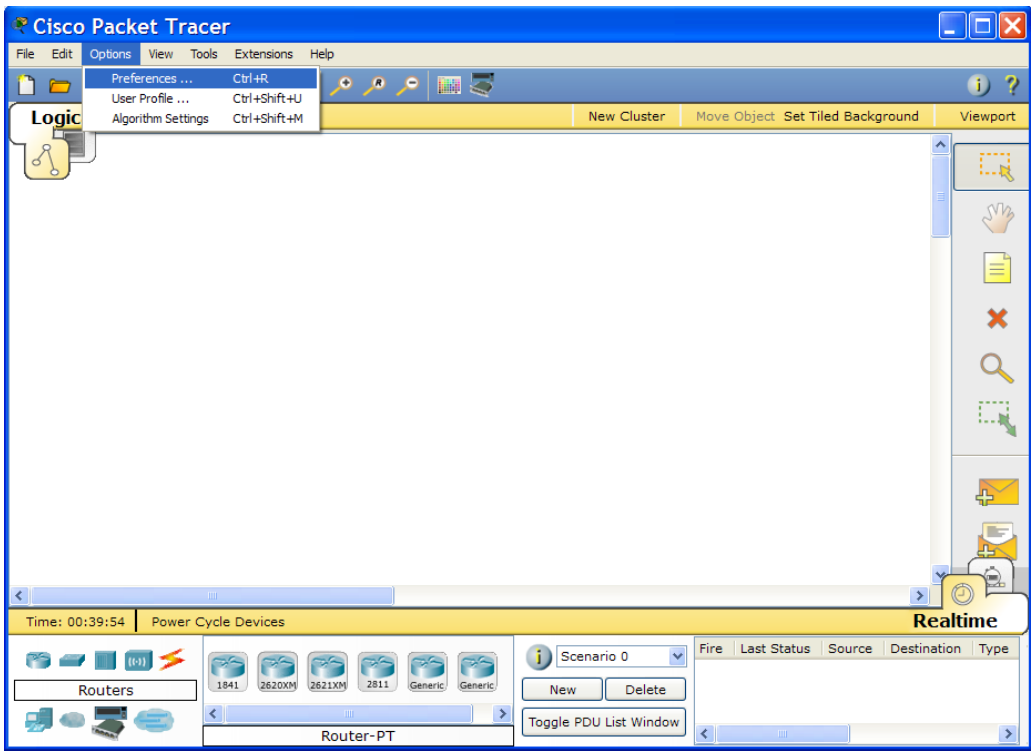


Fuente: Software GNS3.

4.1.3. Instrucciones básicas de configuración

Para personalizar la herramienta en el menú "*Options*" elegir la opción *"Preferencies"* :

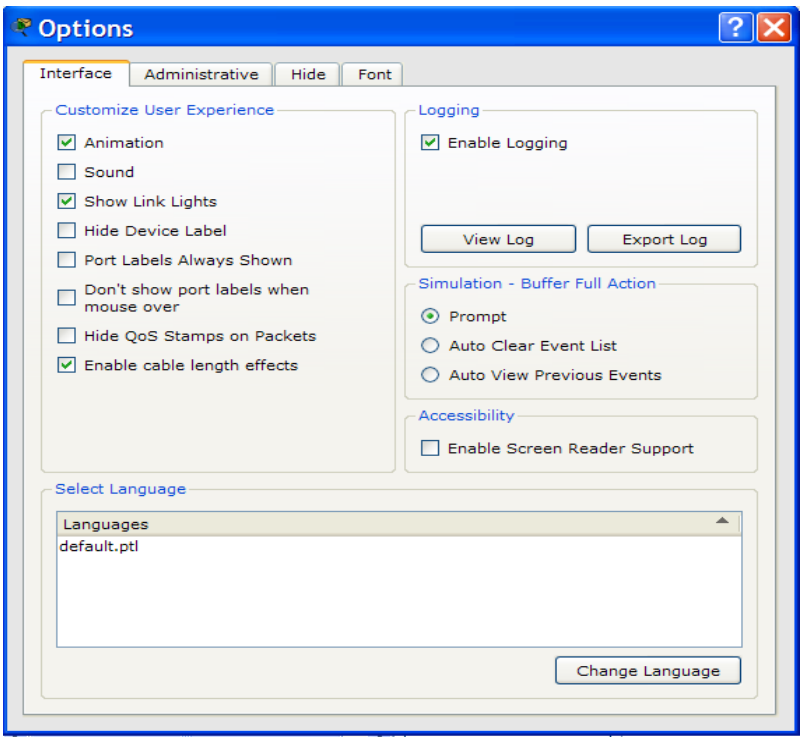
Figura 93. Configuración de preferencias de packet tracer



Fuente: Software GNS3.

La pestaña de "*interface*" permite habilitar o deshabilitar las opciones de animación, sonido, y etiquetas. Además de seleccionar el idioma que dispone la herramienta.

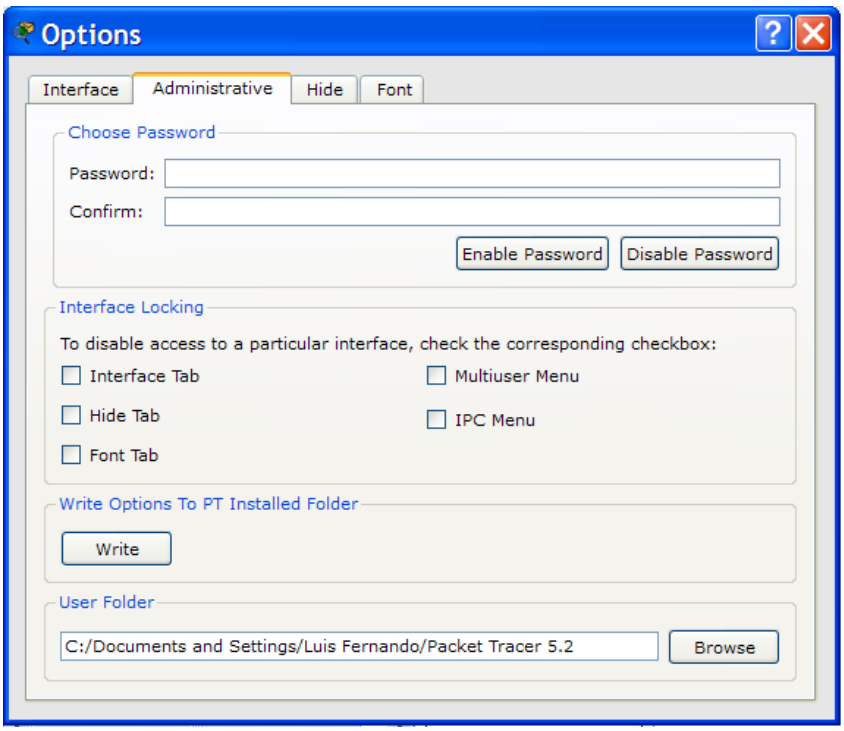
Figura 94. Opciones de la interfaz de packet tracer



Fuente: Software GNS3.

La pestaña de "*Administrative*" contiene opciones adicionales de administración. Entre las cuales dispone de un password y su confirmación para futuras entradas a la herramienta. Al igual que la activación y desactivación del password, el bloqueo del acceso a una interface en particular, entre otros.

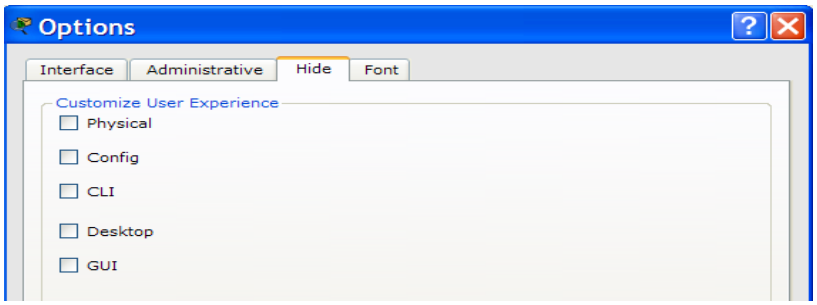
Figura 95. Opciones de administración de packet tracer



Fuente: Software GNS3.

La pestaña de "*Hide"* permite ocultar o mostrar los opciones de *Physical, Config, CLI, Desktop, GUI* de la herramienta.

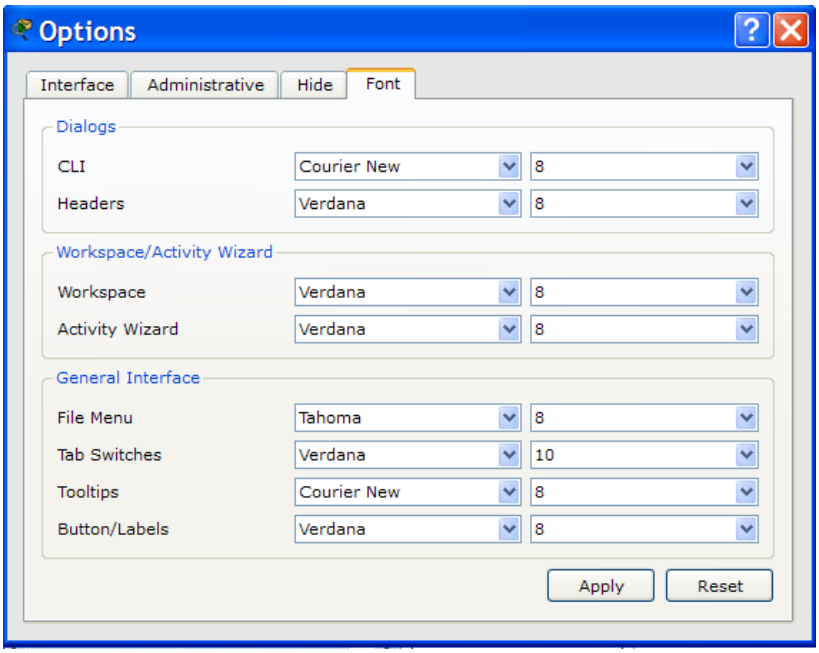
Figura 96. Opciones de configuración de packet tracer



Fuente: Software GNS3.

La pestaña "*font*" permite seleccionar los diferentes tipos de letras, y tamaños para los diálogos, área de trabajo y la interfaz en general.

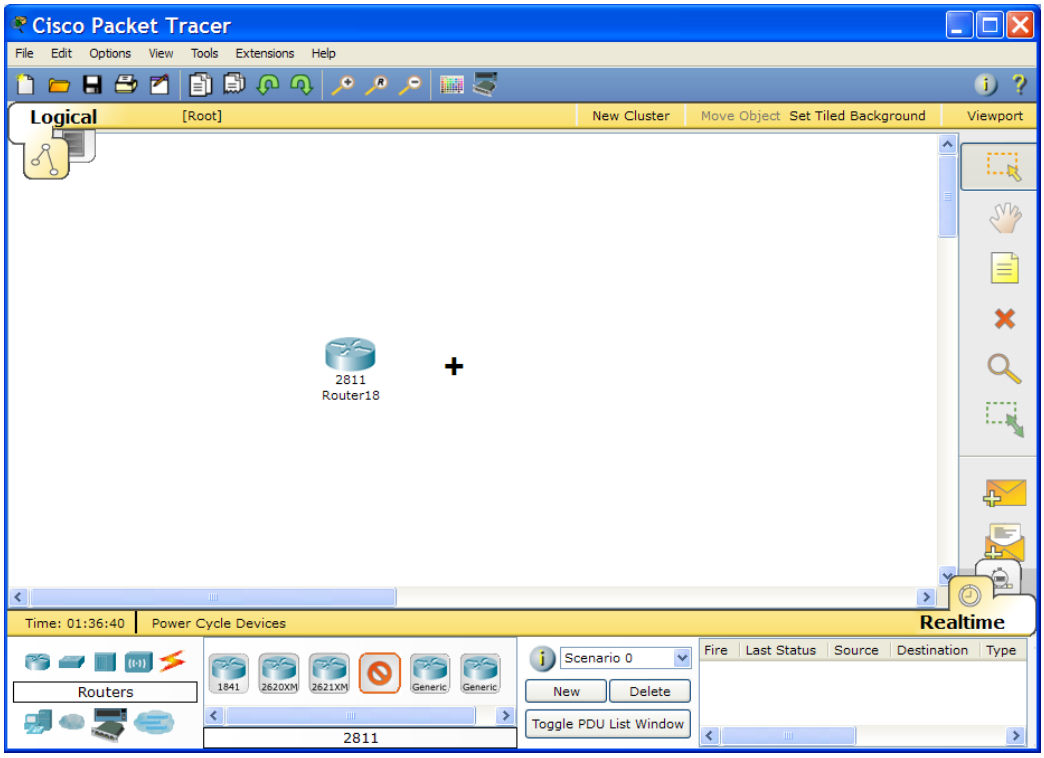
Figura 97. Opciones de configuración de la interfaz de packet tracer.



Fuente: Software GNS3.

Para la creación de una red se deben agregar los dispositivos necesarios, tales como un router, switch, computador, etc. haciendo clic sobre el dispositivo y colocarlo en el área de trabajo. Al dar clic sobre el dispositivo el cursor cambia de una flecha a un signo más (+).Para terminar se digita la tecla ESC, o un clic sobre el botón del dispositivo seleccionado.

Figura 98. Creación de topología en el área de trabajo.



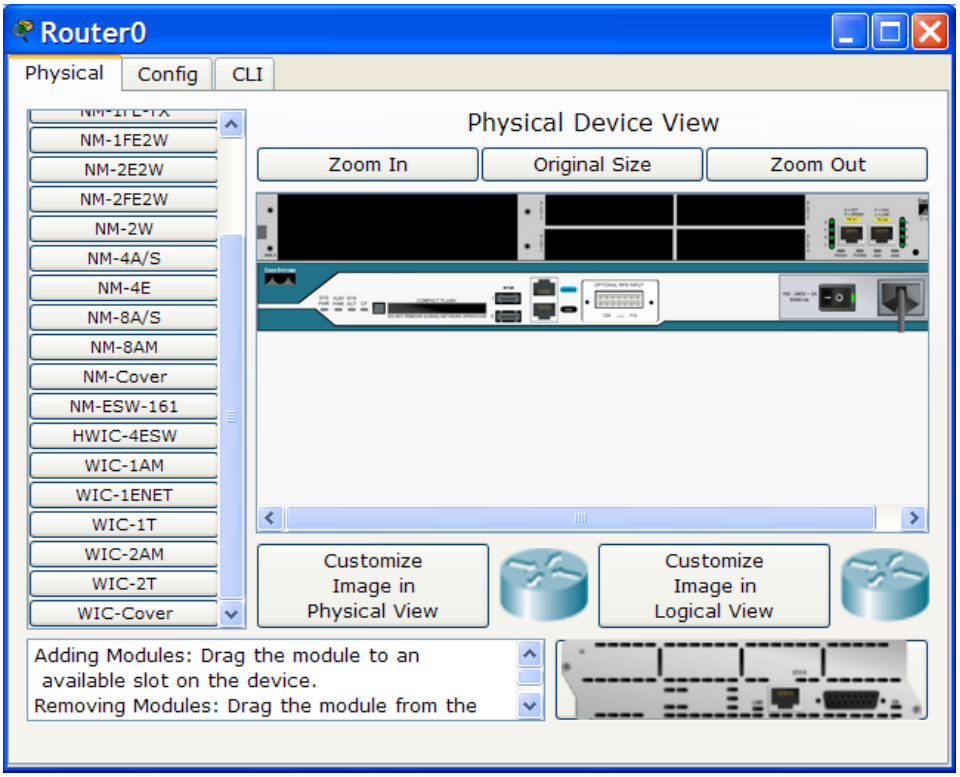
Fuente: Software GNS3.

Para ingresar a la configuración del router se hace doble clic sobre el dispositivo.

En la pestaña "*Physical*" se obtiene la vista física del dispositivo, y los módulos disponibles que se pueden insertar al dispositivo, se debe tener en cuenta que para insertar estos módulos el dispositivo debe estar apagado, para apagarlo debe hacer clic en el botón 

Para agregar un módulo, se debe seleccionar con el mouse y llevarlo hacia la vista física del dispositivo ubicado al lado derecho de la lista de módulos, luego debe encender el dispositivo para continuar con la configuración.

Figura 99. Vista física del dispositivo.



Fuente: Software GNS3.

La pestaña "*Config*" ofrece cuatro niveles generales de configuración:

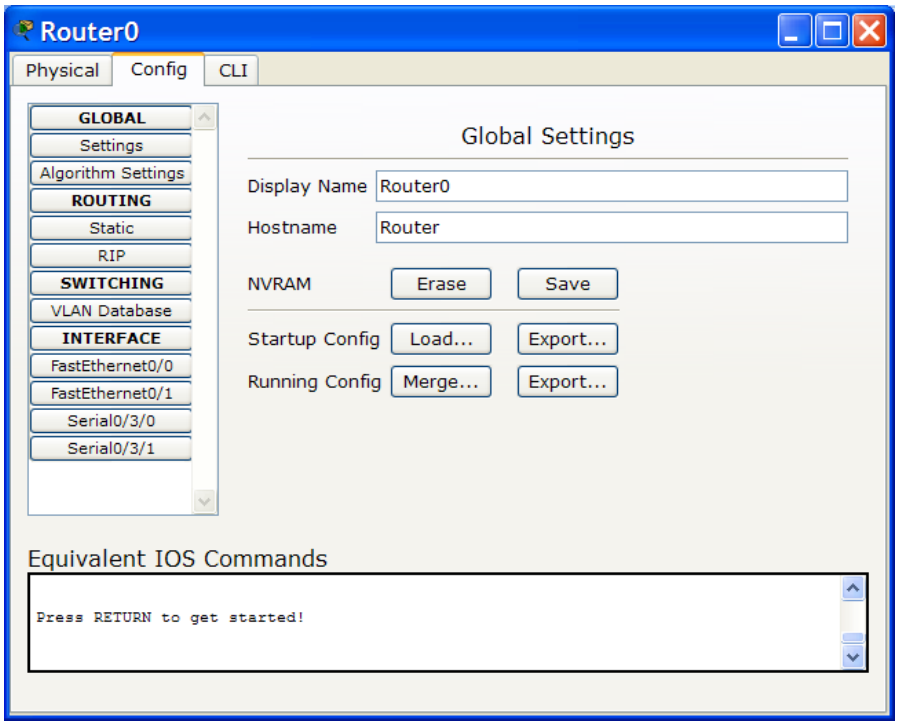
1. GLOBAL *(GLOBAL)*:

   La configuración global permite cambiar el nombre del router como aparece en el área de trabajo y el nombre de hostname como aparece en el software IOS del router. Además puede manipular los archivos de configuración del router y realizar lo siguiente:

   - Borrar la NVRAM (donde se guarda la configuración inicial)
   - Salvar la configuración actual en ejecución para la NVRAM
   - Exportar la configuración de inicio y de ejecución a un archivo de texto externo.
   - Cargar un archivo de configuración existente (formato *.txt) en la configuración de inicio.

- Combinar la configuración en ejecución actual con otro archivo de configuración.

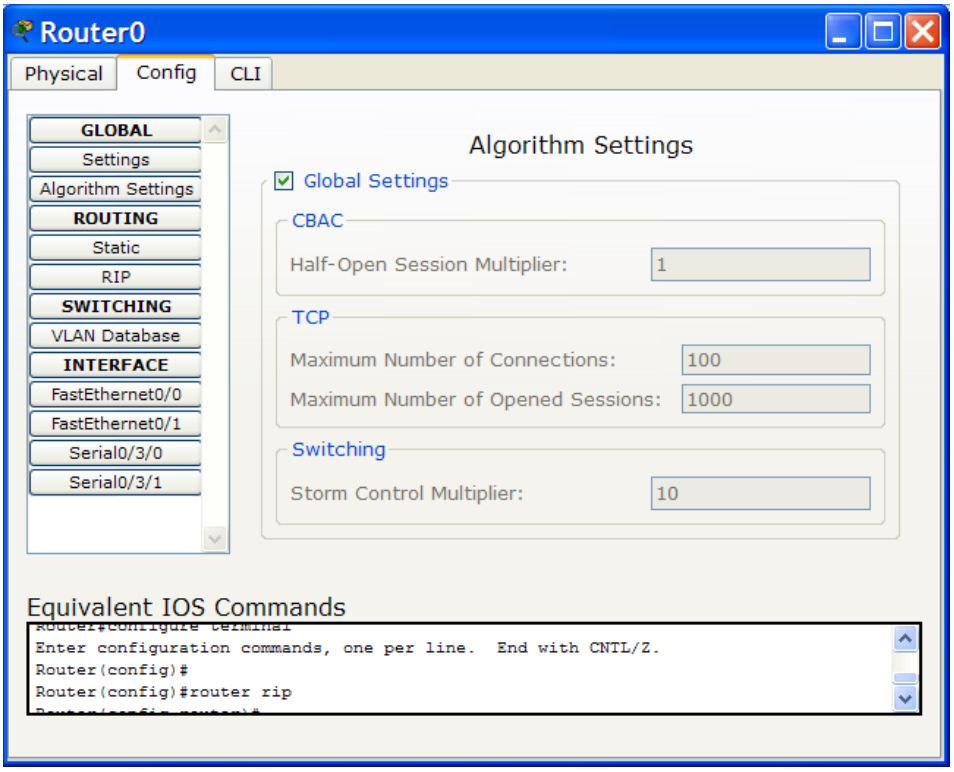
Figura 100. Vista de configuración global del dispositivo.



Fuente: Software GNS3.

En la sección ***Algorithm Settings*** se pueden sobrescribir los algoritmos de configuración global desactivando la opción ***Global Settings*** y asignar valores propios para variables como máximo número de conexiones, máximo número de sesiones abiertas, entre otras.

Figura 101. Vista de configuración del algoritmo.

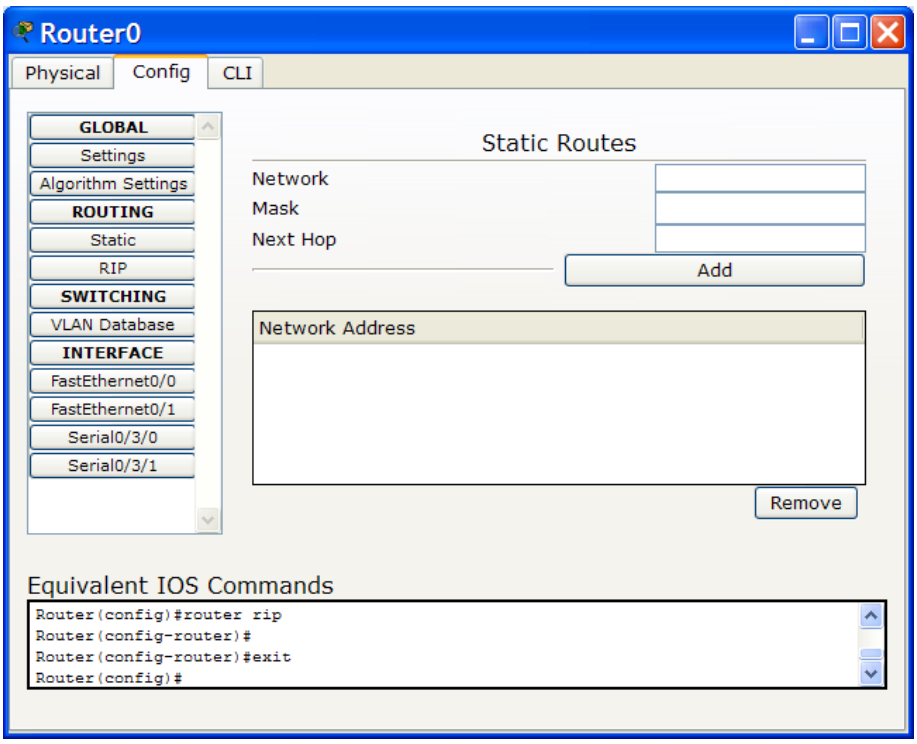


Fuente: Software GNS3.

2. ENRUTAMIENTO *(ROUTING)*:

   Se pueden definir rutas estáticas en el router seleccionando la opción *Static*. Cada ruta estática que se adicione requiere una dirección de red, máscara de subred y dirección del siguiente salto.

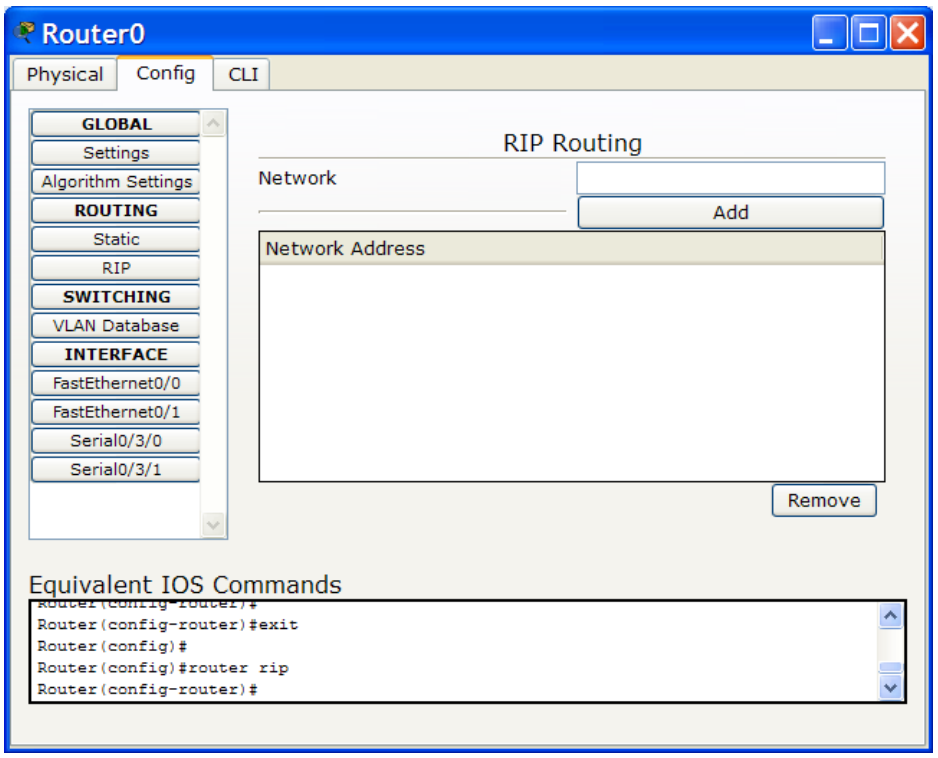
Figura 102. Configuración de enrutamiento estático del dispositivo



Fuente: Software GNS3.

Se habilita RIP versión 1 en redes específicas seleccionando el sub-panel ***RIP.*** Se debe ingresar una dirección IP dentro del campo ***Network*** y a continuación presionar el botón ***Add.*** La red habilitada con RIP se agrega al listado de direcciones de red. Para deshabilitar RIP en una red, se selecciona la dirección y luego hacer clic en el botón ***Remove*** el cual lo eliminará de la lista.

Figura 103. Vista de configuración de enrutamiento Rip del dispositivo

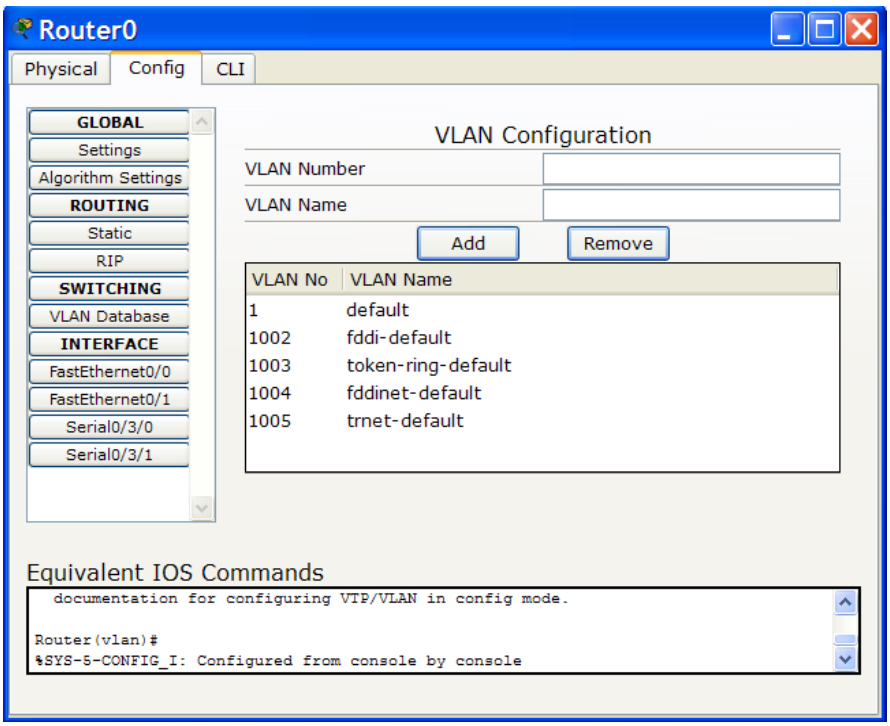


Fuente: Software GNS3.

3. CONMUTACION *(SWITCHING):*

VLAN Database. Los routers Cisco 1841 y 2811 soportan configuración de VLAN. Se pueden administrar las VLANs en un router desde el sub-panel *VLAN Database.* Las VLAN se adicionan ingresando el nombre y el número de la VLAN y a continuación presionar el botón *Add.* De esta forma se actualiza el listado de las VLANs existentes que aparece en la parte inferior de la ventana. Para eliminar una VLAN, se selecciona y luego se oprime *Remove.*

Figura 104. Configuración de la base de datos de la Vlan

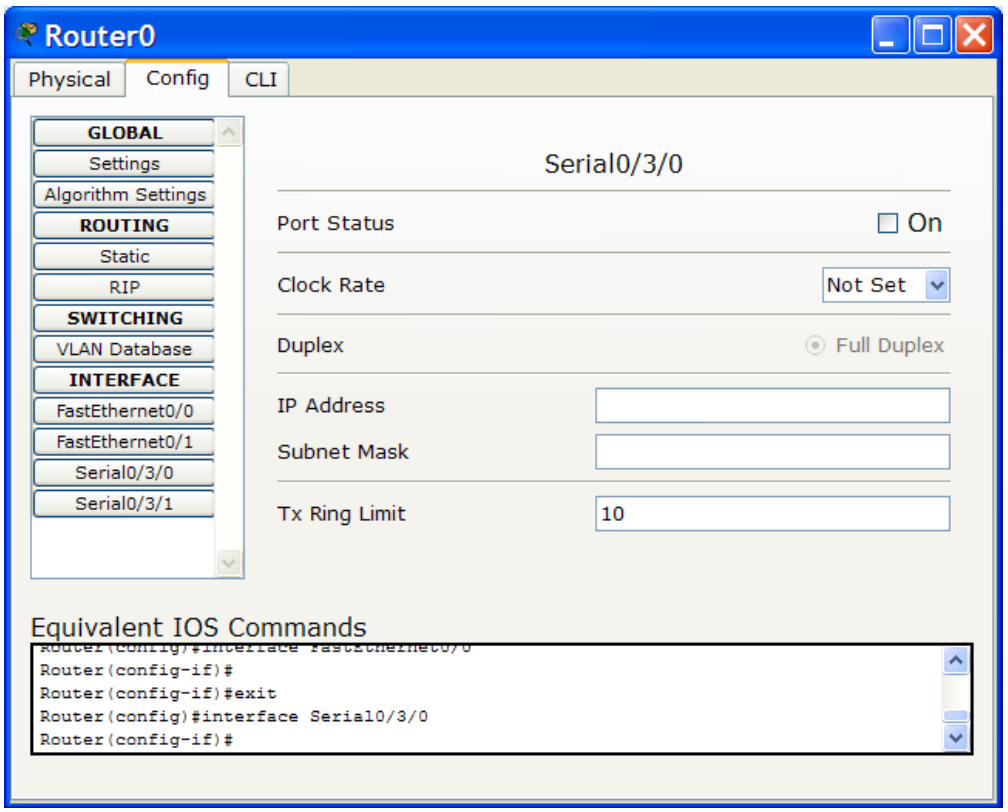


Fuente: Software GNS3.

4. INTERFACE:

Un router puede soportar un amplio rango de interfaces, incluyendo serial, modem y Ethernet. Cada tipo de interfaz puede tener diferentes opciones de configuración, pero en general se puede configurar el estado de puerto como *on/off*, la dirección IP, la máscara de subred,… entre otras.

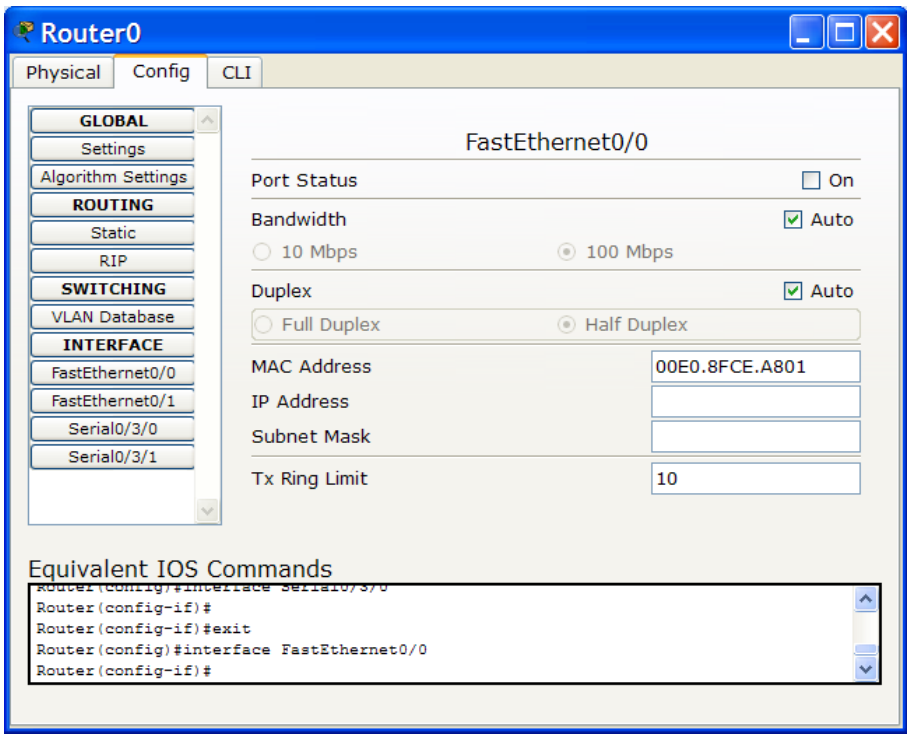
Figura 105. Configuración de la interfaz serial0/0 del router



Fuente: Software GNS3.

Para interfaces Ethernet, también se puede configurar la dirección MAC, el ancho de banda y configuración dúplex. Para interfaces seriales, se puede configurar el *Clock Rate*

Figura 106. Configuración de la interfaz fastethernet0/0 del router

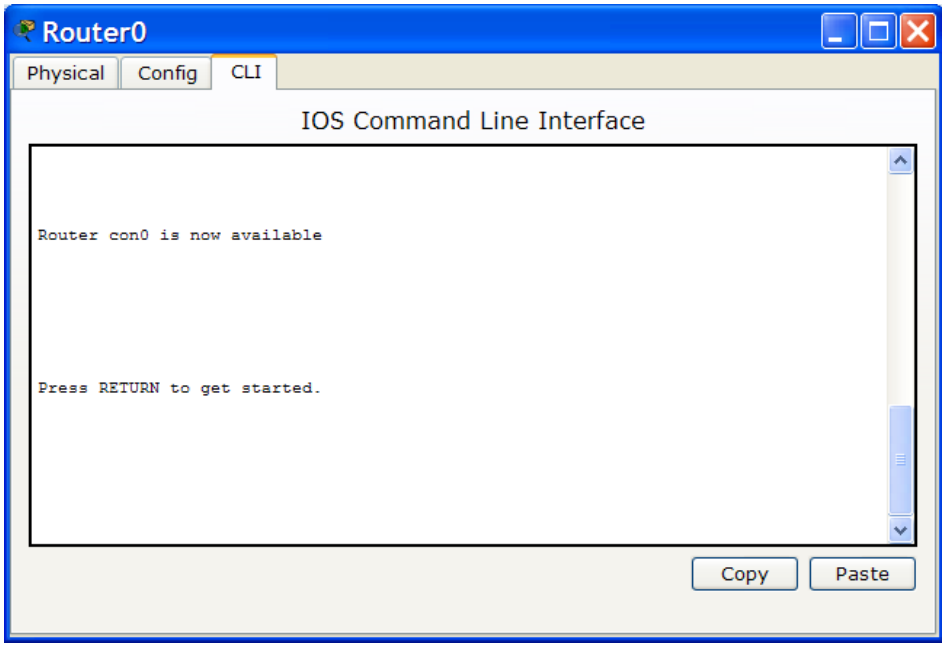


Fuente: Software GNS3.

Packet Tracer utiliza un modelo simplificado de IOS de Cisco, la pestaña "*CLI*" permite el acceso a una ventana de configuración del router para el uso de líneas de comandos de IOS Cisco.

Utilice los botones "*Copy*" y "*Paste*" para copiar y pegar texto desde la línea de comandos

Figura 107. Ventana de configuración línea de comandos



Fuente: Software GNS3.

Al terminar de configurar los router se procede a crear los enlaces entre los dispositivos de la red, para ello debe elegir el botón  ubicado en el área de tipos de dispositivos y seleccionar el tipo de enlace a realizar dentro de una lista que aparece en el área de dispositivos específicos como se muestra a continuación:

Tabla 64. Tipos de conexión disponible en packet tracer

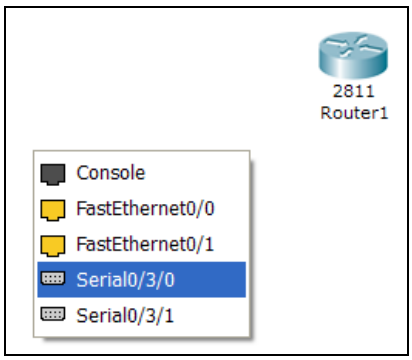
	Conexión automática que detecta el tipo correcto de conexión entre dispositivos.

	Conexión de consola.
	Conexión punto a punto (Cooper Straight - through).
	Conexión cruzada (Cooper Cross -over).
	Conexión con Fibra.
	Conexión telefónica.
	Conexión coaxial.
	Conexión Serial DCE.
	Conexión Serial DTE.

Fuente: Autoras.

Por ejemplo si se desea realizar una conexión serial DCE entre dos router , se selecciona con el mouse el botón y enseguida dar clic primero sobre el router que va a asignar como DCE, para que muestre una pequeña ventana que lista los puertos disponible y que permite elegir el puerto a conectar.

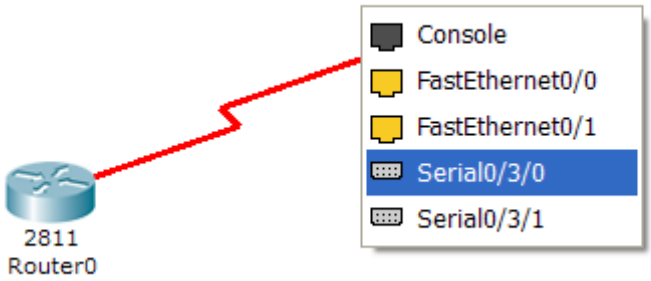
Figura 108. Configuración de tipo de conexión entre dispositivos



Fuente: Software GNS3.

Luego de elegir el puerto serial debe ir al segundo router y con el mouse dar clic sobre él para que muestre nuevamente la ventana que le permite elegir el puerto a conectar.

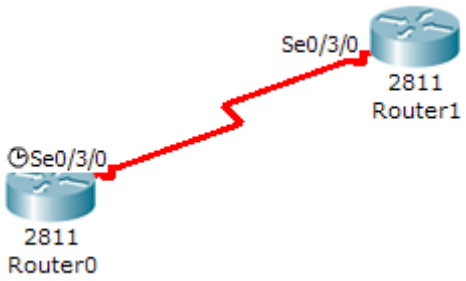
Figura 109. Configuración del enlace Serial entre dos dispositivos



Fuente: Software GNS3.

El proceso de conexión ha terminado y se muestra a continuación, con el DCE configurado en el primer router. Para realizar cualquier tipo de enlace el proceso es el mismo.

Figura 110. Enlace serial entre dispositivos



Fuente: Software GNS3.

Las configuraciones anteriormente explicadas son las más básicas para manejar la herramienta packet tracer en el diseño de una topología de red.

4.2. GNS3

4.2.1. Descripción general del Software GNS3

Debido a que packet tracer tiene algunas limitaciones con protocolos de enrutamiento multicast, en el desarrollo de la presente monografía se utilizó un simulador adicional denominado GNS3, el cual es un simulador gráfico de redes completo y funcional que soporta enrutamiento multicast y permite diseñar topologías de red y ejecutar simulaciones en él.

Gns3 se ejecuta en Windows, Linux y Mac OS X, en otras plataformas diferentes a las anteriormente nombradas no se han realizado pruebas y se requiere de otras dependencias para que GNS3 se pueda ejecutar.

Para permitir completar simulaciones, GNS3 está estrechamente vinculada con: Dynamips, Dynagen y Pemu.

- Dynamips: GNS3 utiliza Dynamips para emular los dispositivos (routers, switchs, PIX, etc.), permitiendo de esta forma extender una red propia, conectándola a la topología virtual. Este emulador es útil para:
    - Ser utilizado como plataforma de entrenamiento, utilizando software del mundo real.
    - Verificar configuraciones rápidamente que serán implementadas en routers reales.

  GNS cuenta con diversas imágenes IOS (sistema operativo de routers) lo cual permite mayor cobertura de dispositivos. Estas IOS, al igual que la aplicación GNS3 se pueden descargar de internet.

  Si se está trabajando en Windows, la imagen debe ser ubicada en *C:\Program Files\Dynamips\images* o si lo prefiere puede ubicar las imágenes en cualquier otra ubicación y configurar a GNS3 en la propiedad *IOS Images and Hypervisors* ubicada en Edit del menú principal para que la busque en la ubicación deseada.

  Dynamips utiliza gran parte de la memoria RAM y de CPU para lograr la emulación. Para Windows Dynamips utiliza por defecto

16MB de RAM por cada instancia para cachear las transacciones JIT. El uso intensivo de CPU se debe a que esta emulando la CPU de un router instrucción por instrucción. Inicialmente no hay forma de saber cuando el router virtual esta en estado ocioso (idle), por esa razón ejecuta diligentemente todas las instrucciones que constituyen las rutinas de idle del IOS, igualmente que las instrucciones que conforman el “real” funcionamiento. Pero una vez que haya ejecutado el proceso de “Idle-PC” para una determinada imagen de IOS, la utilización de CPU decrecerá en forma drástica.

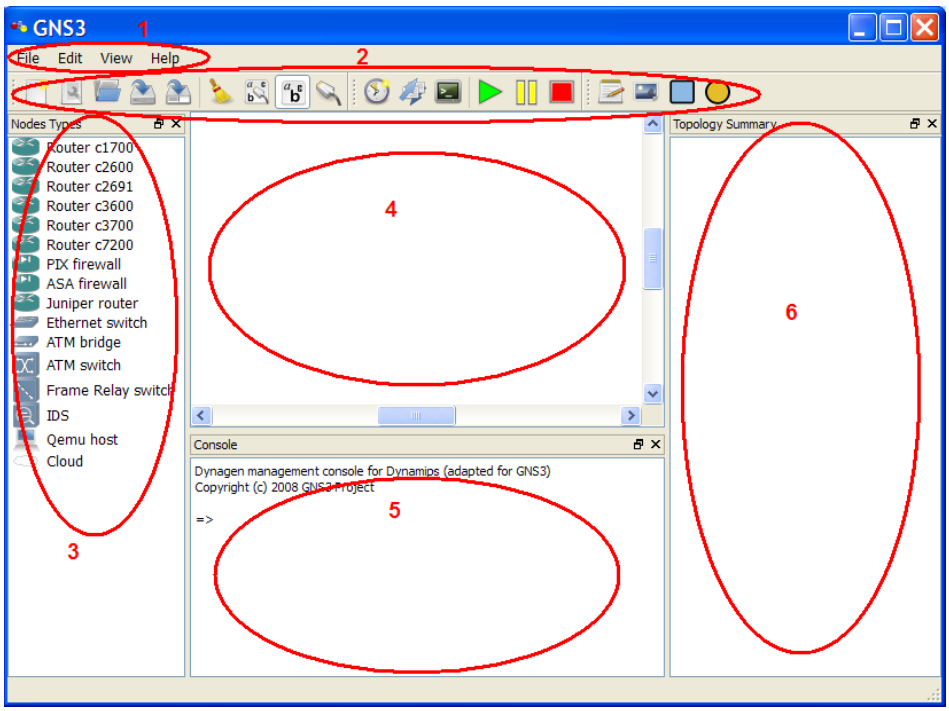
- Dynagen, un texto basado en front-end para Dynamips.

- Pemu, un emulador de PIX. GNS3 es una herramienta complementaria para los administradores de redes.

4.2.2. Entorno de trabajo

A continuación se dará una sencilla explicación del entorno de trabajo de GNS3.

Figura 111. Interfaz gráfica de la herramienta GNS3



Fuente: Software GNS3.

La herramienta GNS3 posee:

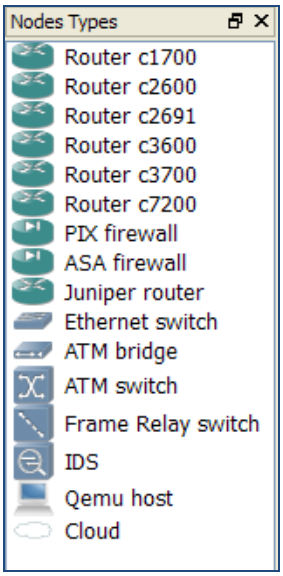
1. Menú principal: Contiene las opciones básicas de *File,Edit,View, Help*
2. Barra de acceso rápido**:** contiene las opciones de *New Project, Edit Project, Open Network File, Save Network File, Save Network File as, Clear the topology, Show interface Names, Show hostnames, Add a link, Snapshot, Extract/Import all startup-configs, Telnet to all IOS, Start/Resume every devices, Suspend every devices, Stop every devices, Add a note, Insert a picture, Draw a rectangle, Draw a elipse.*

Figura 112. Barra de uso rápido de GNS3

Fuente: Software GNS3.

3. Lista Nodos: Esta sección contiene una lista de dispositivos disponibles y permite elegir con el mouse el tipo de dispositivo para llevarlo al área de trabajo.

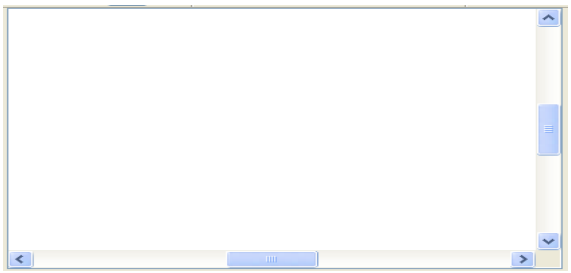
Figura 113. Lista de dispositivos disponibles por GNS3



Fuente: Software GNS3.

4. Área de trabajo: Permite la inserción de los diferentes dispositivos y enlaces para crear la topología de la red.

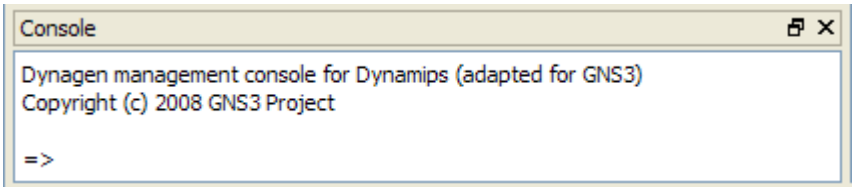
Figura 114. Área de trabajo de GNS3



Fuente: Software GNS3.

5. Consola: el panel de la Consola ubicada en parte inferior estará disponible si se esta a modo emulación. Desde la consola, utilice el comando **help** para visualizar los comandos validos:

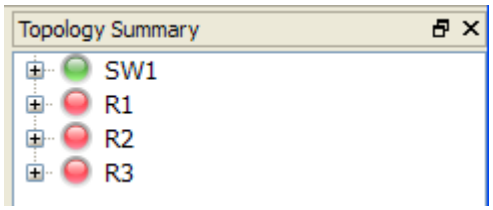
Figura 115. Panel de consola



Fuente: Software GNS3.

6. Ventana de topología resumida: Contiene la lista de los dispositivos que se encuentran ubicados en el área de trabajo, y muestra las conexiones activas de las interfaces de cada dispositivo.

Figura 116. Dispositivos involucrados en la topología de la red



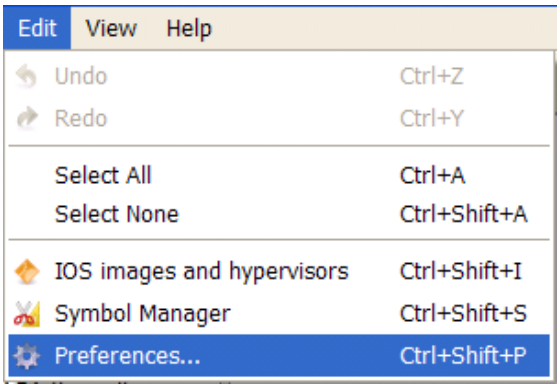
Fuente: Software GNS3.

4.2.3. Instrucciones básicas de configuración

Inicialmente para trabajar con GNS3 se deben configurar las preferencias de Dynamips como se muestra a continuación:

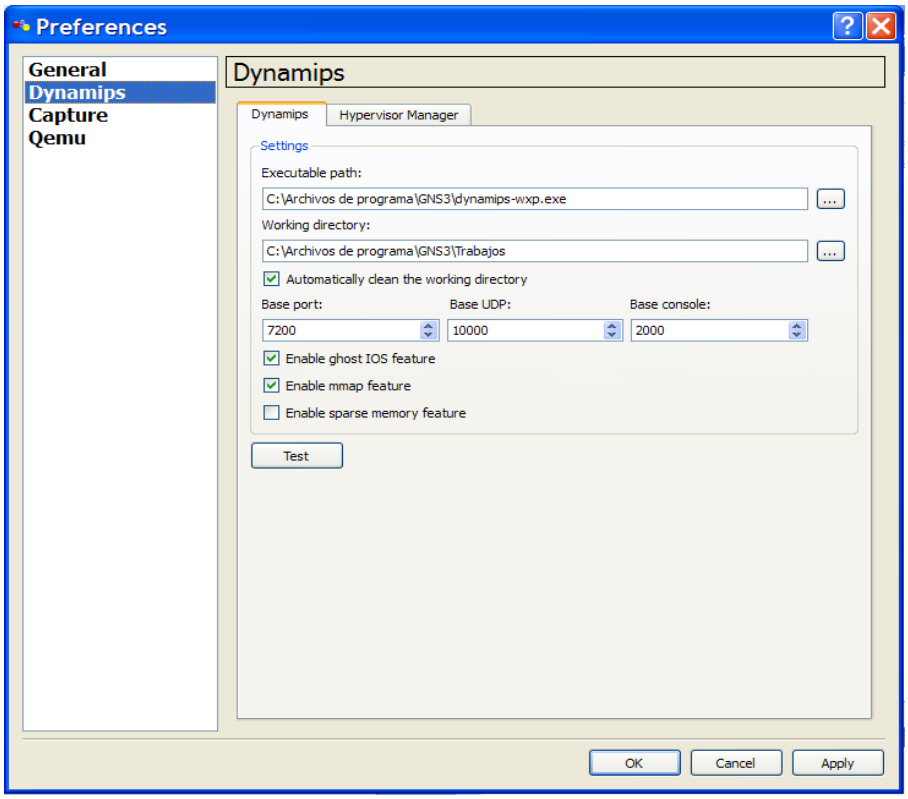
En el menú "*Edit*" se elige la opción "*Preferences*" y a continuación:

Figura 117. Configuración de preferencias de GNS3



Fuente: Software GNS3.

Figura 118. Configuración de dynamips

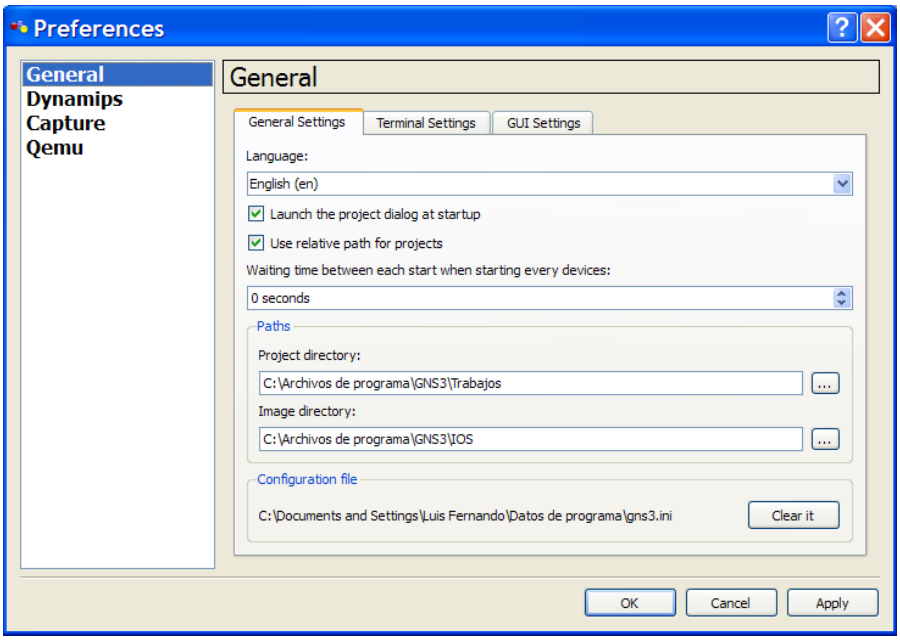


Fuente: Software GNS3.

- Su ubicación (camino del ejecutable) y el puerto base, para que el *Hypervisor Manager* utilice estos valores y para cargar los archivos .net. esta configuración se debe realizar en las preferencias del menú Edit.
    - El directorio de trabajo es el lugar en donde Dynamips almacena todos los archivos generados, esto incluye a la NVRAM de los router virtuales, también la *bootflash*, los *logfiles*, y otros archivos de trabajo.
    - La opción "Habilitar la función de ghost IOS" se activa para utilizar la función ghost de Dynamips en forma global (o no).
    - La opción "Habilitar la función de nmap" se activa para utilizar la función nmap de dynamips en forma global (o no).
    - La opción "Habilitar la función de sparse memory" se activa para utilizar la función *sparsemem* de Dynamips en forma global (o no).

Para poder conectarse a las consolas de los routers virtuales, se deben configurar los comandos de la terminal.

Figura 119. Configuración general de GNS



Fuente: Software GNS3.

GNS3 utiiza una serie de comandos por defecto pero estos pueden ser modificados.

Las siguientes son las substituciones que se realizan:

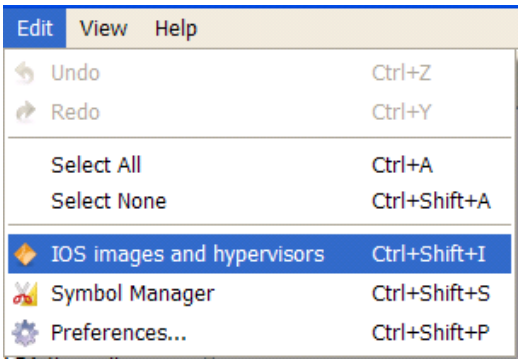
%h = host

%p = puerto

%d = nombre de dispositivo

Luego debe registrar al menos una imagen de IOS, en el menú *Edit* elegir la propiedad *Imágenes IOS e hipervisors*. .

Figura 120. Configuración de la imagen IOS de los dispositivos

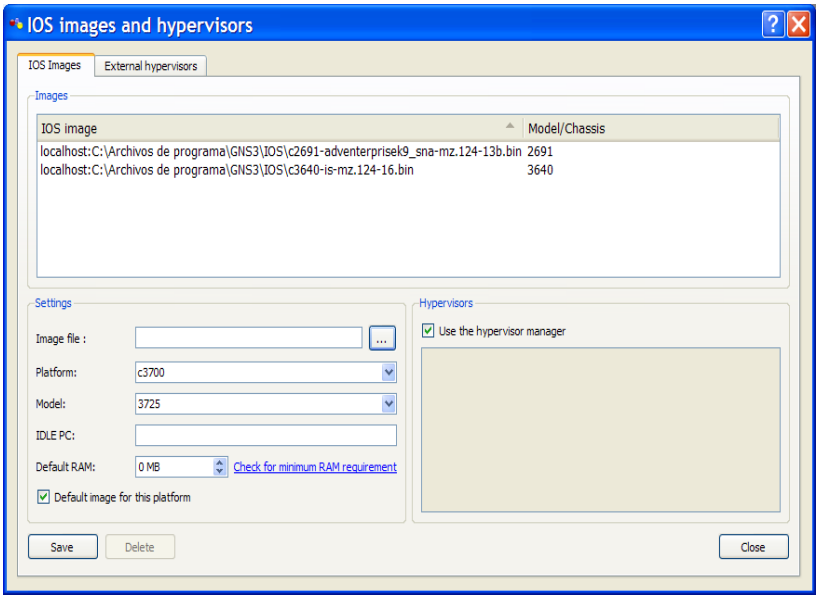


Fuente: Software GNS3.

En settings, en la opción "image file" dar clic en el botón  para ajustar el camino al IOS, estas imágenes pueden ser almacenadas en *C:\Program Files\Dynamips\images* como se menciono anteriormente o en la ubicación que desee.

Elegir la plataforma y el modelo (si es necesario) y si conoce el valor de IDLE PC ingréselo. Por defecto, se utilizara el hypervisor integrado (GNS3 administrara los procesos Dynamips) para ejecutar los IOS para terminar este paso dar clic en la opción de "*Save*" y luego en "*Close*"

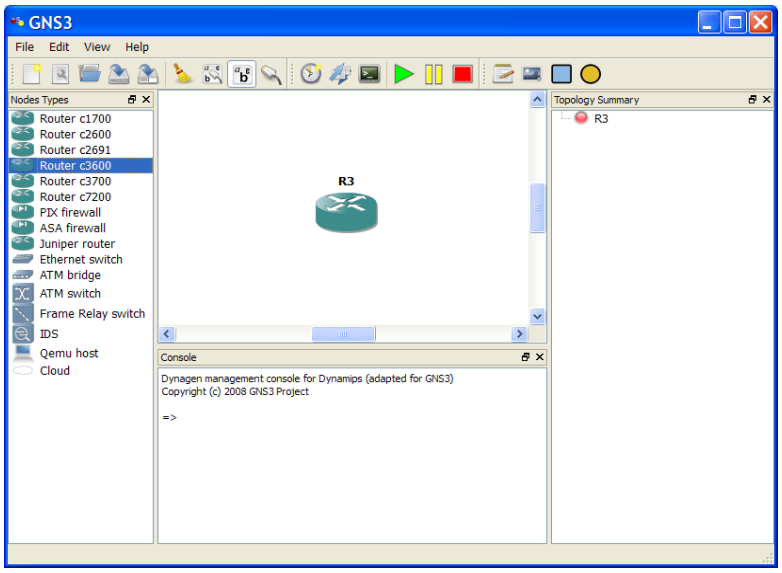
Figura 121. Configuración de las imgenes IOS para los dispositivos



Fuente: Software GNS3.

El paso a seguir es crear la topología, se debe seleccionar con el mouse los nodos que se encuentran al lado izquierdo y llevarlos al área de trabajo.

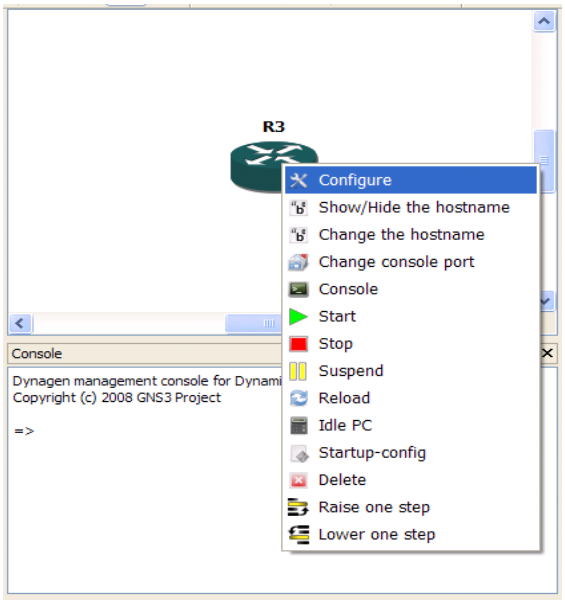
Figura 122. Creación de la topología de la red



Fuente: Software GNS3.

Luego proceder a configurar cada nodo con clic derecho sobre el nodo y seleccionar la opción "*Configure*", Puede aplicar la misma configuración a todos los routers seleccionando "Routers" en el árbol expandido del panel izquierdo o seleccionando un router en particular por su nombre.

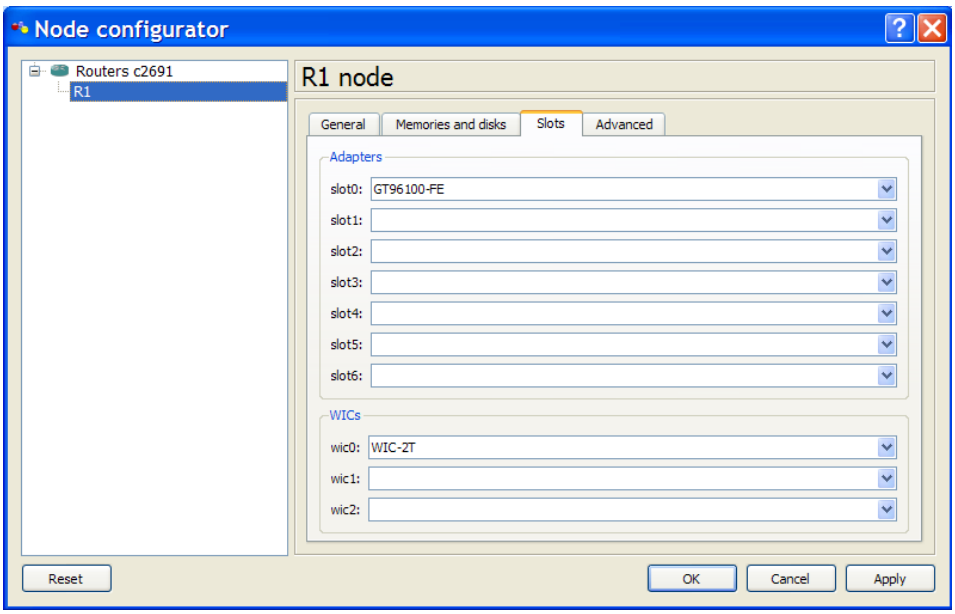
Figura 123. Configuración del router



Fuente: Software GNS3.

Para crear los enlaces en el área de trabajo se debe configurar primero los slots, para el estudio de la presente monografía se utilizaron enlaces FastEthernet y Serial, por tal motivo se configuraron los slots (Slot0, Wic0) como aparecen a continuación.

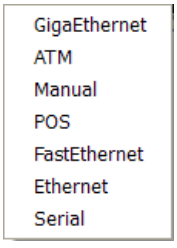
Figura 124. Configuración de Slots y WICs del router



Fuente: Software GNS3.

Los enlaces se crean utilizando el botón  ubicado en el menú principal y permite por medio de una lista seleccionar el tipo de enlace a realizar.

Figura 125. Tipos de enlaces para el router



Fuente: Software GNS3

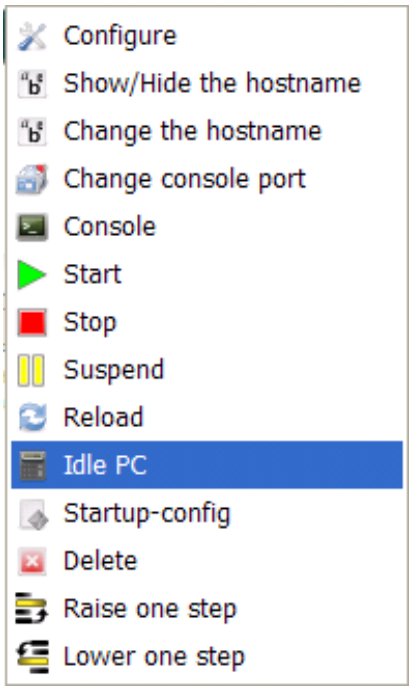
Se debe tener en cuenta que en simulaciones previas el consumo de CPU del sistema alcanza el 100% y permanece allí. Esto se debe a que

Dynamips no detecta cuando el router virtual esta en estado de *idle* o cuando esta operando realmente.

El comando "*idlepc*" efectúa un análisis en la imagen que se esta ejecutando para determinar cuales son los posibles puntos en el código que representan un bucle de idle en la IOS. Una vez aplicado, Dynamips "*duerme*" ocasionalmente al router virtual cuando el bucle *idle* es ejecutado, reduciendo significativamente el consumo de CPU del host sin reducir la capacidad del router virtual de realizar sus tareas.

El *Idle PC* se puede configurar al dar clic derecho sobre el router, y elegir la opción "*Idle PC"*, luego de crear la topología de la red.

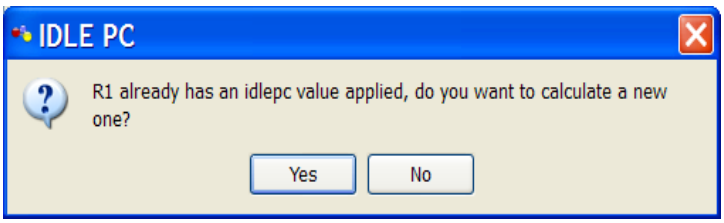
Figura 126. Configuración de la propiedad Idle PC del router



Fuente: Software GNS3.

Luego dar clic en la opción "Yes" para calcular un nuevo valor.

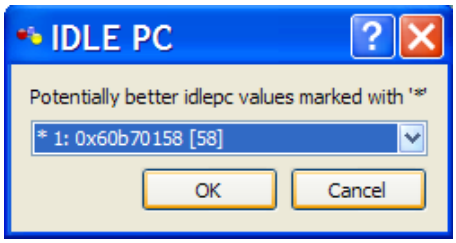
Figura 127. Calculo del nuevo valor de Idle PC



Fuente: Software GNS3.

Y elegir dentro de una lista el valor del Idlepc que este acompañado de un "*" asterisco, que indica que es el valor mas apropiado y que proveerá mejores resultados, y por ultimo dar clic en la opción "*OK* ".

Figura 128. Idle PC apropiado para el router

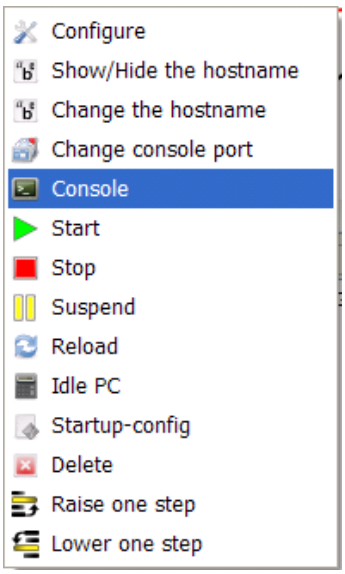


Fuente: Software GNS3.

Luego de elegir este valor el uso de CPU se reduce simultáneamente si esto no ocurre se debe repetir nuevamente este paso y calcular el *Idle PC* hasta obtener mejores resultados.

Cuando la topología está lista, se procede a configurar cada nodo por medio de la consola de comandos, esta consola se activa con el botón  y llama a todas las IOS, pero si se desea trabajar en alguna en particular elegir el nodo deseado, dar clic derecho y seleccionar la opción "*Console*".

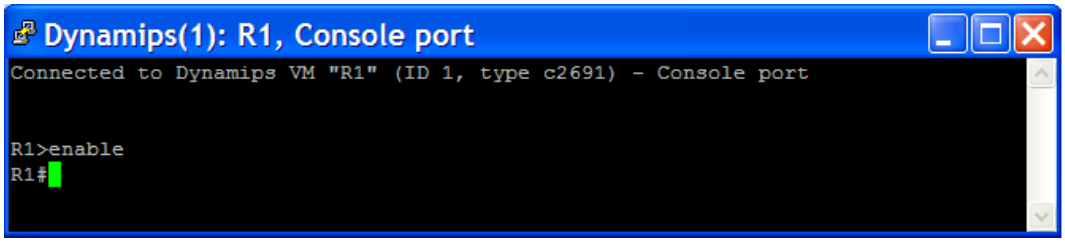
Figura 129. Activación de la consola del dispositivo



Fuente: Software GNS3.

La consola permite trabajar directamente con el software IOS de Cisco de los routers virtuales, y configurarlo mediante comandos como si estuviese configurando un router real.

Figura 130. Ventana de consola del dispositivo



Fuente: Software GNS3.

Estos fueron algunos aspectos básicos que se deben tener en cuenta en el manejo de la Herramienta GNS3 para el desarrollo de una topología de red.

5. SIMULACIONES

A continuación se documentan las prácticas de configuración de enrutamiento realizadas en los simuladores mencionados anteriormente. En cada práctica, se plantea el requerimiento del usuario (planteamiento del problema): una solicitud de configuración de una topología determinada y se procede a configurar la red y comprobar el funcionamiento de la misma.

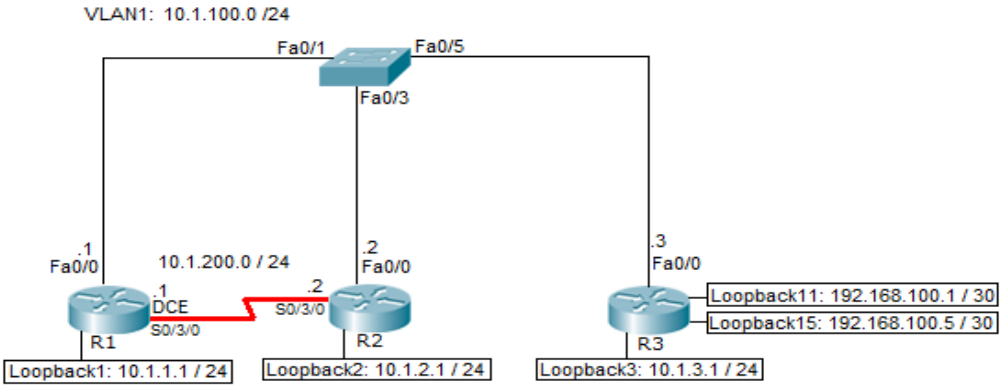
5.1. EIGRP

Planteamiento:

Configurar una red para conectar tres departamentos de una compañía: ingeniería, marketing y contabilidad, representados por las interfaces loopback en cada uno de los 3 routers. Los dispositivos físicos han sido instalados y conectados por FastEthernet y cables seriales. Se debe configurar EIGRP para habilitar la conectividad completa entre todos los departamentos.

Diagrama:

Figura 131. Diagrama de práctica de la simulación en EIGRP



Fuente: Autoras

Solución:

A continuación se describen los pasos que se siguieron para realizar esta simulación. (El simulador utilizado para esta práctica fue Packet Tracer).

Configuración de interfaces en los dispositivos

Inicialmente se realiza el direccionamiento IP basado en el diagrama, se asignan direcciones IP a las interfaces FastEthernet en R1, R2 y R3. Después se crean las interfaces Loopback1 en R1, Loopback2 en R2 y Loopback3 en R3 con su respectivo direccionamiento.

Figura 132. Configuración inicial de R1

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface loopback1
R1(config-if)#description Departamento de Ingenieria
R1(config-if)#ip address 10.1.1.1 255.255.255.0
R1(config-if)#exit
R1(config)#interface fastethernet 0/0
R1(config-if)#ip address 10.1.100.1 255.255.255.0
R1(config-if)#
```

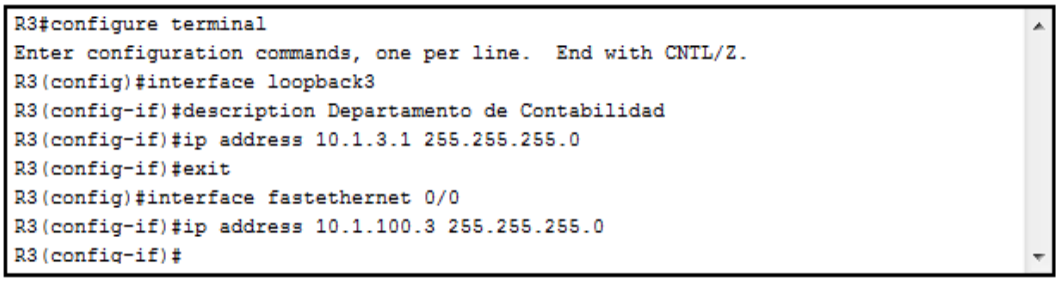
Fuente: Software Packet Tracer 5.2.

Figura 133. Configuración inicial de R2

```
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface loopback2
R2(config-if)#description Departamento de Marketing
R2(config-if)#ip address 10.1.2.1 255.255.255.0
R2(config-if)#exit
R2(config)#interface fastethernet 0/0
R2(config-if)#ip address 10.1.100.2 255.255.255.0
R2(config-if)#
```

Fuente: Software Packet Tracer 5.2.

Figura 134. Configuración inicial de R3

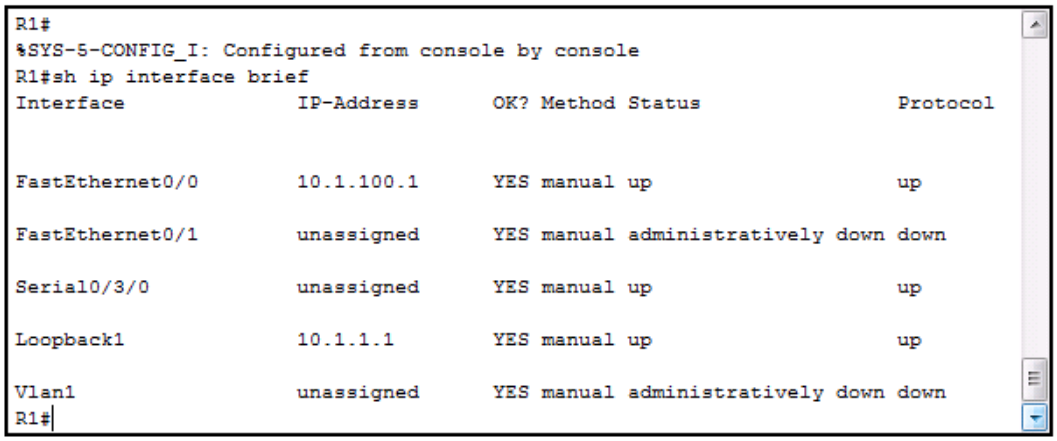


Fuente: Software Packet Tracer 5.2.

Por el momento el switch permanece en su configuración por defecto, en la cual todos los puertos del switch están en la VLAN1 y no están administrativamente abajo. Las interfaces seriales también se dejan en su configuración por defecto. Más adelante se configurarán los enlaces seriales entre R1 y R2.

Se verifica que cada interfaz esté arriba en la columna de "*Protocol*" y de esta manera se pueda ejecutar satisfactoriamente un ping a través de cada enlace.

Figura 135. Verificación del estado de las interfaces en R1



Fuente: Software Packet Tracer 5.2.

Configuración de EIGRP

Después de haber implementado el esquema de direccionamiento, se crea un sistema autónomo (AS) EIGRP en R1 usando los siguientes comandos:

Figura 136. Configuración de EIGRP

```
R1(config)#router eigrp 1
R1(config-router)#network 10.0.0.0
```

Fuente: Software Packet Tracer 5.2.

EIGRP comienza a enviar paquetes *Hello* a todas las interfaces en la red definida (es decir, subredes de la red 10.0.0.0/8). En este caso, EIGRP debería comenzar a enviar paquetes Hello de sus interfaces FastEthernet y loopback. Para revisar si esto está ocurriendo, se utiliza el comando **debug eigrp packets.**

Figura 137. Depuración de paquetes Hello en el router R1

```
R1#debug eigrp packets
EIGRP Packets debugging is on
    (UPDATE, REQUEST, QUERY, REPLY, HELLO, ACK )
R1#
EIGRP: Sending HELLO on Loopback1
  AS 1, Flags 0x0, Seq 1/0 idbQ 0/0 iidbQ un/rely 0/0
EIGRP: Received HELLO on Loopback1 nbr 10.1.1.1
  AS 1, Flags 0x0, Seq 1/0 idbQ 0/0
EIGRP: Packet from ourselves ignored
EIGRP: Sending HELLO on FastEthernet0/0
  AS 1, Flags 0x0, Seq 1/0 idbQ 0/0 iidbQ un/rely 0/0
EIGRP: Sending HELLO on Loopback1
  AS 1, Flags 0x0, Seq 1/0 idbQ 0/0 iidbQ un/rely 0/0
EIGRP: Received HELLO on Loopback1 nbr 10.1.1.1
  AS 1, Flags 0x0, Seq 1/0 idbQ 0/0
EIGRP: Packet from ourselves ignored
EIGRP: Sending HELLO on FastEthernet0/0
  AS 1, Flags 0x0, Seq 1/0 idbQ 0/0 iidbQ un/rely 0/0
EIGRP: Sending HELLO on Loopback1
  AS 1, Flags 0x0, Seq 1/0 idbQ 0/0 iidbQ un/rely 0/0
EIGRP: Received HELLO on Loopback1 nbr 10.1.1.1
  AS 1, Flags 0x0, Seq 1/0 idbQ 0/0
EIGRP: Packet from ourselves ignored
EIGRP: Sending HELLO on FastEthernet0/0
  AS 1, Flags 0x0, Seq 1/0 idbQ 0/0 iidbQ un/rely 0/0
EIGRP: Sending HELLO on Loopback1
  AS 1, Flags 0x0, Seq 1/0 idbQ 0/0 iidbQ un/rely 0/0
EIGRP: Received HELLO on Loopback1 nbr 10.1.1.1
  AS 1, Flags 0x0, Seq 1/0 idbQ 0/0
```

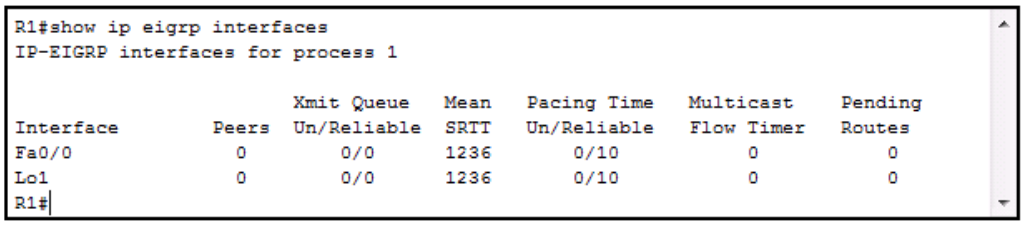
Fuente: Software Packet Tracer 5.2.

Para detener esta depuración se utiliza el comando **undebug all.**

Estos paquetes *Hello* no obtienen respuesta de otros routers, porque EIGRP aún no se ha ejecutado en R2 ni en R3. R1 ignora los paquetes *Hello* que él mismo envía en la Loopback1.

Para identificar las interfaces que participan en el proceso de enrutamiento EIGRP de un router se utiliza el comando **show ip eigrp interfaces.**

Figura 138. Interfaces en el proceso de enrutamiento EIGRP en R1

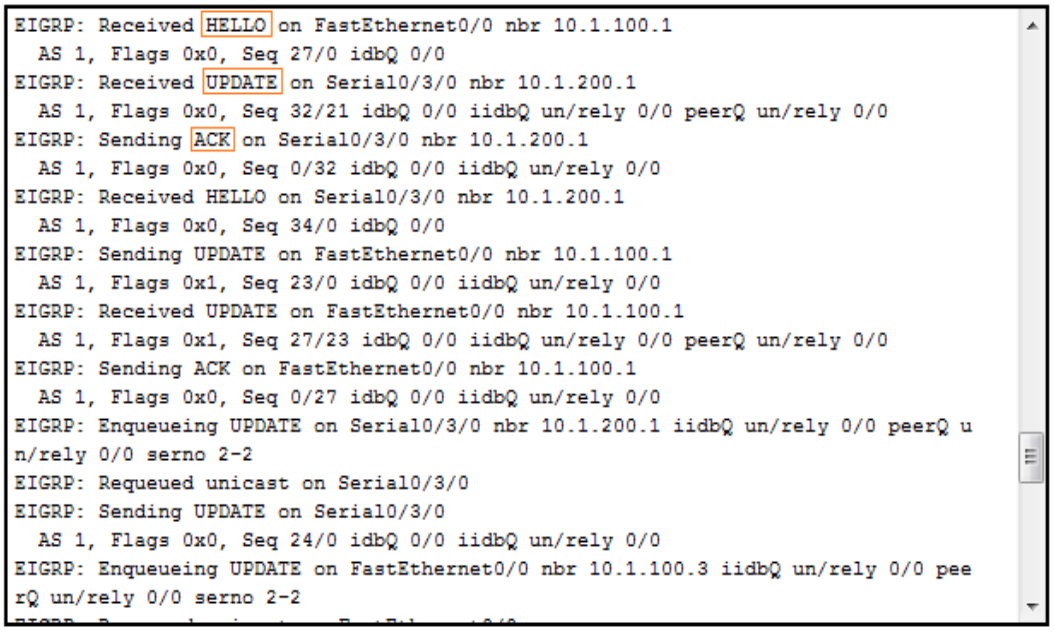


Fuente: Software Packet Tracer 5.2.

Para ver la adyacencia iniciada en R1 y R2, se usa **debug eigrp packets** en R1 y R2 para monitorear la adyacencia en tiempo real mientras se configura R2.

Ahora, en R2 se usan los mismos comandos que en R1 para crear el Sistema Autónomo EIGRP 1 y definir la red 10.0.0.0/8. Se aplicó un cambio en la topología bajando la interfaz fastethernet 0/0 de R1 y se obtuvo la siguiente salida:

Figura 139. Depuración de paquetes EIGRP en el router R1

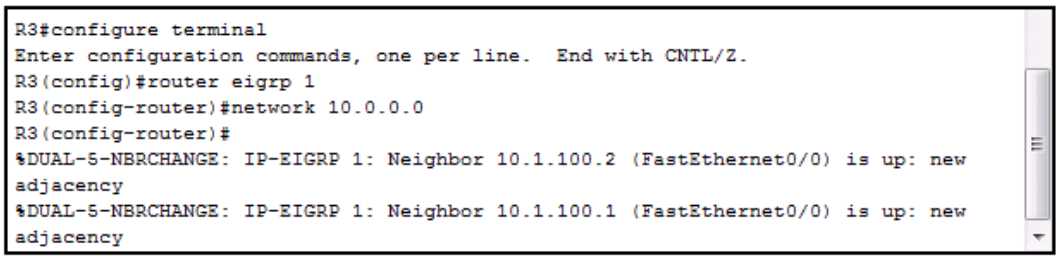


Fuente: Software Packet Tracer 5.2.

La salida de la depuración muestra paquetes EIGRP *Hello, Update,* y *ACK*. Como EIGRP usa RTP (Reliable Transport Protocol) para paquetes *Update*, se ven los routers respondiendo a paquetes *Update* con paquetes *ACK*.

Seguidamente se configura EIGRP en el R3 usando los mismos comandos:

Figura 140. Configuración de EIGRP en el router R3

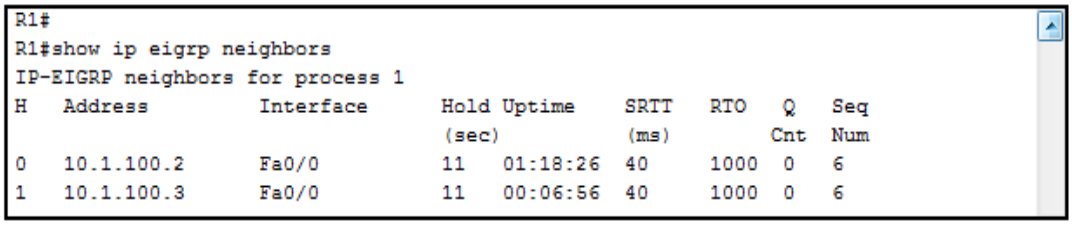


Fuente: Software Packet Tracer 5.2.

Verificación de la configuración EIGRP

Con el comando **show ip eigrp neighbors** se pueden identificar las adyacencias en cada router y de esta forma se comprueba la correcta configuración EIGRP en los routers.

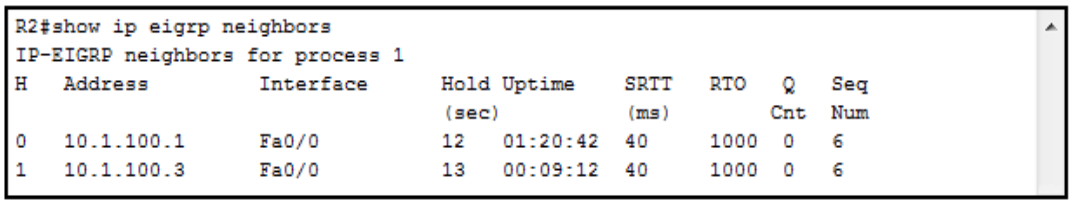
Figura 141. Verificación de adyacencias en el router R1



```
R1#
R1#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address         Interface       Hold Uptime    SRTT   RTO   Q   Seq
                                    (sec)          (ms)       Cnt Num
0   10.1.100.2      Fa0/0           11   01:18:26  40     1000  0   6
1   10.1.100.3      Fa0/0           11   00:06:56  40     1000  0   6
```

Fuente: Software Packet Tracer 5.2.

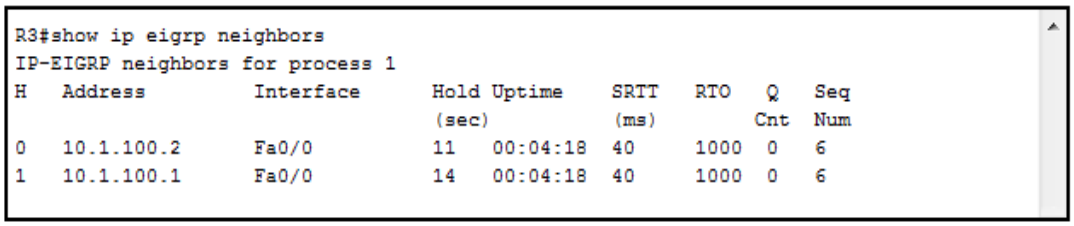
Figura 142. Verificación de adyacencias en el router R2



```
R2#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address         Interface       Hold Uptime    SRTT   RTO   Q   Seq
                                    (sec)          (ms)       Cnt Num
0   10.1.100.1      Fa0/0           12   01:20:42  40     1000  0   6
1   10.1.100.3      Fa0/0           13   00:09:12  40     1000  0   6
```

Fuente: Software Packet Tracer 5.2.

Figura 143. Verificación de adyacencias en el router R3



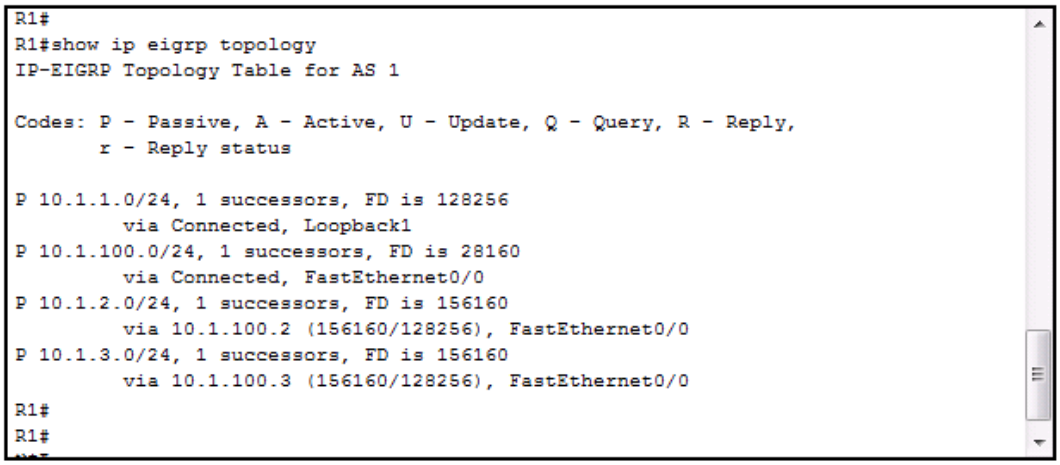
```
R3#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address         Interface       Hold Uptime    SRTT   RTO   Q   Seq
                                    (sec)          (ms)       Cnt Num
0   10.1.100.2      Fa0/0           11   00:04:18  40     1000  0   6
1   10.1.100.1      Fa0/0           14   00:04:18  40     1000  0   6
```

Fuente: Software Packet Tracer 5.2.

Para ver la tabla de topología y el estado de las rutas se usa el comando **show ip eigrp topology**.

Se pueden apreciar todas las redes actuales publicadas por EIGRP en cada router. Se verifica la existencia de las redes loopback existentes en la tabla de topología EIGRP.

Figura 144. Información de la tabla de topología en el router R1

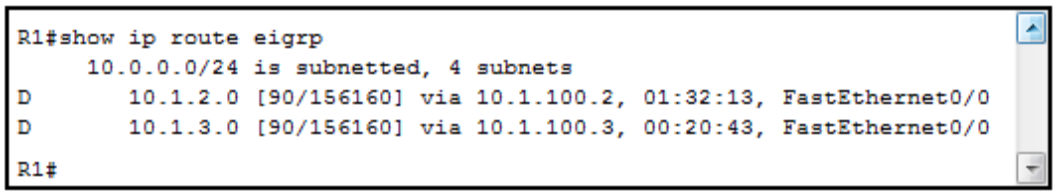


Fuente: Software Packet Tracer 5.2.

Para los routers R2 y R3 la salida es la misma, pero con su respectiva loopback.

Debido a que EIGRP es el único protocolo de enrutamiento en ejecución y que actualmente tiene rutas a estas redes, se puede observar la mejor ruta a la red destino usando el comando **show ip route eigrp**

Figura 145. Información de las rutas a la red destino en el router R1

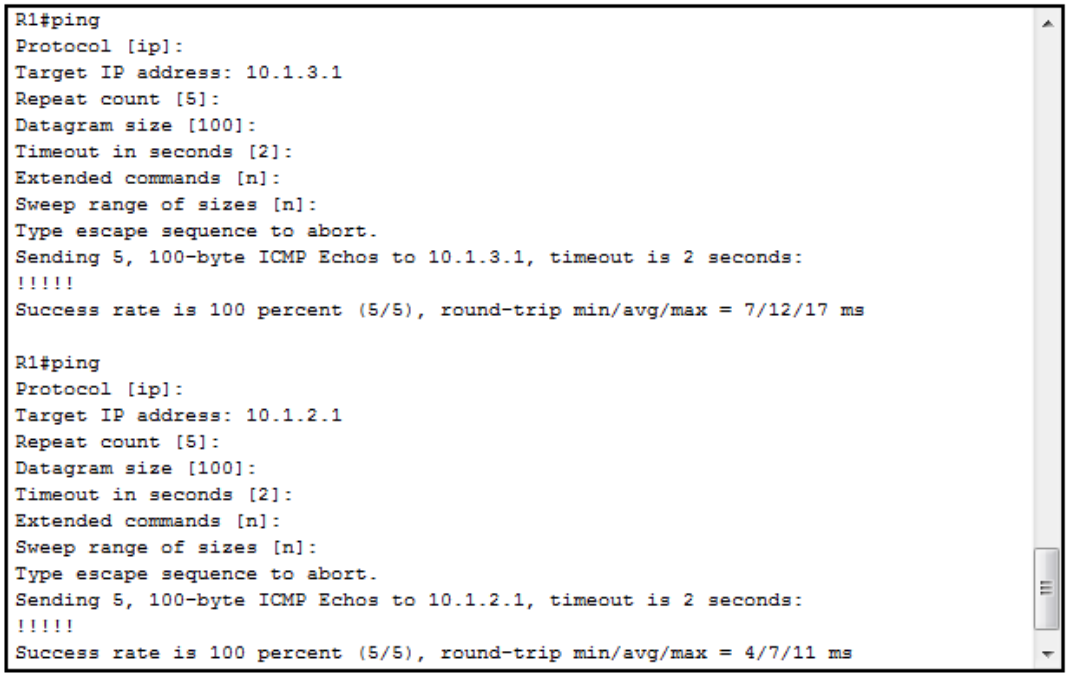


Fuente: Software Packet Tracer 5.2.

Para verificar si se tiene conectividad completa, se hace ping a las loopbacks remotas desde cada router. Si todos los pings son exitosos, la

configuración EIGRP para enrutar entre estas tres redes remotas se ha realizado correctamente. A continuación se verifica la conectividad realizando un ping de R1 a R2 y R3:

Figura 146. Ping a las loopback remotas en el router R1

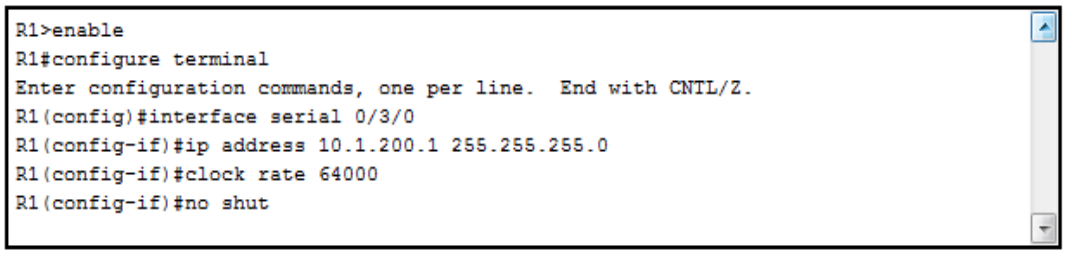


Fuente: Software Packet Tracer 5.2.

Configuración de EIGRP en las interfaces seriales

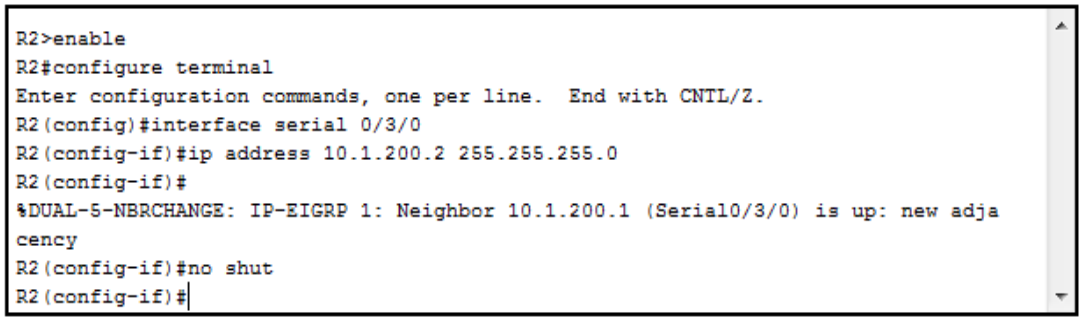
Por el momento las interfaces seriales tienen la configuración por defecto. A continuación se direccionan las interfaces de acuerdo al diagrama, y se asigna un *clockrate* de 64 Kbps.

Figura 147. Configuración de la serial0/3/0 en el router R1



Fuente: Software Packet Tracer 5.2.

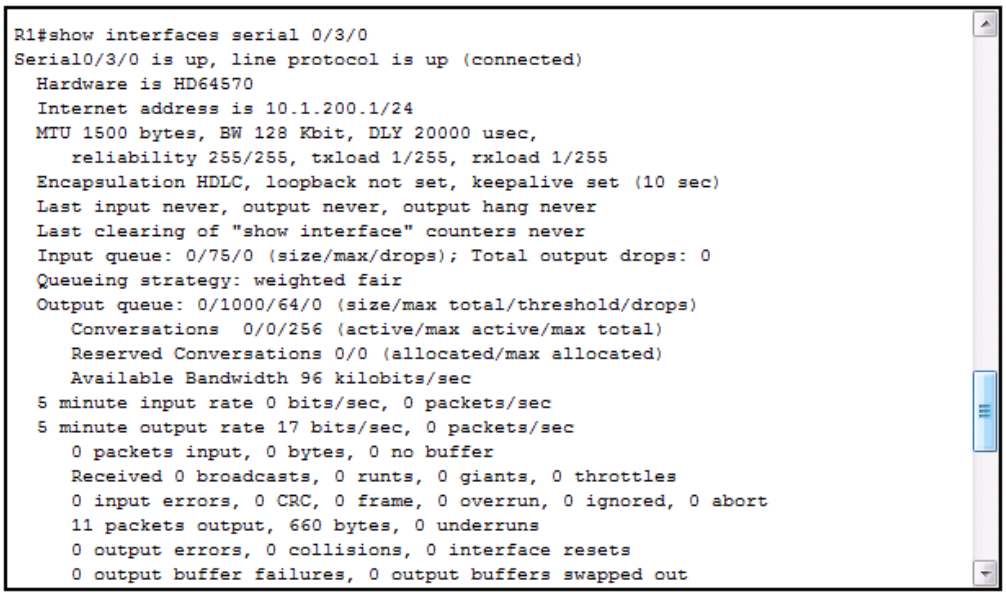
Figura 148. Configuración de la serial0/3/0 en el router R1



Fuente: Software Packet Tracer 5.2.

Se comprueba que aunque se ha sincronizado la interfaz a 64Kbps, el comando **show interface serial 0/3/0** muestra que la interface aún está trabajando a un ancho de banda de 128Kbps.

Figura 149. Información de la serial0/3/0 en el router R1

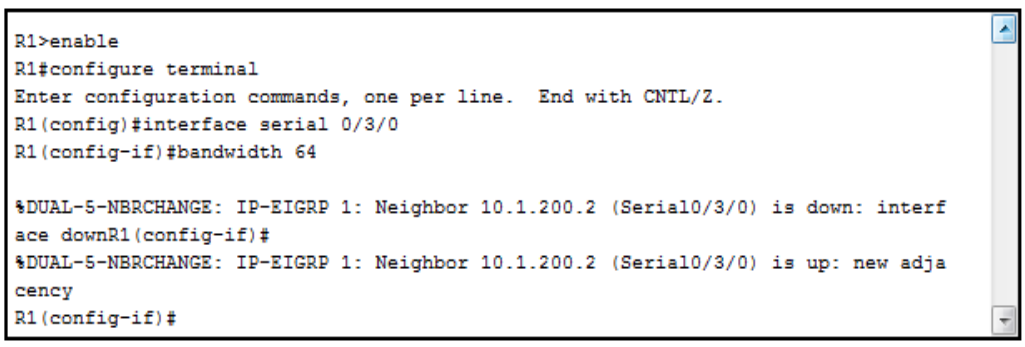


```
R1#show interfaces serial 0/3/0
Serial0/3/0 is up, line protocol is up (connected)
  Hardware is HD64570
  Internet address is 10.1.200.1/24
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 96 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 17 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     11 packets output, 660 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Fuente: Software Packet Tracer 5.2.

EIGRP realiza cálculos de ancho de banda usando una métrica compuesta en la cual una de las variables es el ancho de banda de la interfaz. Para que EIGRP pueda hacer un cálculo exacto, necesita corregir la información acerca del ancho de banda del enlace serial. Por esta razón es necesario configurar manualmente la variable del ancho de banda de las interfaces seriales. Para esto se utiliza el comando **bandwidth 64** tanto en R1 como en R2.

Figura 150. Configuración ancho de banda en la serial0/3/0 en R1



```
R1>enable
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface serial 0/3/0
R1(config-if)#bandwidth 64

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.1.200.2 (Serial0/3/0) is down: interf
ace downR1(config-if)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.1.200.2 (Serial0/3/0) is up: new adja
cency
R1(config-if)#
```

Fuente: Software Packet Tracer 5.2.

Figura 151. Configuración ancho de banda en serial0/3/0 en R2

```
R2>enable
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface serial 0/3/0
R2(config-if)#bandwidth 64

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.1.200.1 (Serial0/3/0) is down: interf
ace downR2(config-if)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.1.200.1 (Serial0/3/0) is up: new adja
cency
```

Fuente: Software Packet Tracer 5.2.

Para verificar el cambio del ancho de banda se utiliza nuevamente el comando **show interfaces serial 0/3/0.**

Figura 152. Información de la serial0/3/0 en el router R1

```
R1#show interfaces serial 0/3/0
Serial0/3/0 is up, line protocol is up (connected)
  Hardware is HD64570
  Internet address is 10.1.200.1/24
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
```

Fuente: Software Packet Tracer 5.2.

Figura 153. Información de la serial0/3/0 en el router R2

```
R2#show interfaces serial 0/3/0
Serial0/3/0 is up, line protocol is up (connected)
  Hardware is HD64570
  Internet address is 10.1.200.2/24
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
```

Fuente: Software Packet Tracer 5.2.

Con el comando **show ip eigrp neighbors** se pueden identificar las adyacencias en cada router y de esta forma se comprueba la correcta configuración EIGRP en los routers.

Figura 154. Adyacencias en el router R1

```
R1>enable
R1#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address         Interface       Hold Uptime    SRTT   RTO   Q   Seq
                                    (sec)          (ms)       Cnt Num
0   10.1.100.2      Fa0/0           14   02:40:46  40     1000  0   16
1   10.1.100.3      Fa0/0           11   02:40:46  40     1000  0   15
2   10.1.200.2      Se0/3/0         14   00:46:09  40     1000  0   17
R1#
```

Fuente: Software Packet Tracer 5.2.

Figura 155. Adyacencias **en el router R1**

```
R2>enable
R2#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address         Interface       Hold Uptime    SRTT   RTO   Q   Seq
                                    (sec)          (ms)       Cnt Num
0   10.1.100.1      Fa0/0           11   02:43:07  40     1000  0   14
1   10.1.100.3      Fa0/0           14   02:43:07  40     1000  0   15
2   10.1.200.1      Se0/3/0         12   00:16:46  40     1000  0   15
R2#
```

Fuente: Software Packet Tracer 5.2.

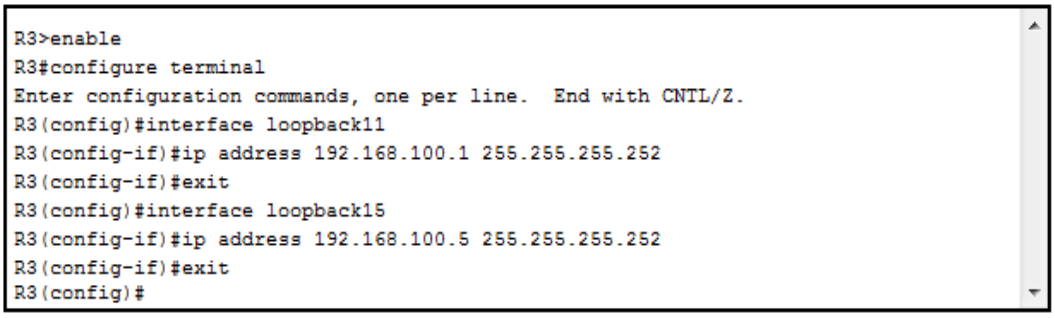
En las salidas obtenidas anteriormente se pueden observar las diferentes interfaces que se configuraron.

Configuración de la máscara Wildcard de la red

En R3, se crean dos nuevas interfaces loopback como se plantean en el diagrama inicial:

- Loopback 11 con dirección IP 192.168.100.1/30
- Loopback15 con dirección IP 192.168.100.5/30

Figura 156. Configuración de loopback 11 y 15 en R3

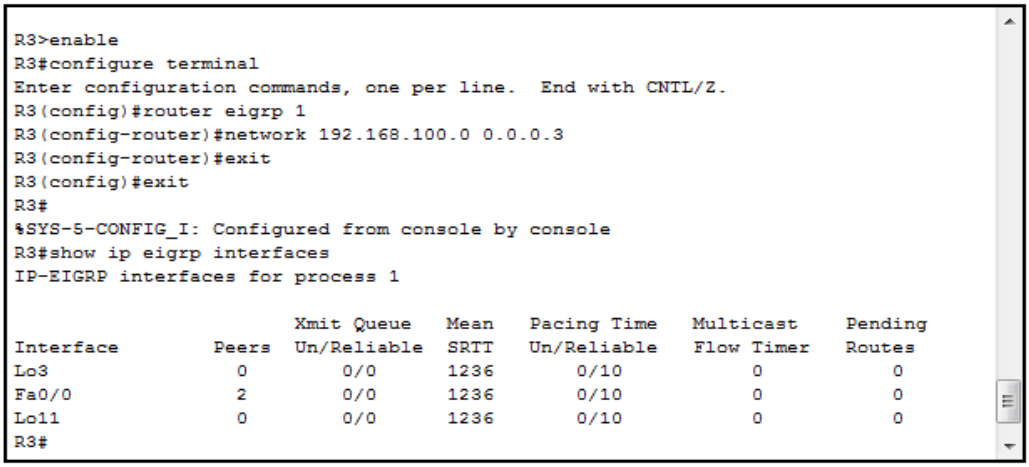


```
R3>enable
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#interface loopback11
R3(config-if)#ip address 192.168.100.1 255.255.255.252
R3(config-if)#exit
R3(config)#interface loopback15
R3(config-if)#ip address 192.168.100.5 255.255.255.252
R3(config-if)#exit
R3(config)#
```

Fuente: Software Packet Tracer 5.2.

Anteriormente, se vio cómo las declaraciones de red seleccionan redes para enrutar usando los límites de la red principal. EIGRP también proporciona una forma de seleccionar redes usando máscaras wildcard. En una máscara wildcard, los bits que pueden variar se denotan por 1s en los valores binarios de bit. Si se quisieran enrutar ambas loopbacks: loopback 11 y loopback 15 con EIGRP, se podría usar una máscara wildcard que incluya ambas direcciones de red, como **network 192.168.100.0 0.0.0.7** ó **network 192.168.100.0 0.0.0.255**. Sin embargo, en este escenario sólo se va a seleccionar la red IP de loopback11.

Figura 157. Configuración de EIGRP y verificación de interfaces en R3

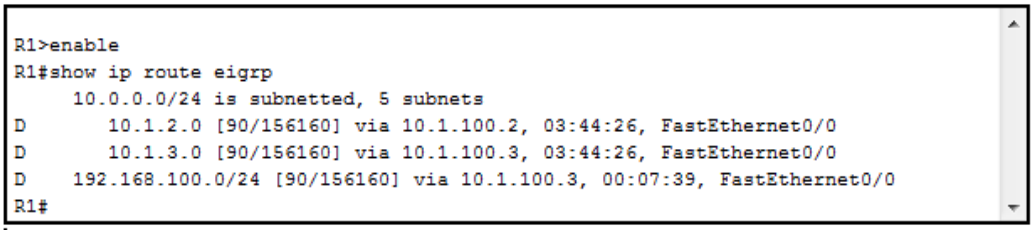


```
R3>enable
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#router eigrp 1
R3(config-router)#network 192.168.100.0 0.0.0.3
R3(config-router)#exit
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#show ip eigrp interfaces
IP-EIGRP interfaces for process 1

                      Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface        Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Lo3                0        0/0      1236       0/10           0           0
Fa0/0              2        0/0      1236       0/10           0           0
Lo11               0        0/0      1236       0/10           0           0
R3#
```

Fuente: Software Packet Tracer 5.2.

Para observar cuál de estas dos redes IP se puede encontrar en la tabla de enrutamiento de R1 después de que EIGRP converja con la nueva red se utiliza el comando **show ip route eigrp** en R1.

Figura 158. Entradas EIGRP en la tabla de enrutamiento en R1



Fuente: Software Packet Tracer 5.2.

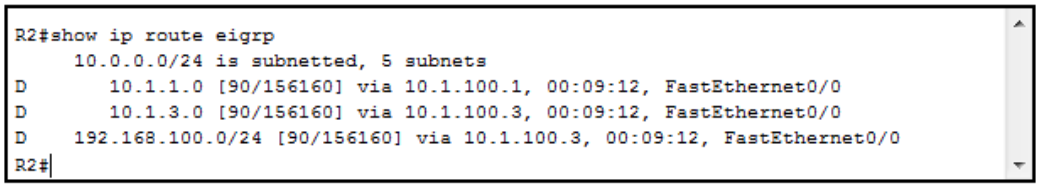
Se observa que la máscara de subred para la red 192.168.100.0 anunciada por R3 tiene 24 bits.

Cambio de topología

La literatura afirma que EIGRP converge significantemente más rápido que otros protocolos de enrutamiento en una topología donde hay múltiples caminos a la red destino. Para probar esto, se verifica que todas las relaciones adyacentes están activas y que las tablas de enrutamiento de cada router tienen las 3 interfaces loopback originales de los otros routers como se describe en el diagrama inicial. (el comando debug ip eigrp 1 se ha ejecutado en todos los routers).

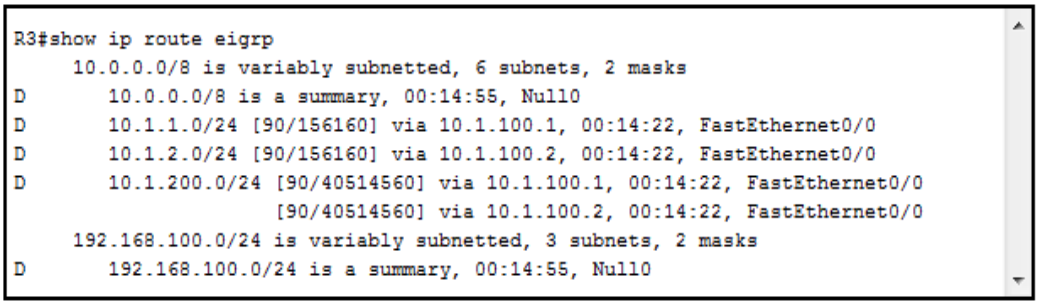
Se observan las siguientes salidas:

Figura 159. Entradas EIGRP en la tabla de enrutamiento en R2



Fuente: Software Packet Tracer 5.2.

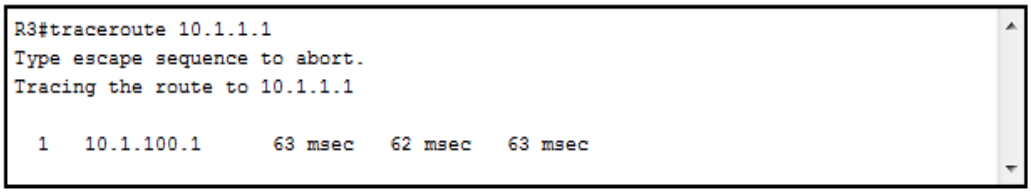
Figura 160. Entradas EIGRP en la tabla de enrutamiento en R3



```
R3#show ip route eigrp
     10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
D       10.0.0.0/8 is a summary, 00:14:55, Null0
D       10.1.1.0/24 [90/156160] via 10.1.100.1, 00:14:22, FastEthernet0/0
D       10.1.2.0/24 [90/156160] via 10.1.100.2, 00:14:22, FastEthernet0/0
D       10.1.200.0/24 [90/40514560] via 10.1.100.1, 00:14:22, FastEthernet0/0
                      [90/40514560] via 10.1.100.2, 00:14:22, FastEthernet0/0
     192.168.100.0/24 is variably subnetted, 3 subnets, 2 masks
D       192.168.100.0/24 is a summary, 00:14:55, Null0
```

Fuente: Software Packet Tracer 5.2.

Figura 161. Seguimiento de la ruta para alcanzar el destino en el router R3



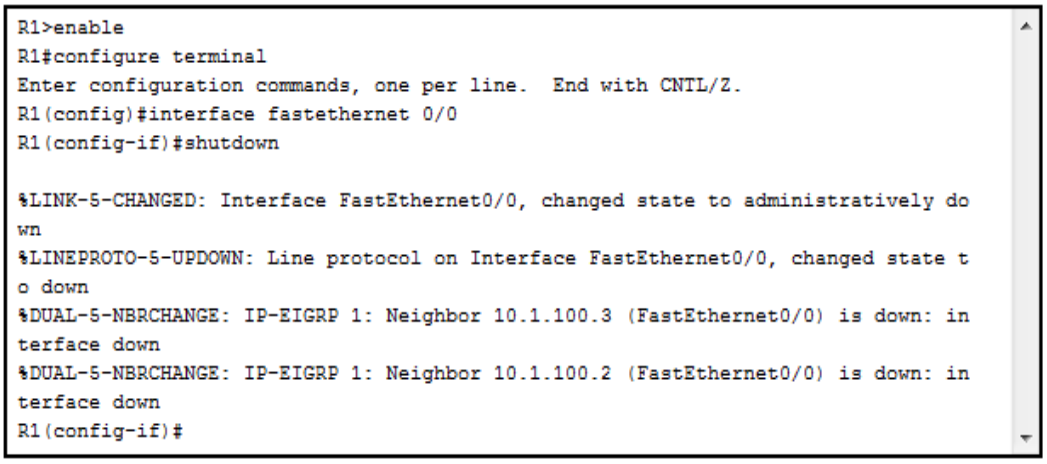
```
R3#traceroute 10.1.1.1
Type escape sequence to abort.
Tracing the route to 10.1.1.1

  1   10.1.100.1      63 msec   62 msec   63 msec
```

Fuente: Software Packet Tracer 5.2.

R3 está usando R1 como el próximo salto para llegar a la red destino 10.1.1.0/24 por la tabla de enrutamiento de R3. Sin embargo, R3 podría potencialmente llegar a R1 a través de R2 vía enlace serial si la fastEthernet en R1 estuviera abajo (shutdown.) Para comprobar esto, se realizará un cambio en la topología bajando la interfaz Fastethernet de R1 mientras se está ejecutando un ping en R3 a la interfaz loopback de R1 con un alto número de repeticiones (1000).

En R1 se baja (shutdown) la interfaz FastEthernet0/0 mientras se está ejecutando un ping.

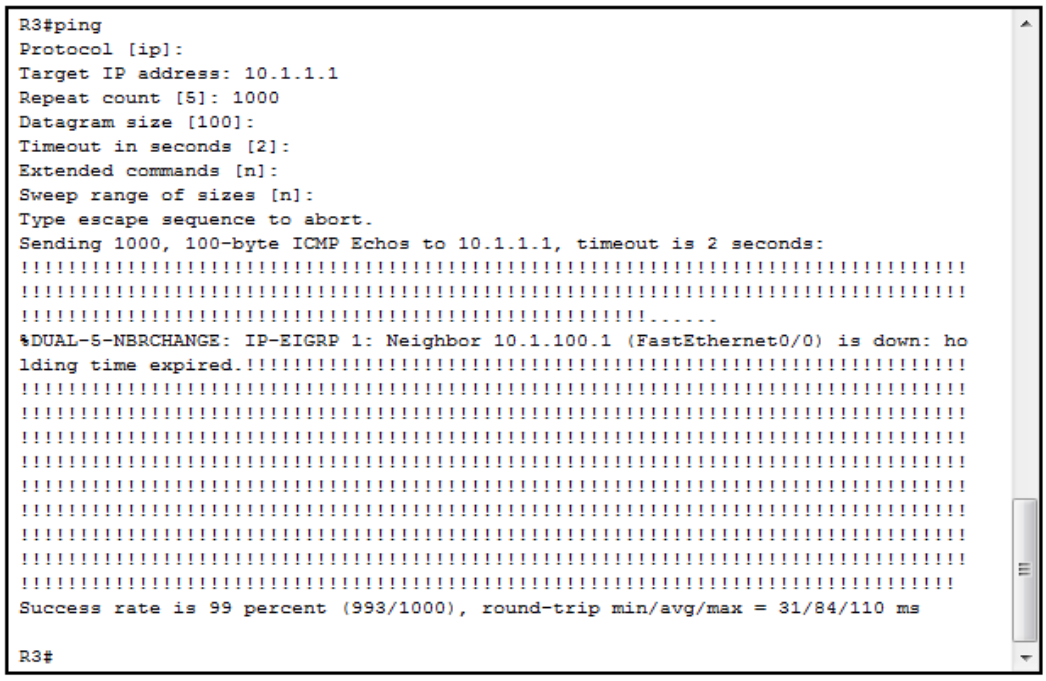
Figura 162. Cambio de estado de la interfaz fastethernet0/0 en el router R1



```
R1>enable
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface fastethernet 0/0
R1(config-if)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to administratively do
wn
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state t
o down
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.1.100.3 (FastEthernet0/0) is down: in
terface down
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.1.100.2 (FastEthernet0/0) is down: in
terface down
R1(config-if)#
```

Fuente: Software Packet Tracer 5.2.

Figura 163. Ping a la loopback de R1 en el router R3



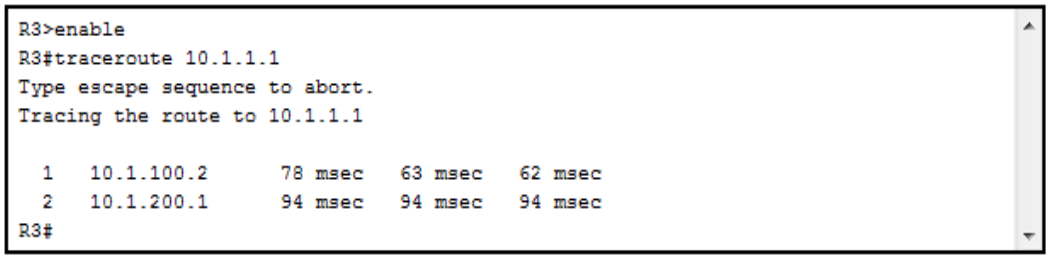
```
R3#ping
Protocol [ip]:
Target IP address: 10.1.1.1
Repeat count [5]: 1000
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 1000, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 99 percent (993/1000), round-trip min/avg/max = 31/84/110 ms

R3#
```

Fuente: Software Packet Tracer 5.2.

El resultado del ping realizado desde R3 a la interfaz loopback de R1 muestra que se pierden 7 paquetes debido a que cuando se baja la

interfaz loopback, R1 envía un mensaje de actualización a R2 el cual envía la actualización a R3. Los routers entran en estado activo para buscar una ruta (si es necesaria) y recalculan. Sin embargo luego de unos segundos se retoma el envío de paquetes ya que encuentra una ruta alternativa. Esto se puede comprobar ejecutando el comando traceroute en R3 a la loopback de R1 como se muestra a continuación:

Figura 164. Seguimiento de la ruta para alcanzar el destino en el router R3

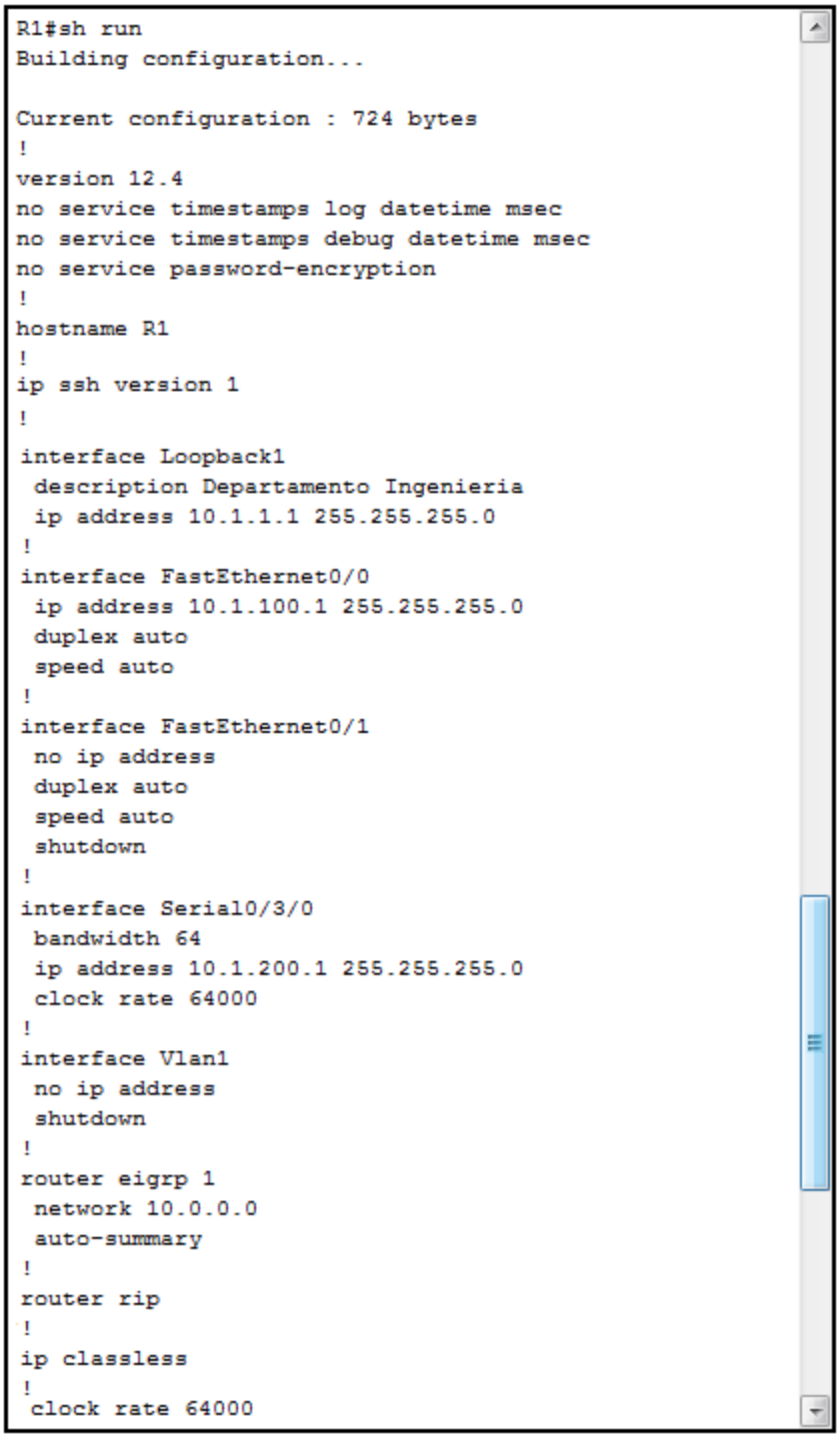


Fuente: Software Packet Tracer 5.2.

Configuración Final

Finalmente se verifica la configuración final de las interfaces en uno de los dispositivos. Existen algunos comandos que permiten mostrar la información relativa al router. Todos comienzan con el prefijo **show** o **sh**. La mayoría deben ser ejecutados desde el modo privilegiado. Uno de estos comandos es **show running-config** (ó **sh run**) que muestra el archivo de configuración actual del router como se muestra a continuación:

Figura 165. Archivo de configuración actual del router R1



```
R1#sh run
Building configuration...

Current configuration : 724 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R1
!
ip ssh version 1
!
interface Loopback1
 description Departamento Ingenieria
 ip address 10.1.1.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 10.1.100.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/3/0
 bandwidth 64
 ip address 10.1.200.1 255.255.255.0
 clock rate 64000
!
interface Vlan1
 no ip address
 shutdown
!
router eigrp 1
 network 10.0.0.0
 auto-summary
!
router rip
!
ip classless
!
 clock rate 64000
```

Fuente: Software Packet Tracer 5.2.

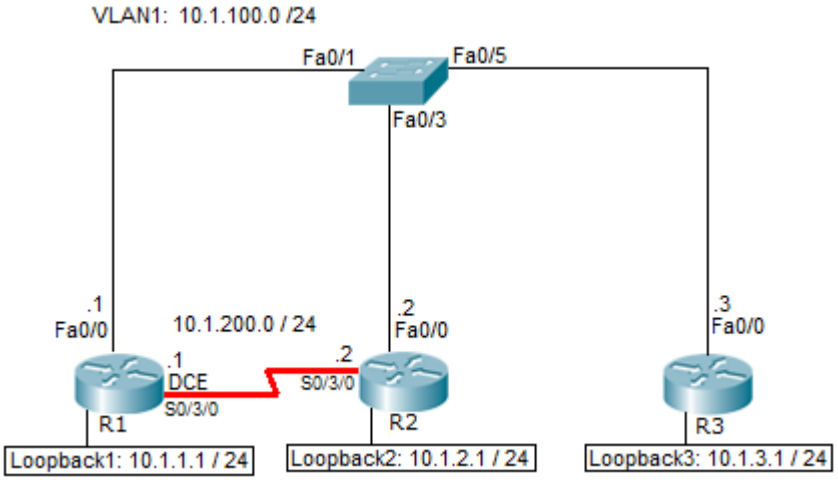
5.2. OSPF

Planteamiento

Configurar una red para conectar los departamentos de ingeniería, marketing y contabilidad de una compañía, representados por las interfaces loopback en cada uno de los 3 routers. Los dispositivos físicos han sido instalados y conectados por FastEthernet y cables seriales. Se debe configurar OSPF para permitir la conectividad completa entre todos los departamentos.

Diagrama

Figura 166. Diagrama del laboratorio OSPF



Fuente: Autoras.

Solución:

A continuación se describen los pasos que se siguieron para realizar esta simulación. (El simulador utilizado para esta práctica fue Packet Tracer).

Configuración de interfaces en los dispositivos

Inicialmente se realiza el direccionamiento IP basado en el diagrama, se crea la interfaz Loopback1 en R1, Loopback2 en R2 y Loopback3 en R3 y se direccionan de acuerdo al diagrama, después se asignan direcciones IP a las interfaces FastEthernet en R1, R2 y R3. Este proceso inicial se sigue de la misma forma en que se trabajó con EIGRP.

Figura 167. Configuración de interfaces loopback1 y fastehternet0/0 en el router R1

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#interface loopback 1

%LINK-5-CHANGED: Interface Loopback1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up
R1(config-if)#description Departamento de Ingenieria
R1(config-if)#ip address 10.1.1.1 255.255.255.0
R1(config-if)#exit
R1(config)#interface fastethernet0/0
R1(config-if)#ip address 10.1.100.1 255.255.255.0
R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state t
o up
R1(config-if)#
```

Fuente: Software Packet Tracer 5.2.

Figura 168. Configuración de loopback2 y fastehternet0/0 en R2

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R2
R2(config)#interface loopback 2

%LINK-5-CHANGED: Interface Loopback2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback2, changed state to up
R2(config-if)#description Departamento de Marketing
R2(config-if)#ip address 10.1.2.1 255.255.255.0
R2(config-if)#exit
R2(config)#interface fastethernet0/0
R2(config-if)#ip address 10.1.100.2 255.255.255.0
R2(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state t
o up
R2(config-if)#
```

Fuente: Software Packet Tracer 5.2.

Figura 169. Configuración de loopback3 y fastehternet0/0 en R3

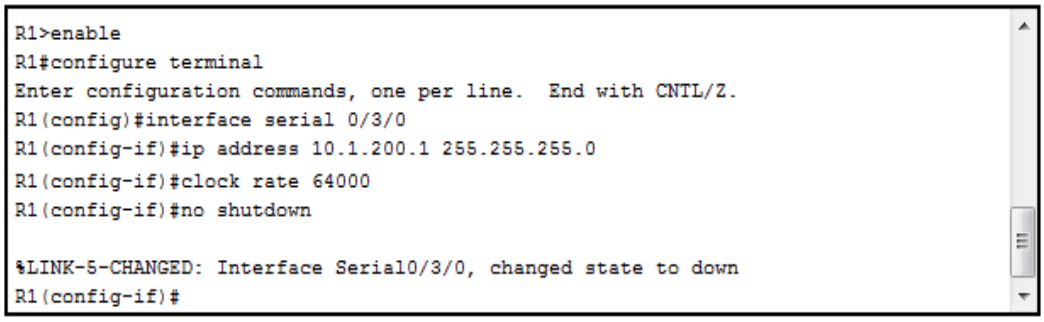
```
R3>enable
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R3
R3(config)#interface loopback 3

R3(config-if)#
%LINK-5-CHANGED: Interface Loopback3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback3, changed state to up
R3(config-if)#description Departamento de Contabilidad
R3(config-if)#ip address 10.1.3.1 255.255.255.0
R3(config-if)#exit
R3(config)#interface fastethernet0/0
R3(config-if)#ip address 10.1.100.3 255.255.255.0
R3(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state t
o up
R3(config-if)#
```

Fuente: Software Packet Tracer 5.2.

El switch se deja en su configuración por defecto, en la cual todos los puertos del switch están en la VLAN1 y no están administrativamente abajo.

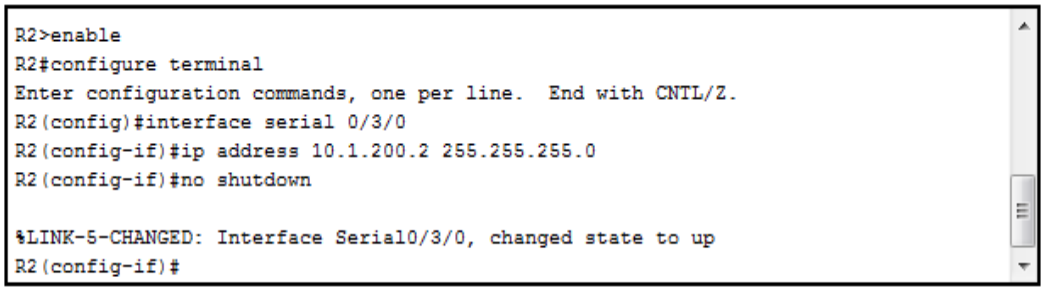
Adicionalmente se configuran las interfaces seriales con las direcciones IP dadas en el diagrama, teniendo en cuenta que se debe configurar el "clock rate" en la interfaz apropiada (DCE).

Figura 170. Configuración de la interfaz serial0/3/0 en el router R1



Fuente: Software Packet Tracer 5.2.

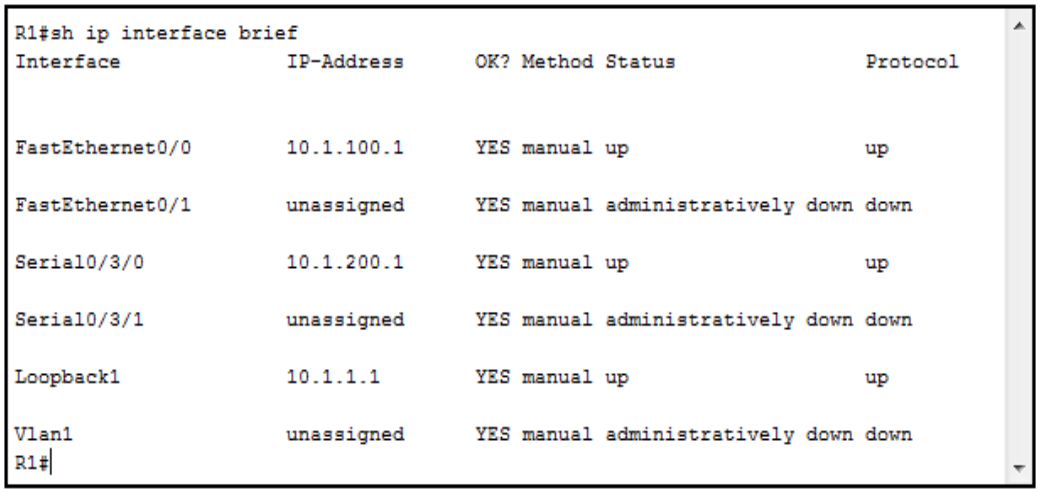
Figura 171. Configuración de la interfaz serial0/3/0 en el router R2



Fuente: Software Packet Tracer 5.2.

Se verifica que cada interfaz esté arriba en la columna de "*Protocol*" y de esta manera se pueda ejecutar satisfactoriamente un ping a través de cada enlace.

Figura 172. Verificación de las interfaces configuradas en el router R1



```
R1#sh ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/0        10.1.100.1      YES manual up                    up

FastEthernet0/1        unassigned      YES manual administratively down down

Serial0/3/0            10.1.200.1      YES manual up                    up

Serial0/3/1            unassigned      YES manual administratively down down

Loopback1              10.1.1.1        YES manual up                    up

Vlan1                  unassigned      YES manual administratively down down
R1#
```

Fuente: Software Packet Tracer 5.2.

Configuración OSPF

Después de establecer el direccionamiento IP y de comprobar conectividad de la red local, se continúa con la adición de interfaces físicas a OSPF. Se puede configurar el proceso OSPF 1. Para ingresar a la configuración OSPF del sistema se utiliza el comando **router ospf *process_number.*** El *process_number* es un número local que no afecta el trabajo de OSPF. Para este laboratorio se usará el número de proceso 1 en todos los routers.

A continuación, se agregan las interfaces con el comando **network *address wildcard_mask* area *area.*** La dirección puede ser cualquier dirección IP. "*area"* es el área OSPF donde se desea colocar la interfaz. Para este laboratorio se usará un área 0 que es el área de *backbone* para todas las interfaces. Este comando indica que cualquier interfaz con una IP que coincida con la combinación de dirección y máscara wilcard en la declaración de red se adiciona al proceso OSPF en esa área.

El comando **Network 10.1.100.0 0.0.0.255 area 0** indica que cualquier interfaz cuya dirección IP coincida con 10.1.100.0 para los primeros 3 octetos, el comando coincidirá y la agregará al área 0. En el último octeto

todos son 1s, porque la máscara wilcard es 255. Esto quiere decir que una interfaz con una IP de 10.1.100.1, 10.1.100.2 ó 10.1.100.250 coincidiría con esta dirección y la combinación wilcard y se agregaría a OSPF.

En OSPF las direcciones de red se configuran con una máscara wildcard y no con una máscara de subred debido a que la máscara wildcard representa el conjunto de direcciones de enlaces o de hosts que admite el segmento.

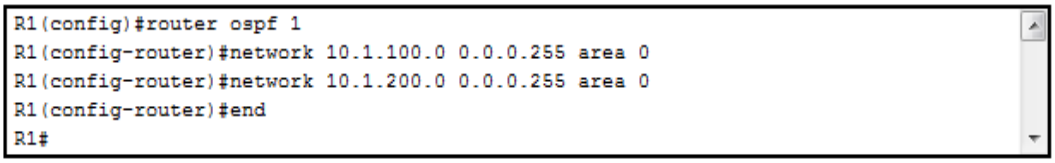
La máscara wilcard no tiene que ser la inversa de una máscara de subred de una interfaz IP, aunque puede ser útil. Una forma fácil de calcular la máscara wilcard a partir de una máscara de subred es restar 255 menos el valor del octeto para cada octeto. Por ejemplo una máscara de subred de 255.255.255.252(/30) se convierte en 0.0.0.3 para capturar todas las interfaces en esta subred. Esto es debido a que 255-255 = 0 y 255-252=3.

La máscara wildcard indica con sus ceros y sus unos qué bits han de compararse o no. Un cero indica que el bit ha de compararse y un uno indica que se ignore. De esta forma se pueden filtrar direcciones IP individuales o en grupos, permitiendo o rechazando el acceso a recursos según el valor de las mismas. La máscara le indica a OSPF, tomando como base la dirección de red, el rango de direcciones que deben considerarse.

Esto es distinto de lo que ocurre con una máscara de subred que se utiliza al configurar las direcciones IP en las interfaces para identificar las porciones de red, de subred y de host de una dirección IP. La única similitud entre la máscara wildcard y la de subred es que ambas tienen 32 bits de longitud y se componen de unos y ceros.

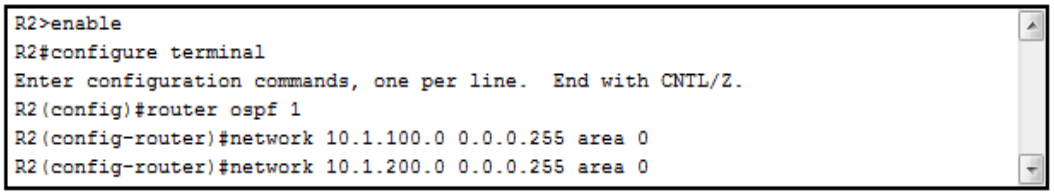
A continuación se configura OSPF en R1, R2 y R3:

Figura 173. Configuración de OSPF en el router R1



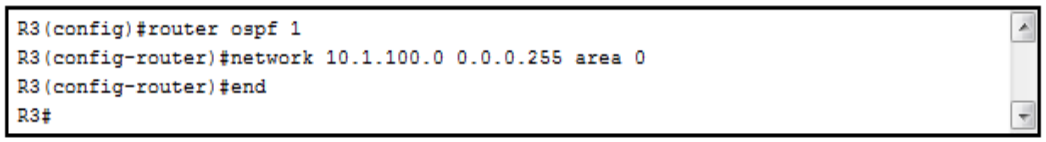
Fuente: Software Packet Tracer 5.2.

Figura 174. Configuración de OSPF en el router R2



Fuente: Software Packet Tracer 5.2.

Figura 175. Configuración de OSPF en el router R3



Fuente: Software Packet Tracer 5.2.

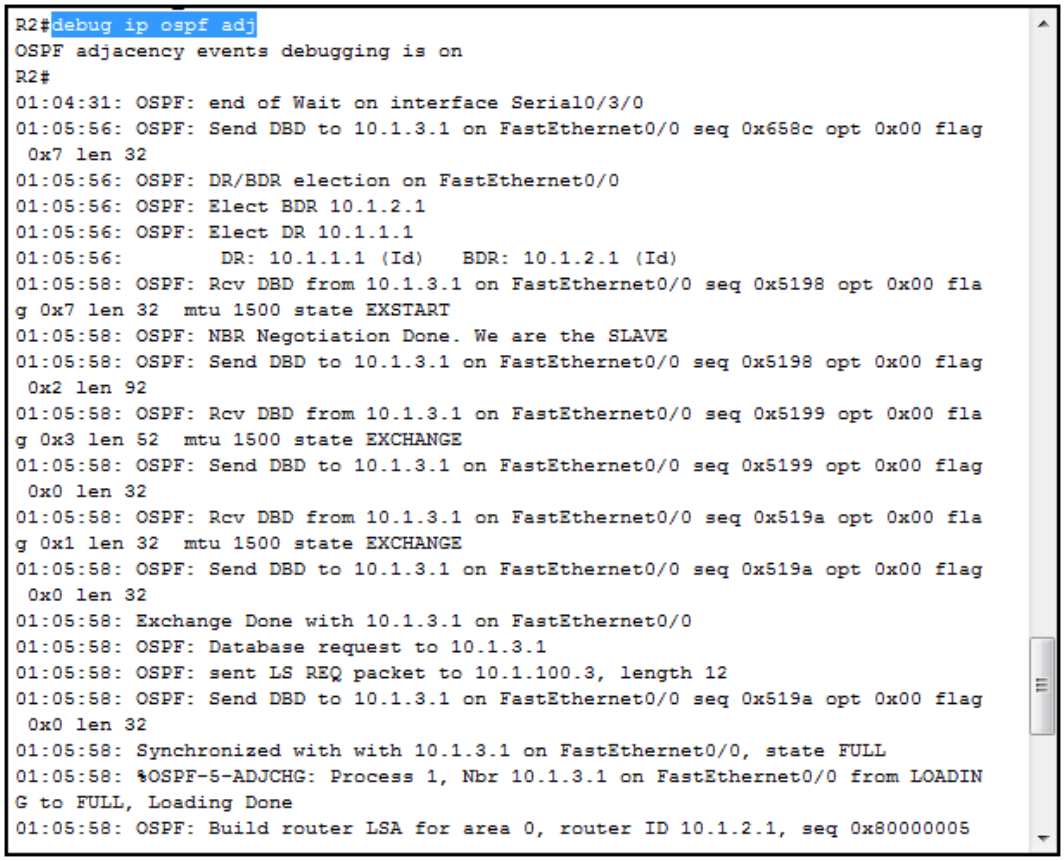
El comando debug ip ospf **adj** muestra los vecinos y sus relaciones. A continuación se ejecuta este comando en los router R1 y R2 y se obtienen las siguientes salidas:

Figura 176. Lista de vecinos y sus relaciones en el router R1

```
R1#debug ip ospf adj
OSPF adjacency events debugging is on
R1#
01:04:07: OSPF: Send DBD to 10.1.2.1 on FastEthernet0/0 seq 0x7b65 opt 0x00 flag
 0x7 len 32
01:04:07: OSPF: DR/BDR election on FastEthernet0/0
01:04:07: OSPF: Elect BDR 10.1.2.1
01:04:07: OSPF: Elect DR 10.1.1.1
01:04:07:         DR: 10.1.1.1 (Id)   BDR: 10.1.2.1 (Id)
01:04:10: OSPF: Rcv DBD from 10.1.2.1 on FastEthernet0/0 seq 0x267b opt 0x00 fla
g 0x7 len 32  mtu 1500 state EXSTART
01:04:10: OSPF: NBR Negotiation Done. We are the SLAVE
01:04:10: OSPF: Send DBD to 10.1.2.1 on FastEthernet0/0 seq 0x267b opt 0x00 flag
 0x2 len 52
01:04:10: OSPF: Rcv DBD from 10.1.2.1 on FastEthernet0/0 seq 0x267c opt 0x00 fla
g 0x3 len 52  mtu 1500 state EXCHANGE
01:04:10: OSPF: Send DBD to 10.1.2.1 on FastEthernet0/0 seq 0x267c opt 0x00 flag
 0x0 len 32
01:04:10: OSPF: Rcv DBD from 10.1.2.1 on FastEthernet0/0 seq 0x267d opt 0x00 fla
g 0x1 len 32  mtu 1500 state EXCHANGE
01:04:10: OSPF: Send DBD to 10.1.2.1 on FastEthernet0/0 seq 0x267d opt 0x00 flag
 0x0 len 32
01:04:10: Exchange Done with 10.1.2.1 on FastEthernet0/0
01:04:10: OSPF: Database request to 10.1.2.1
01:04:10: OSPF: sent LS REQ packet to 10.1.100.2, length 12
01:04:10: OSPF: Send DBD to 10.1.2.1 on FastEthernet0/0 seq 0x267d opt 0x00 flag
 0x0 len 32
01:04:10: Synchronized with with 10.1.2.1 on FastEthernet0/0, state FULL
01:04:10: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.2.1 on FastEthernet0/0 from LOADIN
G to FULL, Loading Done
01:04:10: OSPF: Build router LSA for area 0, router ID 10.1.1.1, seq 0x80000003
01:04:10: OSPF: Build net LSA for area 0, router ID 10.1.1.1, seq 0x80000001
01:04:15: OSPF: Rcv DBD from 10.1.2.1 on Serial0/3/0 seq 0x308 opt 0x00 flag 0x7
 len 32  mtu 1500 state INIT
01:04:15: OSPF: Send DBD to 10.1.2.1 on Serial0/3/0 seq 0x6883 opt 0x00 flag 0x7
 len 32
01:04:15: OSPF: NBR Negotiation Done. We are the SLAVE
01:04:15: OSPF: Send DBD to 10.1.2.1 on Serial0/3/0 seq 0x308 opt 0x00 flag 0x2
len 92
01:04:15: OSPF: Rcv DBD from 10.1.2.1 on Serial0/3/0 seq 0x309 opt 0x00 flag 0x3
 len 92  mtu 1500 state EXCHANGE
01:04:15: OSPF: Send DBD to 10.1.2.1 on Serial0/3/0 seq 0x309 opt 0x00 flag 0x0
len 32
01:04:15: OSPF: Rcv DBD from 10.1.2.1 on Serial0/3/0 seq 0x30a opt 0x00 flag 0x1
 len 32  mtu 1500 state EXCHANGE
01:04:15: OSPF: Send DBD to 10.1.2.1 on Serial0/3/0 seq 0x30a opt 0x00 flag 0x0
```

Fuente: Software Packet Tracer 5.2.

Figura 177. Lista de vecinos y sus relaciones en el router R2



```
R2#debug ip ospf adj
OSPF adjacency events debugging is on
R2#
01:04:31: OSPF: end of Wait on interface Serial0/3/0
01:05:56: OSPF: Send DBD to 10.1.3.1 on FastEthernet0/0 seq 0x658c opt 0x00 flag
 0x7 len 32
01:05:56: OSPF: DR/BDR election on FastEthernet0/0
01:05:56: OSPF: Elect BDR 10.1.2.1
01:05:56: OSPF: Elect DR 10.1.1.1
01:05:56:         DR: 10.1.1.1 (Id)   BDR: 10.1.2.1 (Id)
01:05:58: OSPF: Rcv DBD from 10.1.3.1 on FastEthernet0/0 seq 0x5198 opt 0x00 fla
g 0x7 len 32  mtu 1500 state EXSTART
01:05:58: OSPF: NBR Negotiation Done. We are the SLAVE
01:05:58: OSPF: Send DBD to 10.1.3.1 on FastEthernet0/0 seq 0x5198 opt 0x00 flag
 0x2 len 92
01:05:58: OSPF: Rcv DBD from 10.1.3.1 on FastEthernet0/0 seq 0x5199 opt 0x00 fla
g 0x3 len 52  mtu 1500 state EXCHANGE
01:05:58: OSPF: Send DBD to 10.1.3.1 on FastEthernet0/0 seq 0x5199 opt 0x00 flag
 0x0 len 32
01:05:58: OSPF: Rcv DBD from 10.1.3.1 on FastEthernet0/0 seq 0x519a opt 0x00 fla
g 0x1 len 32  mtu 1500 state EXCHANGE
01:05:58: OSPF: Send DBD to 10.1.3.1 on FastEthernet0/0 seq 0x519a opt 0x00 flag
 0x0 len 32
01:05:58: Exchange Done with 10.1.3.1 on FastEthernet0/0
01:05:58: OSPF: Database request to 10.1.3.1
01:05:58: OSPF: sent LS REQ packet to 10.1.100.3, length 12
01:05:58: OSPF: Send DBD to 10.1.3.1 on FastEthernet0/0 seq 0x519a opt 0x00 flag
 0x0 len 32
01:05:58: Synchronized with with 10.1.3.1 on FastEthernet0/0, state FULL
01:05:58: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.3.1 on FastEthernet0/0 from LOADIN
G to FULL, Loading Done
01:05:58: OSPF: Build router LSA for area 0, router ID 10.1.2.1, seq 0x80000005
```

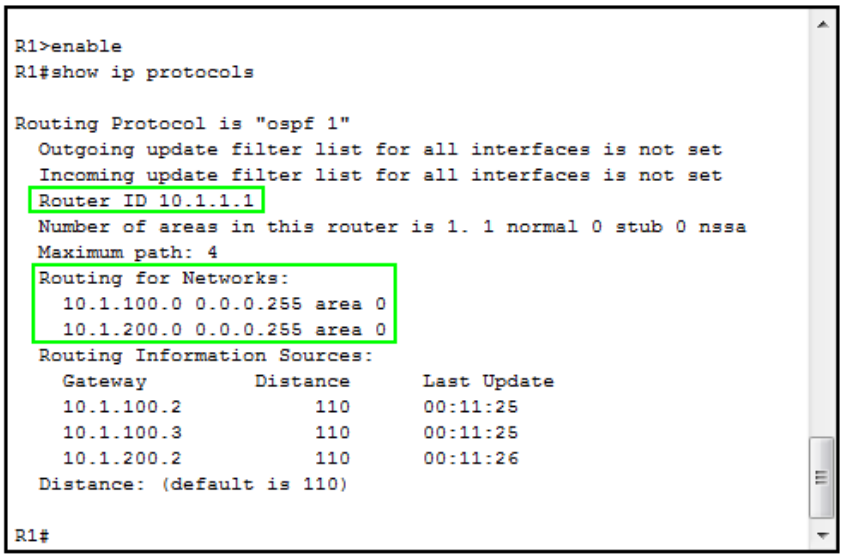
Fuente: Software Packet Tracer 5.2.

Para detener la depuración del comando **debug ip ospf adj** se utiliza el comando **undebug all.**

Como se mencionó anteriormente (capítulo 2. Monitoreo de OSPF), los comandos **show** en OSPF resultan muy útiles a la hora de verificar la configuración de las interfaces y estados de enrutamiento. A continuación se ejecutan algunos comandos **show** para verificar información de configuración.

El comando **show ip protocols** muestra la información básica del protocolo de enrutamiento:

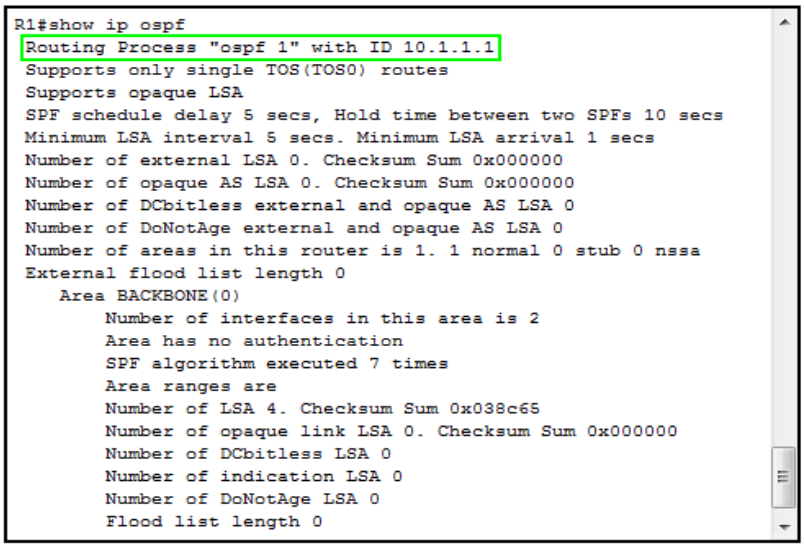
Figura 178. Información básica del protocolo en el router R1



Fuente: Software Packet Tracer 5.2.

Otro comando útil es **show ip ospf**, utilizado para examinar el ID del proceso OSPF y el ID del router. Adicionalmente, este comando muestra la información del área OSPF.

Figura 179. Información del área OSPF en el router R1

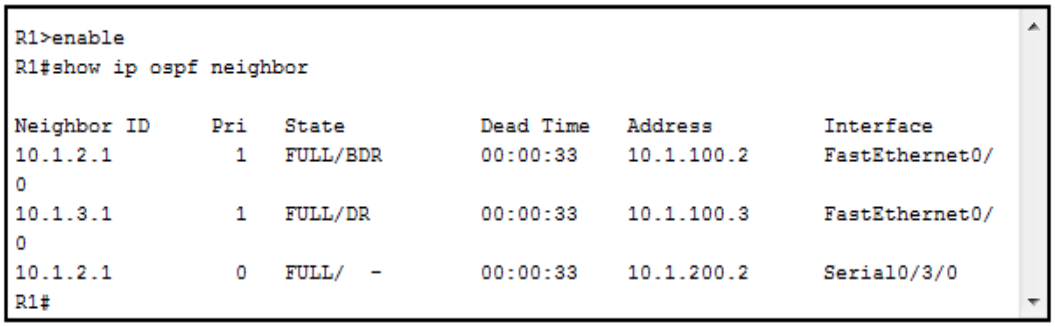


Fuente: Software Packet Tracer 5.2.

En la salida de este comando aparece el ID del router: 10.1.1.1, a pesar de que no se ha configurado esta loopback en el proceso OSPF. El router escoge el ID del router usando la dirección IP más alta en una interface loopback cuando se configura OSPF. Si se adiciona una interfaz loopback con una dirección IP más alta después de haber configurado OSPF, esta dirección no se convierte automáticamente en el ID del router, para que se tome este cambio, el router debe ser reiniciado. Si no hay interfaces loopback presentes en el router, el router toma la dirección IP más alta disponible en una interfaz. Si no hay direcciones IP asignadas a las interfaces, el proceso de OSPF no puede iniciarse.

El comando **show ip ospf neighbor** muestra el estado de los vecinos, incluyendo el estado de la adyacencia, dirección, ID del router e interfaz conectada.

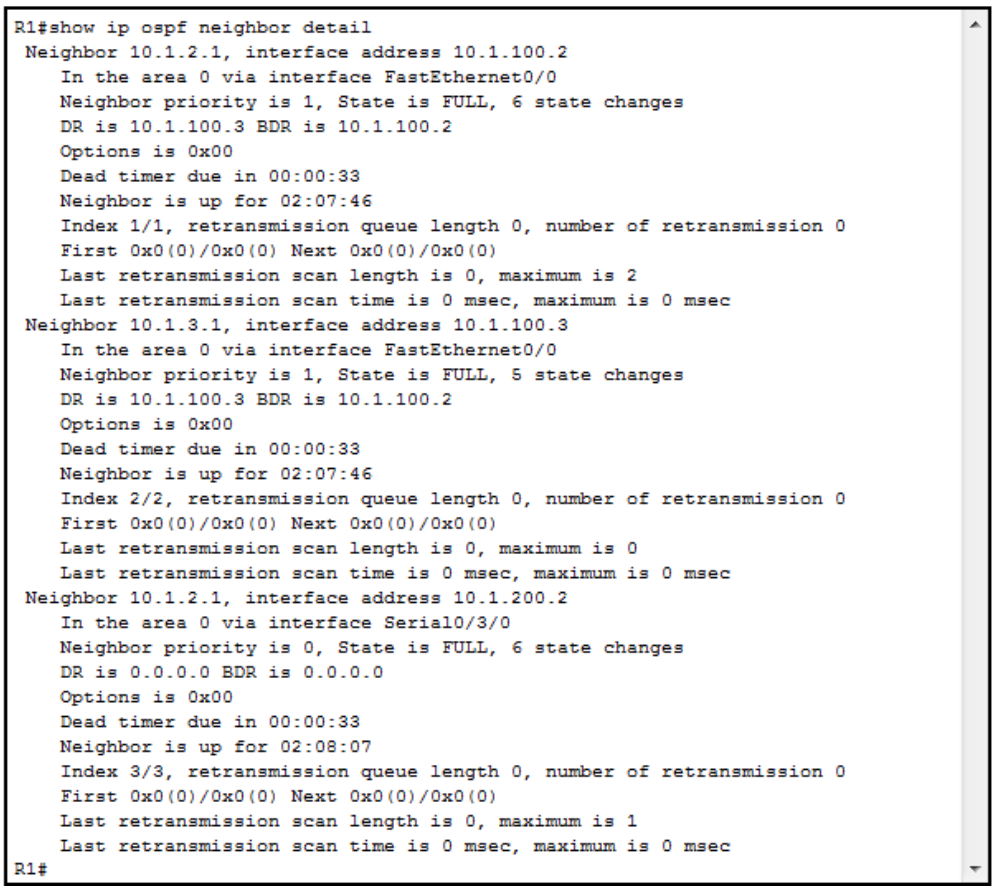
Figura 180. Información del estado de los vecinos en el router R1



Fuente: Software Packet Tracer 5.2.

Para obtener información más detallada se usa el comando **show ip ospf neighbor detail** el cual muestra información más detallada sobre los vecinos. Sin embargo, en la mayoría de los casos el comando **show ip ospf neighbor** muestra la información necesaria.

Figura 181. Información detallada del estado de los vecinos en el router R1

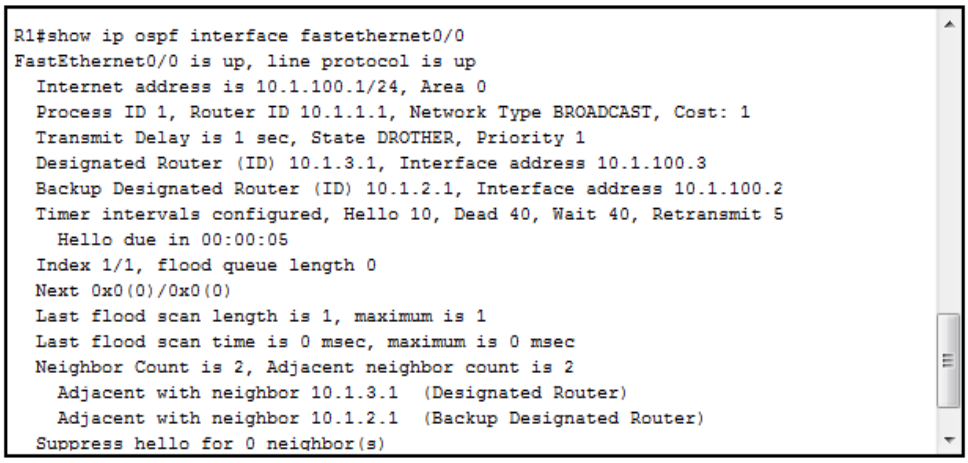


```
R1#show ip ospf neighbor detail
 Neighbor 10.1.2.1, interface address 10.1.100.2
    In the area 0 via interface FastEthernet0/0
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 10.1.100.3 BDR is 10.1.100.2
    Options is 0x00
    Dead timer due in 00:00:33
    Neighbor is up for 02:07:46
    Index 1/1, retransmission queue length 0, number of retransmission 0
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 0, maximum is 2
    Last retransmission scan time is 0 msec, maximum is 0 msec
 Neighbor 10.1.3.1, interface address 10.1.100.3
    In the area 0 via interface FastEthernet0/0
    Neighbor priority is 1, State is FULL, 5 state changes
    DR is 10.1.100.3 BDR is 10.1.100.2
    Options is 0x00
    Dead timer due in 00:00:33
    Neighbor is up for 02:07:46
    Index 2/2, retransmission queue length 0, number of retransmission 0
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 0, maximum is 0
    Last retransmission scan time is 0 msec, maximum is 0 msec
 Neighbor 10.1.2.1, interface address 10.1.200.2
    In the area 0 via interface Serial0/3/0
    Neighbor priority is 0, State is FULL, 6 state changes
    DR is 0.0.0.0 BDR is 0.0.0.0
    Options is 0x00
    Dead timer due in 00:00:33
    Neighbor is up for 02:08:07
    Index 3/3, retransmission queue length 0, number of retransmission 0
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 0, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
R1#
```

Fuente: Software Packet Tracer 5.2.

Otro comando útil es **show ip ospf interface** *interface_type number*. Este comando muestra los temporizadores y los tipos de red de la interfaz.

Figura 182. Información de la interface fastethernet0/0 en el router R1

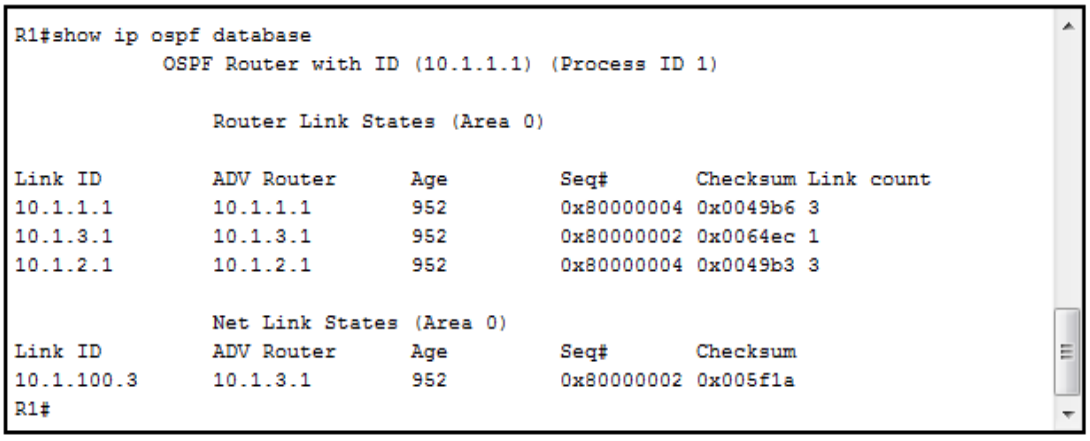


```
R1#show ip ospf interface fastethernet0/0
FastEthernet0/0 is up, line protocol is up
  Internet address is 10.1.100.1/24, Area 0
  Process ID 1, Router ID 10.1.1.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DROTHER, Priority 1
  Designated Router (ID) 10.1.3.1, Interface address 10.1.100.3
  Backup Designated Router (ID) 10.1.2.1, Interface address 10.1.100.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 2, Adjacent neighbor count is 2
    Adjacent with neighbor 10.1.3.1  (Designated Router)
    Adjacent with neighbor 10.1.2.1  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
```

Fuente: Software Packet Tracer 5.2.

El comando **show ip ospf database** muestra los diversos estados de enlace -LSA (*Link State Advertising*) en la base de datos OSPF organizada por área y por tipo.

Figura 183. Información LSA (Link State Advertising) en R1



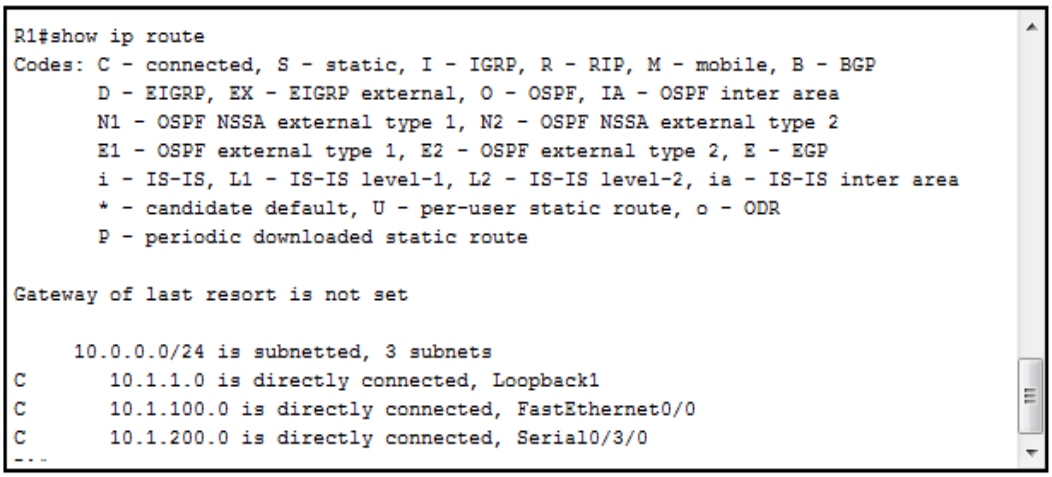
```
R1#show ip ospf database
            OSPF Router with ID (10.1.1.1) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
10.1.1.1        10.1.1.1        952         0x80000004 0x0049b6 3
10.1.3.1        10.1.3.1        952         0x80000002 0x0064ec 1
10.1.2.1        10.1.2.1        952         0x80000004 0x0049b3 3

                Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
10.1.100.3      10.1.3.1        952         0x80000002 0x005f1a
R1#
```

Fuente: Software Packet Tracer 5.2.

Adición de interfaces loopback a OSPF

Hasta el momento, los routers R1, R2, y R3 tienen interfaces loopback, pero éstas no se han publicado en el proceso de enrutamiento. Esto se puede verificar con **show ip route** en los routers.

Figura 184. Información del estado actual de la tabla de enrutamiento en el router R1

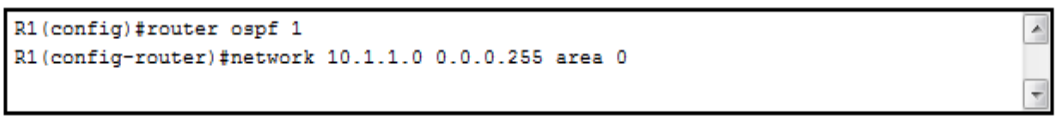


Fuente: Software Packet Tracer 5.2.

Para cada uno de los routers, la única dirección loopback que aparece es la que está localmente conectada.

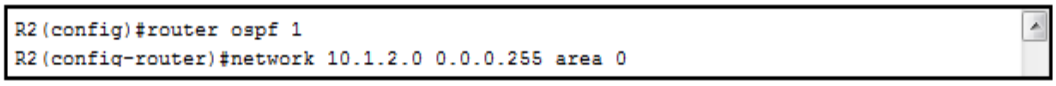
En el proceso de enrutamiento se utiliza el comando **network** para adicionar las interfaces.

Figura 185. Configuración de la red conectada y el área en el router R1



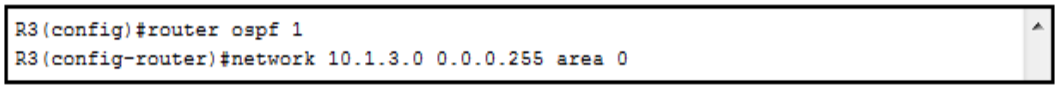
Fuente: Software Packet Tracer 5.2.

Figura 186. Configuración de la red conectada y el área en el router R2



Fuente: Software Packet Tracer 5.2.

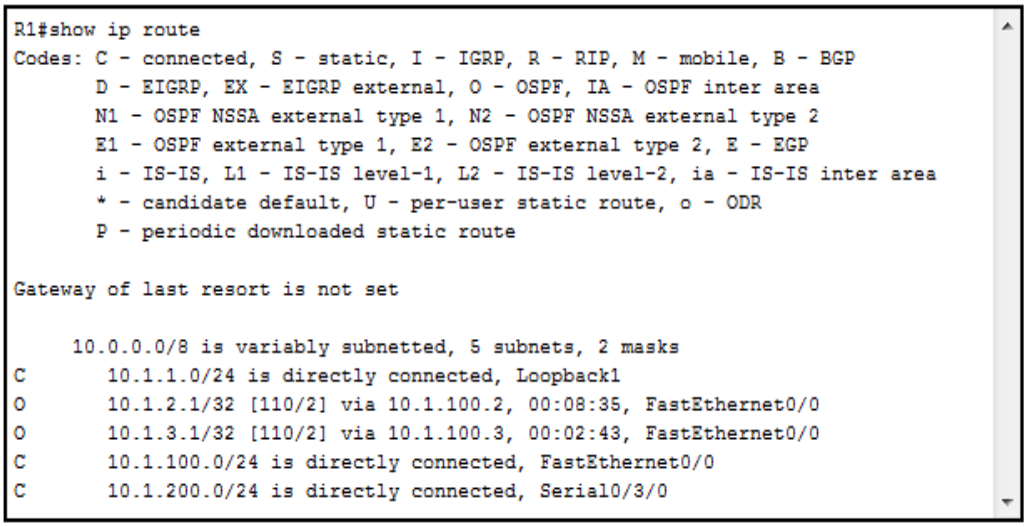
Figura 187. Configuración de la red conectada y el área en el router R3



Fuente: Software Packet Tracer 5.2.

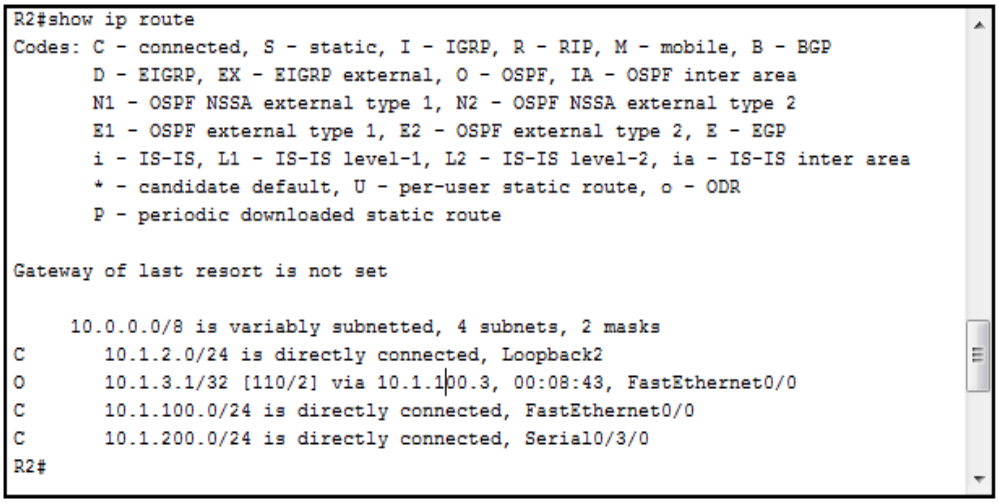
Para comprobar que estas redes han sido adicionadas a la tabla de enrutamiento se usa nuevamente el comando **show ip route**

Figura 188. Información de la tabla de enrutamiento en R1



Fuente: Software Packet Tracer 5.2.

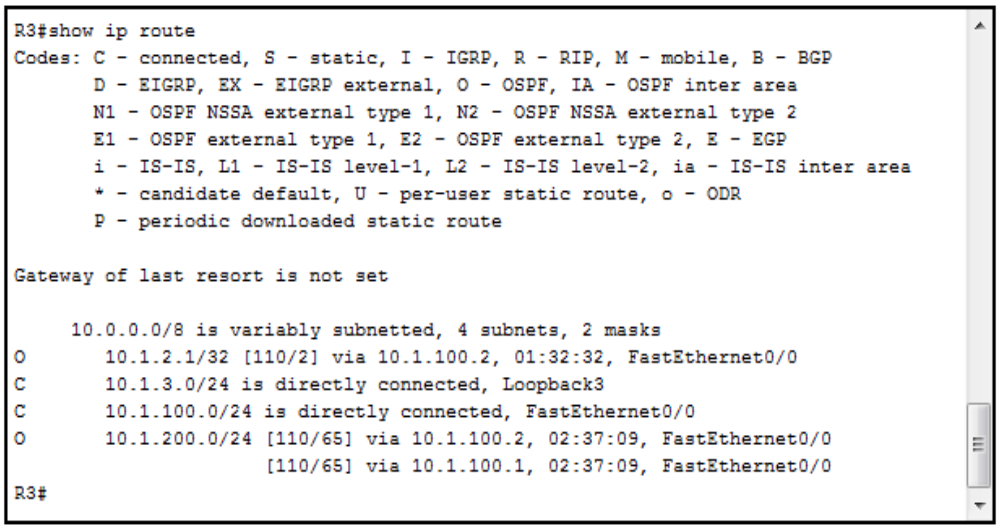
Figura 189. Información de la tabla de enrutamiento en R2



```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.1.2.0/24 is directly connected, Loopback2
O       10.1.3.1/32 [110/2] via 10.1.100.3, 00:08:43, FastEthernet0/0
C       10.1.100.0/24 is directly connected, FastEthernet0/0
C       10.1.200.0/24 is directly connected, Serial0/3/0
R2#
```

Fuente: Software Packet Tracer 5.2.

Figura 190. Información de la tabla de enrutamiento en R3



```
R3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
O       10.1.2.1/32 [110/2] via 10.1.100.2, 01:32:32, FastEthernet0/0
C       10.1.3.0/24 is directly connected, Loopback3
C       10.1.100.0/24 is directly connected, FastEthernet0/0
O       10.1.200.0/24 [110/65] via 10.1.100.2, 02:37:09, FastEthernet0/0
                      [110/65] via 10.1.100.1, 02:37:09, FastEthernet0/0
R3#
```

Fuente: Software Packet Tracer 5.2.

En la salida se puede verificar que para cada router, sus respectivas redes aparecen con la máscara real (/24); sin embargo las direcciones loopback de los routers vecinos se muestran como (/32), ya que las identifica como direcciones de soporte. Para cambiar esto *en un entorno*

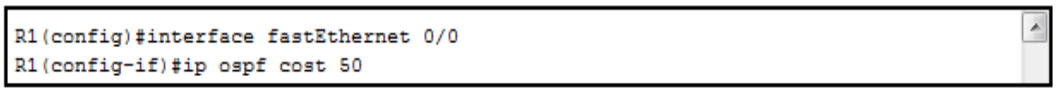
real, se usa el comando **ip ospf network point-to-point** (este comando no es aceptado por el simulador packet tracer) en modo de configuración de interfaz.

Modificación de costos de enlace en OSPF

Al usar el comando **show ip route** en R1, se puede apreciar que la ruta más directa a la loopback de R2 es a través de la conexión Ethernet. Al lado de esta se encuentra un par en la forma [Distancia administrativa / métrica]. La distancia administrativa es 110 que es la distancia por defecto de OSPF en los routers cisco. La métrica depende del tipo de enlace. OSPF selecciona la ruta con la métrica más baja, la cual es una suma de los costos de enlace. El costo de un enlace se puede modificar usando el comando **ip ospf cost** *cost* en los dos extremos del enlace.

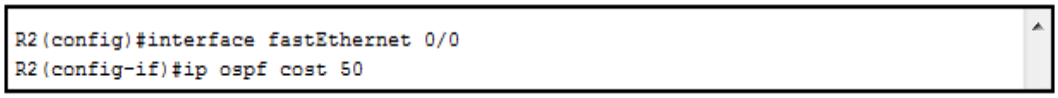
A continuación se cambian los costos de enlace en los tres routers a un costo de 50. Se puede apreciar el cambio en las métricas en la tabla de enrutamiento.

Figura 191. Cambio del costo del enlace en el router R1



Fuente: Software Packet Tracer 5.2.

Figura 192. Cambio del costo del enlace en el router R2



Fuente: Software Packet Tracer 5.2.

Figura 193. Cambio del costo del enlace en el router R3

```
R3(config)#interface fastethernet 0/0
R3(config-if)#ip ospf cost 50
```

Fuente: Software Packet Tracer 5.2.

Con el comando **show ip route**, se comprueba que al cambiar el costo se modifica la métrica (/51), ya que el costo de una ruta OSPF es el valor acumulado desde un router hasta la red de destino. En este caso, se definió que R1 tiene un costo de 50 para alcanzar la red

Figura 194. Información de la tabla de enrutamiento en R3

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
C       10.1.1.0/24 is directly connected, Loopback1
O       10.1.2.1/32 [110/51] via 10.1.100.2, 00:33:45, FastEthernet0/0
O       10.1.3.1/32 [110/51] via 10.1.100.3, 00:33:45, FastEthernet0/0
C       10.1.100.0/24 is directly connected, FastEthernet0/0
C       10.1.200.0/24 is directly connected, Serial0/3/0
R1#
```

Fuente: Software Packet Tracer 5.2.

La tabla de enrutamiento en R1 muestra un costo de 51 para alcanzar la red 10.1.2.1/24 en R2. Debido a que 10.1.2.1/24 está conectada a la interfaz FastEthernet, R2 asigna el valor de 1 como costo para 10.1.2.1/24. R1 luego agrega el valor del costo adicional de 50 para enviar datos a través del enlace predeterminado entre R1 y R2.

Cambio de prioridades de interfaz

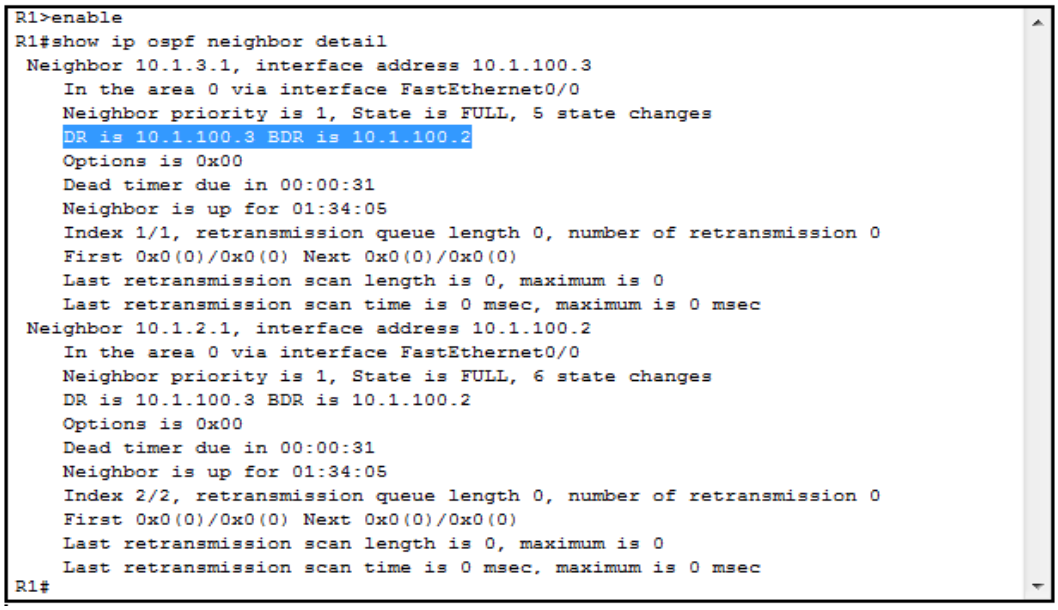
Con el comando **show ip ospf neighbor detail** se puede ver en cualquiera de los routers, que para la red Ethernet, R3 es el router designado (DR) y R2 es el router designado de respaldo (BDR). Estos roles son determinados por la prioridad de la interfaz para todos los routers en esa red.

La prioridad por defecto es 1. Si todas las prioridades son iguales (por defecto), la elección del DR se basa en el ID del router, de esta forma el router con mayor ID se convierte en el DR y el segundo más alto en el BDR.

Cuando el DR falla, el BDR se convierte en el nuevo DR y se selecciona un nuevo BDR entre los DROthers.

Si se agrega un router con una prioridad de interfaz OSPF alta y el DR y BDR funcionan correctamente, estas asignaciones no se modifican ya que el DR y el BDR solo pierden sus funciones si falla el router o la interfaz de acceso múltiple.

Figura 195. Información del DR y BDR en el router R1



Fuente: Software Packet Tracer 5.2.

A continuación se cambiarán las prioridades OSPF en R1 y R2 para convertir a R1 en DR y R2 en BDR. Para realizar estos cambios se usa el comando **ip ospf priority** *number.*

Figura 196. Cambio de prioridad OSPF en el router R1

```
R1>enable
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface fastethernet 0/0
R1(config-if)#ip ospf priority 10
R1(config-if)#
```

Fuente: Software Packet Tracer 5.2.

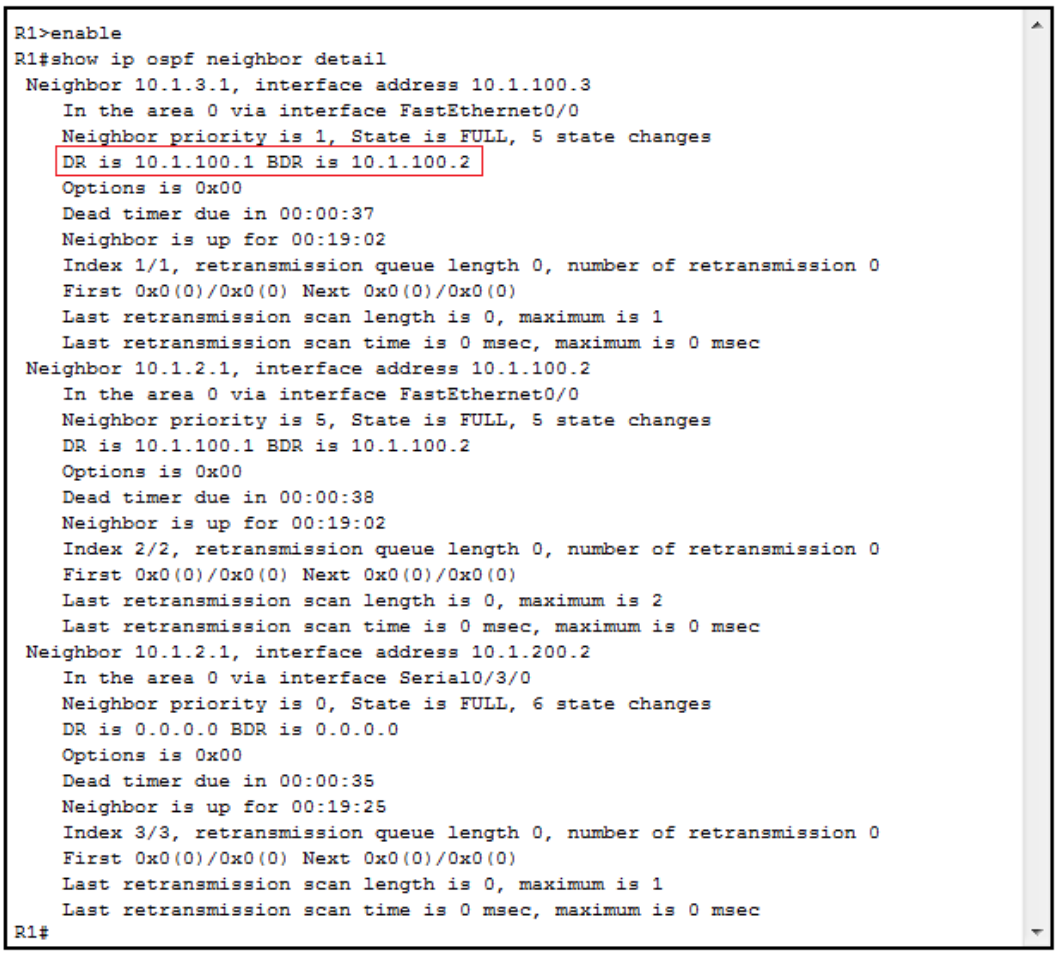
Figura 197. Cambio de prioridad OSPF en el router R2

```
R2>enable
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface fastethernet 0/0
R2(config-if)#ip ospf priority 5
```

Fuente: Software Packet Tracer 5.2.

Después de cambiar las prioridades en las interfaces se analiza la información con el comando **show ip ospf neighbor detail.**

Figura 198. Información del DR y BDR en el router R1



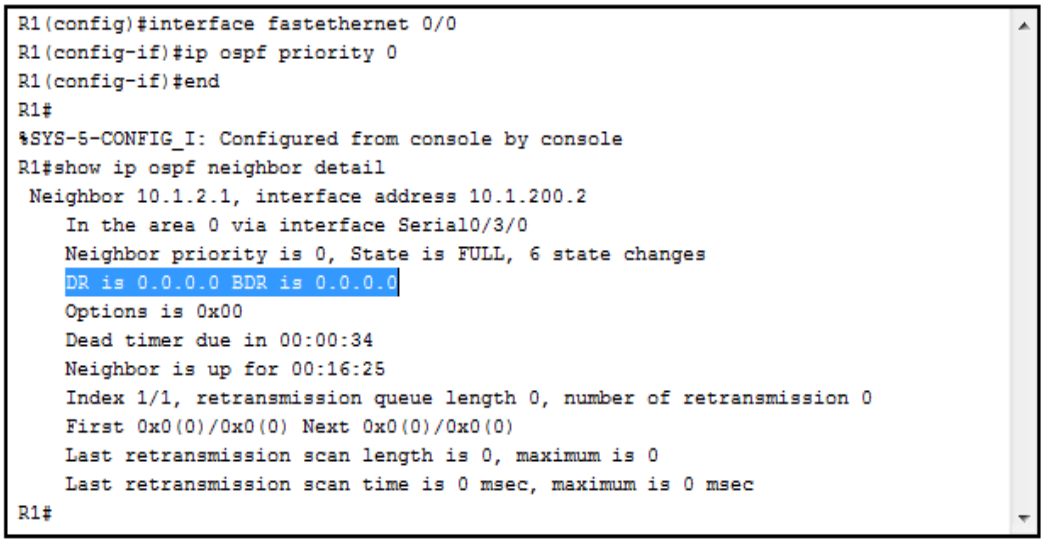
```
R1>enable
R1#show ip ospf neighbor detail
 Neighbor 10.1.3.1, interface address 10.1.100.3
    In the area 0 via interface FastEthernet0/0
    Neighbor priority is 1, State is FULL, 5 state changes
    DR is 10.1.100.1 BDR is 10.1.100.2
    Options is 0x00
    Dead timer due in 00:00:37
    Neighbor is up for 00:19:02
    Index 1/1, retransmission queue length 0, number of retransmission 0
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 0, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
 Neighbor 10.1.2.1, interface address 10.1.100.2
    In the area 0 via interface FastEthernet0/0
    Neighbor priority is 5, State is FULL, 5 state changes
    DR is 10.1.100.1 BDR is 10.1.100.2
    Options is 0x00
    Dead timer due in 00:00:38
    Neighbor is up for 00:19:02
    Index 2/2, retransmission queue length 0, number of retransmission 0
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 0, maximum is 2
    Last retransmission scan time is 0 msec, maximum is 0 msec
 Neighbor 10.1.2.1, interface address 10.1.200.2
    In the area 0 via interface Serial0/3/0
    Neighbor priority is 0, State is FULL, 6 state changes
    DR is 0.0.0.0 BDR is 0.0.0.0
    Options is 0x00
    Dead timer due in 00:00:35
    Neighbor is up for 00:19:25
    Index 3/3, retransmission queue length 0, number of retransmission 0
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 0, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
R1#
```

Fuente: Software Packet Tracer 5.2.

Si se asigna una prioridad de interfaz OSPF igual a 0, esta interfaz de router está descalificada para convertirse en DR o BDR.

A continuación se asigna prioridad 0 a las fastethernet de R1, R2 y R3, y se verifica que todas las interfaces quedan descalificadas y no asigna DR ni BDR.

Figura 199. Cambio de prioridad OSPF y chequeo de DR y BDR en R1



Fuente: Software Packet Tracer 5.2.

El DR en OSPF es el router responsable de establecer las adyacencias entre todos los vecinos de una red de multiacceso. Un DR lleva a cabo tareas de envío y sincronización y se asegura que todos los routers tengan una base de datos topológica idéntica. El BDR en OSPF tiene la tarea de asumir las funciones del DR en caso de que este falle.

Cambio de topología

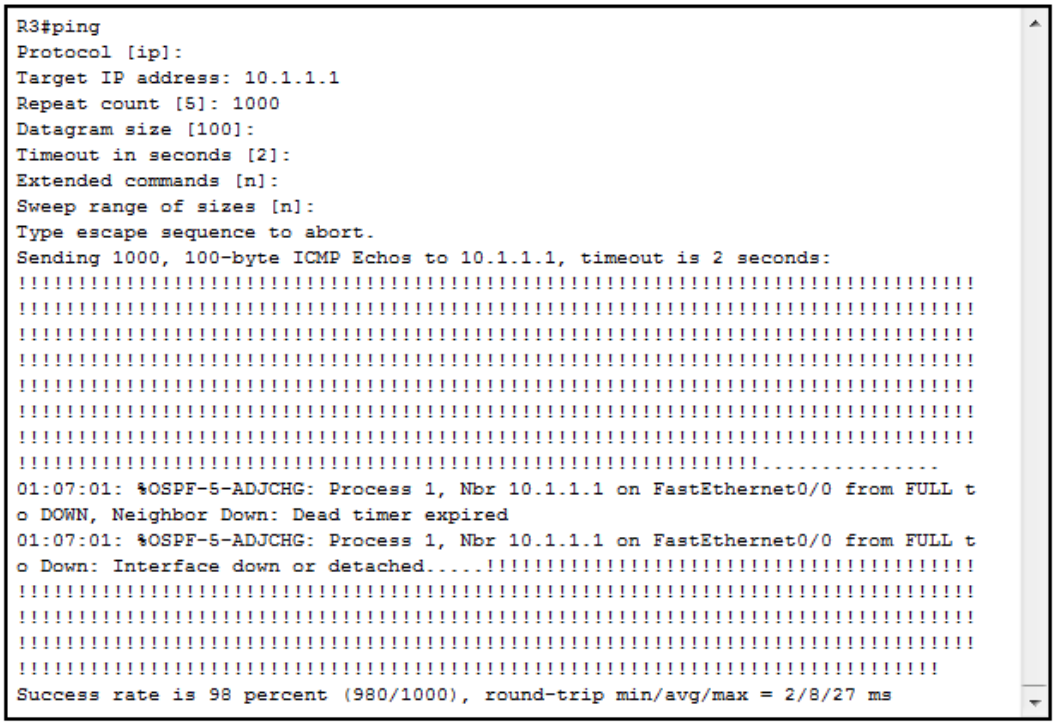
OSPF, como muchos protocolos de estado de enlace, es rápido cuando converge. Para probar esto se realiza un ping desde R3 a la loopback de R1 con un gran número de repeticiones. Por defecto, los pings toman el camino de R3 a R1 sobre Ethernet, porque tiene el costo total más bajo. Esto se puede confirmar ejecutando un **traceroute** en R3 a la loopback de R1.

Figura 200. Seguimiento de la ruta para alcanzar el destino en el router R3

Fuente: Software Packet Tracer 5.2.

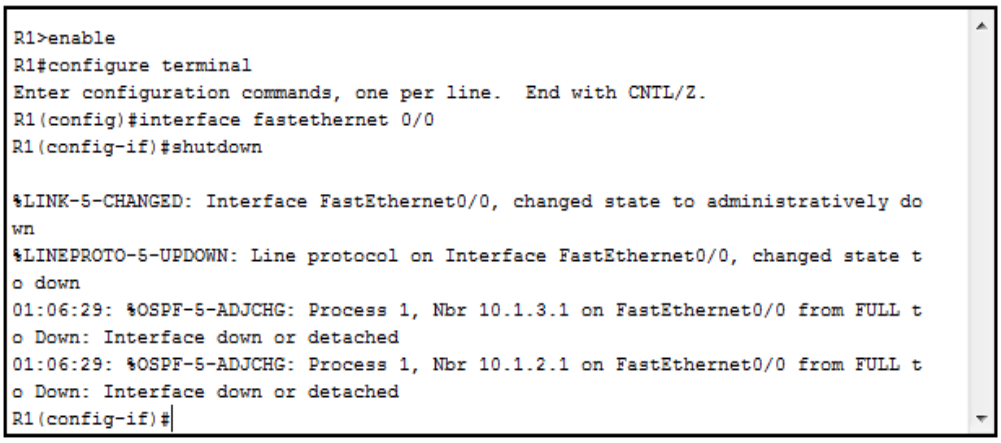
A continuación se realizará un cambio en la topología bajando la interfaz FastEthernet de R1 mientras se está ejecutando un ping en R3 a la interfaz loopback de R1 con un alto número de repeticiones (1000).

Figura 201. Ping en el router R3 a la interfaz loopback del router R1



Fuente: Software Packet Tracer 5.2.

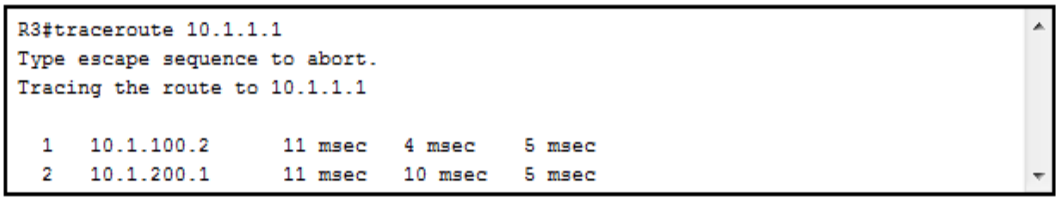
Figura 202. Cambio del estado de la interfaz fastethernet0/0 en el router R1



Fuente: Software Packet Tracer 5.2.

El resultado del ping realizado a la interfaz loopback de R1 muestra que se pierden algunos paquetes cuando se baja la intefaz fastethernet de R1; sin embargo luego de unos segundos se retoma el envío de paquetes ya que encuentra una ruta alternativa. Esto se puede comprobar ejecutando el comando traceroute en R3 a la loopback de R1 como se muestra a continuación:

Figura 203. Seguimiento de la ruta para alcanzar el destino en el router R3



Fuente: Software Packet Tracer 5.2.

Después de estudiar los protocolos de enrutamiento EIGRP y OSPF y realizar laboratorios prácticos, se presenta un comparativo de las principales características entre los protocolos de enrutamiento EIGRP y OSPF (con el fin de complementar estos protocolos, se incluye el protocolo RIP).

Tabla 65. Comparativo OSPF vs. Otros protocolos de enrutamiento.

CARACTERISTICAS	**RIP (Routing Internet Protocol)**	**OSPF (Open Short Path First)**	**EIGRP (Enhanced Interior Gateway Routing Protocol)**
Clase	Vector distancia	Estado de enlace	Hibrido
Tipo	IGP	IGP	IGP
Tiempo de convergencia	Lento	Rápido	Rápido
Modo	Clasfull(RipV1), Clasless(RipV2)	Clasless	Clasless
Algoritmo	Bellman-Ford	Dijkstra(SPF)	DUAL(cisco)
Soporta VLSM y CIDR	No(RipV1),Si(RipV2)	Si	Si
Consumo de ancho de banda	Alto	Bajo	Bajo
Consumo de recursos	Bajo	Alto	Bajo
Mejor escalabilidad	No	Si	Si
Métrica	Conteo de saltos	Costo	Compuesta(Ancho de banda+Retraso)
Distancia	120	110	5(Rutas

administrativa			sumarizadas), 90(Rutas internas), 170(Rutas externas)
Fórmula de Cálculo de costo	Sólo cuenta saltos	100.000.000/Ancho de banda en bps	Ancho de banda en bps+retraso del enlace(Delay)
Tipos de paquetes	1.Query 2.Reply	1.Hello 2.DBD(Database Description) 3. LSR (Link State Request) 4. LSU (Link State Update) 5. LSAck (Link State Ack)	1.Hello 2.Update 3.Query 4.Replay 5.Ack
De uso libre o propietario	Libre uso	Libre uso	Propietario

Fuente: http://www.slideshare.net/Ingcarlosadarragamejia/act-3-protocolos-de-enrutamiento

5.3. PIM-DM

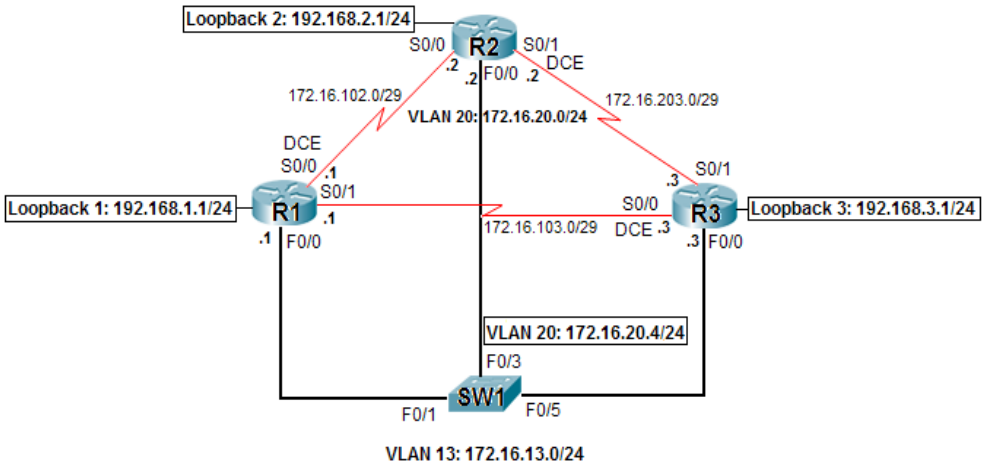
Planteamiento

La empresa “X” requiere implementar IP Multicast en su red, el departamento de relaciones públicas desea difundir videos en vivo para impactar a sus clientes, sin embargo es importante el uso adecuado de los recursos de red.

La empresa cuenta con 3 sitios remotos conectados por una malla de líneas seriales. Los sitios 1 y 3 (R1 y R3) también están conectados vía Fast Ethernet. La fuente multicast es un host en VLAN20, el cual conecta en capa 3 a la interfaz fast-Ethernet del router R2. Una red remota en cada sitio se representa por una interface loopback que debería recibir el mensaje. Mientras se realiza la prueba sobre este escenario, se debe crear una interfaz de conmutación virtual (*SVI Switched Virtual Interface*) en SW1 par simular la fuente multicast. A la interfaz de cada miembro del grupo multicast se debería elegir el camino de menor costo a la fuente multicast de acuerdo con la tabla de enrutamiento multicast subyacente.

Diagrama:

Figura 204. Diagrama de la práctica de la simulación PIM-DM



Fuente: Autoras

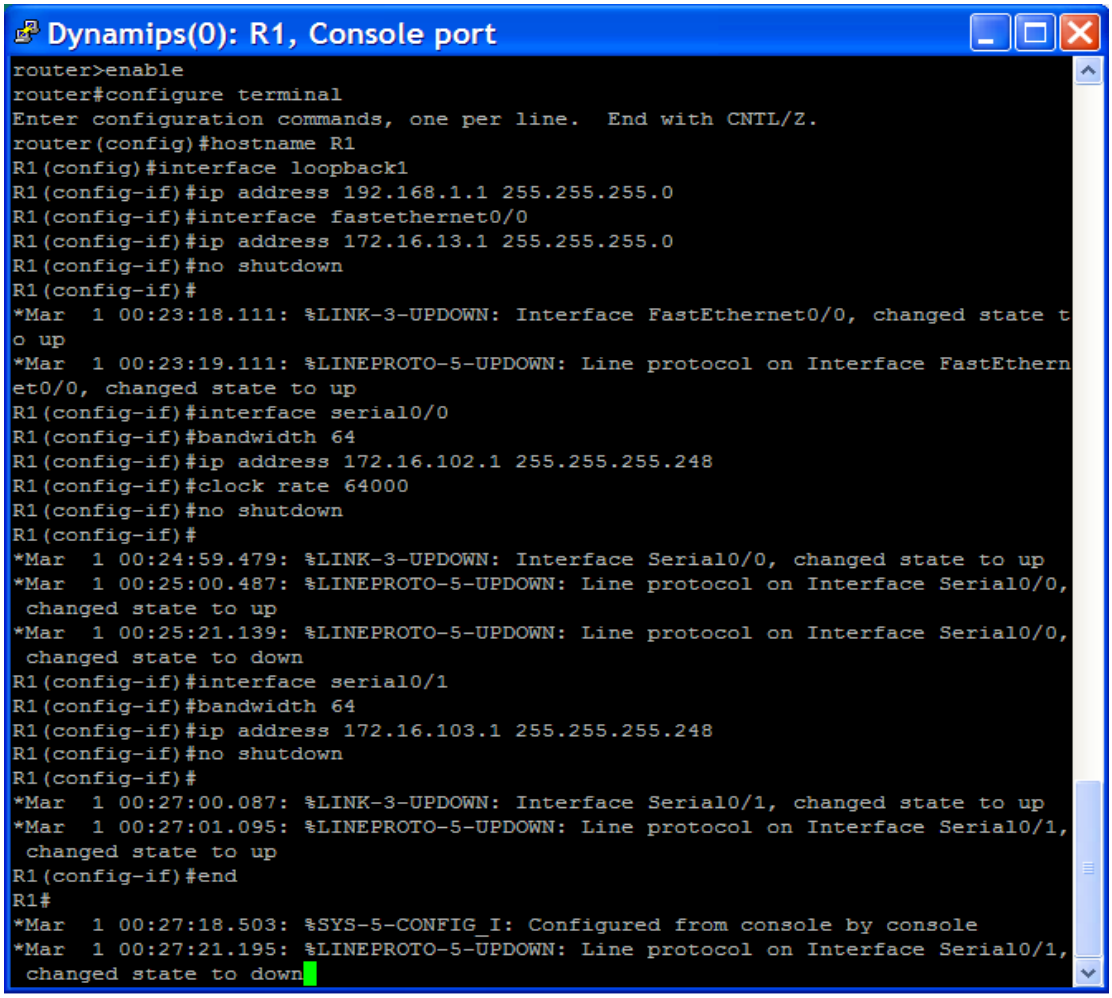
Solución:

A continuación se describen los pasos que se siguieron para realizar esta simulación. (El simulador utilizado para esta práctica fue GNS3).

Configuración de interfaces en los dispositivos y configuración IGMP

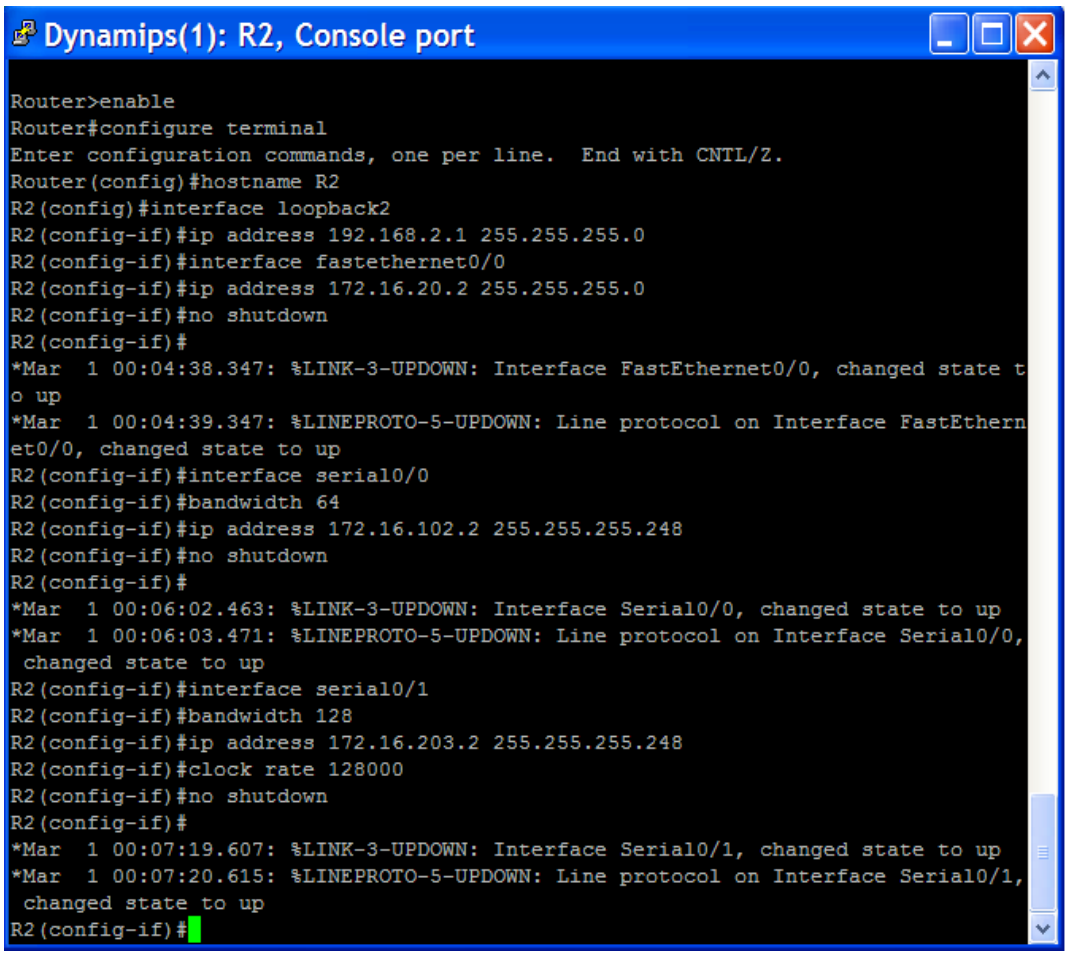
Inicialmente se configuran las interfaces de los dispositivos:

Figura 205. Configuración inicial del router R1



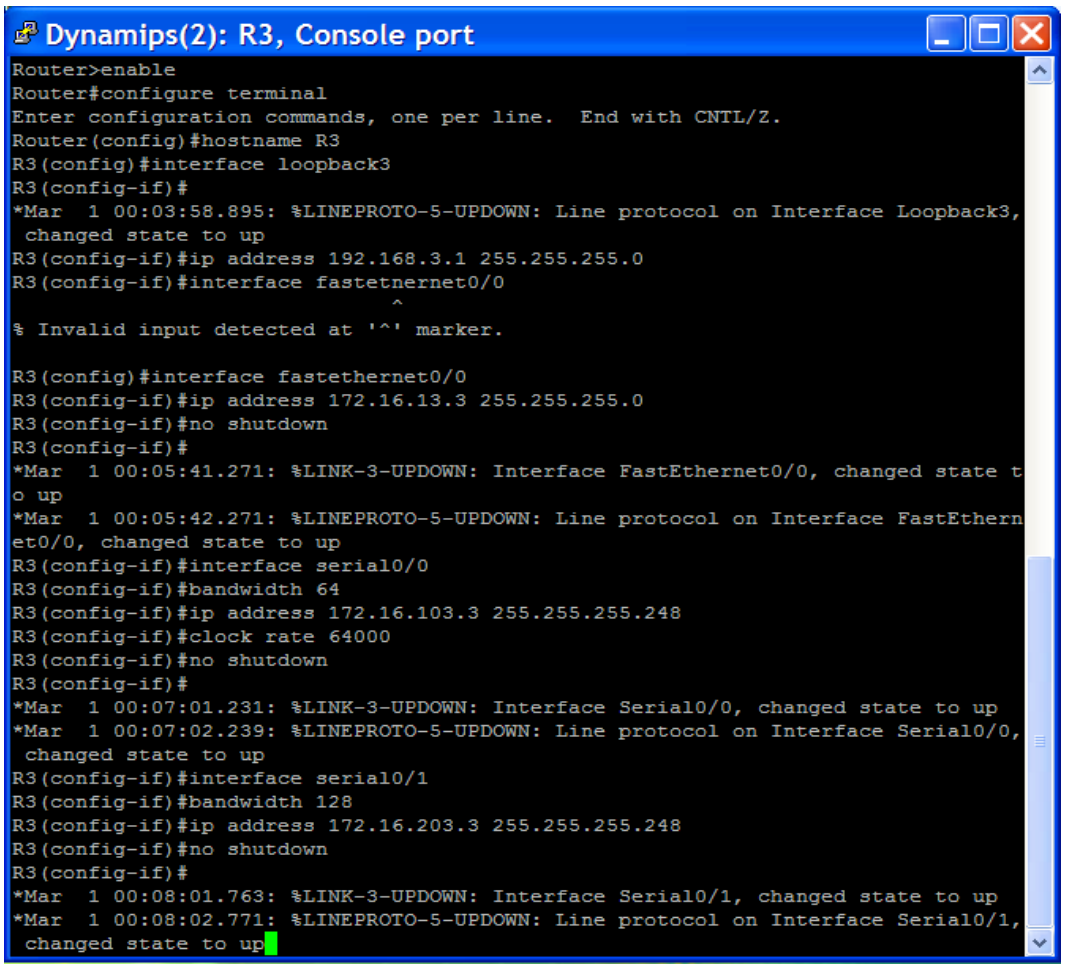
Fuente: Software GNS3.

Figura 206. Configuración inicial del router R2



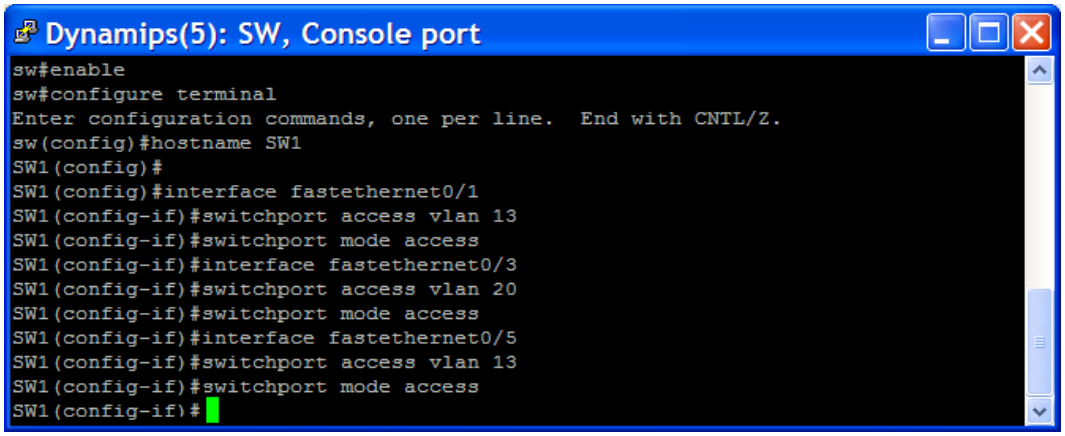
Fuente: Software GNS3.

Figura 207. Configuración inicial del router R3



Fuente: Software GNS3.

Figura 208. Configuración inicial del switchSW1 (Fuente multicast)

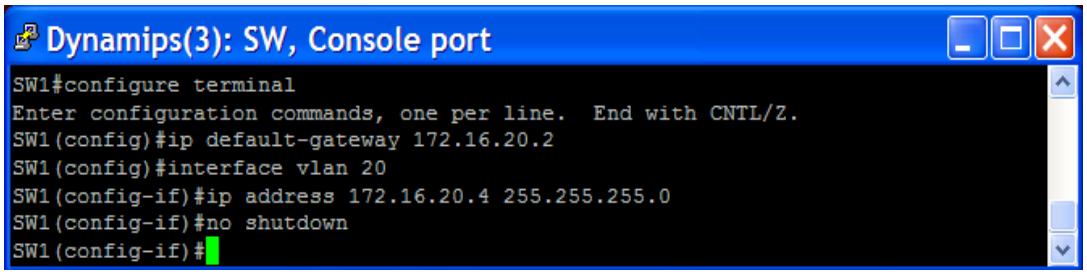


Fuente: Software GNS3.

Se utiliza una interfaz virtual conmutada (SVI) en el Switch 1 para simular una fuente multicast en la subred VLAN20. Esta será utilizada para generar pings multicast repetidos para simular el tráfico multicast mientras se instala la red.

Se asigna la la dirección ip 172.6.20.4/24 a SVI con una puerta de enlace de 172.16.20.2.

Figura 209. Asignación de dirección IP y puerta de enlace a SW1

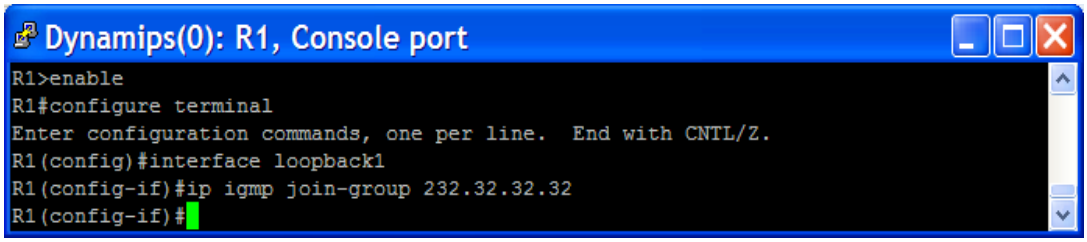


Fuente: Software GNS3.

A continuación se suscribe cada interfaz loopback en los 3 routers al grupo multicast 232.32.32.32 usando el protocolo IGMP.

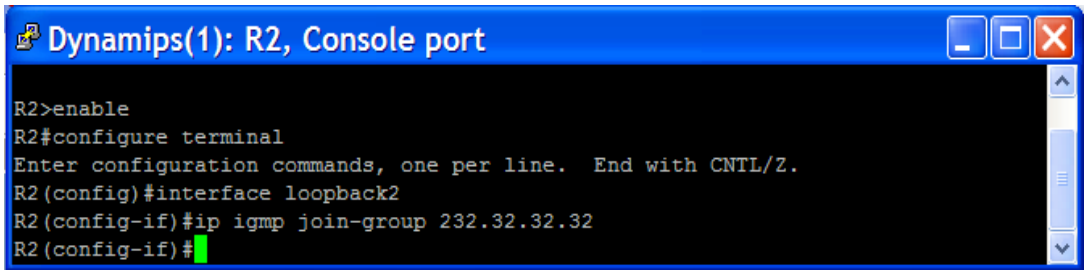
Las siguientes 3 figuras describen los comandos utilizados para la suscripción de las interfaces loopback en el grupo multicast.

Figura 210. Suscripción de la interface loopback 1 de R1 al grupo multicast



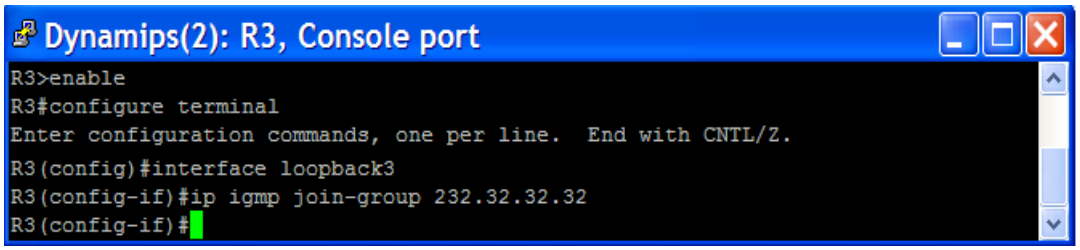
Fuente: Software GNS3.

Figura 211. Suscripción de la interface loopback 2 de R2 al grupo multicast



Fuente: Software GNS3.

Figura 212. Suscripción de la interface loopback 3 de R3 al grupo multicast



Fuente: Software GNS3.

Para verificar que todas las interfaces se han suscrito al grupo multicast se usa el comando **show ip igmp groups** en cada router.

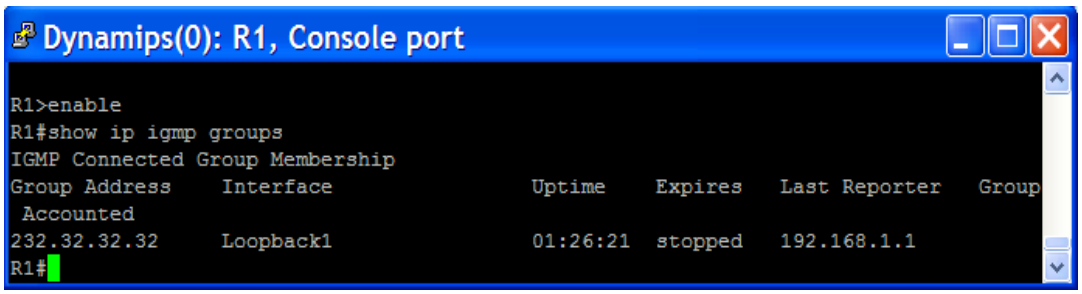
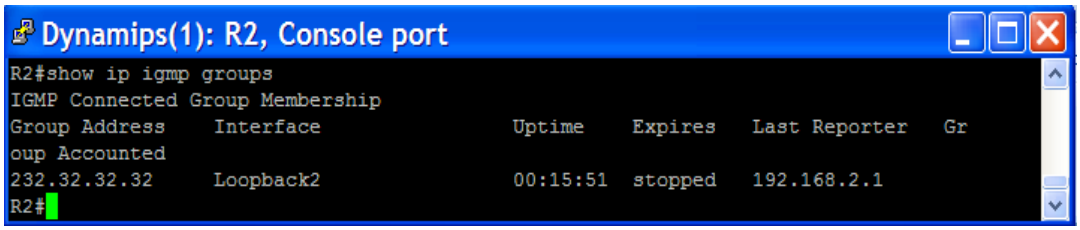


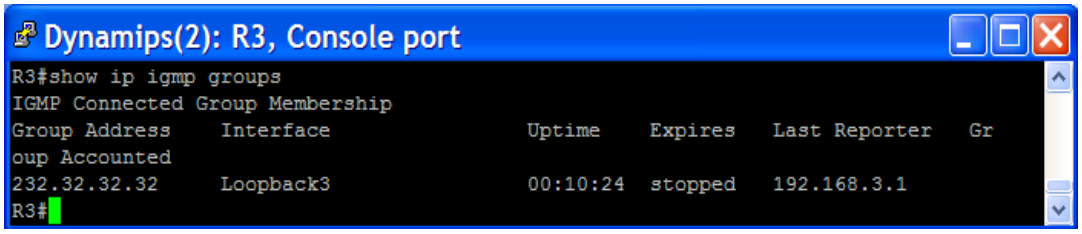
Figura 213. Comando show ip igmp groups en R1

Figura 214. Comando show ip igmp groups en R2



Fuente: Software GNS3.

Figura 215. Comando show ip igmp groups en R3

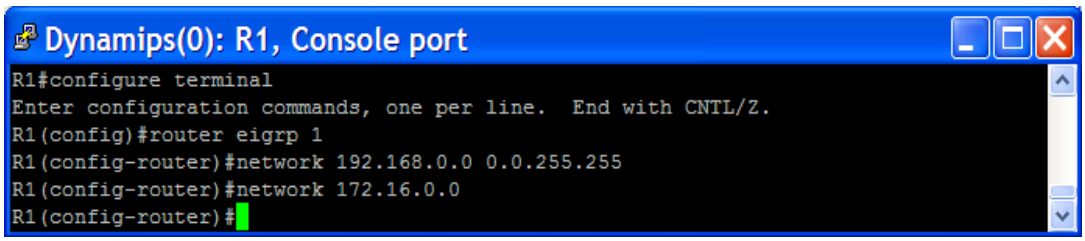


Fuente: Software GNS3.

Configuración de EIGRP

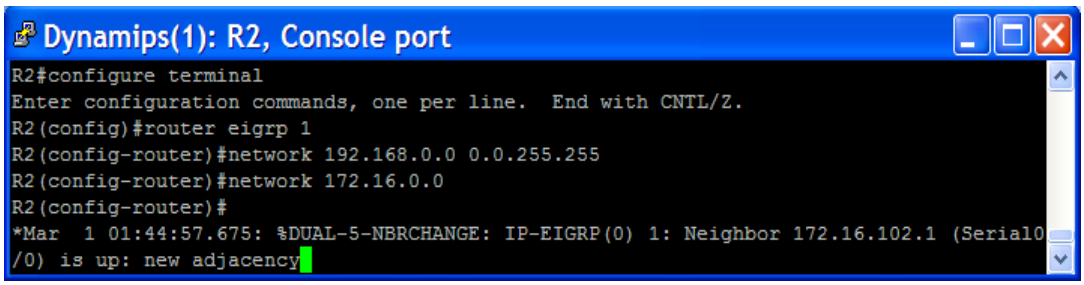
Se configura el protocolo EIGRP en cada router como se muestra a continuación.

Figura 216. Configuración de EIGRP en R1



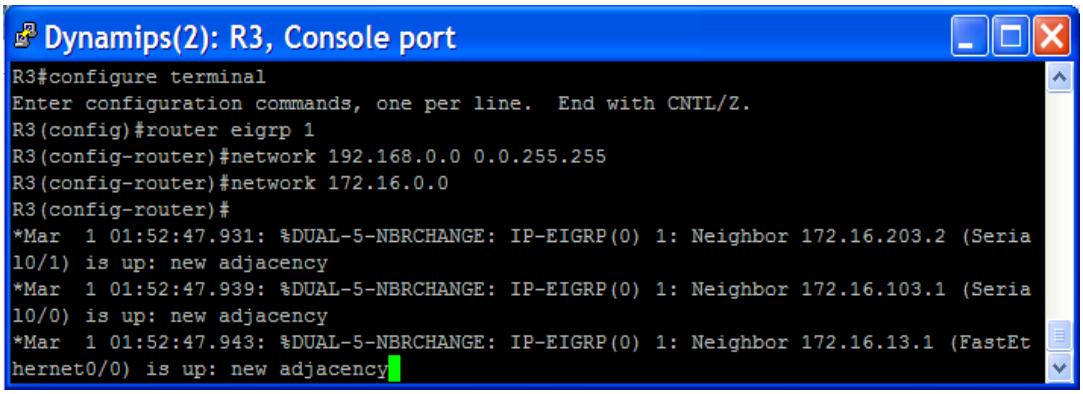
Fuente: Software GNS3.

Figura 217. Configuración de EIGRP en R2



Fuente: Software GNS3.

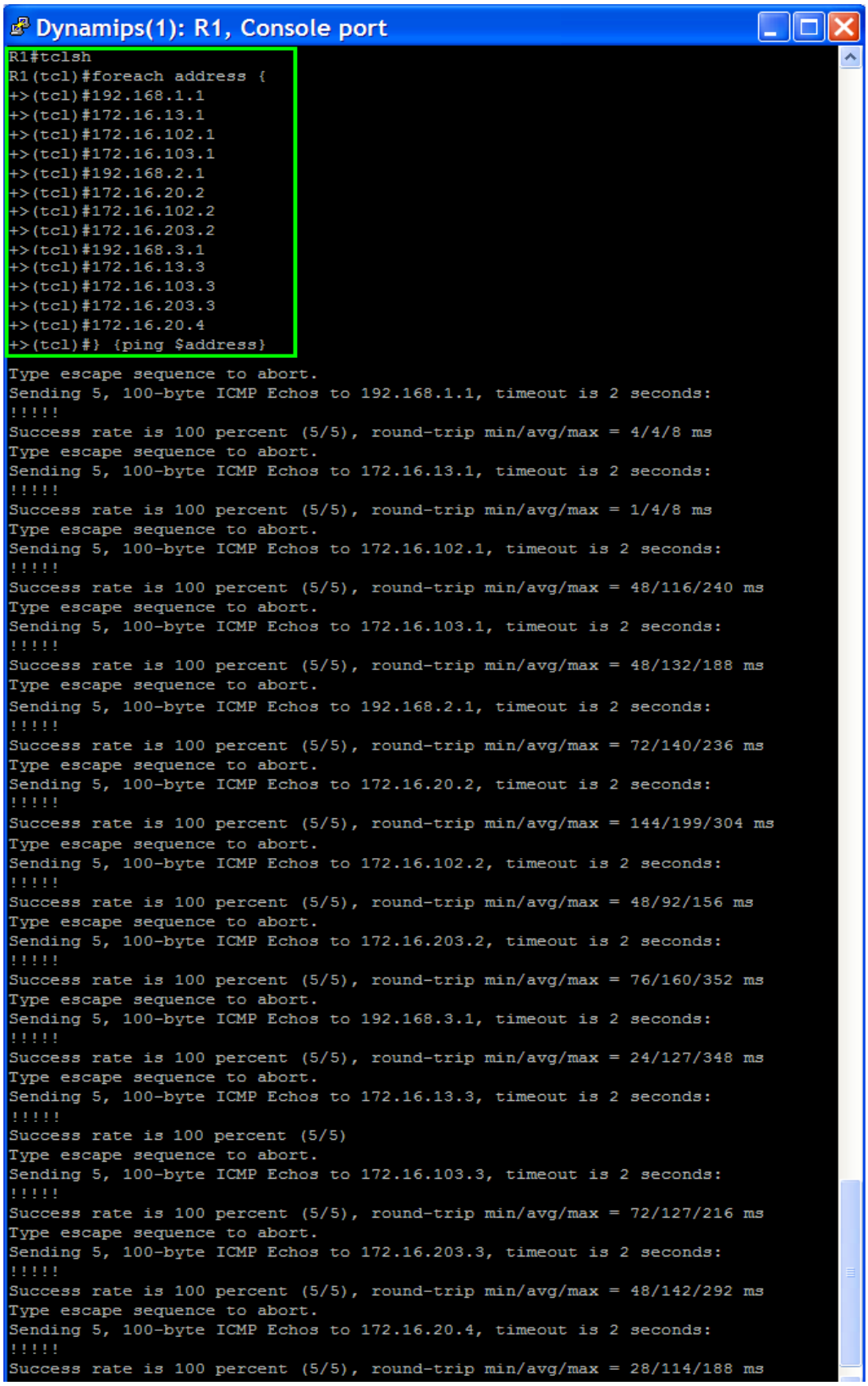
Figura 218. Configuración de EIGRP en R3



Fuente: Software GNS3.

Después de formar las adyacencias EIGRP, se ejecuta el siguiente script TCL en los routers para comprobar la completa conectividad unicast:

Figura 219. Script de comprobación de conectividad unicast en R1



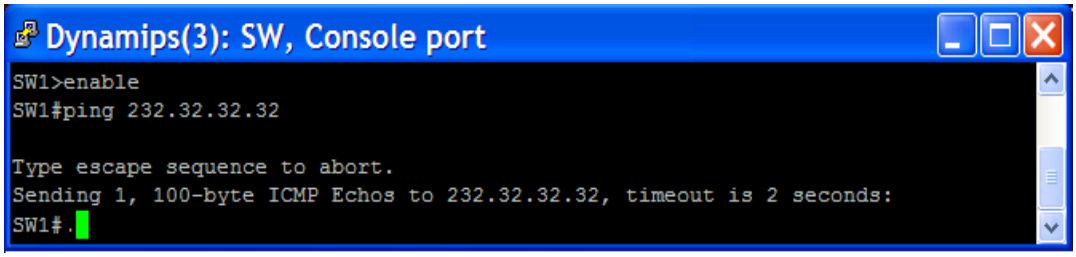
Fuente: Software GNS3.

Se observa que todos los pings son exitosos, Se debe asegurar que se tenga respuesta ICMP del host. Si el host tiene una puerta de enlace alcanzable de la interfaz FastEthernet0/0 de R2 y todos los routers tienen completa conectividad entre las subredes, se pueden realizar pings al host y recibir todas las respuestas.

Implementación de PIM-DM

Se realiza ping a la dirección multicast 232.32.32.32 multicast desde VLAN20 SVI del SW1 (discutida anteriormente).

Figura 220. Ping al grupo multicast 232.32.32.32



Fuente: Software GNS3.

Como se muestra en la salida anterior, no se recibieron *echo replies* desde las interfaces loopback, ya que los paquetes multicast no serán enrutados desde una interfaz a otra hasta que se configure el enrutamiento multicast y el modo denso con los comandos **ip multicast-routing** e **ip pim dense-mode.**

El host no recibe respuestas ICMP porque los paquetes no se enrutan desde una interfaz a otra, por lo tanto los paquetes multicast no son transmitidos. Dado que ningún paquete llegará a los suscriptores del grupo multicast IGMP, los suscriptores no tienen la oportunidad de responder a los pings.

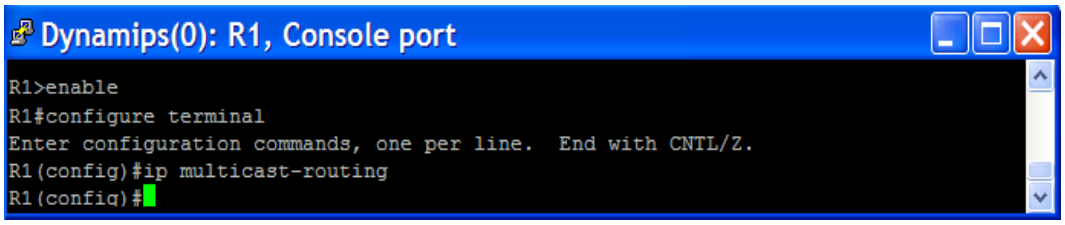
Los protocolos de enrutamiento son ante todo útiles para “introducir” fuentes multicast a sus receptores, un procedimiento conocido como descubrimiento de la fuente. En redes IP unicast, un dispositivo capa 3 debe conocer el siguiente salto *downstream* o interfaz para enrutar un paquete unicast a una red destino. De forma similar, un router ip multicast debe conocer el árbol a través del cual los datos multicast de una fuente deberían fluir a los receptores.

Como se mencionó en la sección de protocolos de enrutamientos de este documento, el protocolo independiente multicast (PIM) tiene dos modos: modo esparcido (SM) y modo denso (DM). El IOS de Cisco soporta ambos modos. PIM-DM está diseñado para redes en las cuales los dispositivos en la mayoría de las subredes se suscriben a los grupos disponibles. PIM-DM es útil en configuraciones de laboratorio y en situaciones en donde la mayoría de segmentos capa 2 involucrados tienen suscripciones a grupos multicast. PIM-SM está diseñado para redes multicast en las cuales los grupos multicast no tienen suscriptores o muchas subredes.

Cuando un router PIM recibe un paquete para un grupo multicast, éste debe determinar cuáles interfaces para ese grupo están en un estado de reenvío antes de envíar el paquete.

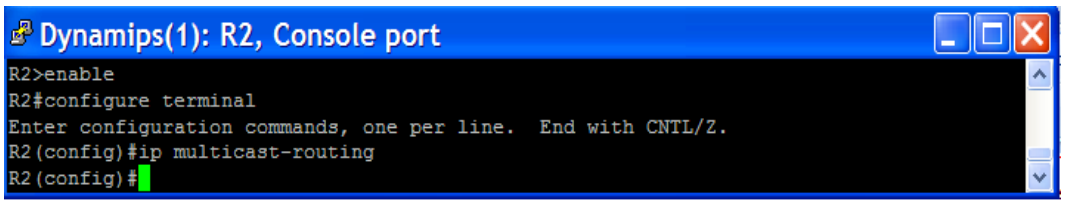
Para habilitar el enrutamiento multicast se utiliza el comando **ip multicast-routing** en modo global de configuración en cada uno de los routers:

Figura 221. Activación de enrutamiento multicast en R1



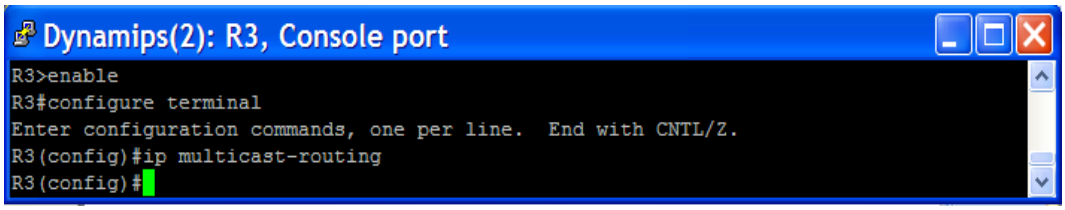
Fuente: Software GNS3.

Figura 222. Activación de enrutamiento multicast en R2



Fuente: Software GNS3.

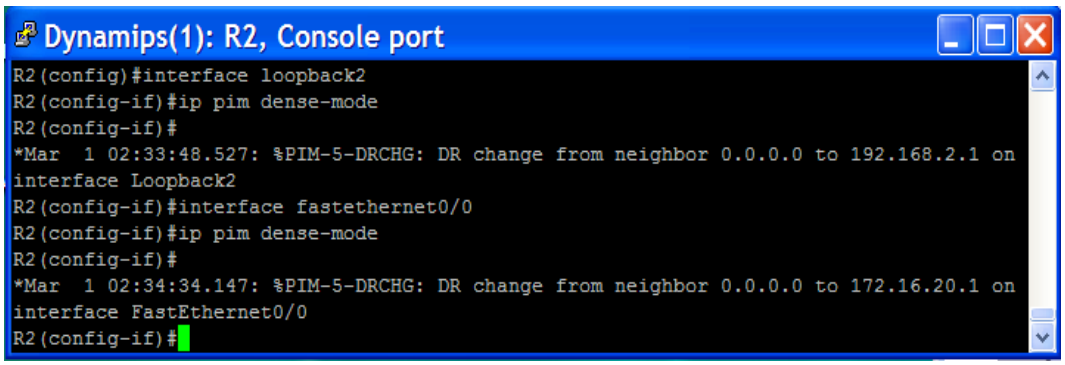
Figura 223. Activación de enrutamiento multicast en R3



Fuente: Software GNS3.

Para habilitar PIM-DM en las interfaces Loopback2 y FastEthernet0/0 en R2, se utiliza el comando ip pim dense-mode en modo de configuración.

Figura 224. Activación de PIM-DM en interfaces de R2

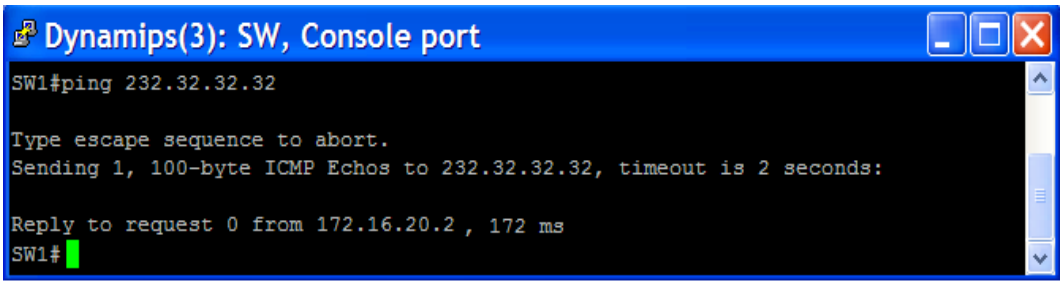


Fuente: Software GNS3.

Ahora que el enrutamiento multicast y PIM-DM están habilitados en R2, un ping desde SW1 al grupo 232.32.32.32 sí recibirá repuesta, ya que R2 definirá la interfaz FastEthernet 0/0 como la interfaz *upstream* y enviará

paquetes abajo del árbol fuente a cualquier interfaz *downstream*. La interfaz loopback de R2 es una interfaz *downstream*. La interfaz loopback recibe el paquete multicast y responde a SW1 originando la respuesta de su interfaz más cercana de acuerdo a la tabla de enrutamiento multicast.
Se verifica la conectividad haciendo ping al grupo multicast desde SW1 y se comprueba que se obtiene respuesta:

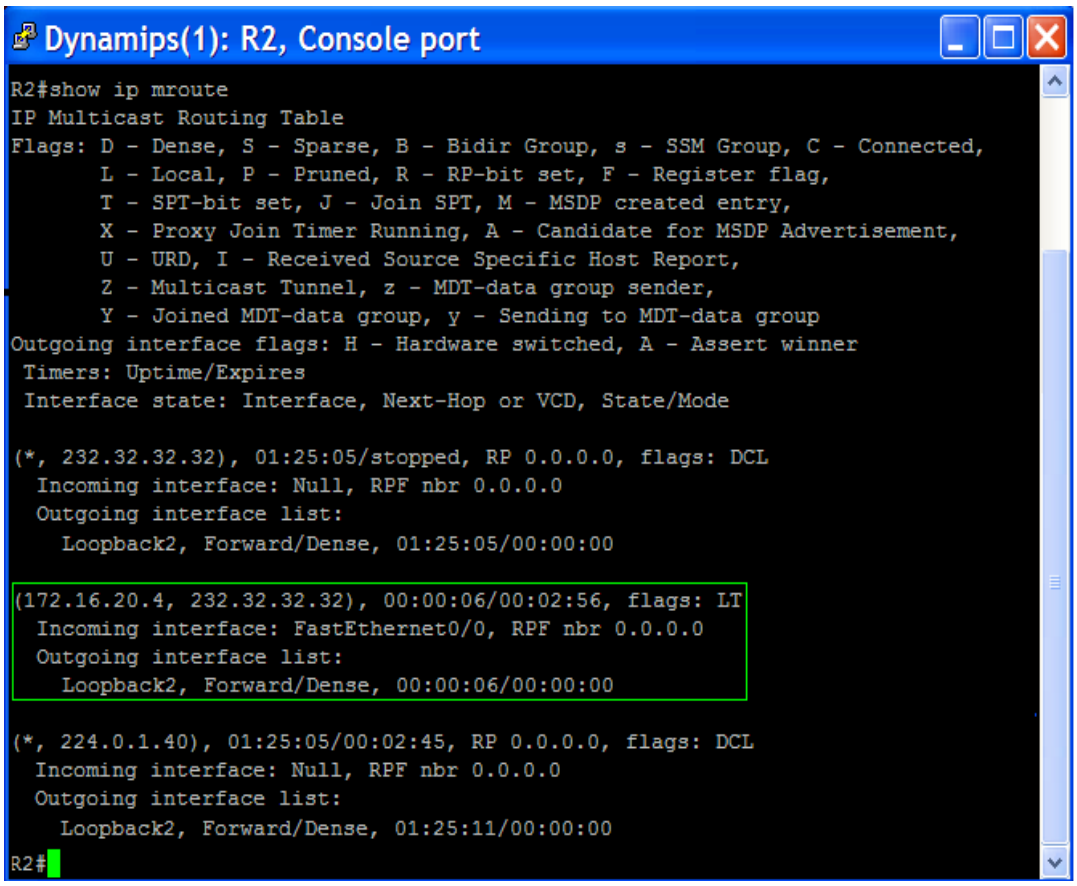
Figura 225. Ping desde SW1 al grupo multicast



Fuente: Software GNS3.

Como se mencionó anteriormente, sin IGMP snooping el tráfico multicast capa 2 que viaja a través de la Ethernet se maneja como tráfico broadcast. El switch entonces reenvía tráfico multicast a todos los puertos que normalmente deberían recibir un broadcast de la misma fuente. Sin embargo, en capa 3 el tráfico multicast es descartado, a menos que el router reciba directivas de IGMP para enviar tráfico por determinadas interfaces de salida. Si IGMP había registrado esos mensajes, el estado sería mostrado enla tabla de enrutamiento multicast. A continuación se muestra la tabla de enrutamiento multicast para chequear las interfaces de salida para envío de tráfico multicast al grupo 232.32.32.32.

Figura 226. Tabla de enrutammiento multicast para R2

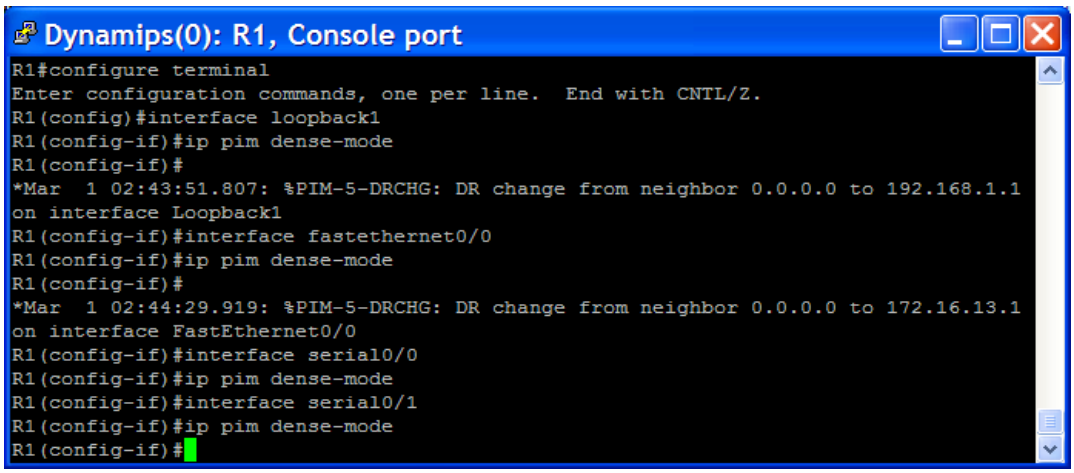


Fuente: Software GNS3.

Debido a que IGMP solo require interfaces que ejecuten PIM-DM, las suscripciones para las interfaces loopback remotas no han sido reportadas para R2 y por lo tanto están en un estado de no-reenvío. Sólo la interface Loopback2 de R2 recibirá paquetes multicast destinados a 232.32.32.32.

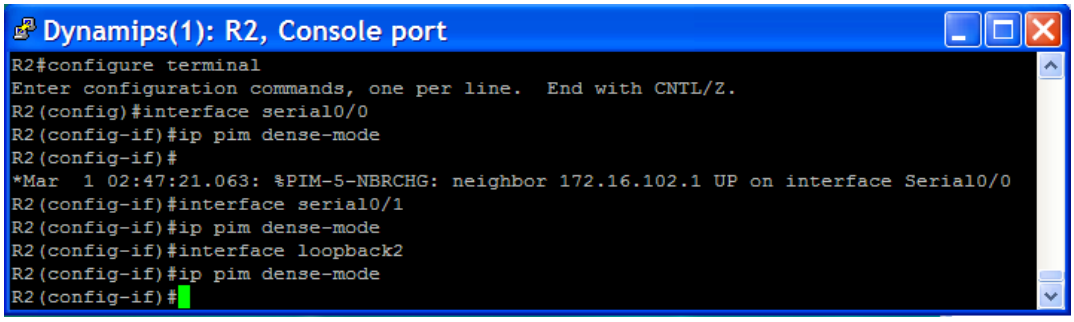
Para resolver esta situación se puede ejecutar el comando **ip pim dense-mode** para las interfaces restantes en la topología como se muestra a continuación.

Figura 227. Activación de PIM-DM en interfaces restantes de R1



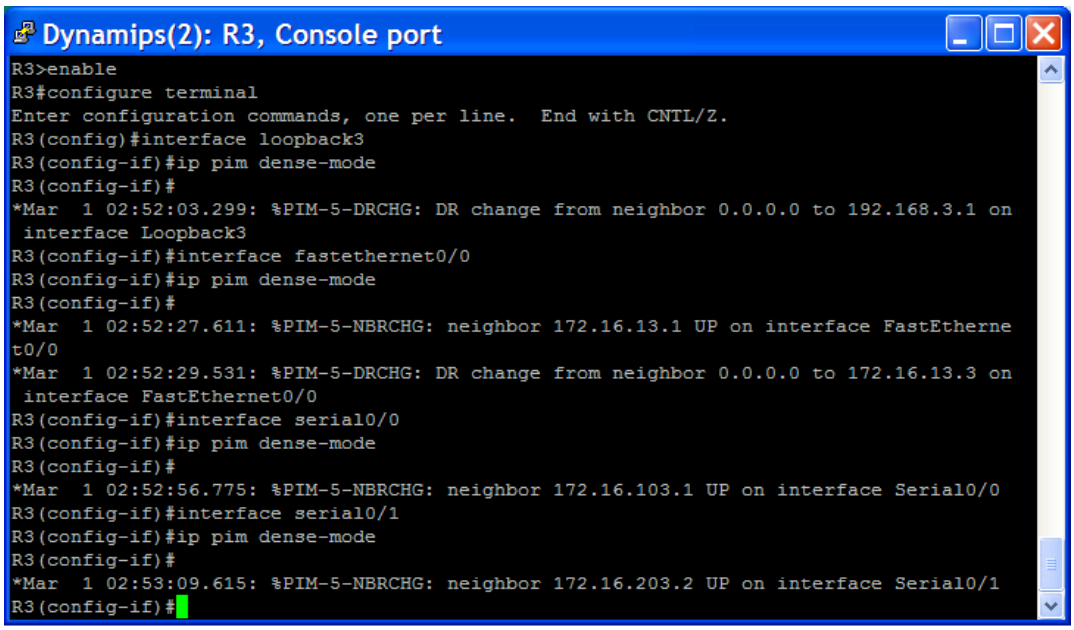
Fuente: Software GNS3.

Figura 228. Activación de PIM-DM en interfaces restantes de R2



Fuente: Software GNS3.

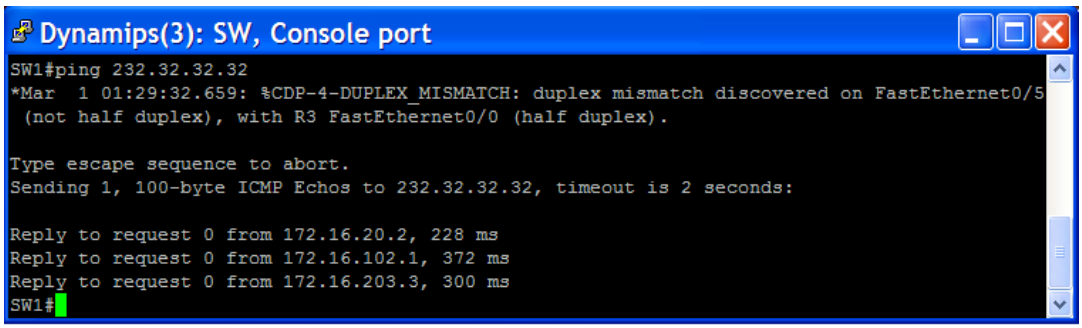
Figura 229. Activación de PIM-DM en interfaces restantes de R3



Fuente: Software GNS3.

Al realizar nuevamente ping al grupo multicast desde SW1, se reciben respuestas de cada router. Se observa que no se reciben respuestas de la dirección ip de la interfaz sobre la cual se recibió el paquete multicast sino de cualquier la interfaz en el router que responde el paquete de retorno encapsulado.

Figura 230. Ping al grupo multicast 232.32.32.32 desde SW1



Fuente: Software GNS3.

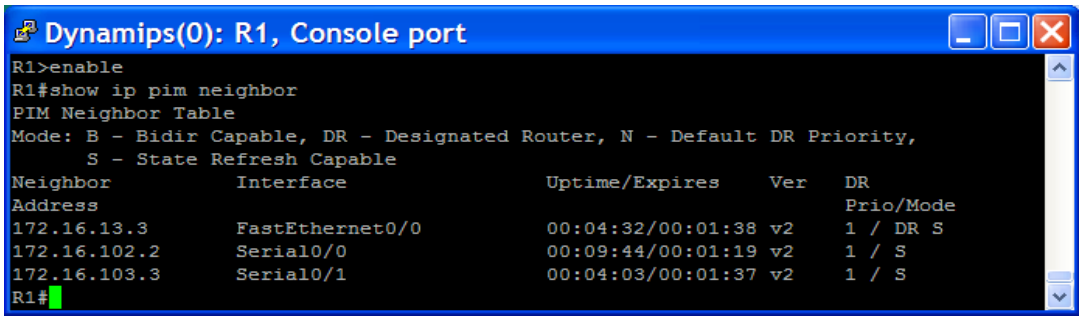
Los *echo replies* son enviadas desde las interfaces mostradas en la figura anterior debido a que cuando un router origina paquetes a un destino remoto, este usa como dirección fuente la dirección ip de la interfaz de la cual enviará esos paquetes, en este caso, los paquetes no serán enviados de la interfaz loopback (aunque ahí es donde fueron recibidos) sino de la interfaz serial más cercana 172.16.20.0/24.

Adyacencias PIM

A continuación se exploran las adyacencias PIM y como funciona PIM sobre diversos medios capa 2.

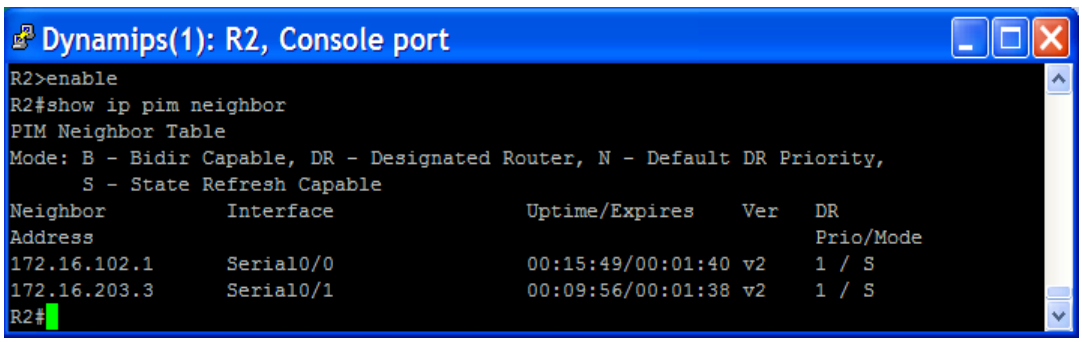
Con el comando **show ip pim neighbor** en cada uno de los routers se muestran las subredes conectadas (capa 3).

Figura 231. Comando show ip pim neighbor en R1



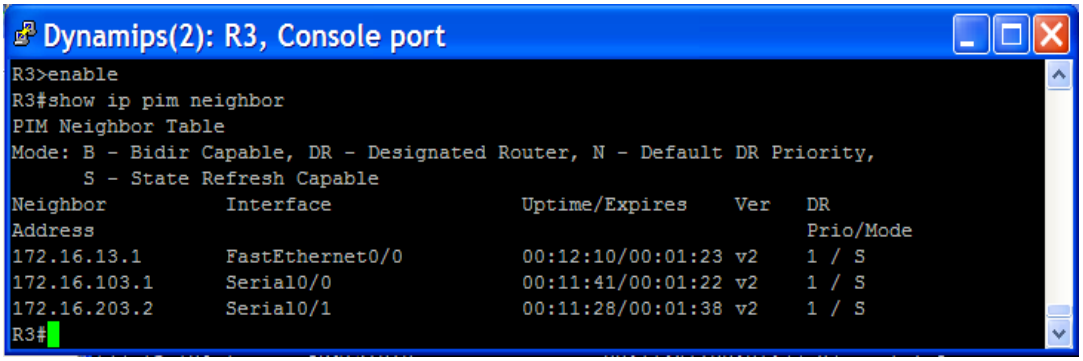
Fuente: Software GNS3.

Figura 232. Comando show ip pim neighbor en R2



Fuente: Software GNS3.

Figura 233. Comando show ip pim neighbor en R3

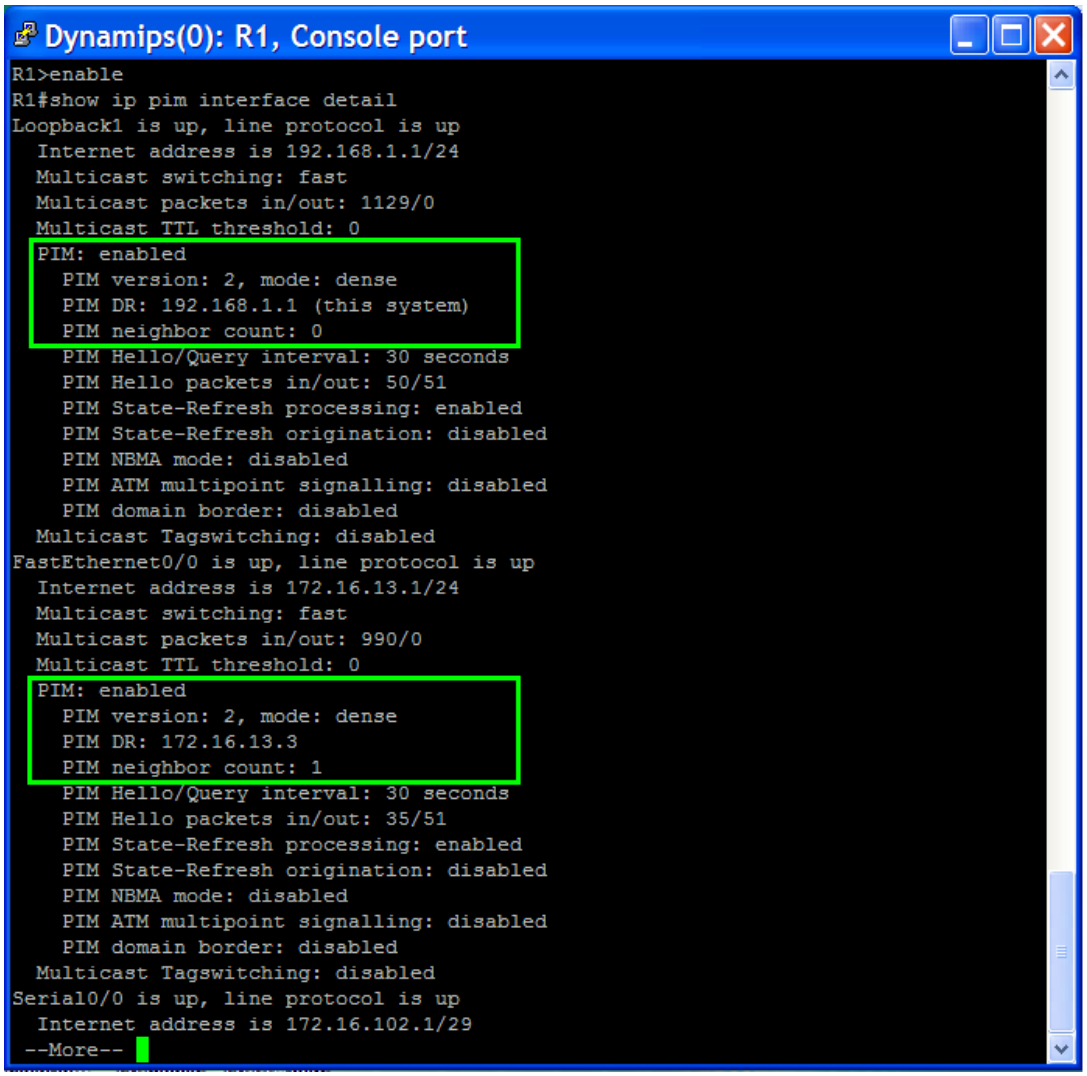


Fuente: Software GNS3.

Recordando el concepto de router designado (DR) en OSPF; este protocolo de estado de enlace permite que los dispositivos capa 3 ejecuten ese protocolo para llegar a ser adyacentes sólo con el dispositivo maestro para ese medio multiacceso capa 2. Este comportamiento disminuye el control de tráfico de la red y proporciona una fuente autorizada para información de enrutamiento en ese segmento de red. Existe una situación similar para el control de tráfico IGMP en medios multiacceso, así como Ethernet. En lugar de tener cada router multicast ejecutando sus propias consultas IGMP, PIM-DM elige un router para manejar las consultas IGMP para todo el segmento de red. PIM elige un DR para esa subred seleccionando el router con dirección IP más alta.

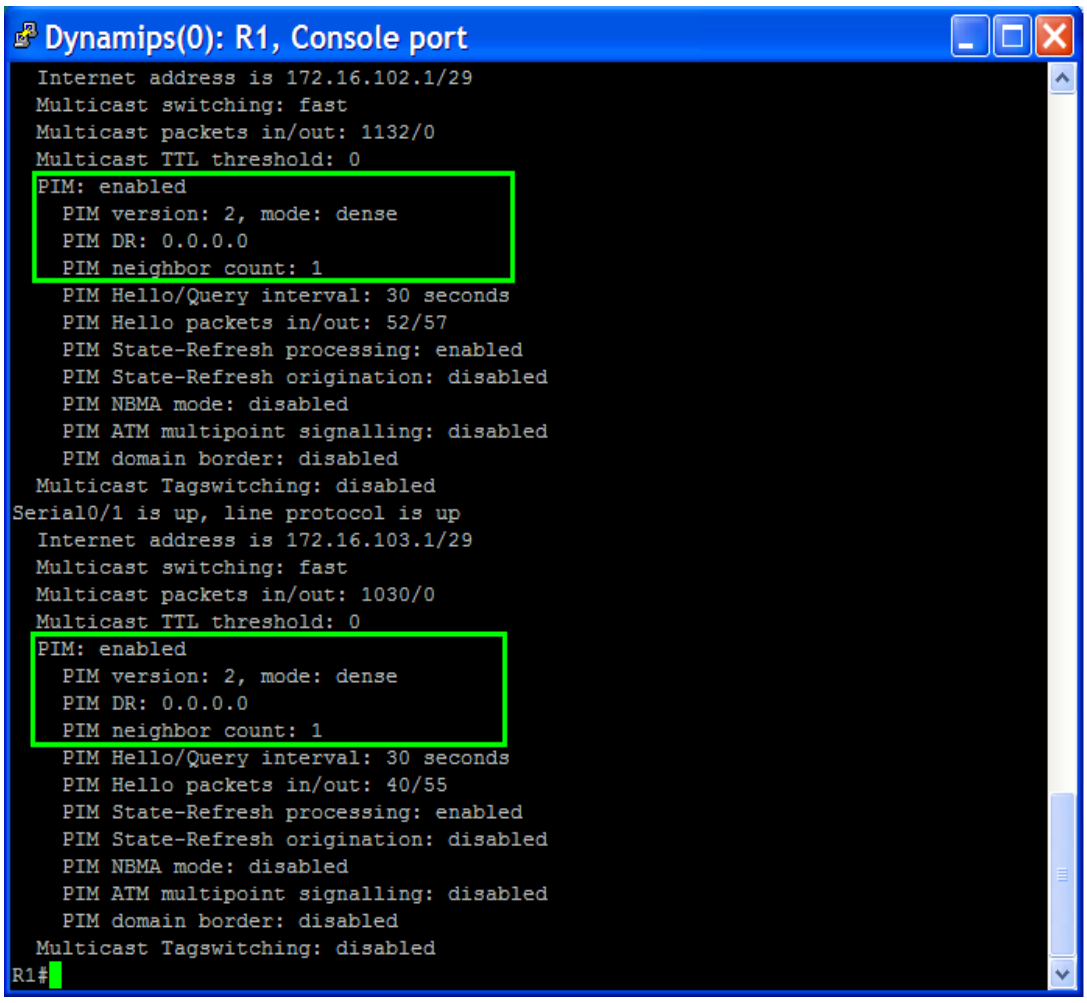
Para mostrar la información detallada sobre las interfaces PIM habilitadas se utiliza el comando **show ip pim interface detail**.

Figura 234. Comando show ip pim interface detail en R1 (Parte 1)



Fuente: Software GNS3.

Figura 235. Comando show ip pim interface detail en R1 (Parte 2)



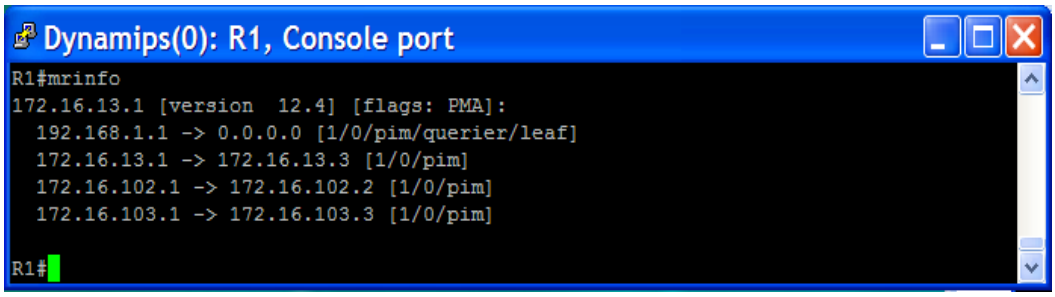
Fuente: Software GNS3.

En la figura anterior se puede apreciar que las dos interfaces seriales usan la dirección DR por defecto 0.0.0.0 como el DR para la interface. Debido a que el paquete multicast es recibido ya sea por 0 o 1 router remoto en un segmento serial, PIM no necesita establecer una relación compleja con el vecino.

Funcionamiento de enrutamiento multicast

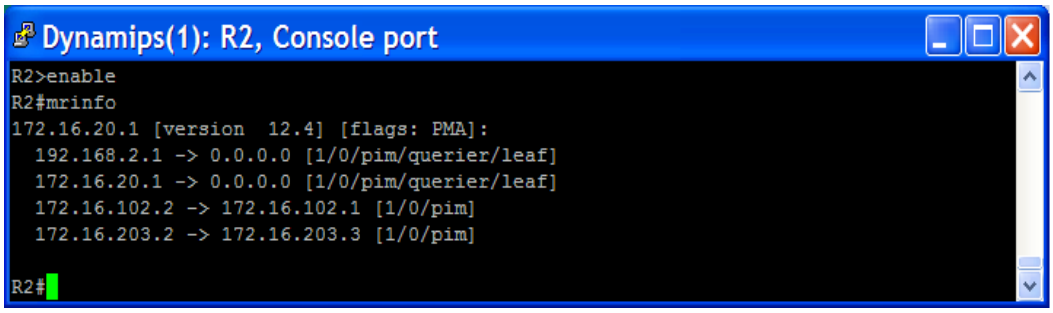
En cada router se usa el comando **mrinfo** para visualizar la información sobre los routers multicast conectados y habilitados.

Figura 236. Comando mrinfo en R1



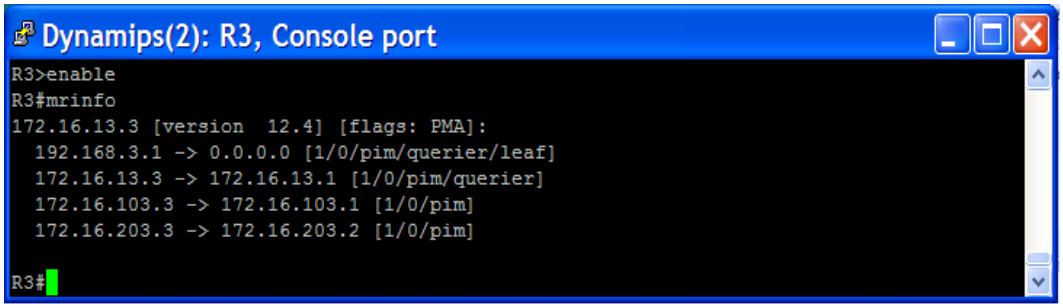
Fuente: Software GNS3.

Figura 237. Comando mrinfo en R2



Fuente: Software GNS3.

Figura 238. Comando mrinfo en R3



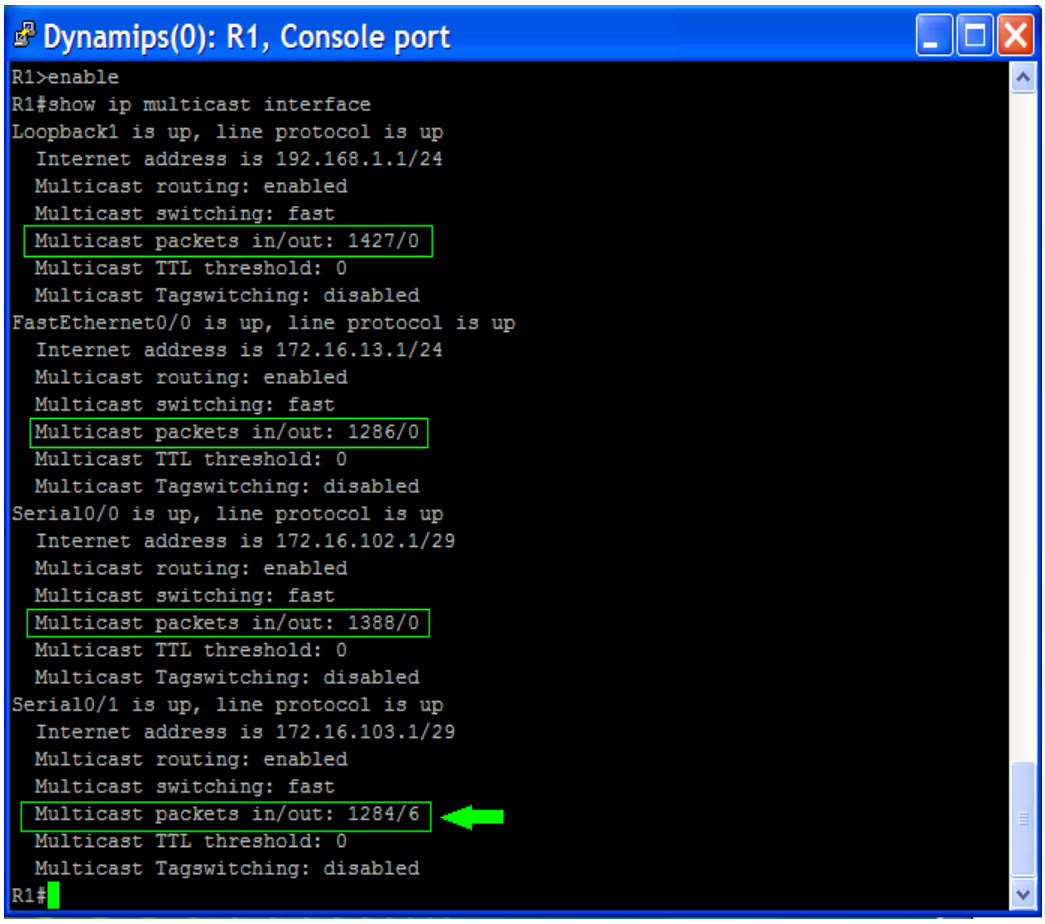
Fuente: Software GNS3.

Cada router identifica a las interfaces loopback como "*hojas topológicas*" en las cuales PIM nunca establecerá una adyacencia con ningún otro

router. Estos routers también registran las direcciones de enrutamiento multicast de los vecinos y los protocolos de enrutamiento que ellos usan.

El comando **show ip multicast interface** se utiliza para mostrar estadísticas acerca del tráfico multicast que pasa a través del router. Para cada router se obtiene una salida similar a la que se muestra a continuación:

Figura 239. Estadísticas de tráfico multicast en R1

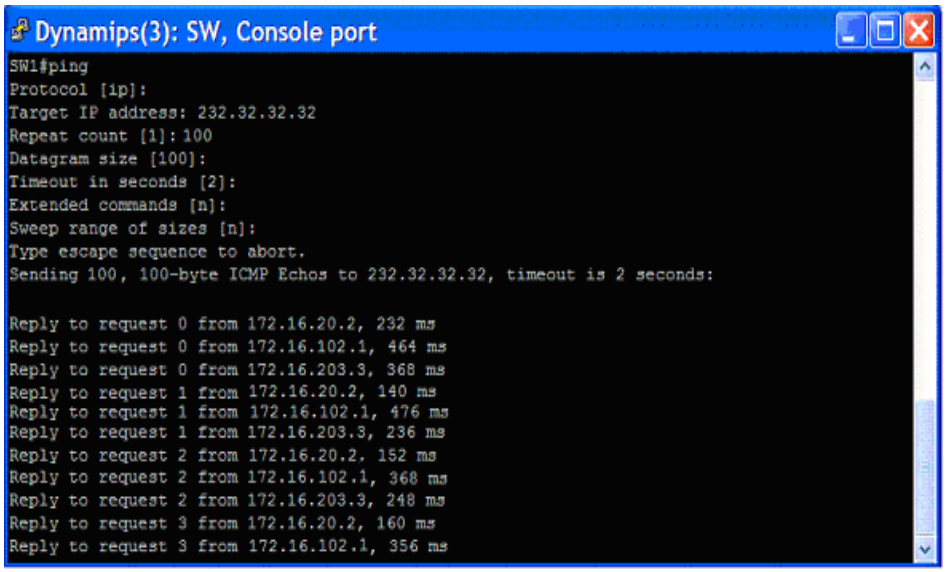


Fuente: Software GNS3.

De acuerdo a la salida mostrada anteriormente se puede determinar que la interfaz serial 0/1 está enviando tráfico multicast a 232.32.32.32 porque esta interfaz tiene un valor <>0 en el contador de paquetes de salida.

A continuación se genera un stream de datos multicast para el grupo multicast por medio de un ping extendido desde el switch SW1 con 100 repeticiones:

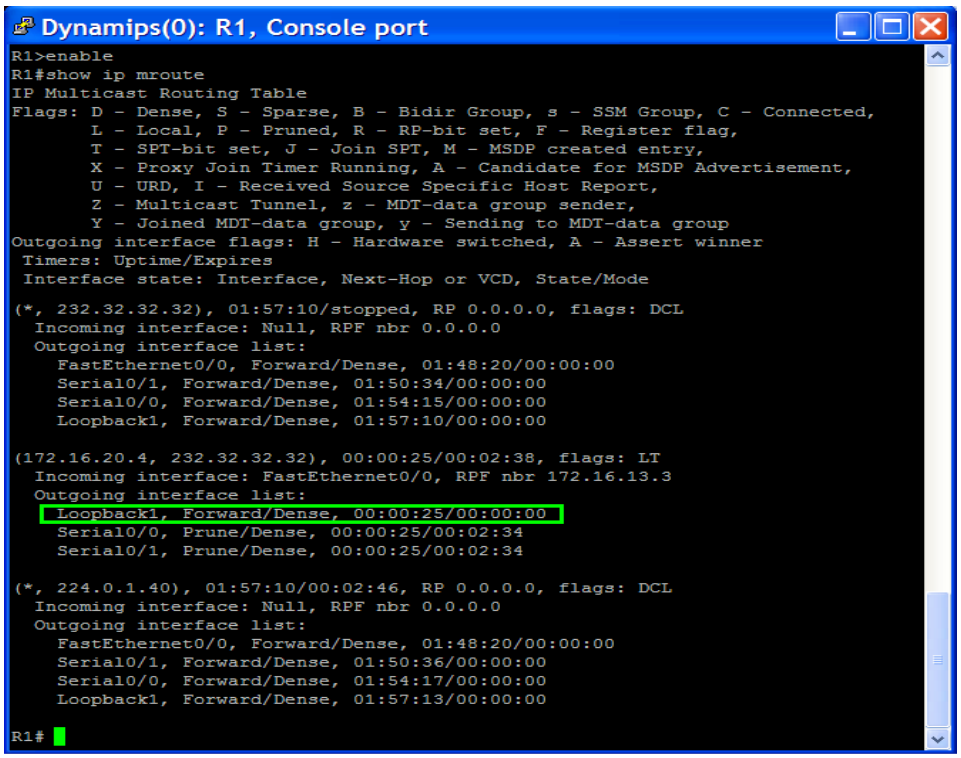
Figura 240. Ping desde SW1 al grupo multicast 232.32.32.32



Fuente: Software GNS3.

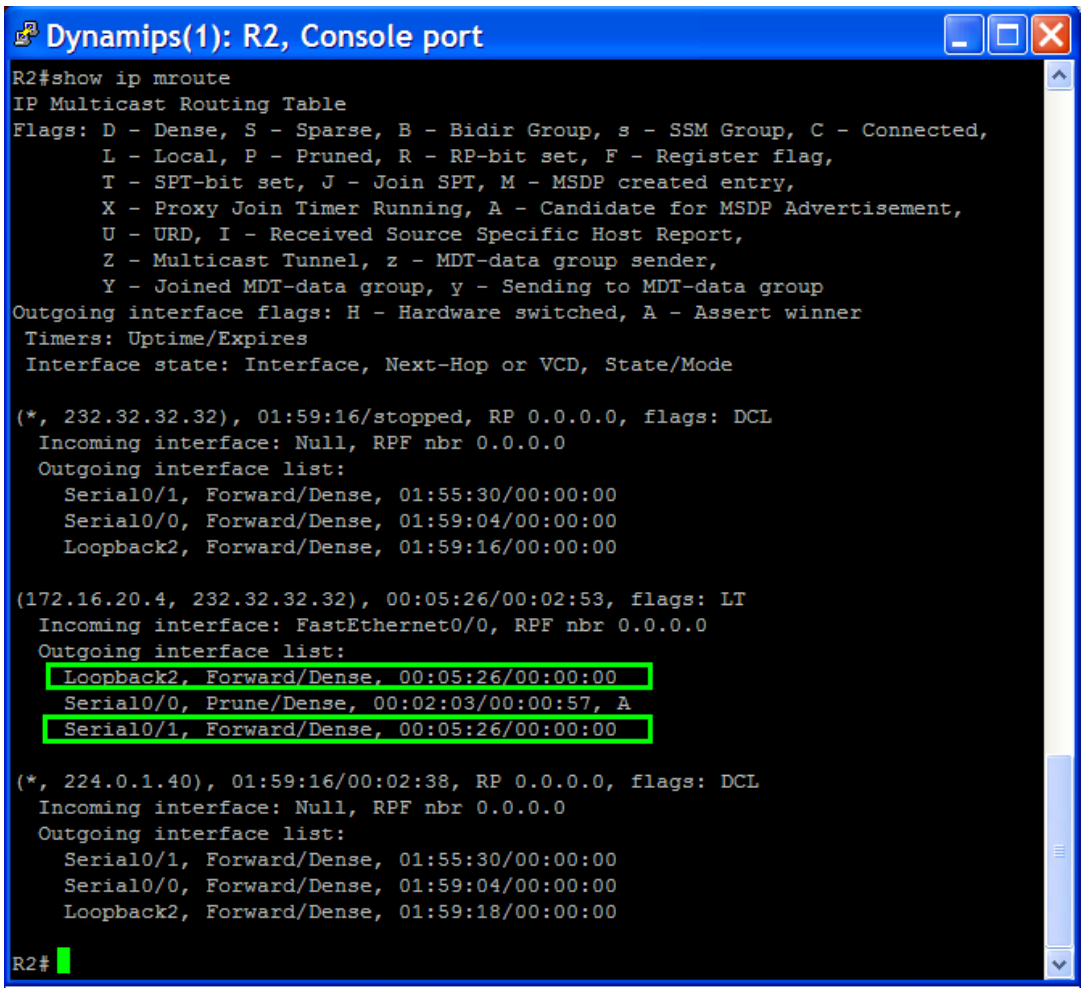
En cada uno de los routers se debe reflejar que PIM e IGMP se han comunicado para establecer el grupo multicast 232.32.32.32 en la tabla de enrutamiento multicast. Esta afirmación se verifica ejecutando el comando **show ip mroute** en cada uno de los routers.

Figura 241. Tabla de enrutamiento multicast de R1



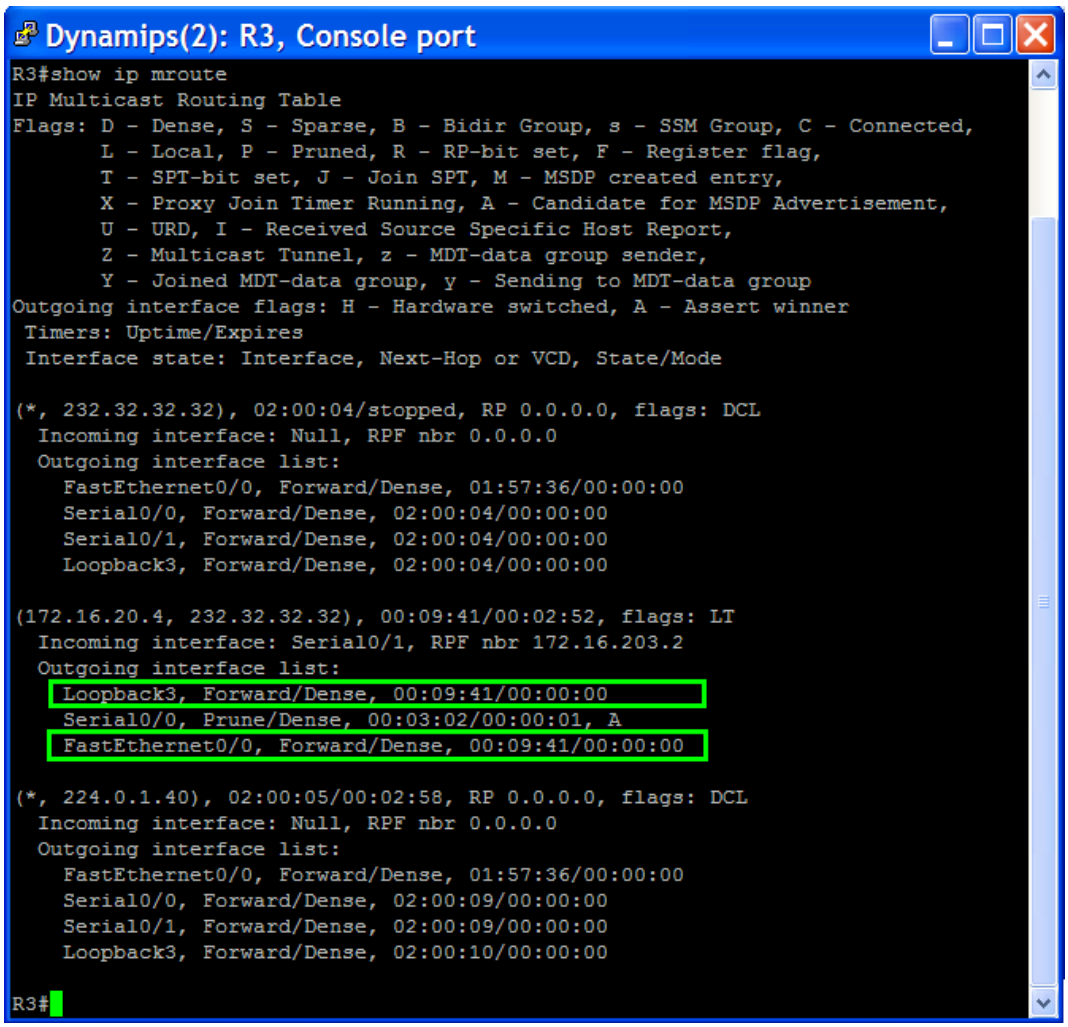
Fuente: Software GNS3.

Figura 242. Tabla de enrutamiento multicast de R2



Fuente: Software GNS3.

Figura 243. Tabla de enrutamiento multicast de R3



Fuente: Software GNS3.

Los dos temporizadores que aparecen en la primera línea de la entrada (S, G) en cada rotuer indican el tiempo desde el primer multicast para ese grupo y el momento en el que expira la entrada. De esta forma, el router recibe cada vez un paquete multicast emparejando la entrada (S, G) (172.16.20.4, 232.32.32.32), IGMP reajusta la caducidad del temporizador a 3 minutos.

Por defecto, IGMP envía una consulta general cada 60 segundos en cada interfaz PIM. Una consulta general realiza peticiones a los dispositivos

que corren IGMP en esa subred para reportar los grupos suscritos al router de consulta. Si no se escuchan reportes de afiliación para un grupo en esa interfaz en un tiempo de 3 veces el intervalo de consulta, el router multicast declara que no hay ningún miembro activo del grupo en la interfaz. Si un router no recibe multicasts desde un par (S, G) por tres minutos, la tabla de enrutamiento borra la entrada (S, G).

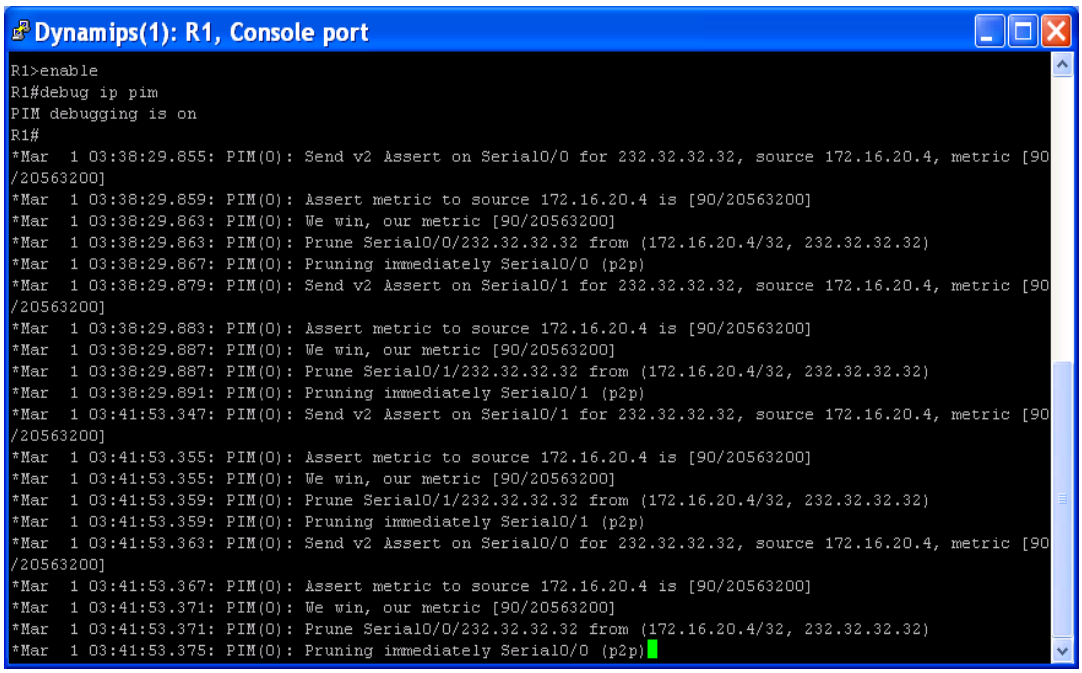
Basado en las tablas de enrutamiento multicast mostradas anteriormente se puede deducir que:

a. En R1, la interfaz loopback está enviando tráfico a 232.32.32.32.
b. En R2, la interfaces loopback2 y Serial 0/1 están enviando tráfico a 232.32.32.32
c. En R3, las interfaces loopback3 y fastEthernet0/0 están enviado tráfico a 232.32.32.32.

Comportamiento *Flood* y *Prune* en PIM-DM

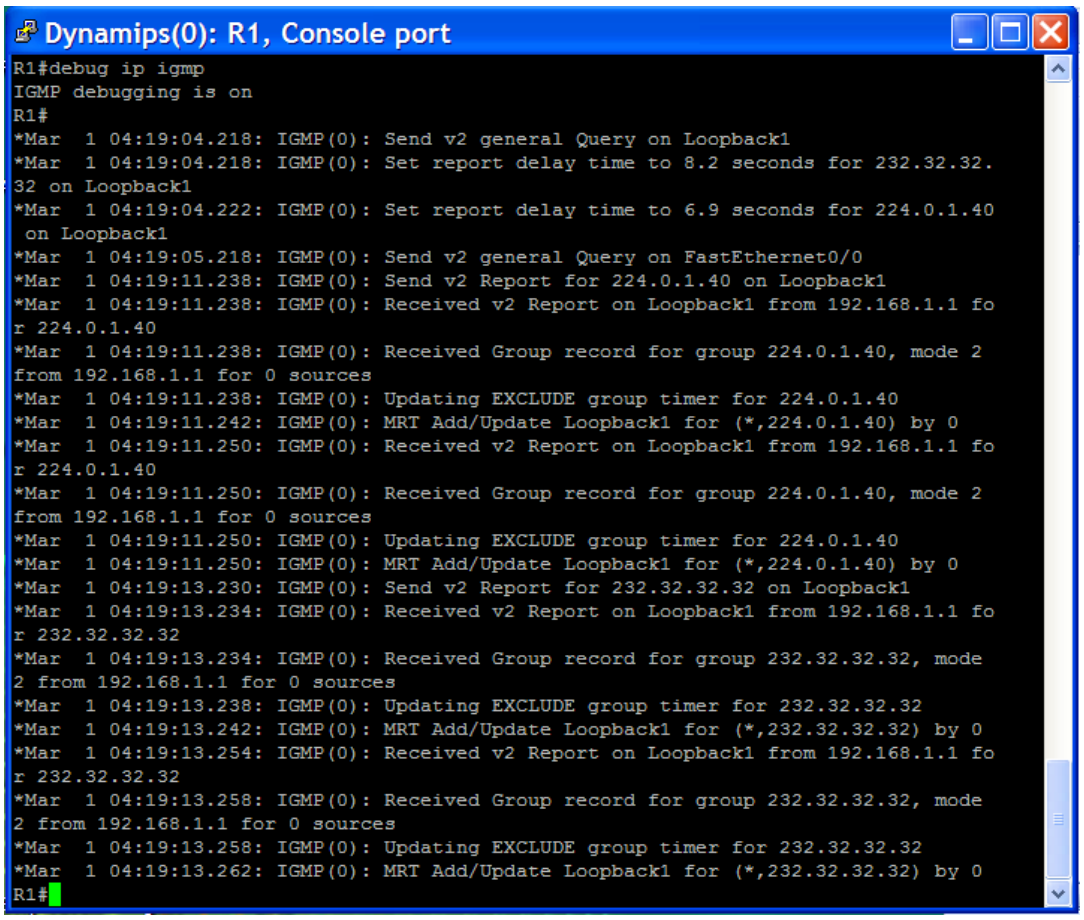
Para visualizar el comportamiento *flood-prune* de PIM-DM, se espera a que el flujo de datos desde 172.16.20.4 se complete y que las tablas de enrutamiento multicast para el estado (S, G) expiren. A continuación se ejecutan los comandos **debug ip igmp** y **debug ip pim** en todos los routers.

Figura 244. Comando debug ip pim en el router R1.



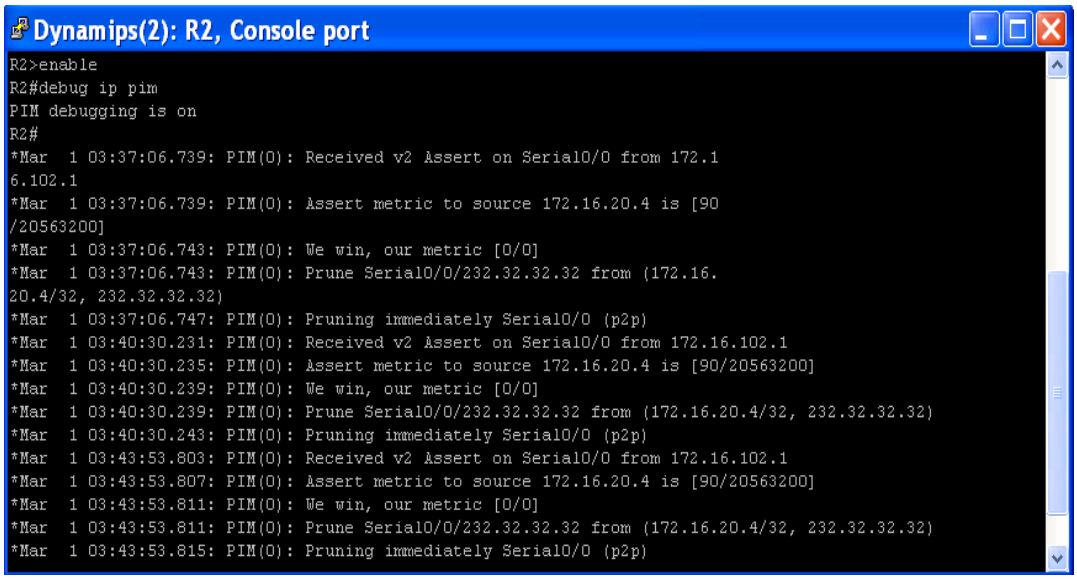
Fuente: Software GNS3.

Figura 245. Comando debug ip igmp en el router R1.



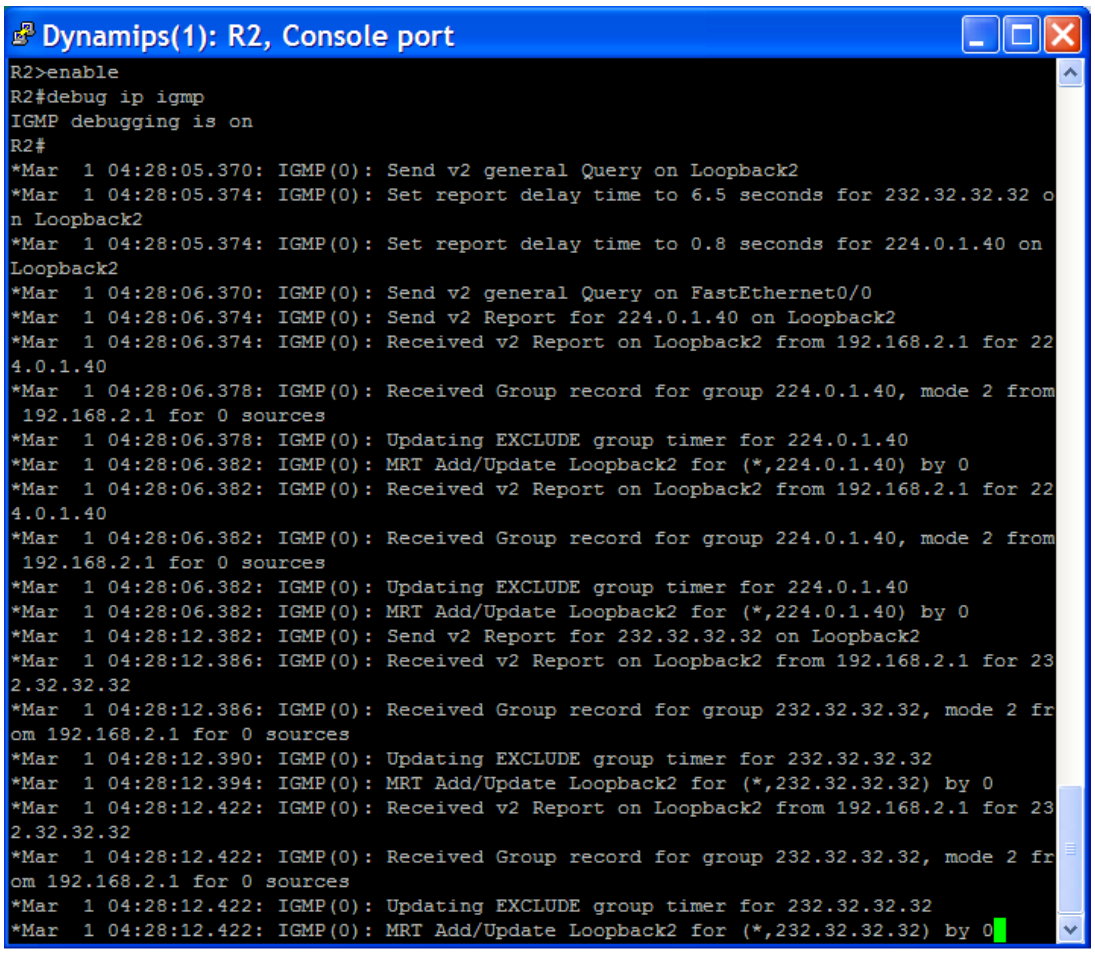
Fuente: Software GNS3.

Figura 246. Comando debug ip pim en el router R2.



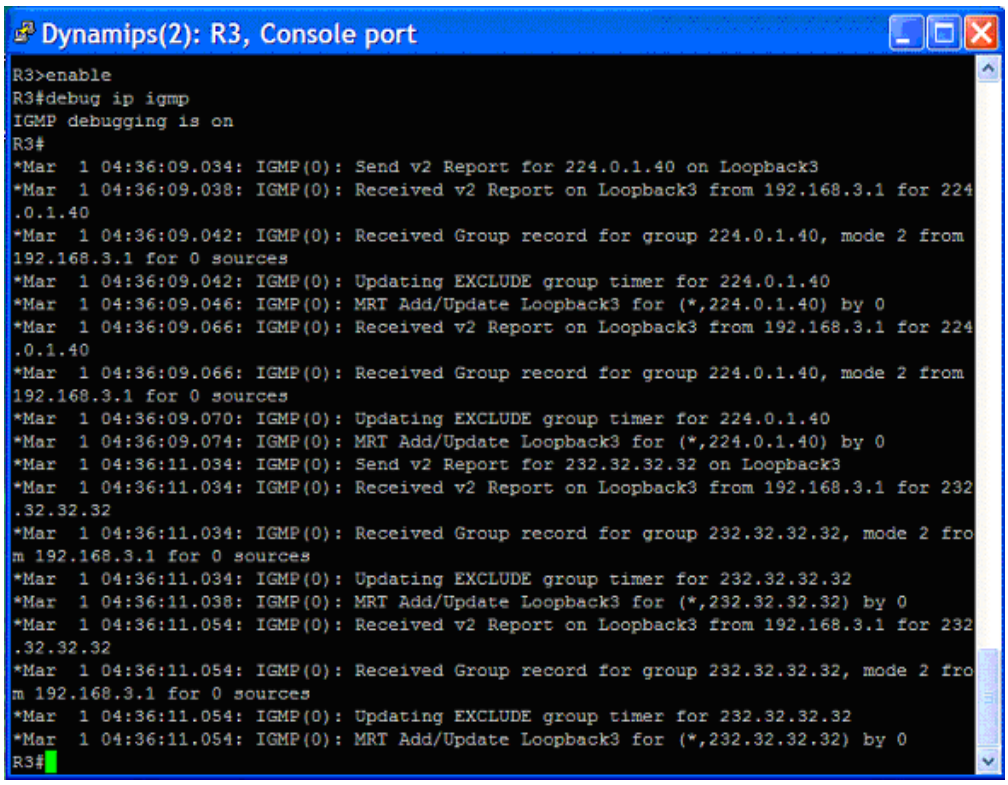
Fuente: Software GNS3.

Figura 247. Comando debug ip igmp en el router R2



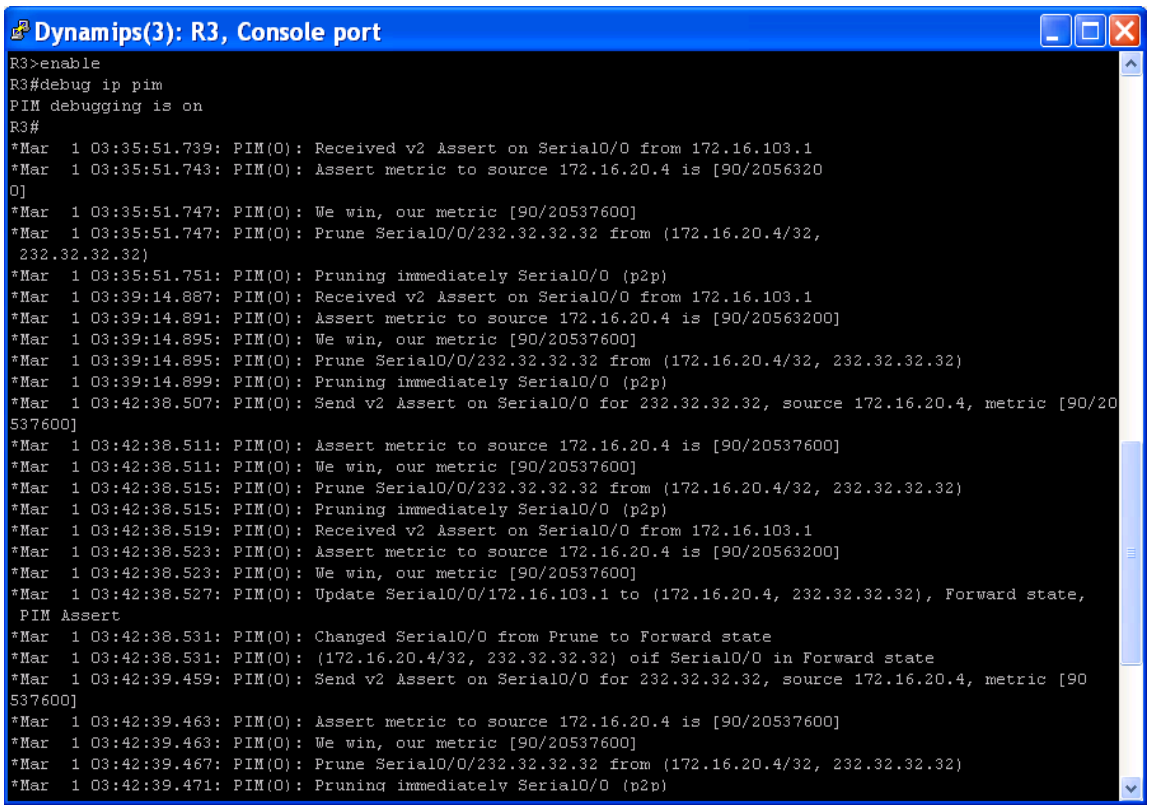
Fuente: Software GNS3.

Figura 248. Comando debug ip igmp en el router R3.



Fuente: Software GNS3.

Figura 249. Comando debug ip pim en el router R3.



Fuente: Software GNS3.

PIM se basa en la tabla de enrutamiento ip unicast para construir árboles de caminos más cortos a los suscriptores multicast. Los vecinos PIM envían mensajes de control para determinar cuál vecino está más cerca de la fuente en términos de la información de enrutamiento unicast en cada vecino. Los vecinos PIM en la subred eligen un router en particular como el promotor de ese par (S, G) usando mensajes de afirmación. Cada mensaje de afirmación lleva la mejor distancia administrativa y métrica que el router publicado tiene a la fuente. El router PIM con la mejor distancia administrativa es elegido como el *forwarder* (retransmisor) para la entrada (S, G) o (*, G). El *forwarder* entonces poda ese par (S, G) de ser enviado por otros routers en la subred.

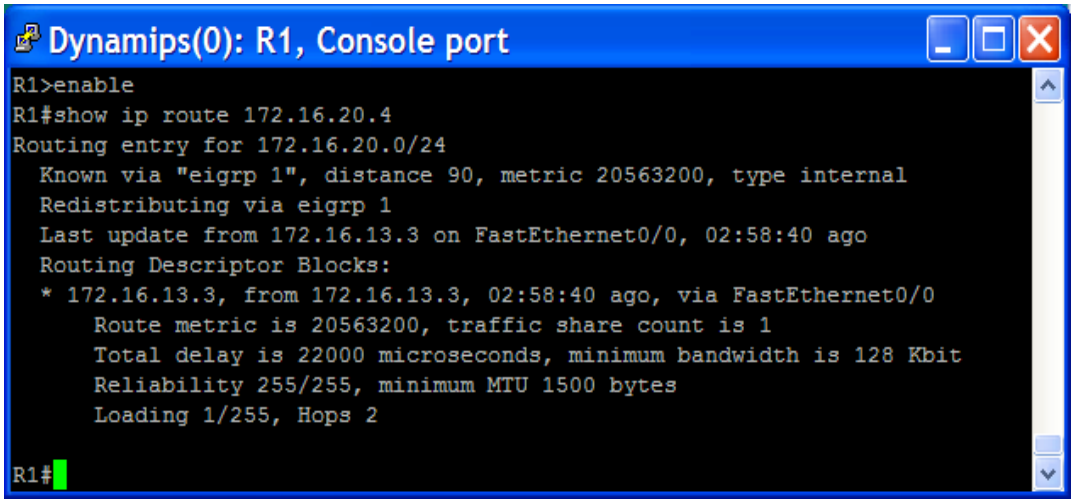
No se debe confundir el DR con el *forwarder*, aunque ambos son elegidos en redes multiacceso, el rol del DR no incluye la responsabilidad de

reenviar tráfico multicast. Como se define por IGMPv1, un DR es elegido basado en la dirección IP más alta para controlar las consultas IGMP. Así, un DR existe para identificar cuáles receptores existen en una subred realizando sondeos a los receptores de cualquier grupo. Sólo puede haber un DR a la vez en una subred.

En contraste, cada subred multi-acceso elige *forwarders* individualmente para cada par (S, G) y (*, G). El *forwarder* es elegido basado en la mejor distancia administrativa y métrica a la fuente. El *forwarder* es el router en la subred más cercano métricamente a la fuente.

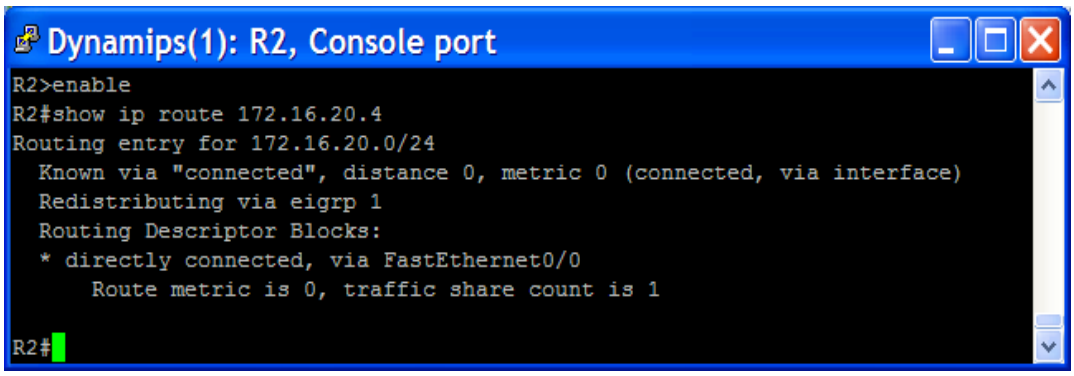
Para mostrar la entrada de la tabla de enrutamiento multicast para 172.16.20.4 en cada router se usa el comando **show ip route 172.16.20.4**

Figura 250. Tabla de enrutamiento multicast para 172.16.20.4 en R1.



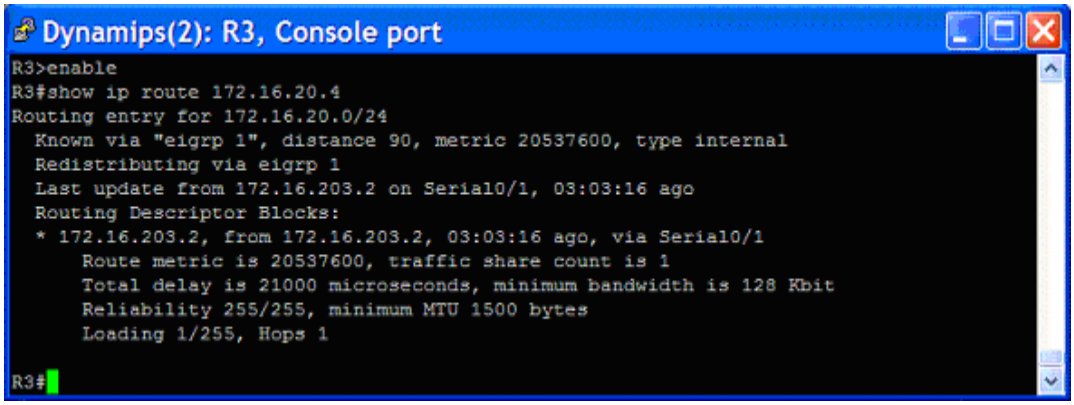
Fuente: Software GNS3.

Figura 251. Tabla de enrutamiento multicast para 172.16.20.4 en R2.



Fuente: Software GNS3.

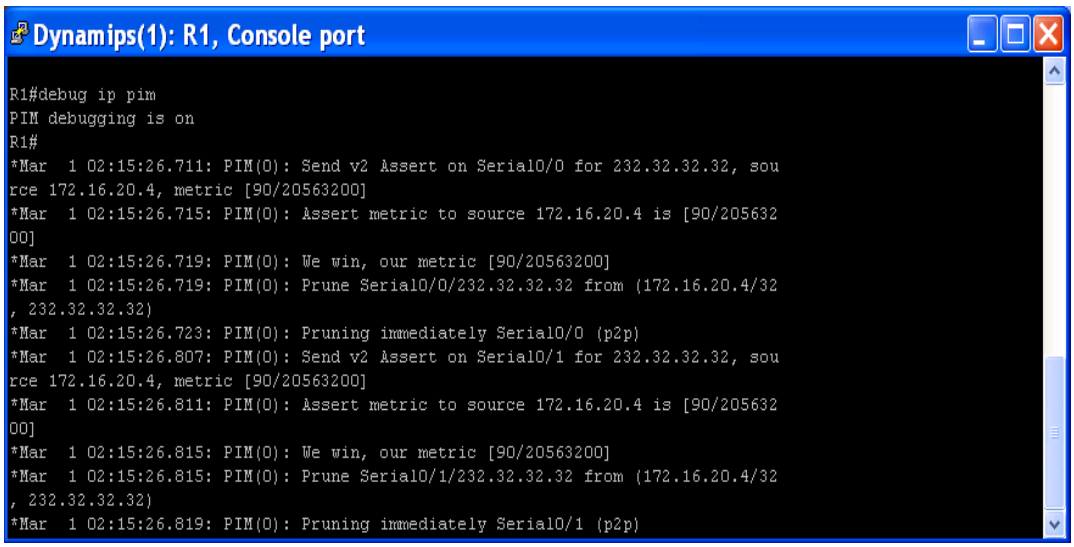
Figura 252. Tabla de enrutamiento multicast para 172.16.20.4 en R3.



Fuente: Software GNS3.

A continuación se realiza el mismo ping extendido en SW1 al grupo multicast y se revisan los mensajes de depuración mostrados en uno de los routers.

Figura 253. Mensajes de depuración PIM en router R1.

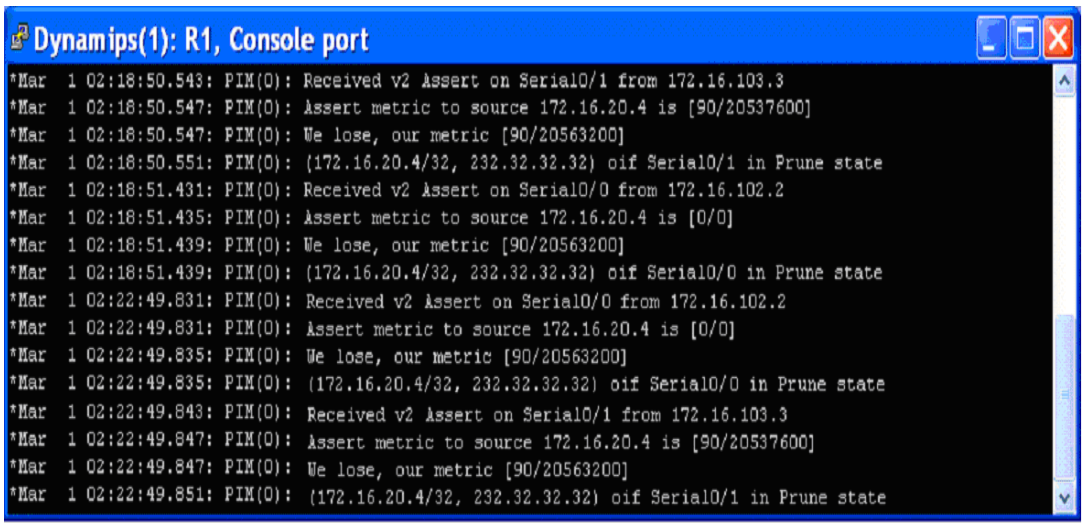


Fuente: Software GNS3.

Como R1 no ha recibido ningún mensaje de afirmación PIMv2 de sus vecinos en la Serial0/0/ ni Serial0/1, se ha elegido a sí mismo como el *forwarder* para (172.16.20.4/32, 232.32.32.32) en ambas interfaces y ha podado otros flujos de tráfico.

En un enlace punto a punto, un router PIM-DM debe afirmarse a sí mismo como el *forwarder* en la subred para el grupo, a menos que otro router envíe un mensaje de afirmación con una métrica menor a la fuente. Este comportamiento permite a PIM-DM tener éxito en un caso simple de un router multicast único en una subred. En este caso, el router no puede esperar por otros routers multicast para responder al mensaje de afirmación antes de la inundación de datos multicast, éste debe comenzar simplemente enviando datos hasta que otro router con una métrica menor a la fuente lo pode.

Figura 254. Mensajes de depuración PIM en router R1



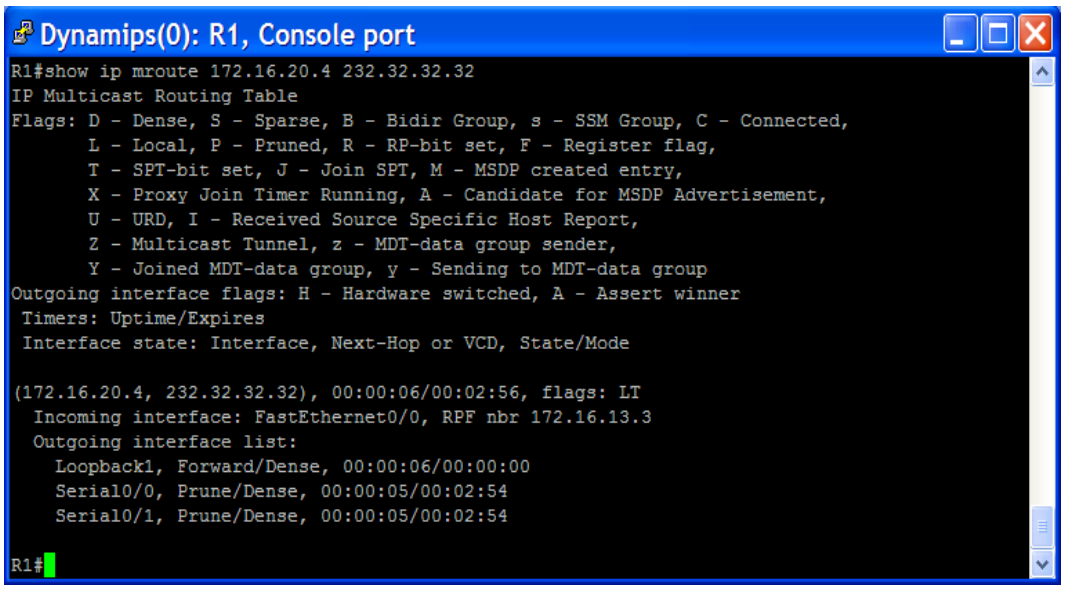
Fuente: Software GNS3.

PIM elige el router con la distancia administrativa más baja para ser el *forwarder* designado para la subred para el par (S, G). En caso de un empate, PIM elige el router con la métrica más baja.

Exploración de la tabla de enrutamiento multicast

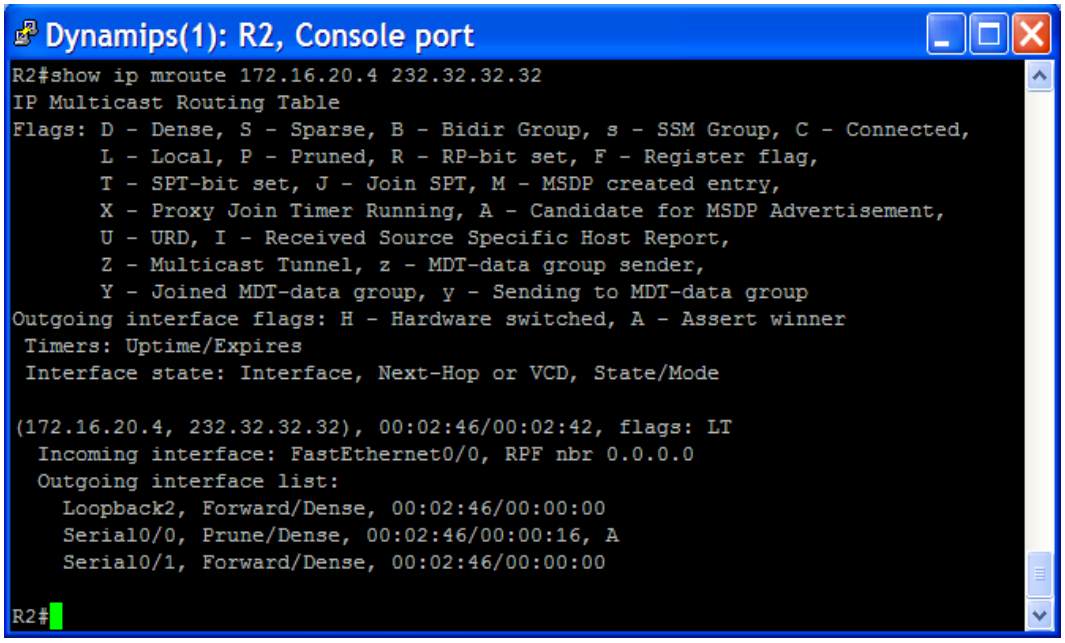
Se verifica el estado de la tabla de enrutamiento de R1 para la pareja (S, G) = (172.16.20.4, 232.32.32.32) utilizando el comando **show ip mroute *source_address group_address:***

Figura 255. Tabla de enrutamiento multicast (S, G) en R1



Fuente: Software GNS3.

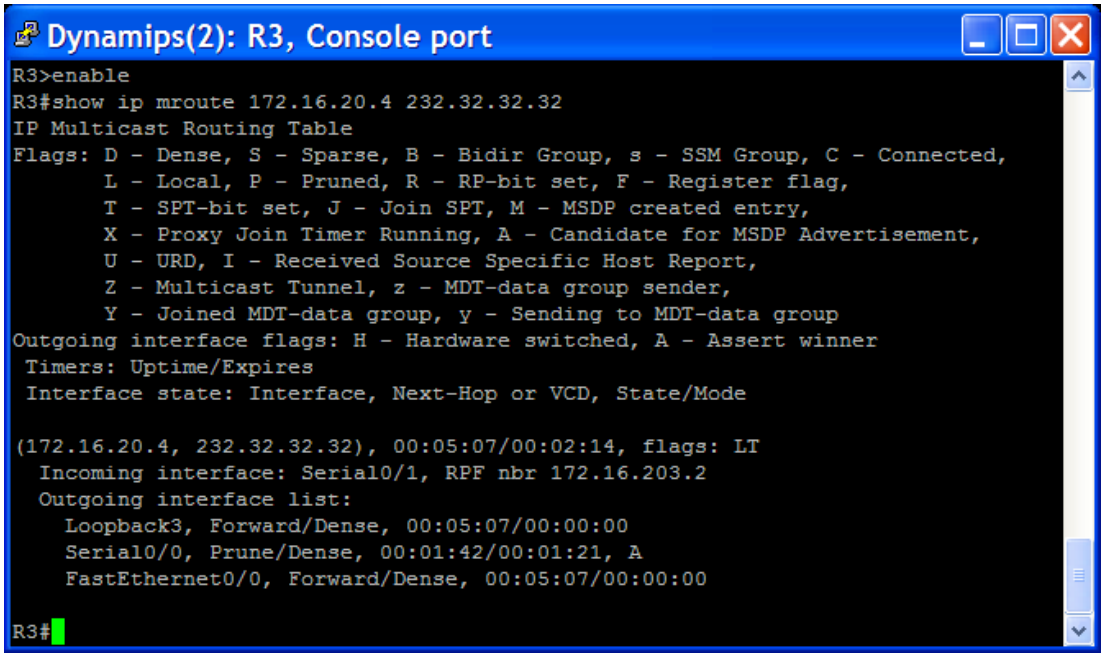
Figura 256. Tabla de enrutamiento multicast (S, G) en R2



Fuente: Software GNS3.

De las salidas anteriores se puede afirmar que la interfaz de entrada para la pareja (172.16.20.4, 232.32.32.32) es la FastEthernet 0/0. Para asignar esta interfaz de entrada, el IOS hace una búsqueda RPF y asigna la interfaz de salida en la tabla de enrutamiento unicast para ser la interfaz de entrada en la tabla de enrutamiento multicast.

Figura 257. Tabla de enrutamiento multicast (S, G) en R3



Fuente: Software GNS3.

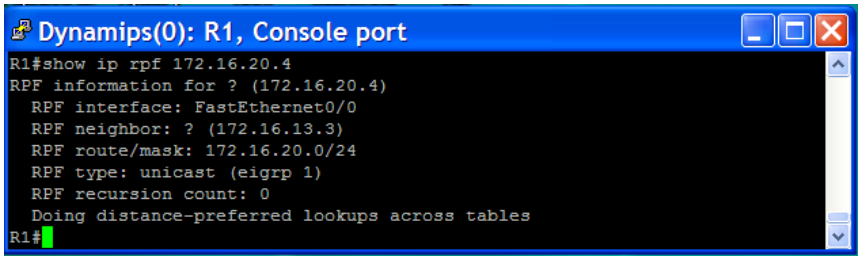
Debido a que PIM no usa su propio algoritmo topológico para localizar fuentes multicast, debe haber una forma para determinar cuál interfaz se encarga del vecino *upstream* del árbol derivado de la fuente multicast. PIM usa la confirmación RPF (reverse-path Forwarding) para encontrar la interfaz más cercana a la fuente en términos de destino basado en enrutamiento unicast.

El IOS de Cisco permite ejecutar confirmaciones RPF para fuentes específicas con el comando **show ip rpf *source_address***; aunque la

tabla de enrutamiento multicast incluye información RPF, este comando puede ser útil cuando se depuran cuestiones ocultas de multicast.

A continuación se utiliza **show ip rpf** en R1 para encontrar la interfaz de entrada para la pareja (172.16.20.4, 232.32.32.32).

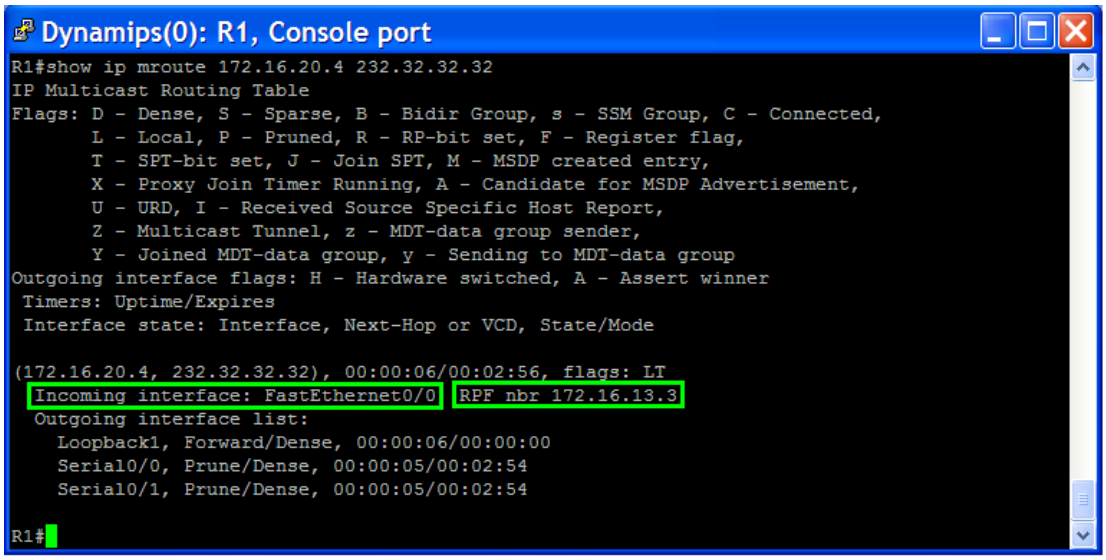
Figura 258. Confirmación RPF para la fuente 172.16.20.1 en R1



Fuente: Software GNS3.

Basados en la siguiente salida obtenida al ejecutar el comando **show ip mroute** para (S, G)= (172.16.20.4, 232.32.32.32) en R1 se puede determinar que:

Figura 259. Comando show ip mroute en R1



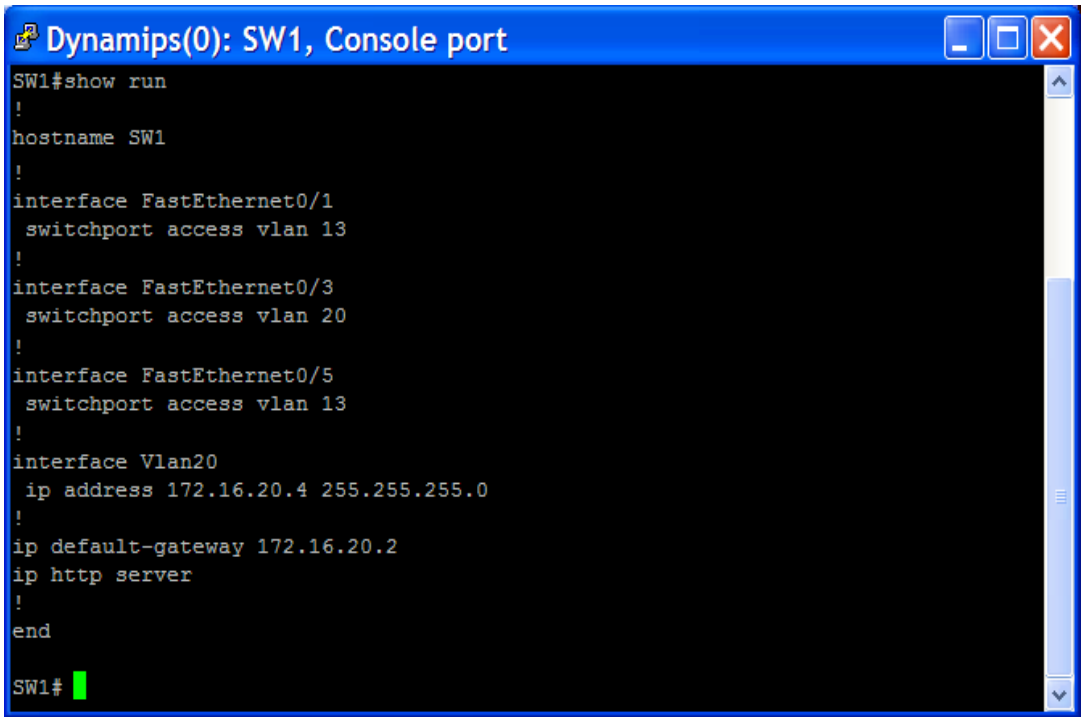
Fuente: Software GNS3.

- La interfaz de entrada es la FastEthernet0/0; ésta es asignada cuando el IOS realiza un *RPF lookup* (búsqueda RPF) para 172.16.20.4 y asigna la interfaz de salida en la tabla de enrutamiento unicast para ser la interfaz de entrada para la tabla de enrutamiento multicast.
- El router R3 aparece como el siguiente salto upstream hacia la fuente multicast 172.16.20.4, porque la dirección RPF neighbor es la 172.16.13.3, la dirección IP de la interfaz FastEthernet0/0 de R3.

Configuración Final

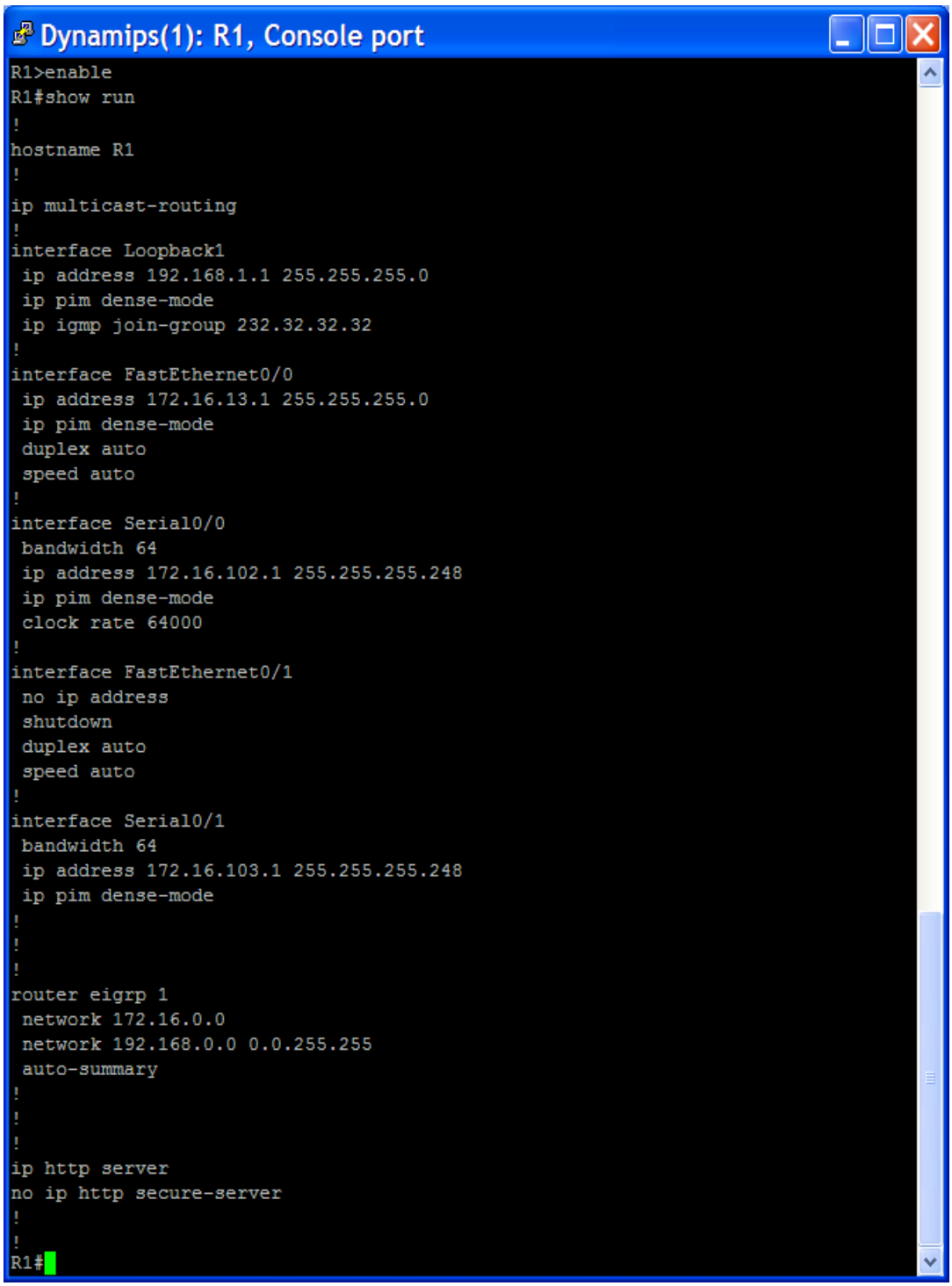
Finalmente se verifica la configuración final de las interfaces en todos los dispositivos con el comando **show run** como se muestra a continuación.

Figura 260. Configuración final de SW1



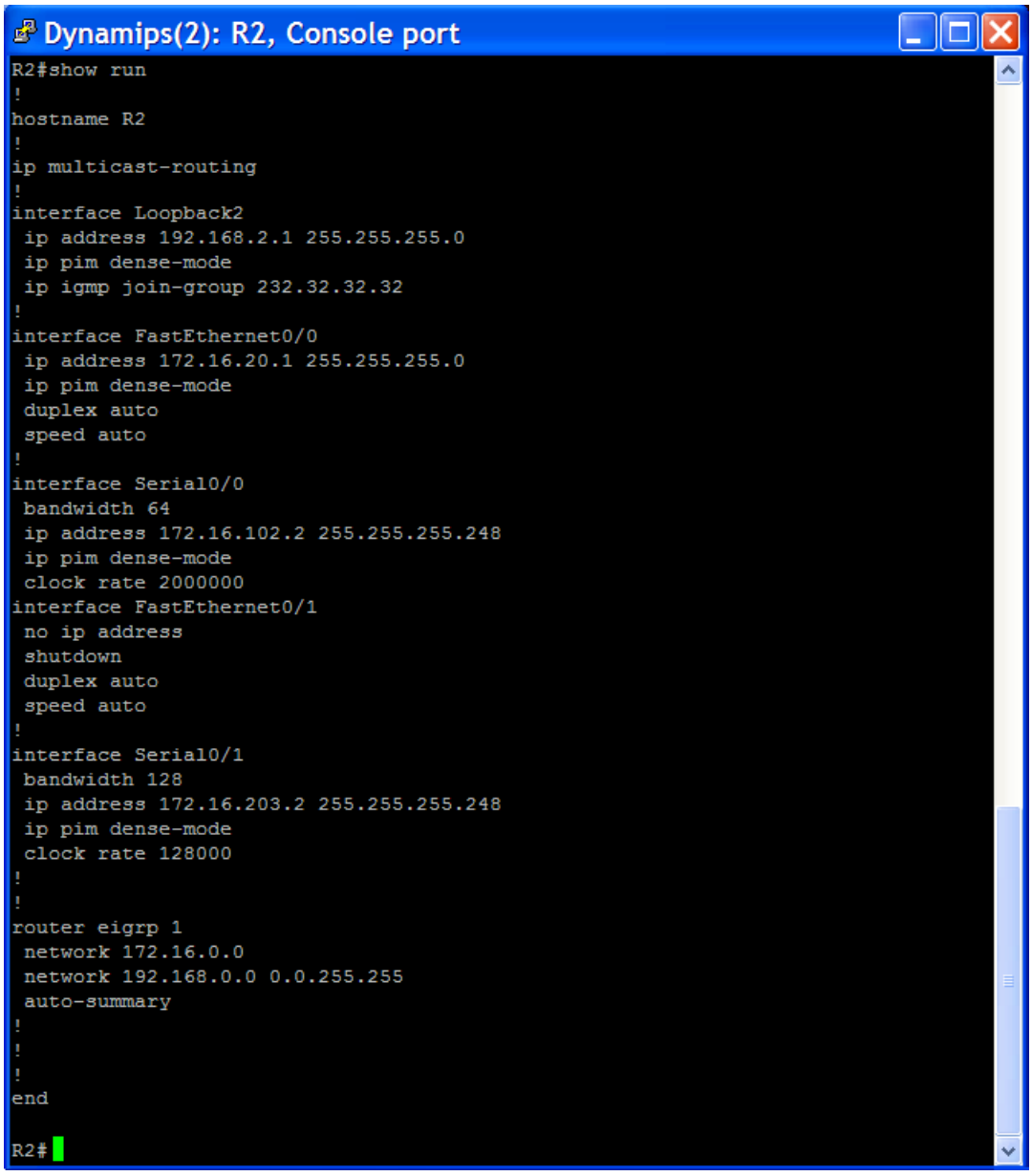
Fuente: Software GNS3.

Figura 261. Configuración final de R1



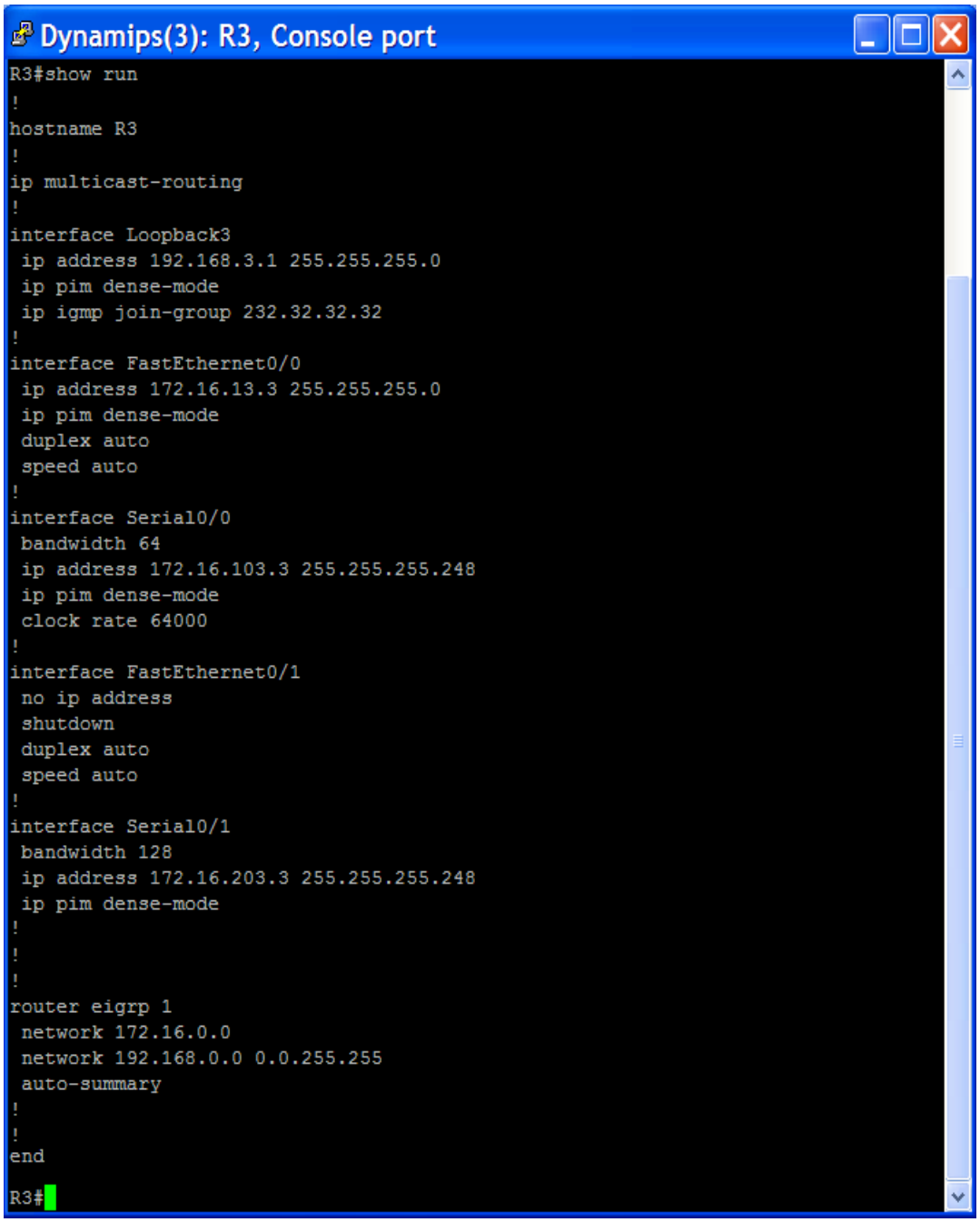
Fuente: Software GNS3.

Figura 262. Configuración final de R2



Fuente: Software GNS3.

Figura 263. Configuración final de R3



Fuente: Software GNS3.

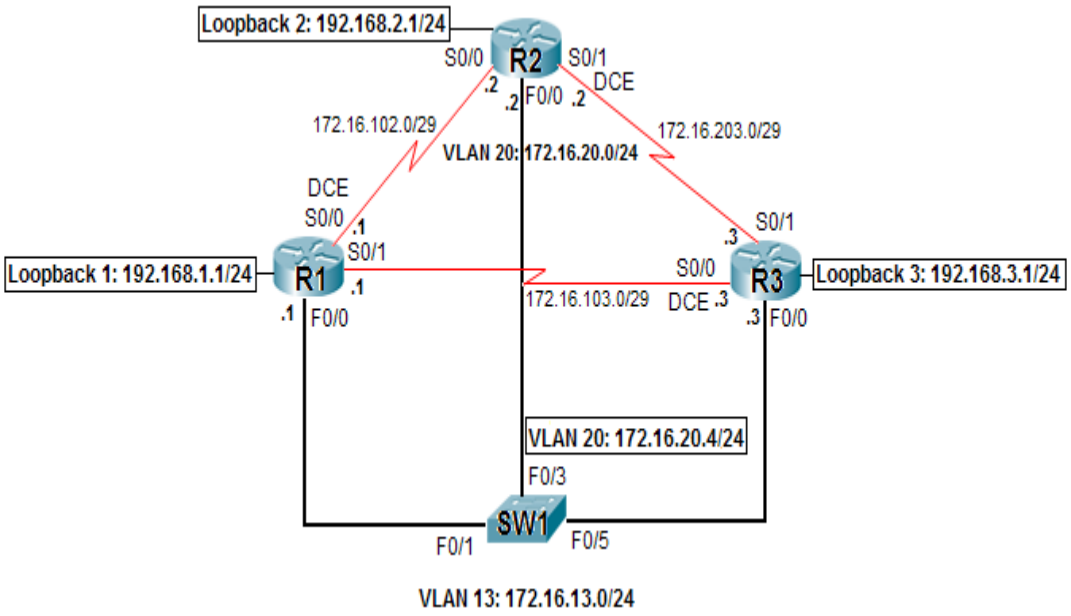
5.4. PIM-SM

Planteamiento:

La empresa “X” a la que se le implementó anteriormente IP multicast en la red, utilizando PIM-DM, ha tenido un incremento de usuarios interesados en usar la red. Desafortunadamente, la inundación y la poda con PIM-DM que se configuró anteriormente, no puede manejar las nuevas demandas que se están realizando en la red. Por tal razón se ha decidido implementear PIM-SM para crear una topología multicast basada en suscripción en la red de la empresa.

Diagrama:

Figura 264. Diagrama de la práctica de la simulación PIM-SM



Fuente: Autoras.

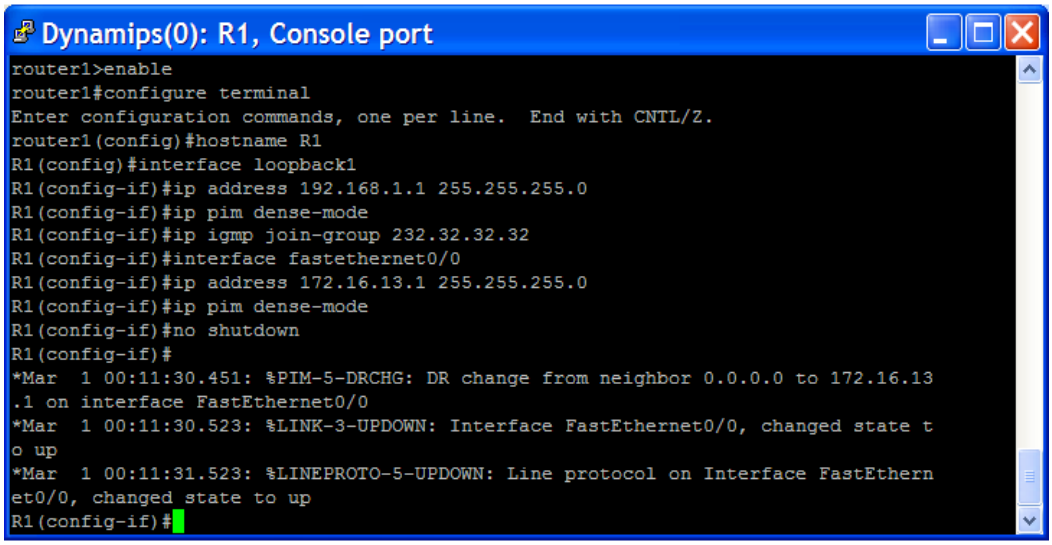
Solución:

A continuación se describen los pasos que se siguieron para realizar esta simulación. (El simulador utilizado para esta práctica fue GNS3).

Configuración de interfaces de los dispositivos

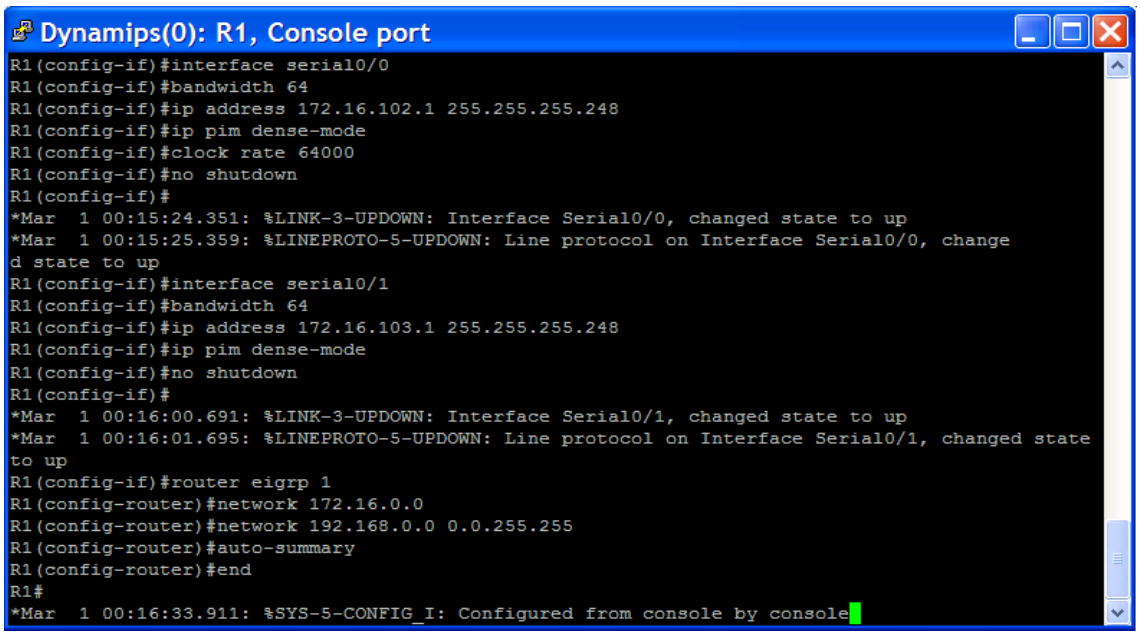
Basados en las configuracions finales del laboratorio de PIM-DM se configuran las interfaces en cada uno de los routers, asignándoles su dirección IP y suscribiendo sus respectivas interfaces loopback al grupo multicast 232.32.32.32

Figura 265. Configuración inicial de loopback1 y FastEthernet de R1



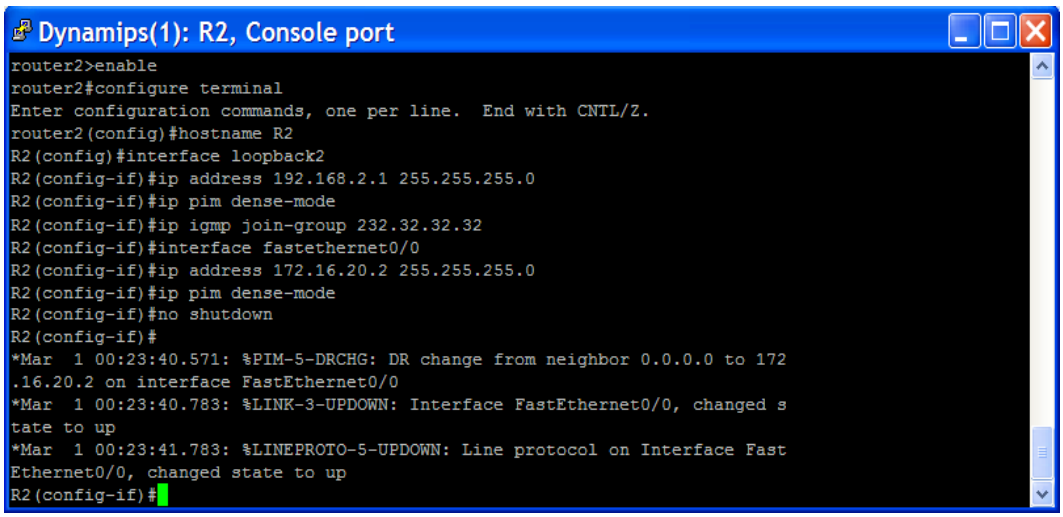
Fuente: Software GNS3.

Figura 266. Configuración de interfaces seriales en R1



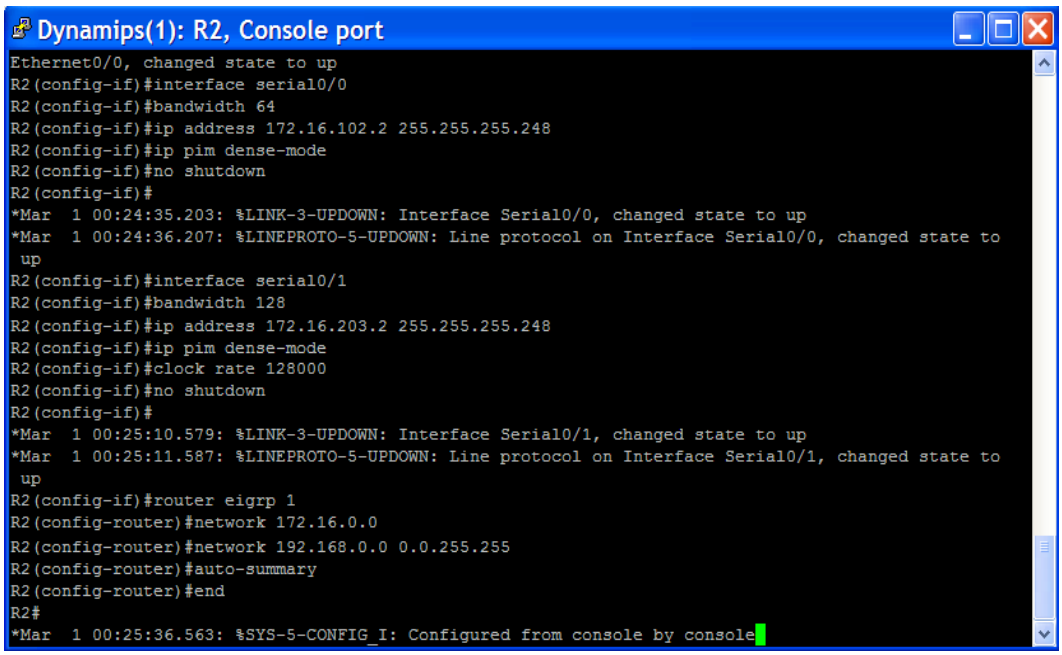
Fuente: Software GNS3.

Figura 267. Configuración de la interfaz loopback2 y FastEthernet de R2



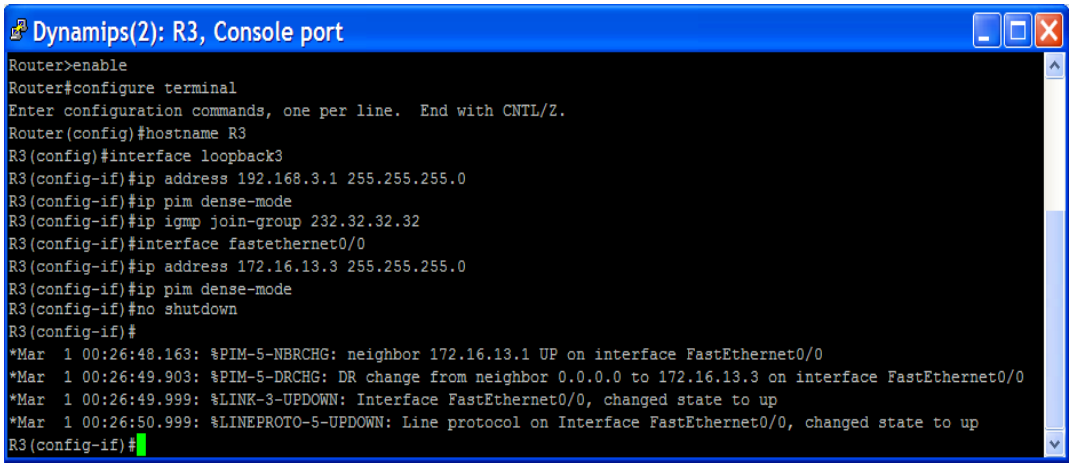
Fuente: Software GNS3.

Figura 268. Configuración de interfaces seriales en R2



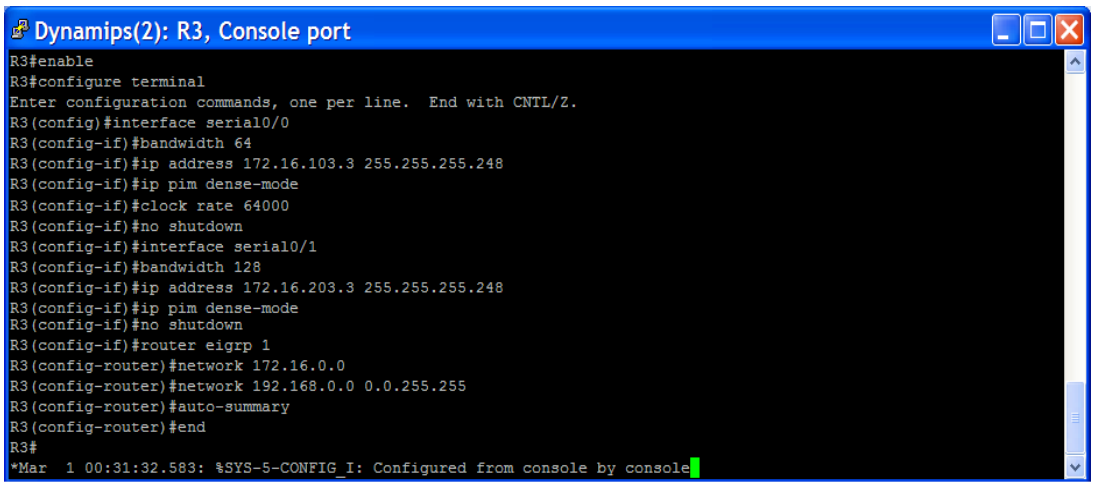
Fuente: Software GNS3.

Figura 269. Configuración de la interfaz loopback3 y FastEthernet de R3



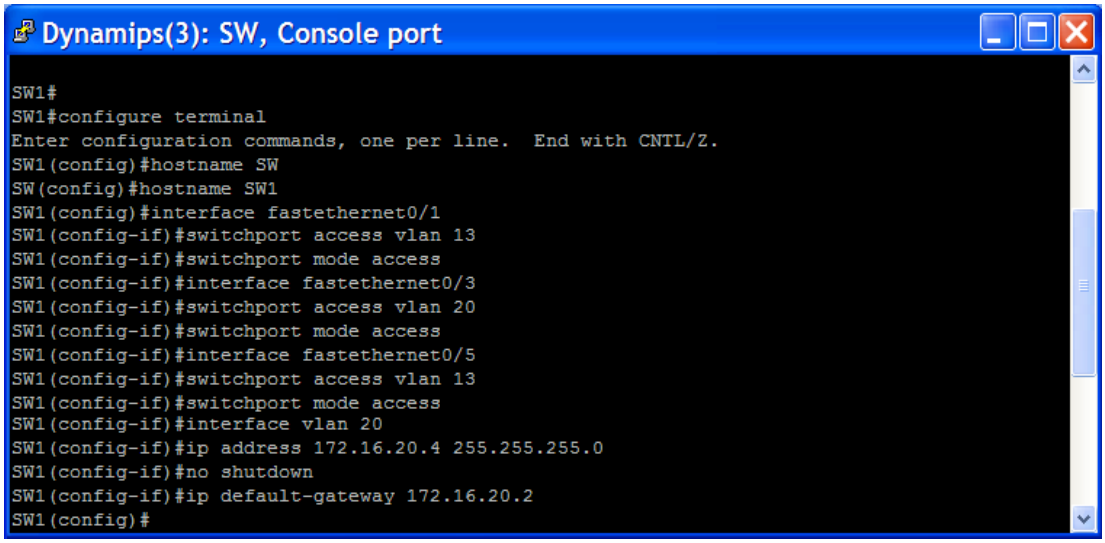
Fuente: Software GNS3.

Figura 270. Configuración de interfaces seriales en R3



Fuente: Software GNS3.

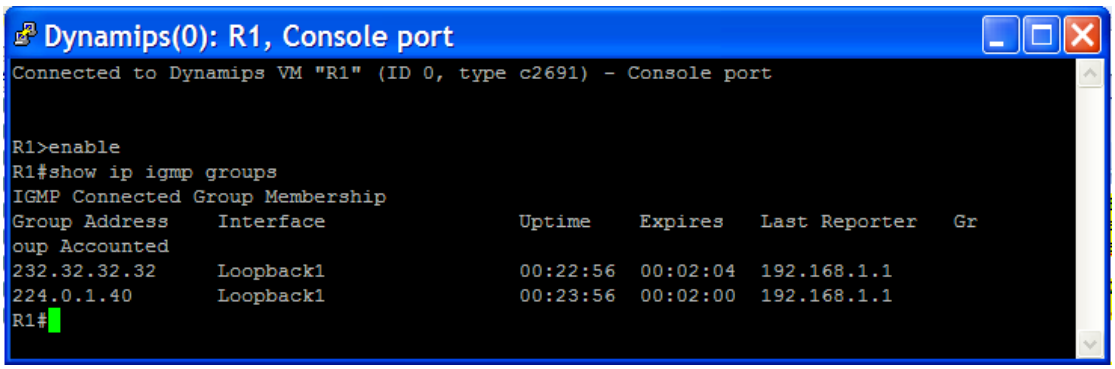
Figura 271. Configuración inicial del switchSW1



Fuente: Software GNS3.

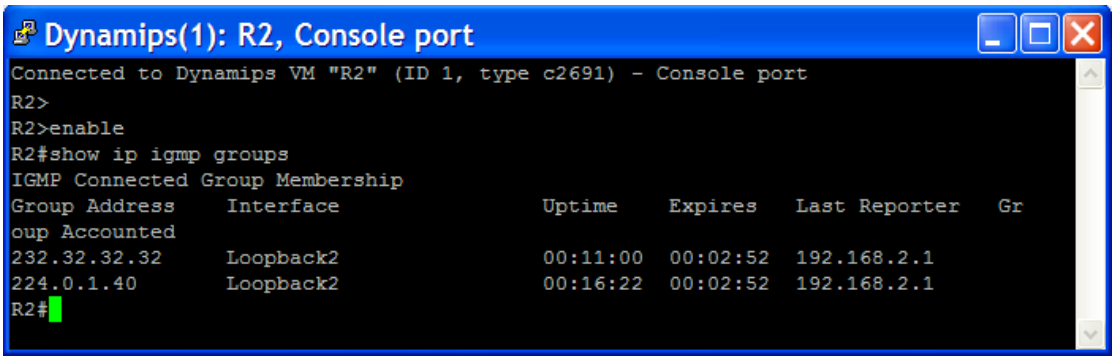
Se verifica que todas las interfaces se han suscrito al grupo multicast se usa el comando **show ip igmp groups** en cada router.

Figura 272. Comando show ip igmp groups en R1



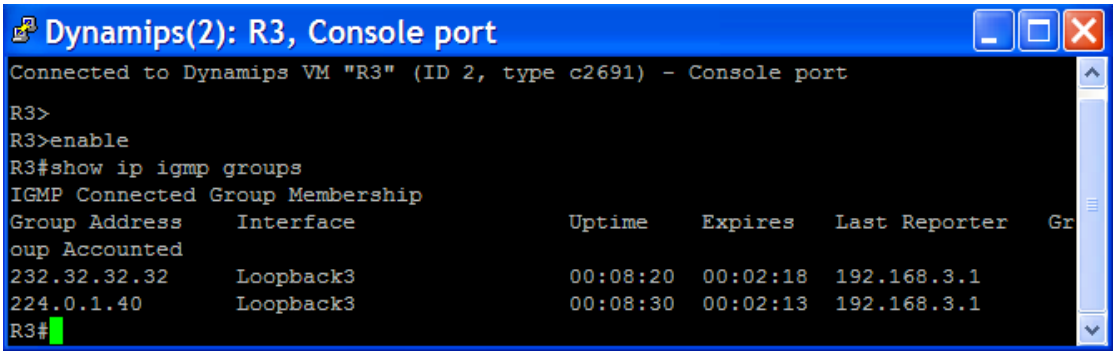
Fuente: Software GNS3.

Figura 273. Comando show ip igmp groups en R2



Fuente: Software GNS3.

Figura 274. Comando show ip igmp groups en R3



Fuente: Software GNS3.

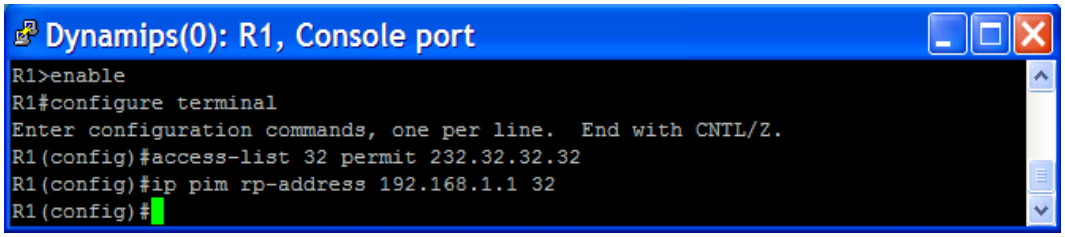
Implementación de PIM-SM

La planeación es importante cuando se crean redes PIM-SM, debido a que el tráfico no es simplemente inundado a todas las interfaces como en las redes PIM-DM, se debe tener en cuenta que para PIM-SM es necesario ubicar el punto de encuentro (RP) en una ubicación central.

Se decidió que para este laboratorio el RP debería estar localizado en R1. Esta ubicación le permite observar la transición de árbol compartido a árbol fuente, ya que R2 y R3 tienen caminos más cortos para 172.16.20.4 que aquellos a través de R1.

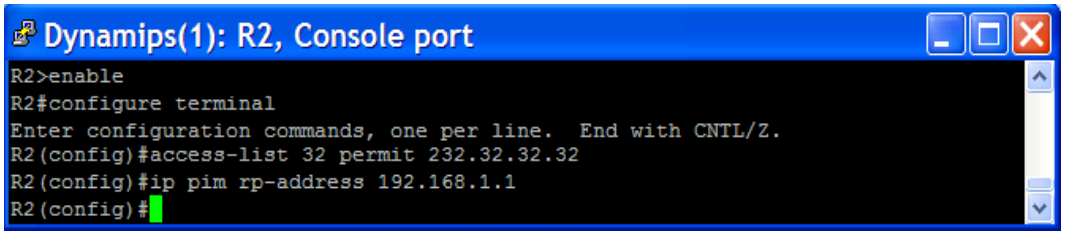
Antes de habilitar PIM-SM en las interfaces, se asigna la dirección RP estática a la Loopback1 de R1 usando el comando **ip pim rp-address *rp-address [access-list].*** Se puede asignar un router para ser el RP global para todos los grupos multicast ó tenerlo para un grupo determinado usando una lista de acceso. En este caso, se asigna R1 como el RP solo para el grupo multicast 232.32.32.32. Este comando debe ser utilizado en todos los routers que corren PIM-SM.

Figura 275. Asignación de loopback1 como RP para 232.32.32.32 en R1



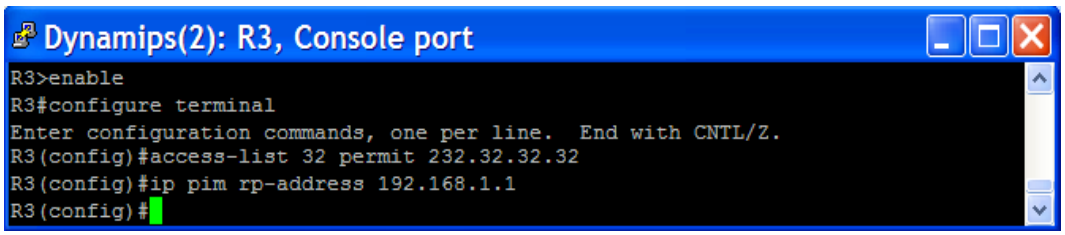
Fuente: Software GNS3.

Figura 276. Asignación de loopback1 como RP para 232.32.32.32 en R2



Fuente: Software GNS3.

Figura 277. Asignación de loopback1 como RP para 232.32.32.32 en R3



Fuente: Software GNS3.

Los RPs se usan en PIM-SM para proporcionar puntos de encuentro entre las fuentes multicast y los miembros de un grupo en una red multicast. Los RPs crean un punto común para que los routers multicast instalen árboles compartidos.

El hecho de que un RP pueda ser asignado a grupos específicos permite que se puedan tener varios RP estáticos en una red multicast, de hecho cada grupo podría tener un único RP.

PIM-SM tiene más formas redundantes de configurar RPs y agentes de mapeo. En este ejemplo se nota que cada router multicast tiene una dirección RP estática apuntando a un router específico en la red.

En PIM-DM, todas las entradas (S, G) son presentadas en cada tabla de enrutamiento IP multicast en la red multicast mientras que la fuente es broadcast. Si se estuvieran usando muchos grupos o muchas fuentes para cada grupo, el tamaño de la tabla de enrutamiento multicast incrementaría drásticamente.

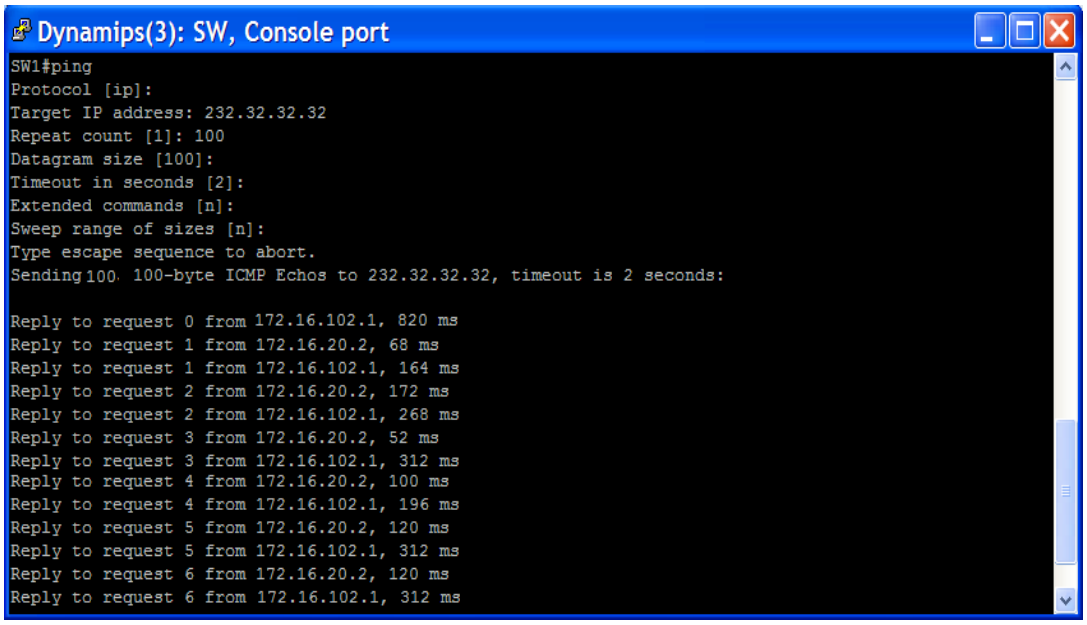
Los RPs en PIM-SM introducen fuentes multicast actuando como el receptor de la red que conoce la ubicación de todas las fuentes multicast. PIM-SM crea un árbol de distribución compartida representado por (*, G) en cada tabla de enrutamiento multicast. Este árbol compartido es calculado usando la interfaz *upstream* RPF para el RP para ese grupo. De esta forma, el árbol compartido es escencialmente el árbol de camino más corto a la dirección RP.

PIM-SM reduce la cantidad de estado multicast en la red usando entradas de árbol compartido (*, G) en routers a través de los cuales no hay fuentes enviando tráfico para un grupo dado *G*.

PIM-SM está diseñado para redes multicast escasamente pobladas en las cuales no es necesario inundar de tráfico multicast a cada subred. SM es un modo multicast de propósito general que debería ser usado en la mayoría de las circunstancias.

Así como se hizo en el laboratorio de Modo Denso, se realizará un ping repetodo desde SW1 para generar el estado (S, G) en PIM-DM antes de aplicar PIM-SM a las interfaces.

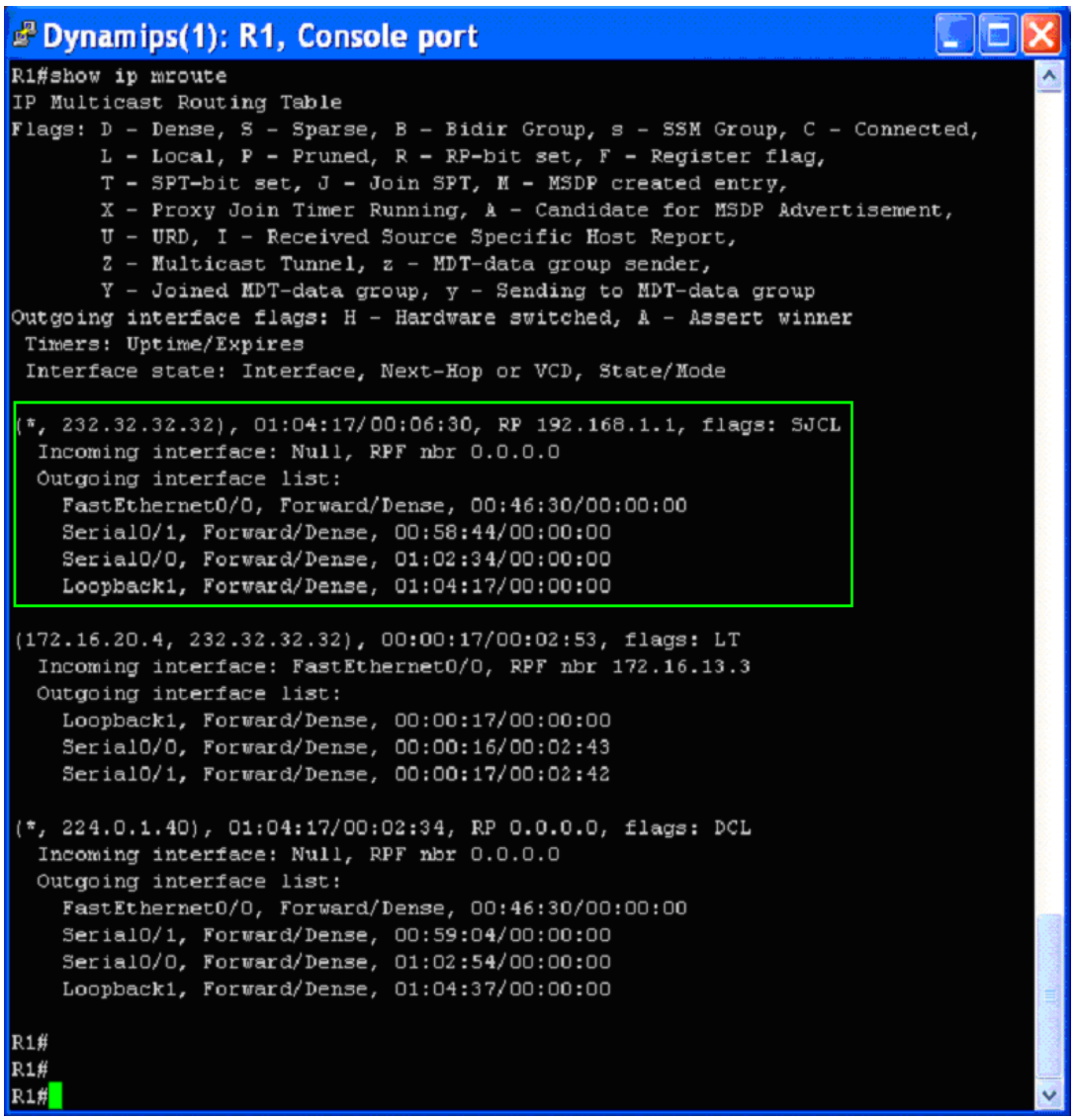
Figura 278. Ping al grupo multicast desde SW1



Fuente: Software GNS3.

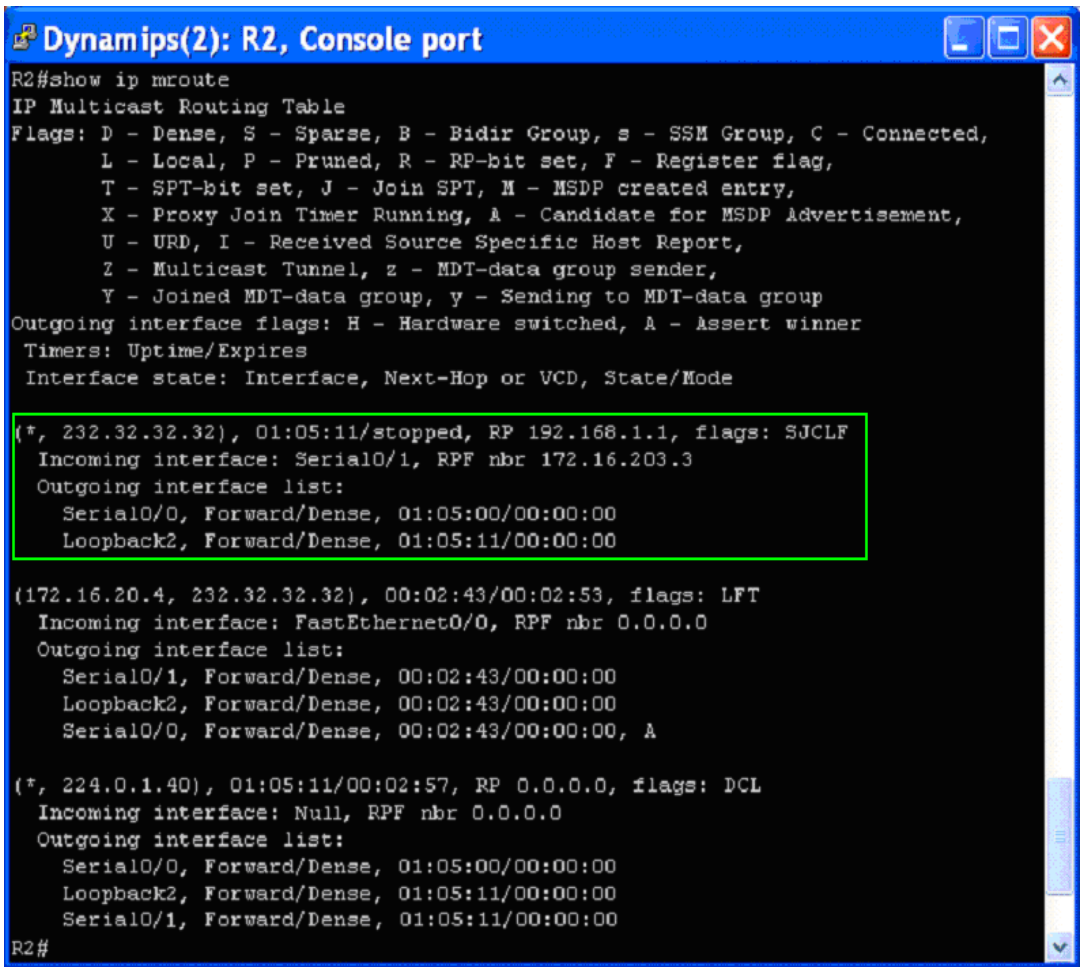
Con el comando **show ip mroute** se muestra la tabla de enrutamiento multicast:

Figura 279. Tabla de enrutamiento multicast de R1



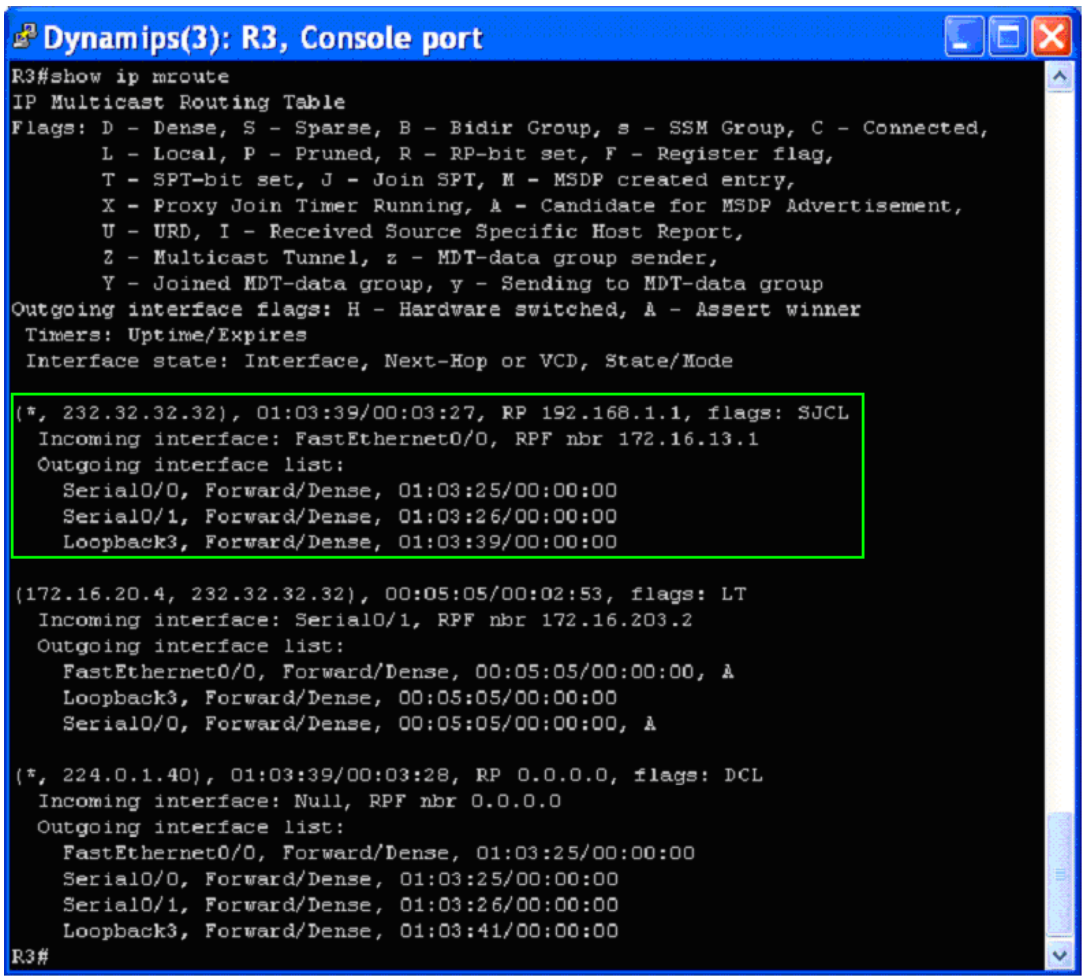
Fuente: Software GNS3.

Figura 280. Tabla de enrutamiento multicast de R2



Fuente: Software GNS3.

Figura 281. Tabla de enrutamiento multicast de R3

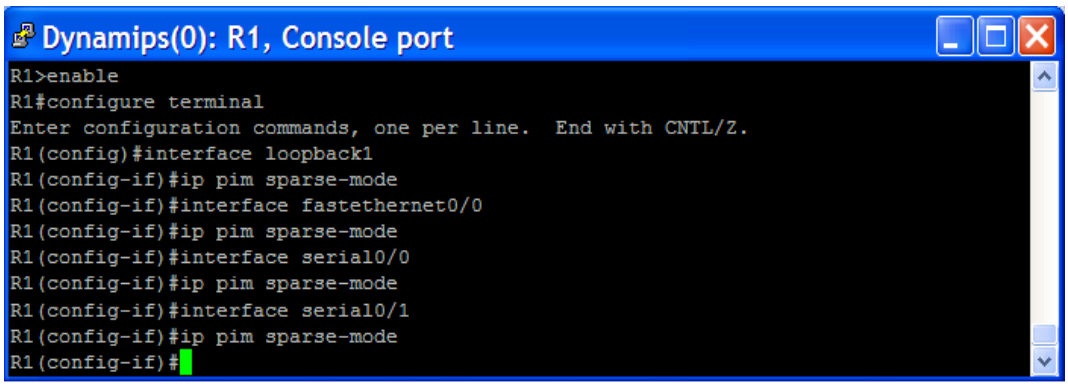


Fuente: Software GNS3.

De las figuras anteriores se observa que R1 tiene a 0.0.0.0 como el vecino RPF de la entrada (*, G), indicando que es el RP para el grupo multicast 232.32.32.32. R2 y R3 escuchan tráfico multicast en el árbol compartido que proviene de sus vecinos RPF para esa entrada (*, G) en sus tablas de enrutamiento multicast.

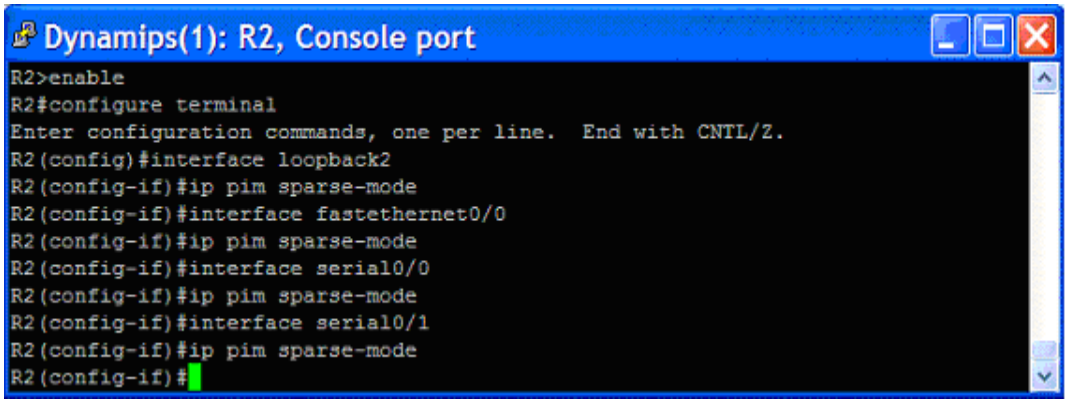
A continuación se habilita PIM-SM en todas las interfaces de cada router usando el comando **ip pim sparse-mode** en modo de configuración de interface:

Figura 282. Tabla de enrutamiento multicast de R3



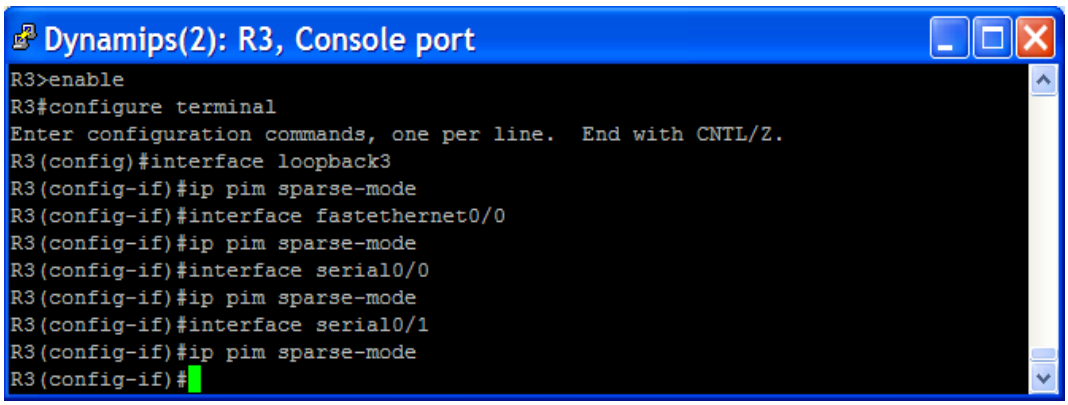
Fuente: Software GNS3.

Figura 283. Activación de PIM-SM en las interfaces de R2



Fuente: Software GNS3.

Figura 284. Activación de PIM-SM en las interfaces de R3

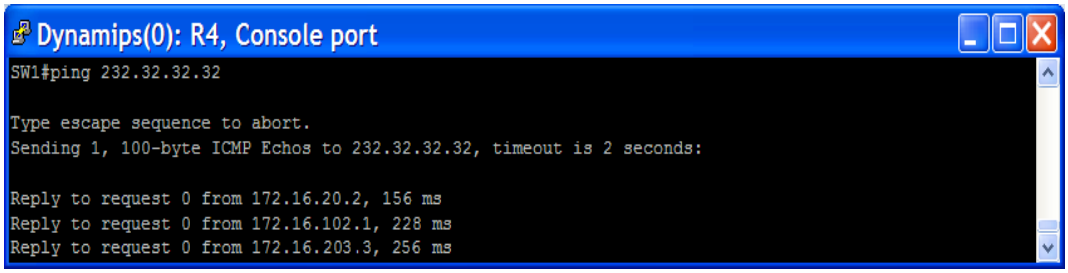


Fuente: Software GNS3.

Ahora que el enrutamiento multicast y PIM-SM están habilitados en R2, un ping de SW1 al grupo 232.32.32.32 sí recibirá respuesta como se puede apreciar en la siguiente figura, ya que las respuestas *echo* serán enviadas desde cada router debido a que PIM-SM está activo en toda la red y hay suscriptores para el grupo 232.32.32.32.

Es necesario aclarar que no se recibirán necesariamente respuestas de la dirección IP de la interfaz sobre la cual el paquete multicast fue recibido sino desde cualquier interfaz en el router que responde el paquete de retorno encapsulado.

Figura 285. Ping desde SW1 al grupo multicast 232.32.32.32



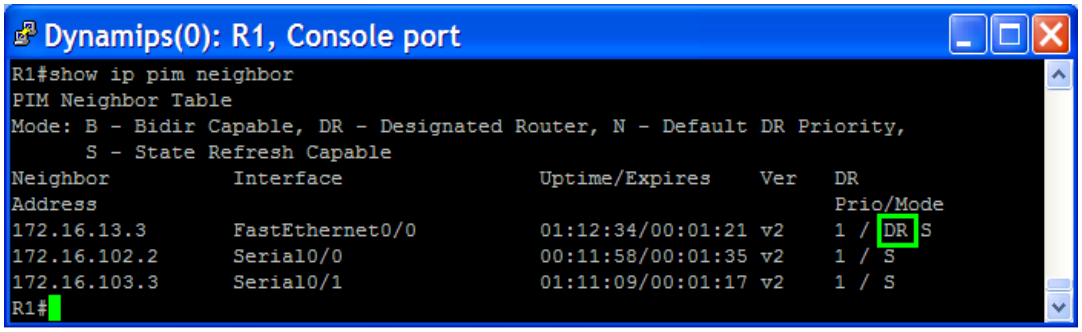
Fuente: Software GNS3.

La interfaz donde se originan los *echo replies* es determinada por la tabla de enrutamiento multicast. Los paquetes de salida son etiquetados con la dirección IP de la interface de salida por la cual los paquetes fluirán a 172.16.20.4.

Adyacencias PIM

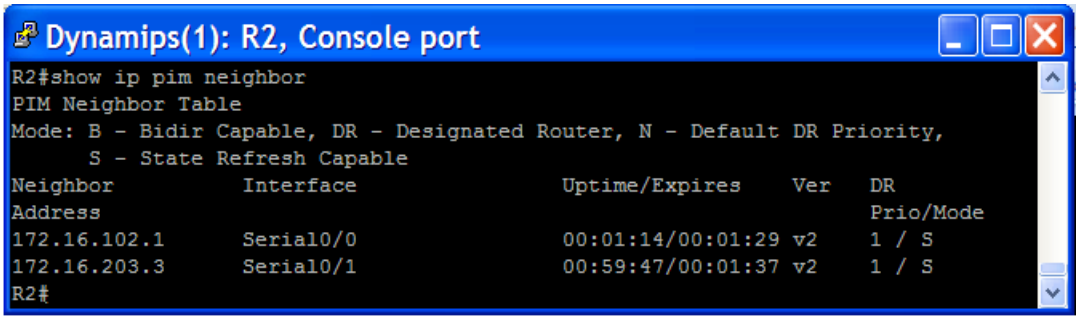
A continuación se exploran las adyacencias PIM y cómo funciona PIM sobre varios medios capa 2. Para visualizar todos los routers PIM adyacentes se utiliza el comando **show ip pim neighbors:**

Figura 286. Comando show ip pim neighbor en R1



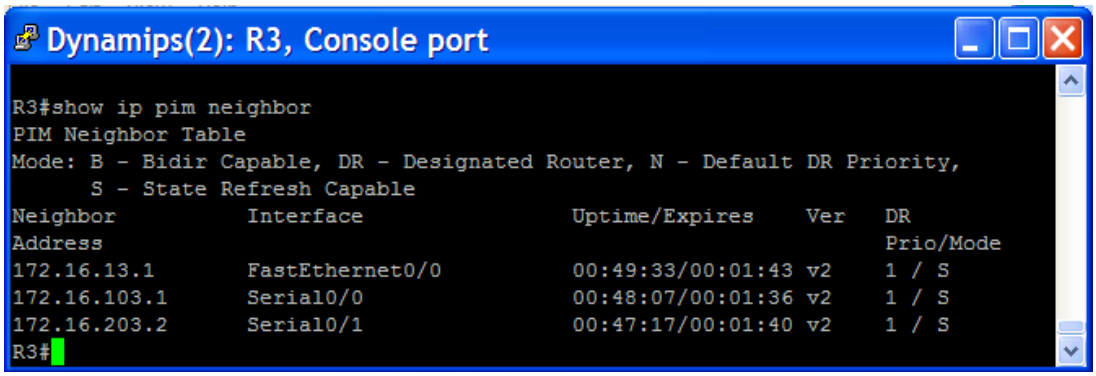
Fuente: Software GNS3.

Figura 287. Comando show ip pim neighbor en R2



Fuente: Software GNS3.

Figura 288. Comando show ip pim neighbor en R3

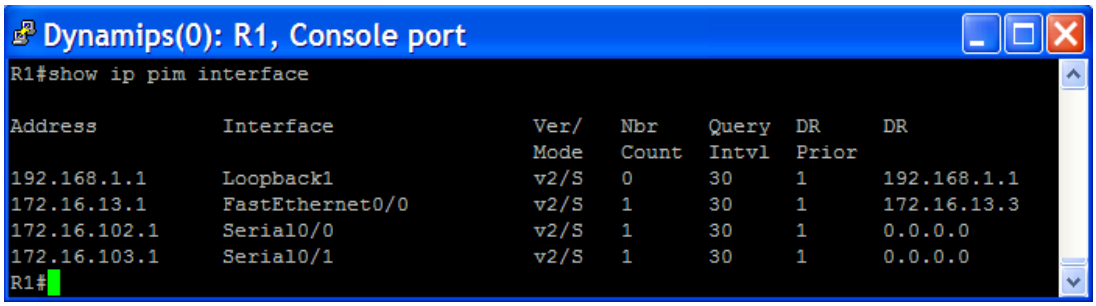


Fuente: Software GNS3.

PIM-DM usa un DR como la fuente de consultas IGMPv1. PIM-SM también soporta este tipo de comportamiento debido a que es requerido en el protocolo IGMPv1. En la configuración actual R1 es el DR para la subred 172.16.13.0 y por consiguiente funciona como el *IGMP querier.*

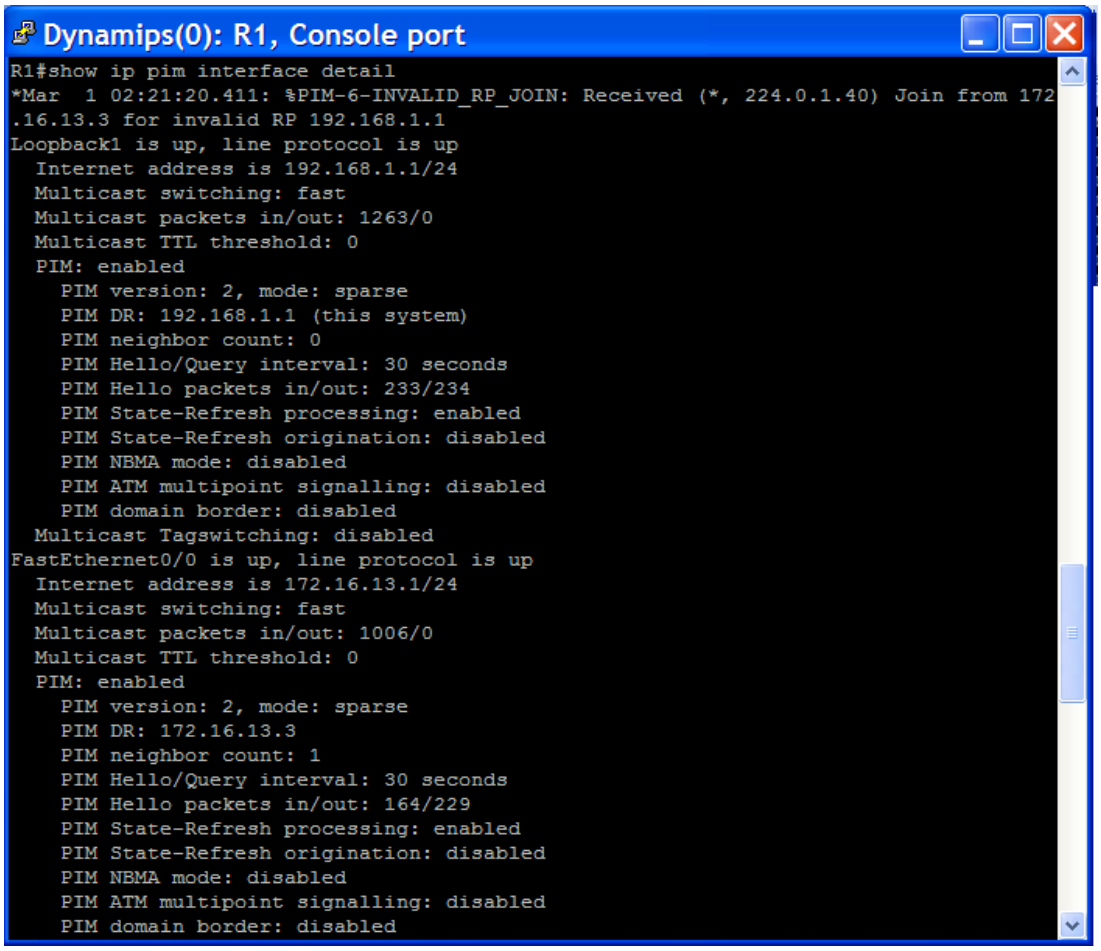
La información sobre las interfaces PIM habilitadas se muestran con el comando **show ip pim interface detail:**

Figura 289. Comando show ip pim interface en R1



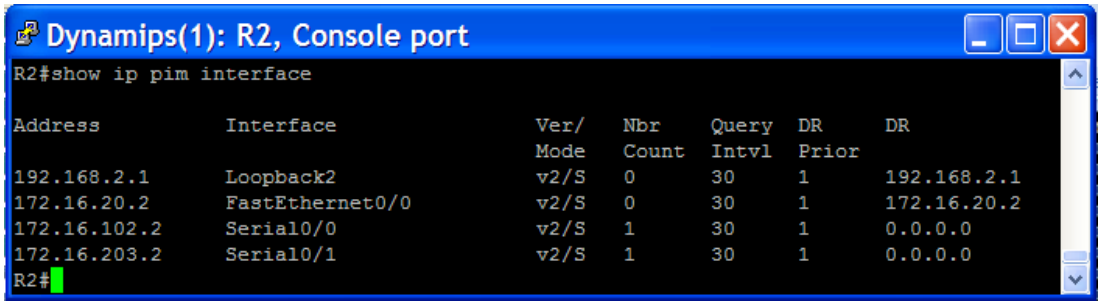
Fuente: Software GNS3.

Figura 290. Comando show ip pim interface detail en R1



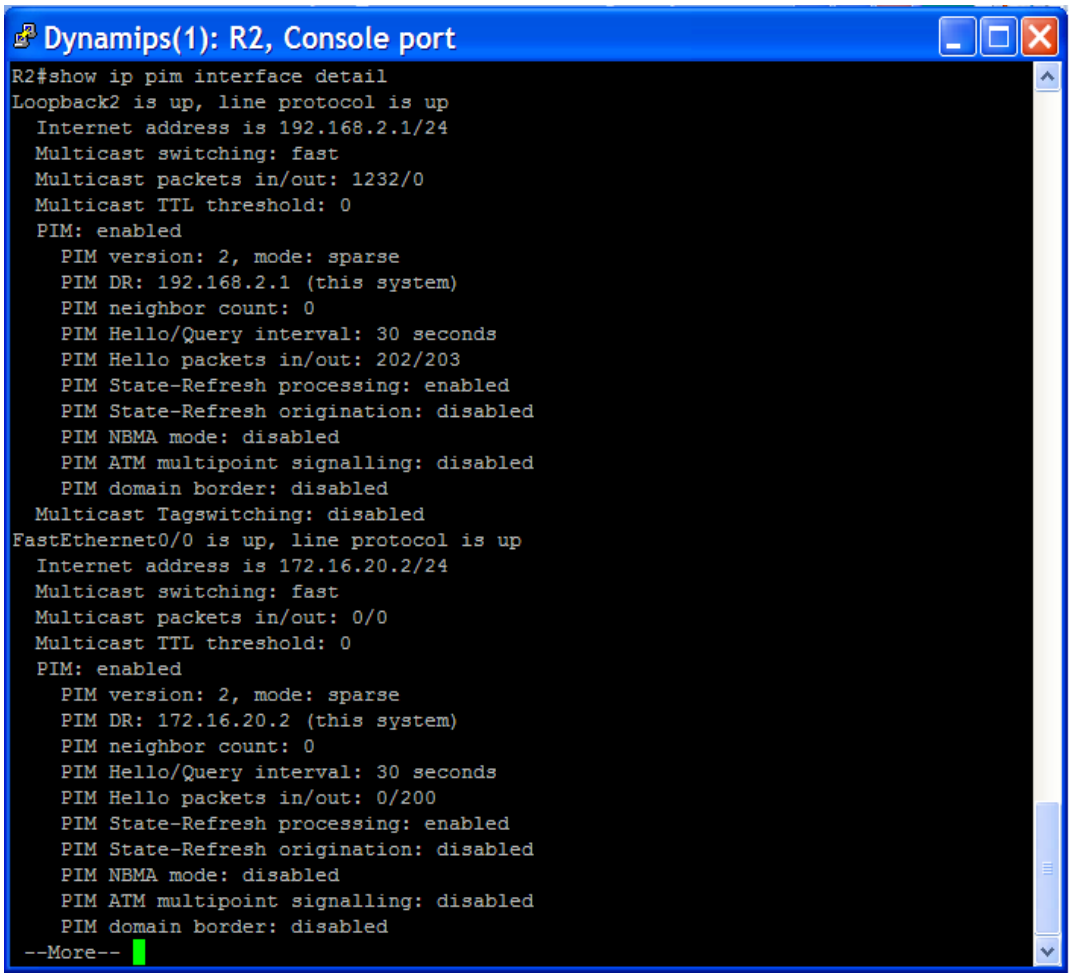
Fuente: Software GNS3.

Figura 291. Comando show ip pim interface en R2



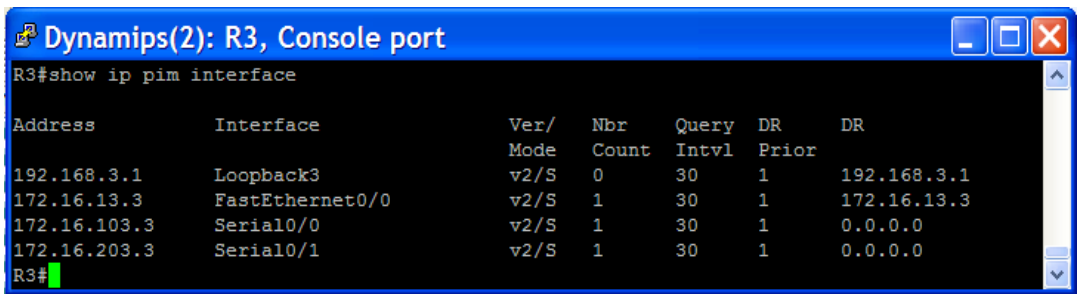
Fuente: Software GNS3.

Figura 292. Comando show ip pim interface detail en R2



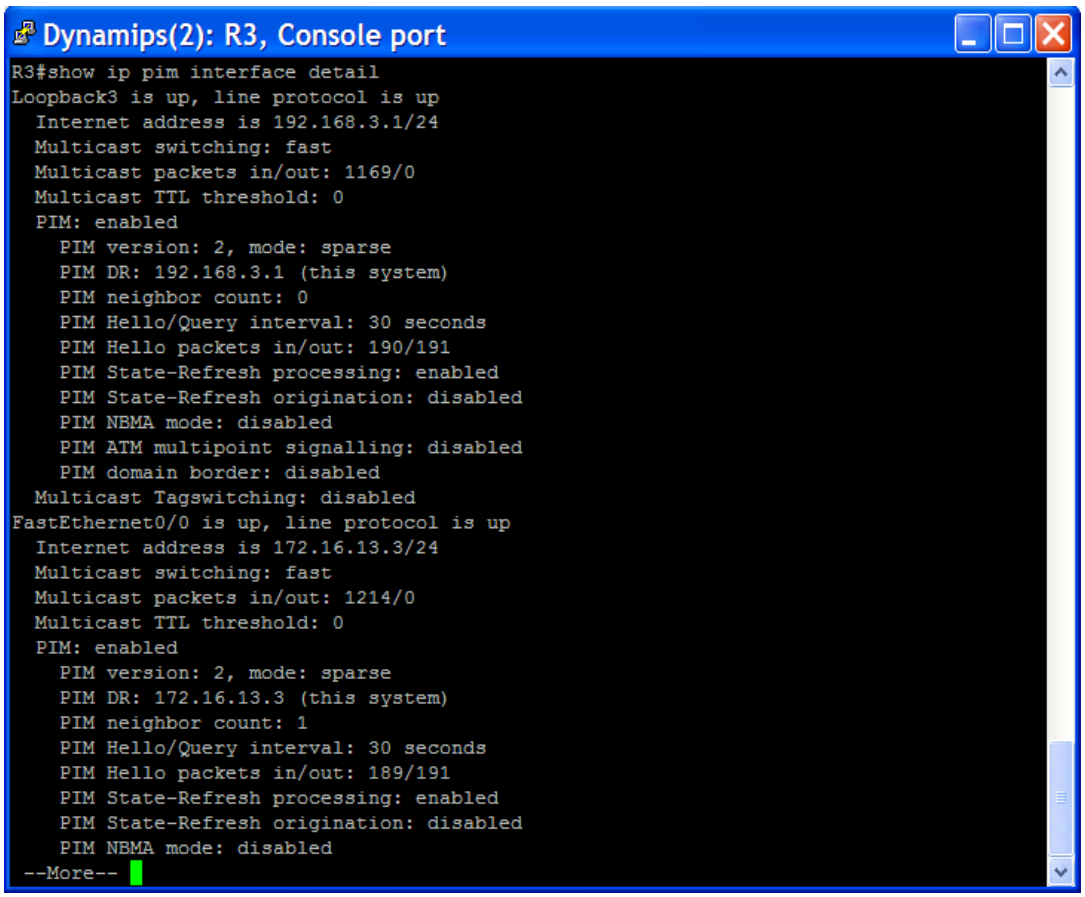
Fuente: Software GNS3.

Figura 293. Comando show ip pim interface en R3



Fuente: Software GNS3.

Figura 294. Comando show ip pim interface detail en R3



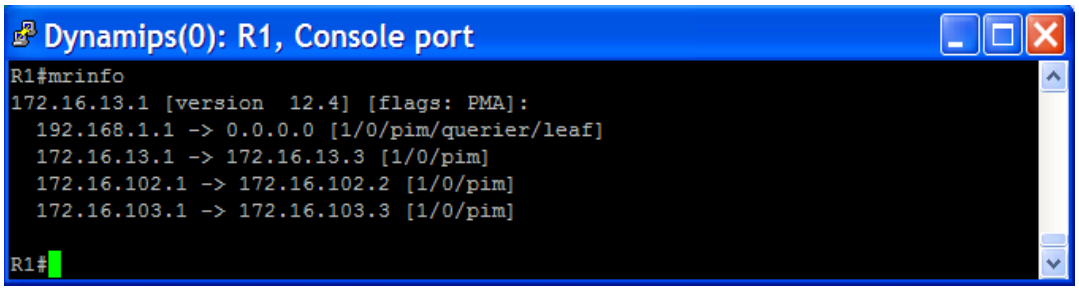
Fuente: Software GNS3.

De las figuras anteriores se puede determinar que las interfaces seriales usan la dirección DR por defecto 0.0.0.0 como el DR para la interfaz. Debido a que multicast es recibido ya sea por 0 ó 1 routers remotos en un segmento serial, PIM no necesita establecer una relación compleja con el vecino. La columna *Ver/Mode* muestra la versión PIM y el modo de ejcución en cada interfaz. ***S*** hace referencia a modo esparcido (**S**parse mode). ***D*** es usado para modo denso (***D****ense mode)* y ***SD*** indica el modo híbrido esparcido-denso (***S****parse* - ***D****ense mode.)*

Funcionamiento del enrutamiento multicast

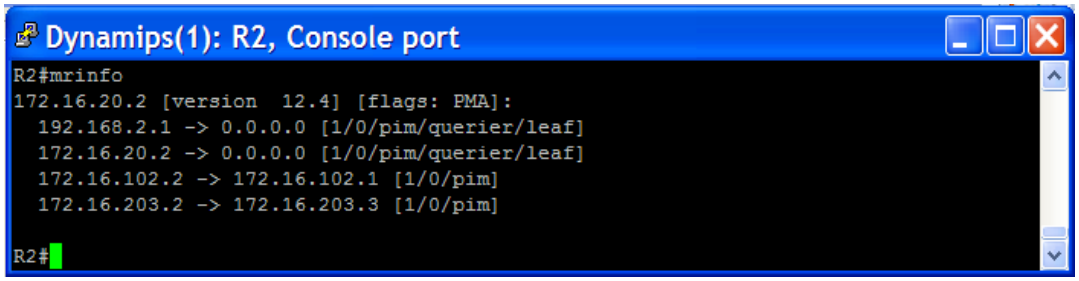
Para visualizar información sobre los routers multicast conectados y habilitados se usa el comando **mrinfo**.

Figura 295. Routers multicast conectados en R1



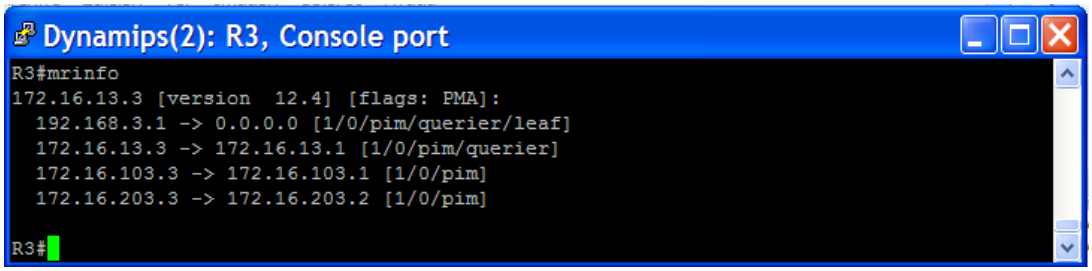
Fuente: Software GNS3.

Figura 296. Routers multicast conectados en R2



Fuente: Software GNS3.

Figura 297. Routers multicast conectados en R3



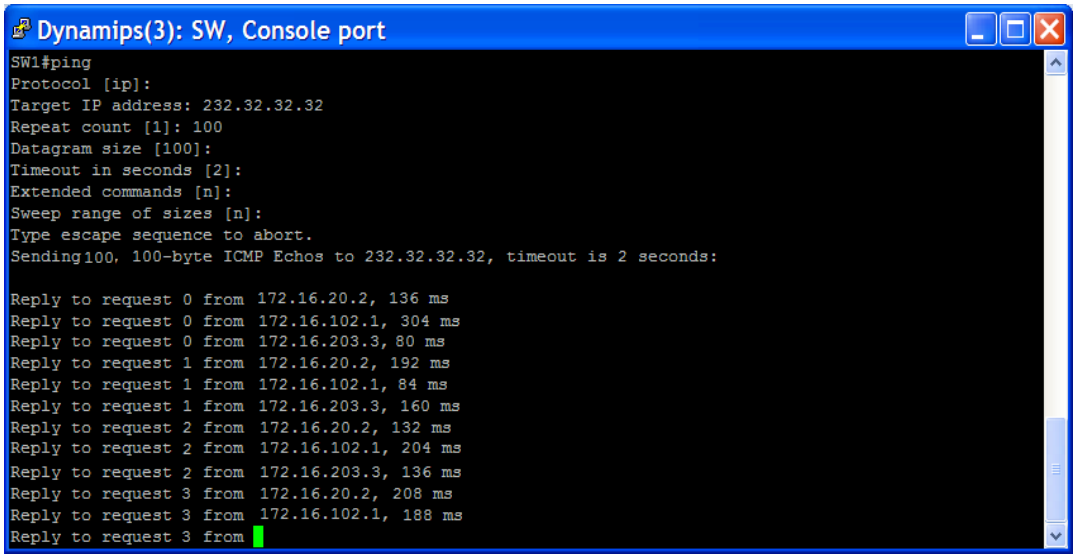
Fuente: Software GNS3.

Cada router nota que las interfaces loopback son *"hojas topológicas"* en las cuales PIM nunca establecerá una adyacencia con ningún otro router. Estos routers también registran direcciones de routers multicast vecinos y protocolos de enrutamiento que ellos utilizan.

Como se discutió en el paso anterior, IGMPv1 requiere el protocolo de enrutamiento mulitcast para elegir un *querier* en una red multiacceso. Para el ejemplo actual el *querier* en la VLAN 13 (sub red 172.16.13.0/24) es la interfaz FastEthernet 0/0 de R1 (con dirección IP 172.16.13.1).

Para probar conectividad, se genera un flujo de datos multicast al grupo por medio de un ping extendido desde SW1 con un contador de 100 repeticiones.

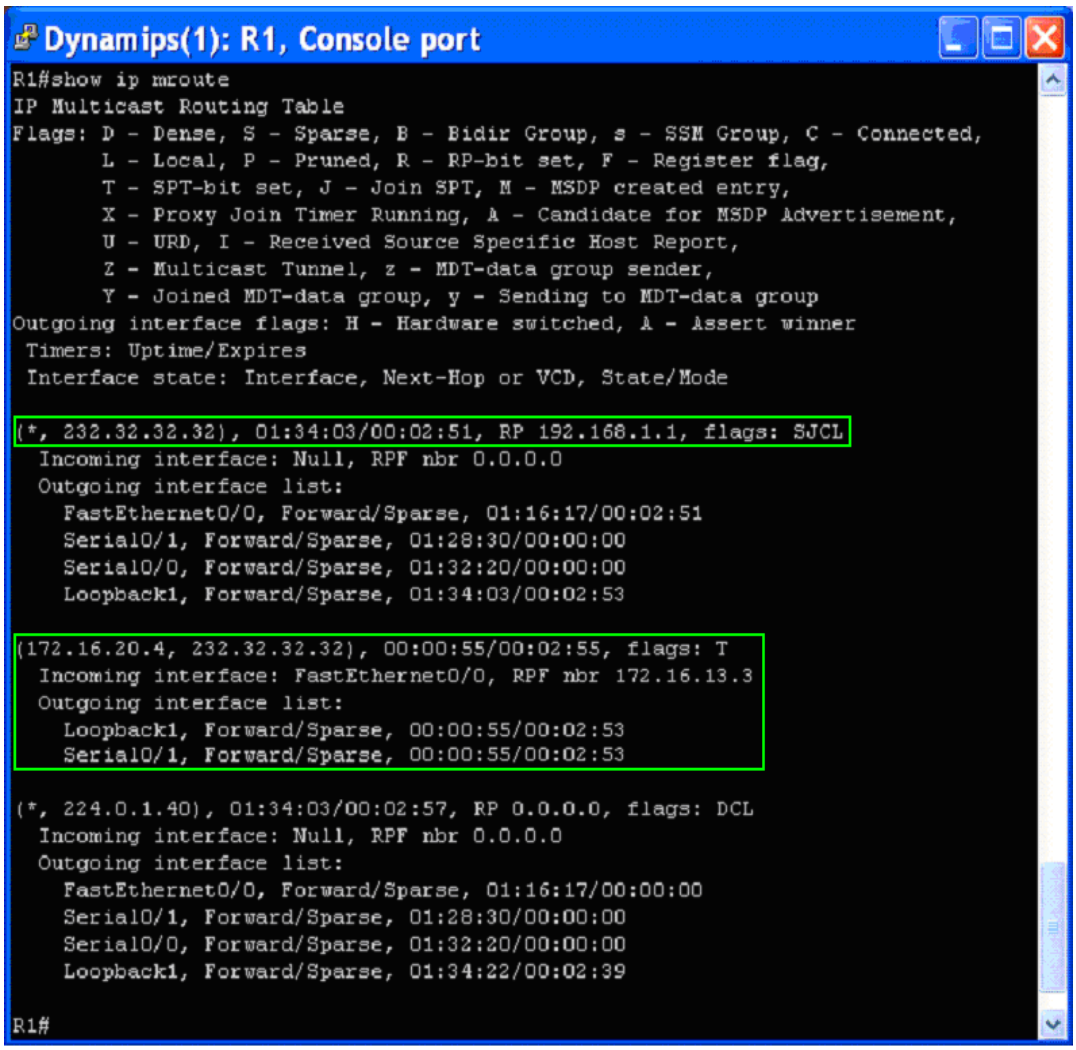
Figura 298. Ping extendido en el switch SW1



Fuente: Software GNS3.

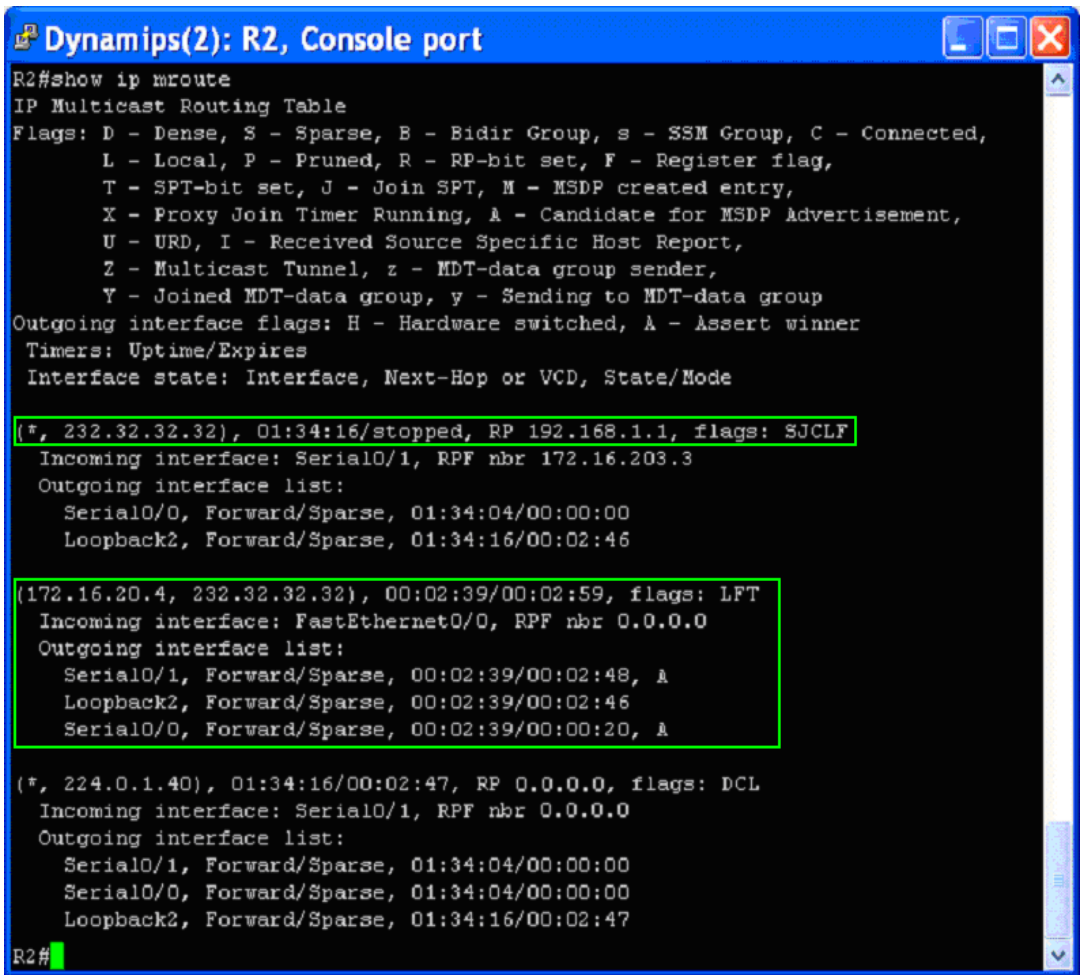
En cada uno de los routers, se debe ver que PIM e IGMP se han comunicado para instalar el gupo multicast 232.32.32.32 en la tabla de enrutamiento multicast. Esto se verifica con el comando **show ip mroute** en cada router.

Figura 299. Tabla de enrutamiento en el router R1



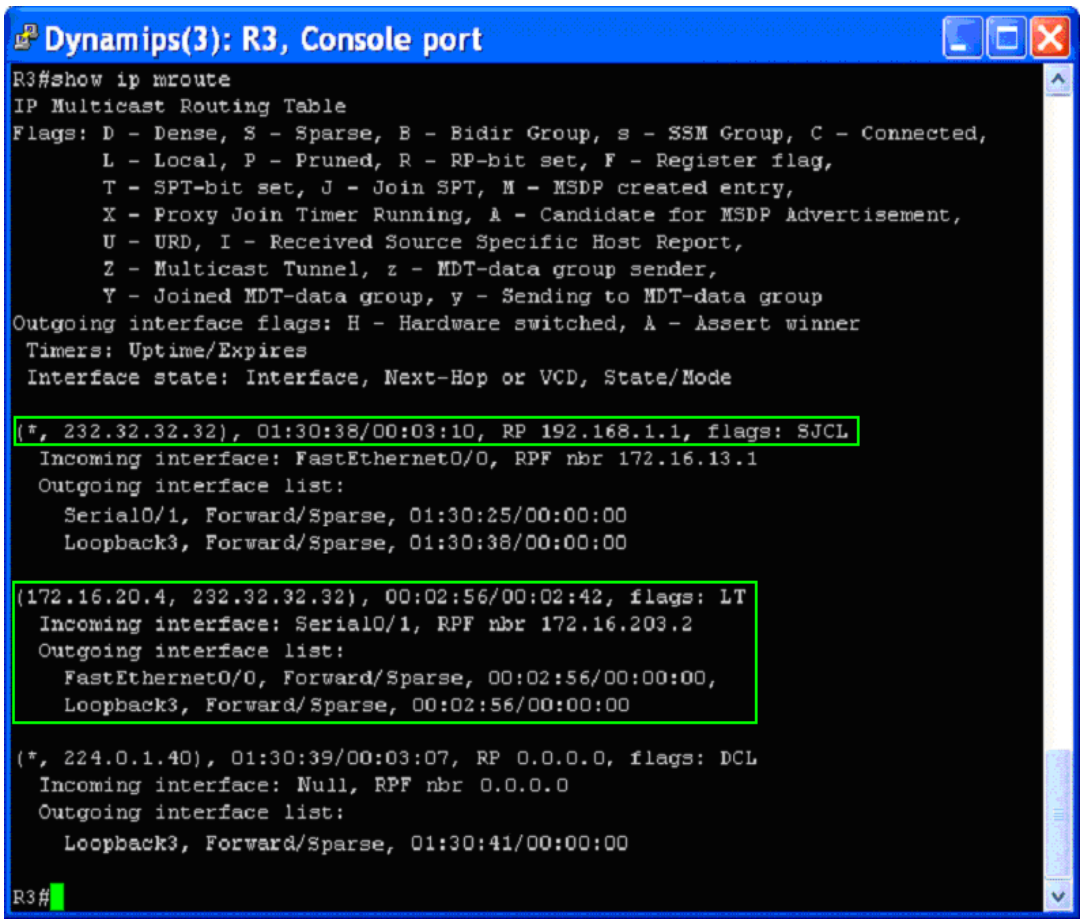
Fuente: Software GNS3.

Figura 300. Tabla de enrutamiento en el router R2



Fuente: Software GNS3.

Figura 301. Tabla de enrutamiento IP multicast de R3



Fuente: Software GNS3.

El estado de envío multicast se refiere al conjunto actual de entradas (S, G) y (*, G) en la tabla de enrutamiento multicast. En general “estado” es definido como un conjunto de propiedades almacenadas en un tiempo dado. En tablas unicast, el estado para una red destino es la ruta a esa red. Una ruta IP unicast es esencialmente almacenada en una tabla de enrutamiento unicast como una dirección y máscara de red destino junto con la información de enrutamiento del siguiente salto.

Las tablas de enrutamiento multicast contienen más información significativa que las tablas de enrutamiento unicast debido a que las tablas de enrutamiento multicast deben explorar muchas variables basadas en el tiempo tanto para fuentes como para miembros del grupo.

Por ejemplo, un router multicast debe explorar el tiempo cuando el último paquete es recibido de una fuente, la lista de interfaces de salida (*Outgoing interface list)* y los vecinos RPF para cada fuente y árbol compartido que mantiene. Estas variables no son almacenadas en una tabla de topología PIM pero si en una tabla de enrutamiento multicast nativa**.** El estado de enrutamiento multicast está sujeto a cambios rápidos basados en los registros de fuentes y suscripciones de grupo.

En PIM-DM, la tabla de enrutamiento multicast indica si las interfaces PIM son negociadas para inundar (*flood*) datos multicast a ese grupo o podar *(prune)* (S,G) tráfico multicast de ser enviado a esa interfaz.

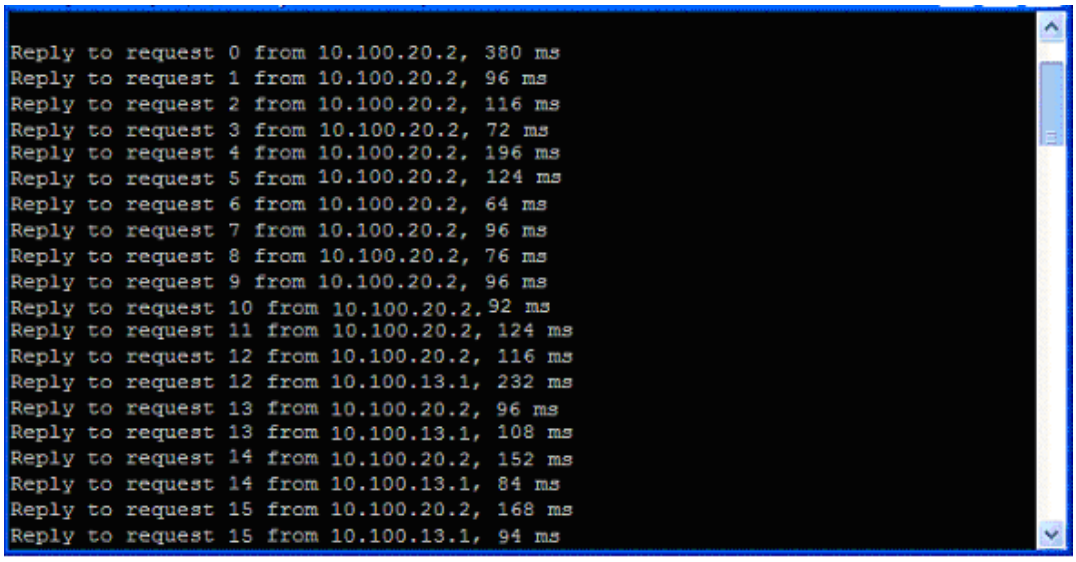
En las tablas multicast generadas anteriormente, se nota que PIM-SM no se refiere a interfaces como podadas.

Cuando un router PIM-SM recibe un mensaje *join* explícito de IGMP en una interfaz, adiciona la interfaz a la lista de interfaces de salida del árbol basado en el origen (*source-based*). El árbol basado en el origen es también conocido como el árbol del camino más corto y es representado en la tabla de enrutamiento por una entrada (S, G). Ya que PIM-SM es un servicio multicast basado en registro, éste simplemente elimina de la lista las interfaces a las cuales no necesita enviar datos.

Verificación del registro de PIM-SM y cambio de RPT a SPT

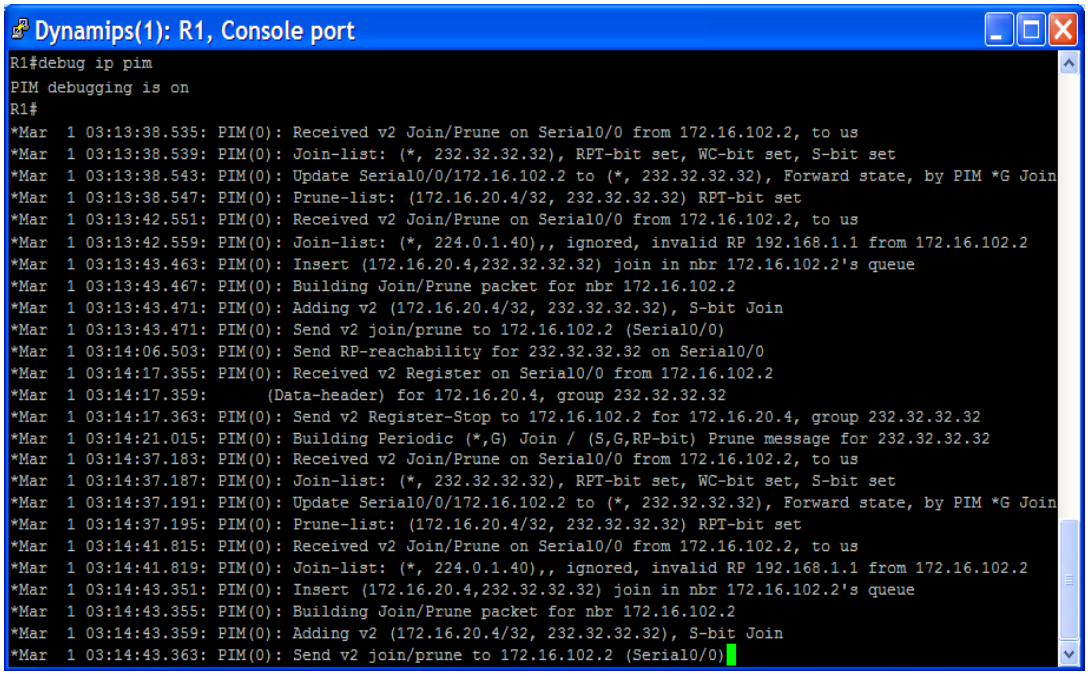
Para conocer cómo se registran las fuentes con el RP y explorar la poda de datos desde el árbol compartido y la transición al árbol fuente, se espera que se complete el *stream* muticast desde 172.16.20.4 y el estado (S, G) en las tablas de enrutamiento multicast a expirar y después se ingresan los comandos **debug ip igmp** y **debug ip pim** en todos los routers.

Figura 302. Comando debug ip igmp en el router R1



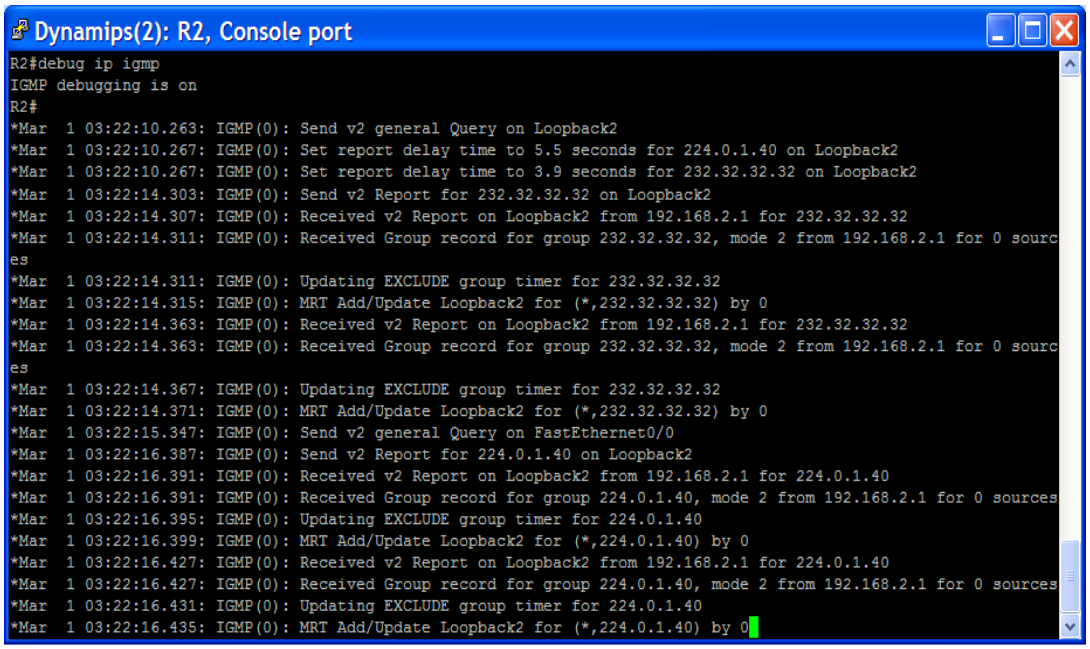
Fuente: Software GNS3.

Figura 303. Comando debug ip pim en el router R1



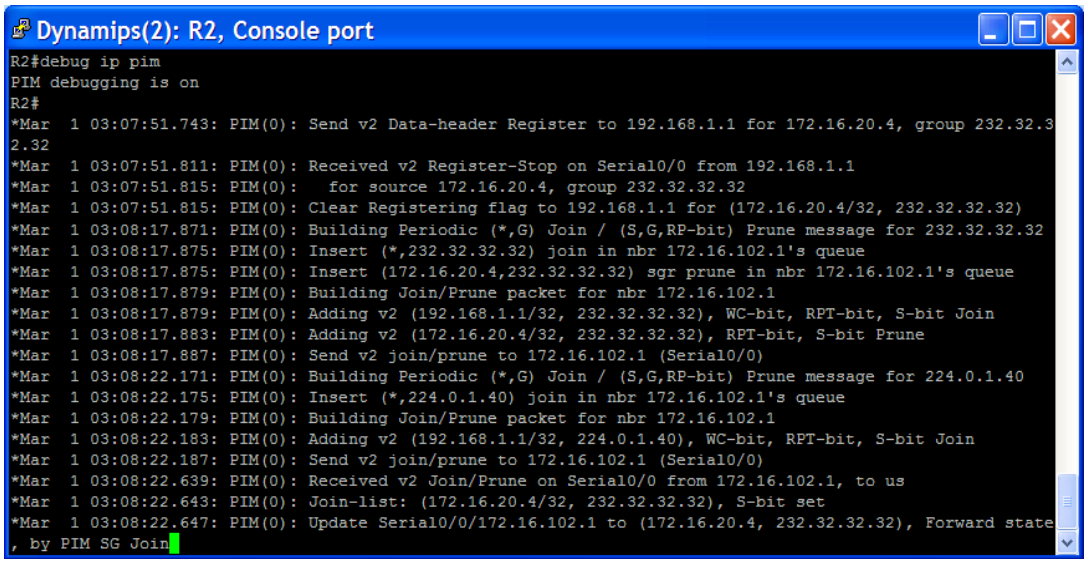
Fuente: Software GNS3.

Figura 304. Comando debug ip igmp en el router R2



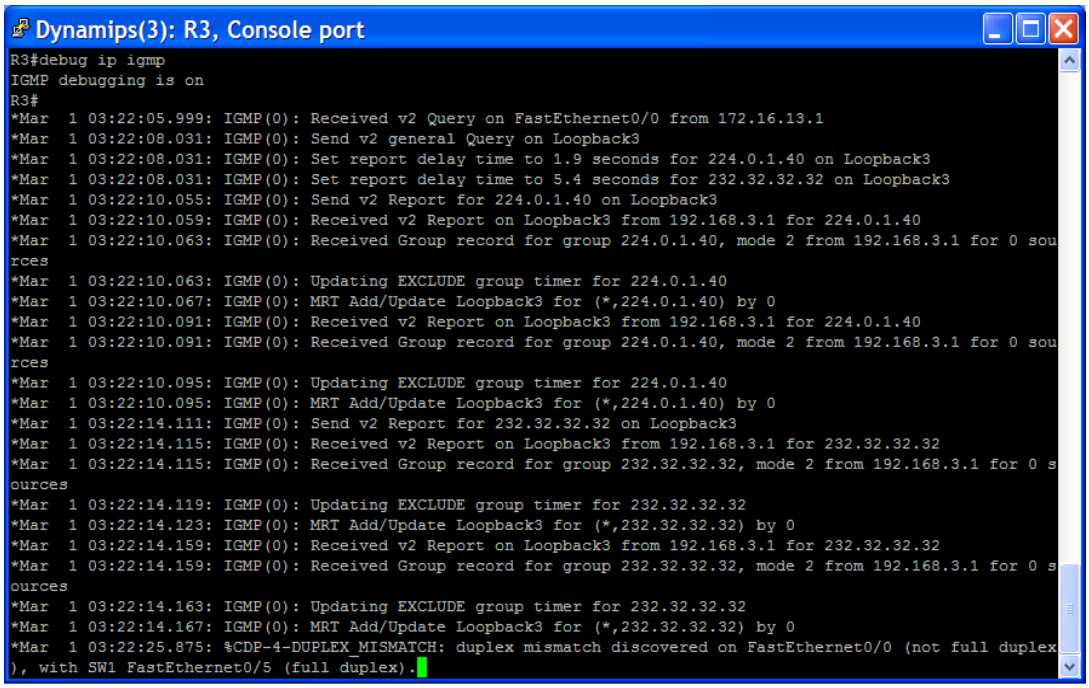
Fuente: Software GNS3.

Figura 305. Comando debug ip pim en el router R2



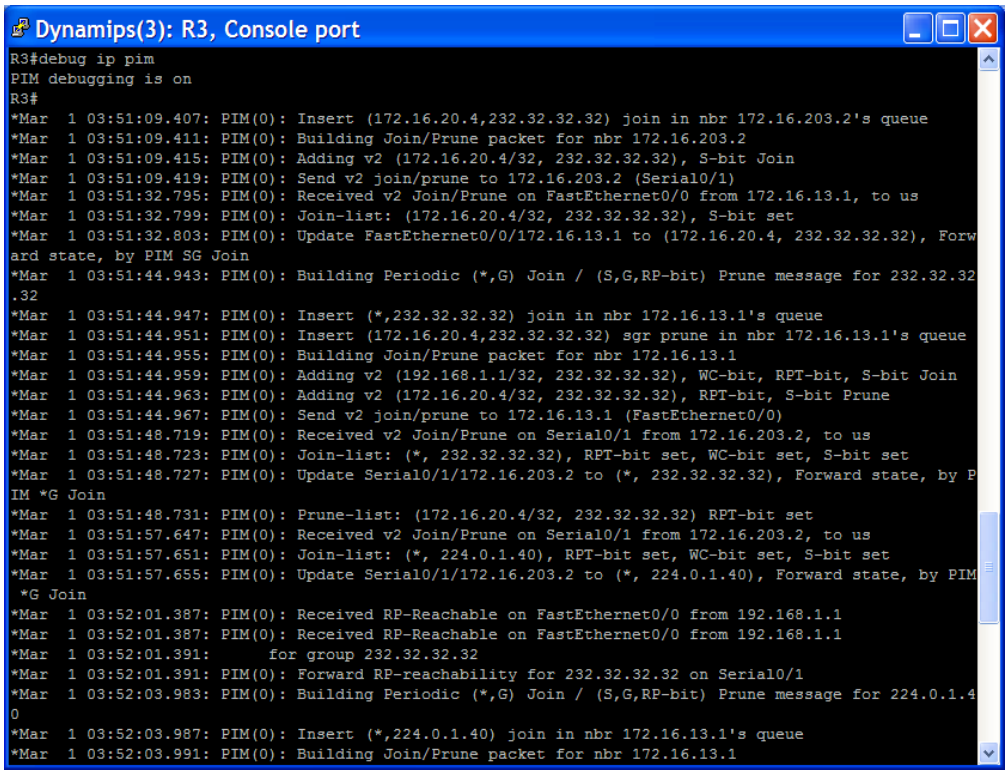
Fuente: Software GNS3.

Figura 306. Comando debug ip igmp en el router R3



Fuente: Software GNS3.

Figura 307. Comando debug ip pim en el router R3

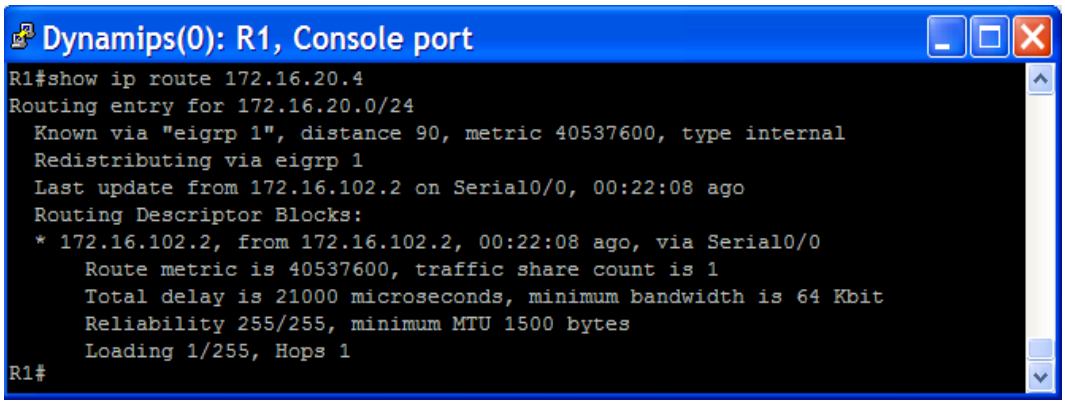


Fuente: Software GNS3.

PIM se basa en la tabla de enrutamiento unicast para construir árboles de camino más corto desde las fuentes a los suscriptores multicast. Las interfaces PIM envían mensajes de control para determinar cuál vecino es más cercano a la fuente en términos de información de enrutamiento multicast en cada vecino. Los vecinos PIM-SM eligen un router particular en la subred como el *forwarder* para esa pareja (S, G) y después podan esa pareja (S, G) de ser reenviada por cualquier otro router en la subred.

A continuación se muestra la tabla de enrutamiento unicast en cada router para 172.16.20.4.

Figura 308. Tabla de enrutamiento unicast para 172.16.20.4 en R1

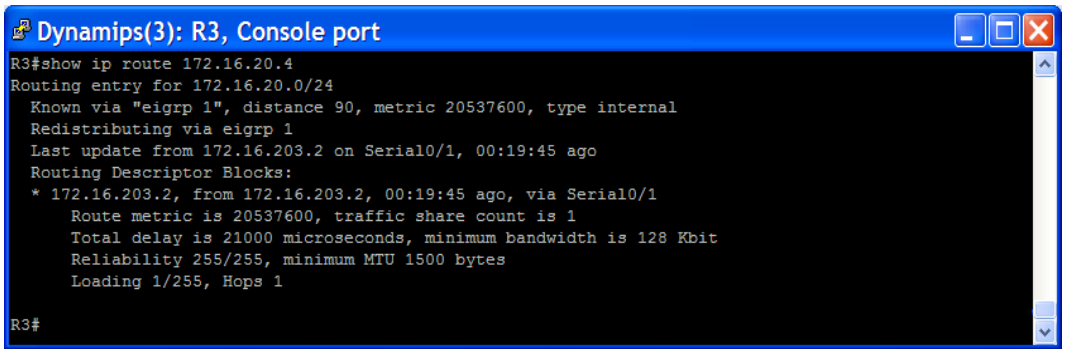


Fuente: Software GNS3.

Figura 309. Tabla de enrutamiento unicast para 172.16.20.4 en R2

Fuente: Software GNS3.

Figura 310. Tabla de enrutamiento unicast para 172.16.20.4 en R3



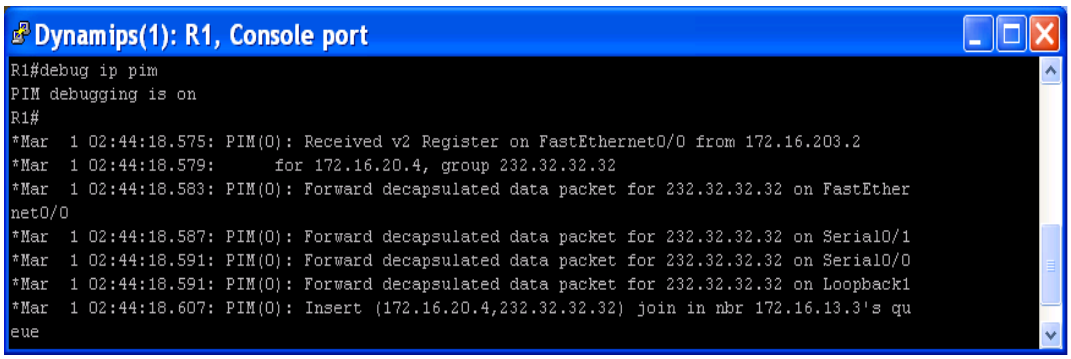
Fuente: Software GNS3.

De acuerdo a las salidas anteriores se puede concluir que:

- La interfaz Loopback1 de R1 recibirá datos de la interfaz serial 0/0 de R2 (172.16.102.2).
- PIM enviará tráfico directamente a la loopback2 de R2 (172.16.20.4, 172.16.13.3)
- La interfaz loopback 3 deR3 recibirá datos de la interfaz serial0/1 de R2 (172.16.203.2)

A continuación se realizará un ping extendido en SW1 al grupo multicast y se examinarán los mensajes de depuración mostrados en R1.

Figura 311. Depuración ip pim en el router R1. Parte 1

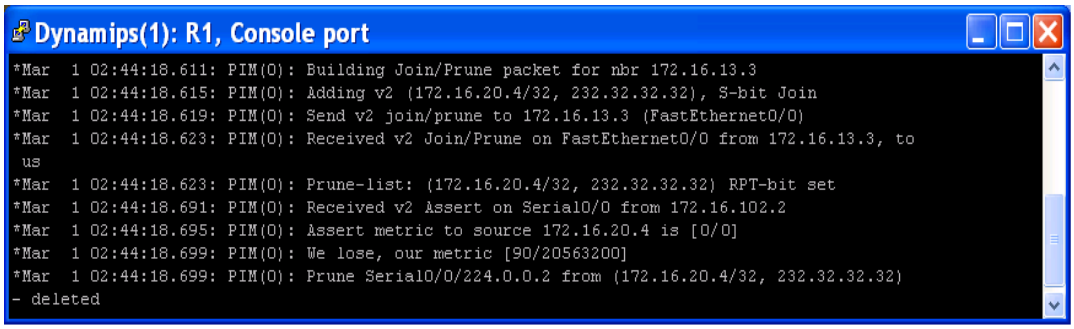


Fuente: Software GNS3.

Inicialmente, R2 comienza encapsulando paquetes multicast desde 172.16.20.4 en paquetes de registros unicast PIMv2 y envía esos mensajes unicast al RP. Este paquete es enviado a través el camino más corto de R2 a 192.168.1.1 y recibido en la interfaz FastEthernet0/0 de R1.

El RP envía un mensaje PIM al vecino *downstream* en el árbol compartido que le indica a R3 que registre el estado (172.16.20.4, 232.32.32.32) en su tabla de enrutamiento multicast. R1 después envía los paquetes multicast que se han descapsulado a 232.32.32.32.

Figura 312. Depuración ip pim en el router R1. Parte 2



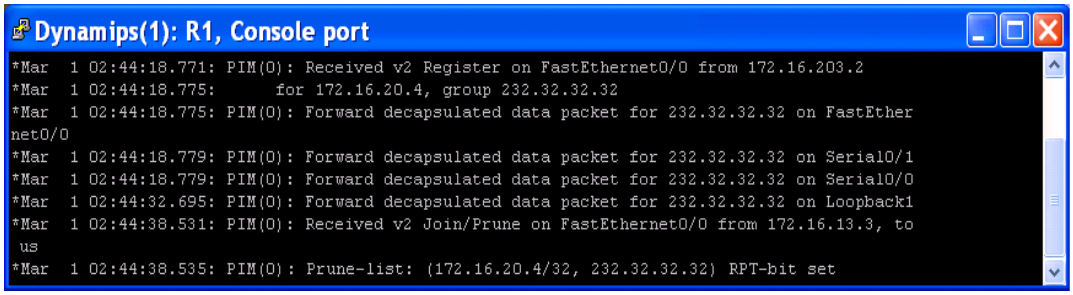
Fuente: Software GNS3.

Como la interfaz Loopback 1 recibió el primer paquete multicast de SW1, R1 cambia de RPT a SPT. R1 construye y envía un paquete *join* para R3 porque R3 es su vecino RPF para la fuente 172.16.20.4. Tan pronto como los routers PIM acumulan estado acerca del par (S, G), ellos pueden comenzar a cambiar del árbol compartido al árbol basado en el origen.

Por defecto, cuando un router PIM con un nodo multicast recibe el primer paquete desde una fuente a un grupo a través del árbol compartido, éste cambia al árbol de camino más corto (SPT). Esto también se puede configurar manualmente como un umbral de ancho de banda usando el comando **ip pim spt-threshold.** Cuando el flujo (S, G) alcanza el umbral del ancho de banda (en Kbps), el router PIM cambia a SPT. El proceso de cambio es iniciado en R2 y R3 por el primer paquete multicast

(172.16.20.4, 232.32.32.32). R1 y R2 comparan distancias administrativas y métricas respecto a sus caminos más cortos a la fuente y R2, el ganador, envía un mensaje de poda a R1 indicando que éste no debería enviar tráfico a la serial 0/0 para el grupo 232.32.32.32. El proceso de estado SPT de R2 se completa.

Figura 313. Depuración ip pim en el router R1. Parte 3

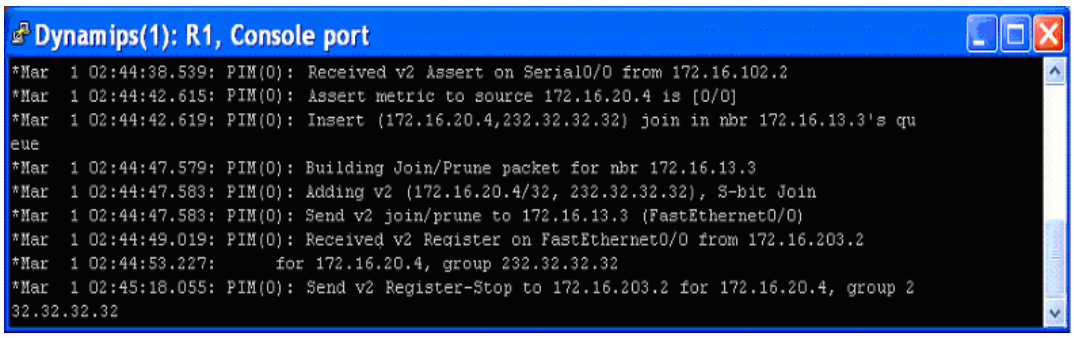


Fuente: Software GNS3.

R2 continúa encapsulando datos multicast en paquetes unicast y enviándolos al RP por medio de R3.

Como todos los receptores multicast han obtenido el estado (S, G) a través de SPT para (172.16.20.4, 232.32.32.32), R3 decide que no necesita a R1 para continuar enviando este tráfico a través del árbol compartido. R3 envía un mensaje de poda a R1 por medio de la interfaz FastEthernet.

Figura 314. Depuración ip pim en el router R1. Parte 4



Fuente: Software GNS3.

Los primeros dos mensajes indican que R2 envía un mensaje *Assert* periódico en el enlace serial entre ellos. Los mensajes *Insert, Building, Adding y Send* muestran a R1 actuando como un router standard multicast y enviando un mensaje *join* a su vecino SPT *upstream* el cual requiere que el tráfico (S, G) continúe.

R2 envía otro paquete *Register* al RP con un paquete multicast encapsulado. R1, actuando como el RP, revisa la tabla de enrutamiento para interfaces de salida en el árbol compartido. Como todas las ramas descendentes del árbol compartido han sido podadas, indicando que R2 y R3 han pasado al SPT, R1 envía un mensaje *Register-Stop* a R2 indicándole que detenga el reenvio de paquetes al RP.

En este punto, todos los routers multicast están escuchando directamente a la fuente por medio del camino más corto a 172.16.20.4 y los receptores actuales no necesitan al RP ni al árbol compartido debido a que ellos están escuchando directamente a la fuente por medio del SPT. Es común que el router que actúa como RP aún sea una parte del SPT, como sucede en este caso, debido a que la interfaz loopback1 de R1 suscribe al grupo 232.32.32.32. Sin embargo, R1 está actuando simplemente como un suscriptor al grupo y no como el RP.

Inicialmente R2 encapsula los datos multicast en un paquete unicast ya que R2 no puede permitir el tráfico directamente dentro de una red

multicast o PIM-SM se degradaría a PIM-DM. El tráfico primero necesita ser enviado al RP en el que otros routers han fijado sus árboles compartidos. El tráfico será enviado hacia abajo del árbol compartido hasta que todas las fuentes hayan cambiado al árbol basado en el origen. Para enviar tráfico al RP sin enviarlo a través de la red multicast (de esta forma crea estado multicast), PIM-SM envía los datos como un unicast al RP.

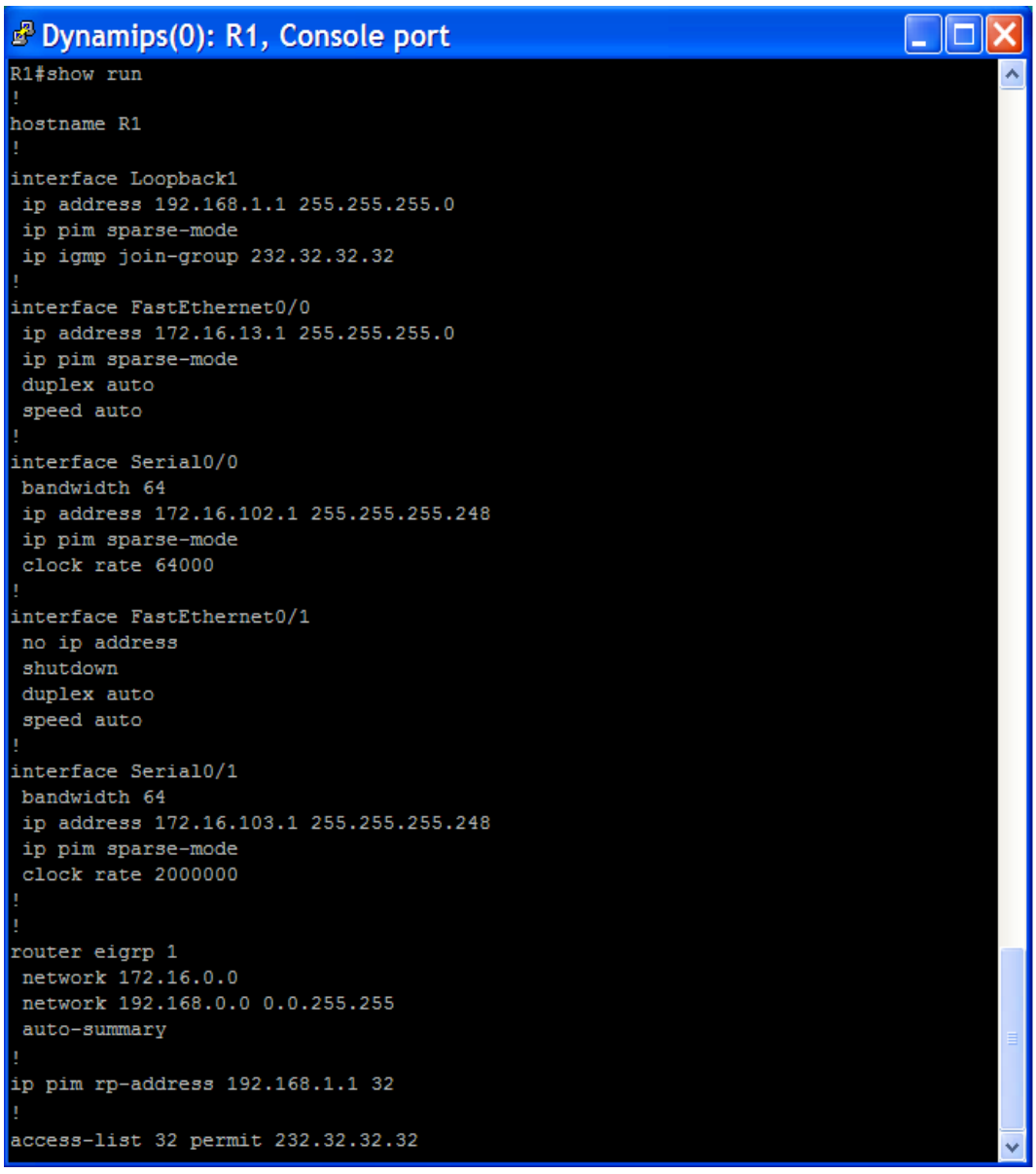
De las pantallas anteriores pordemos concluir que cuando los datos multicast alcanzan el RP, los paquetes unicast son desencapsulados y los paquetes son enviados como multicast hacia abajo del árbol compartido.

Si R2 solo reenviara los datos a todos los receptors conectados usando paquetes multicast, la red PIM-SM se degradaría a PIM-DM.

Configuración Final

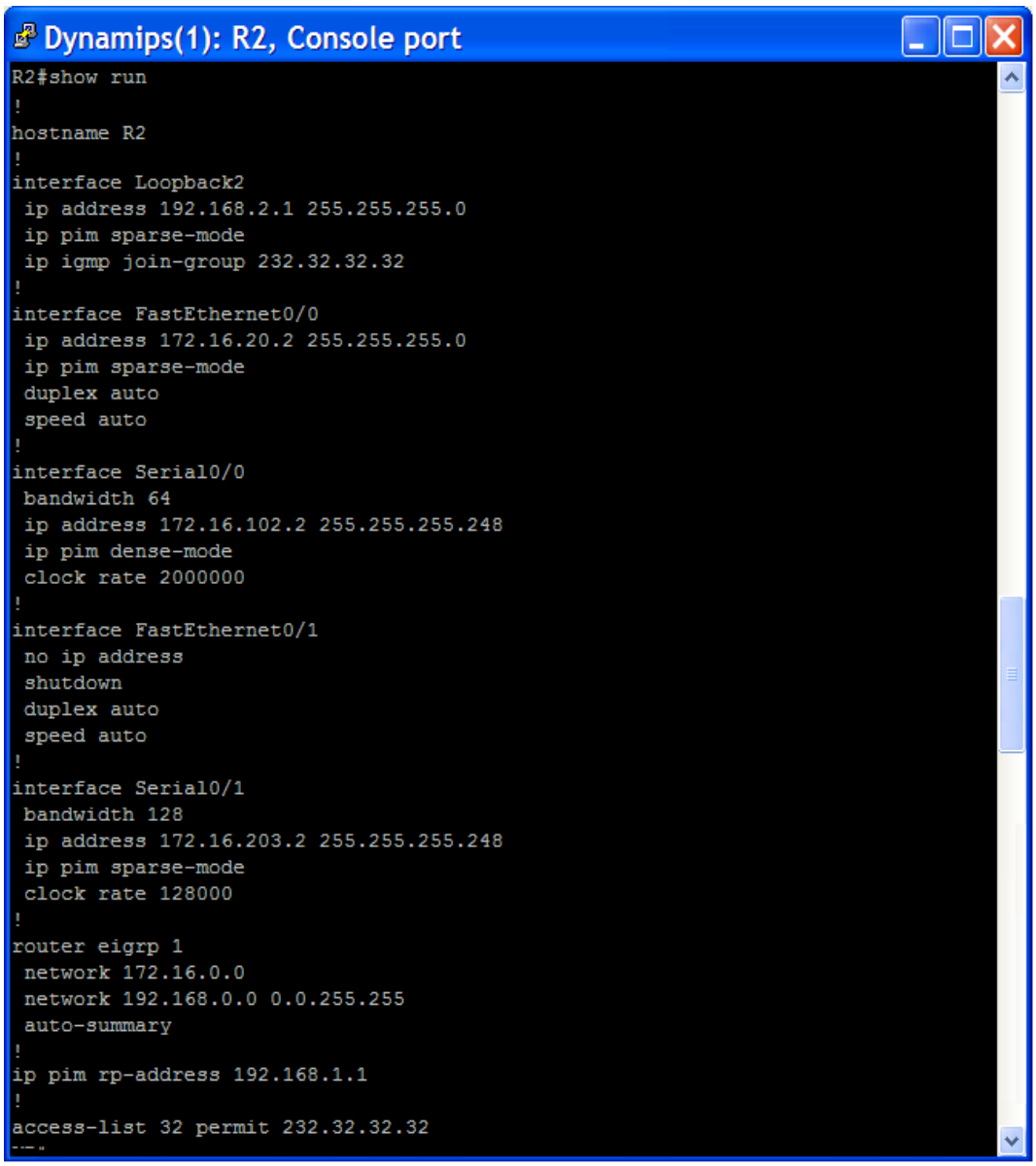
Finalmente se verifica la configuración final de las interfaces en todos los dispositivos con el comando **show run** como se muestra a continuación.

Figura 315. Configuración final de R1



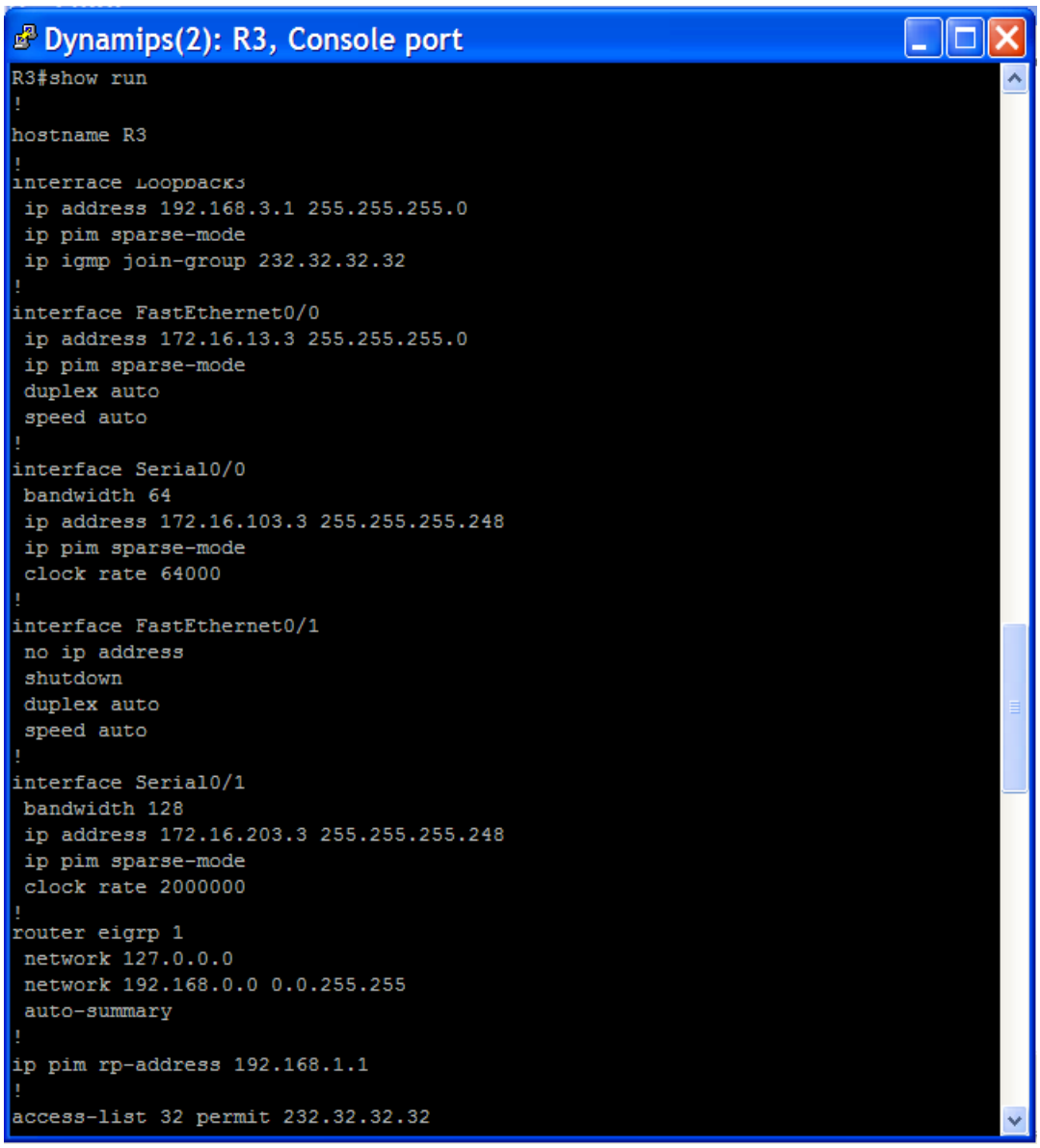
Fuente: Software GNS3.

Figura 316. Configuración final de R2



Fuente: Software GNS3.

Figura 317. Configuración final de R3



Fuente: Software GNS3.

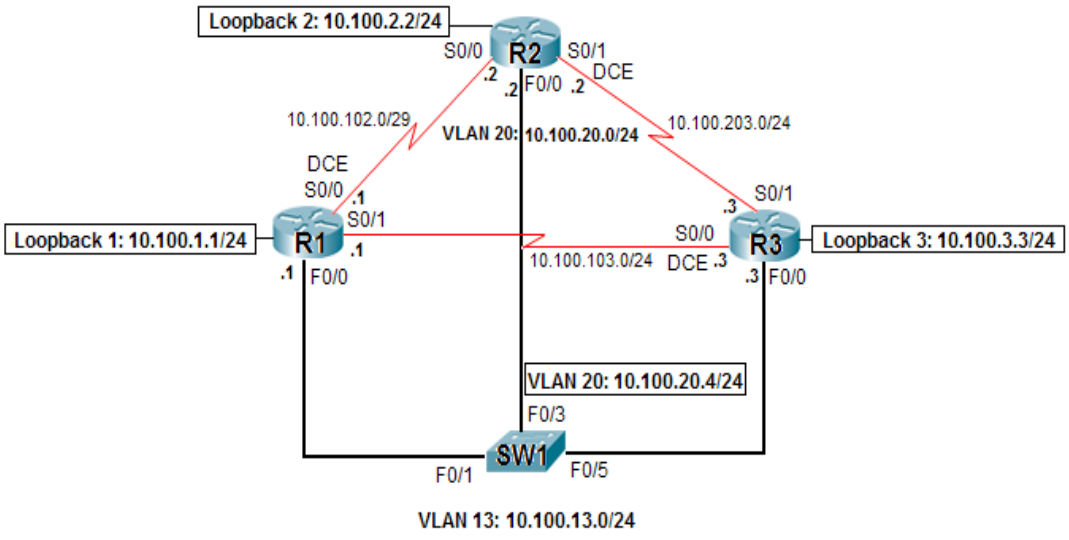
5.5. PIM-DSM

Planteamiento:

La empresa “X” comenzó a producir anuncios publicitarios de televisión para dar a conocer sus productos al público. Se requiere implementar multicast en la red de la empresa, de modo que la gerencia pueda previsualizar los anuncios antes de lanzarlos al público. Se requiere implementar PIM en una forma escalable y redundante, de tal forma que los receptores multicast en redes remotas reciban flujo multicast aún si el RP se pierde.

Diagrama:

Figura 318. Diagrama de práctica de la simulación PIM-SDM



Fuente: Autoras.

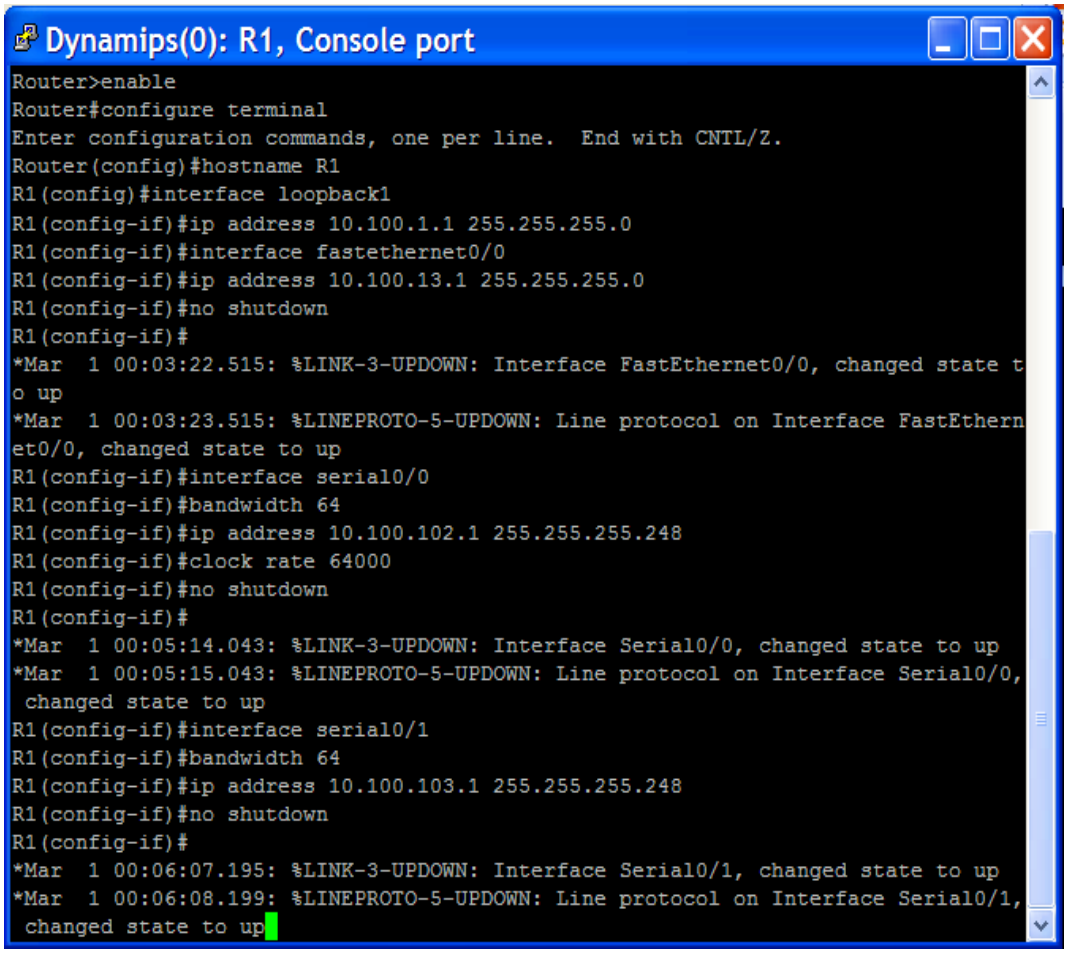
Solución:

A continuación se describen los pasos que se siguieron para realizar esta simulación. (El simulador utilizado para esta práctica fue GNS3).

Configuración de interfaces en los dispositivos y configuración IGMP

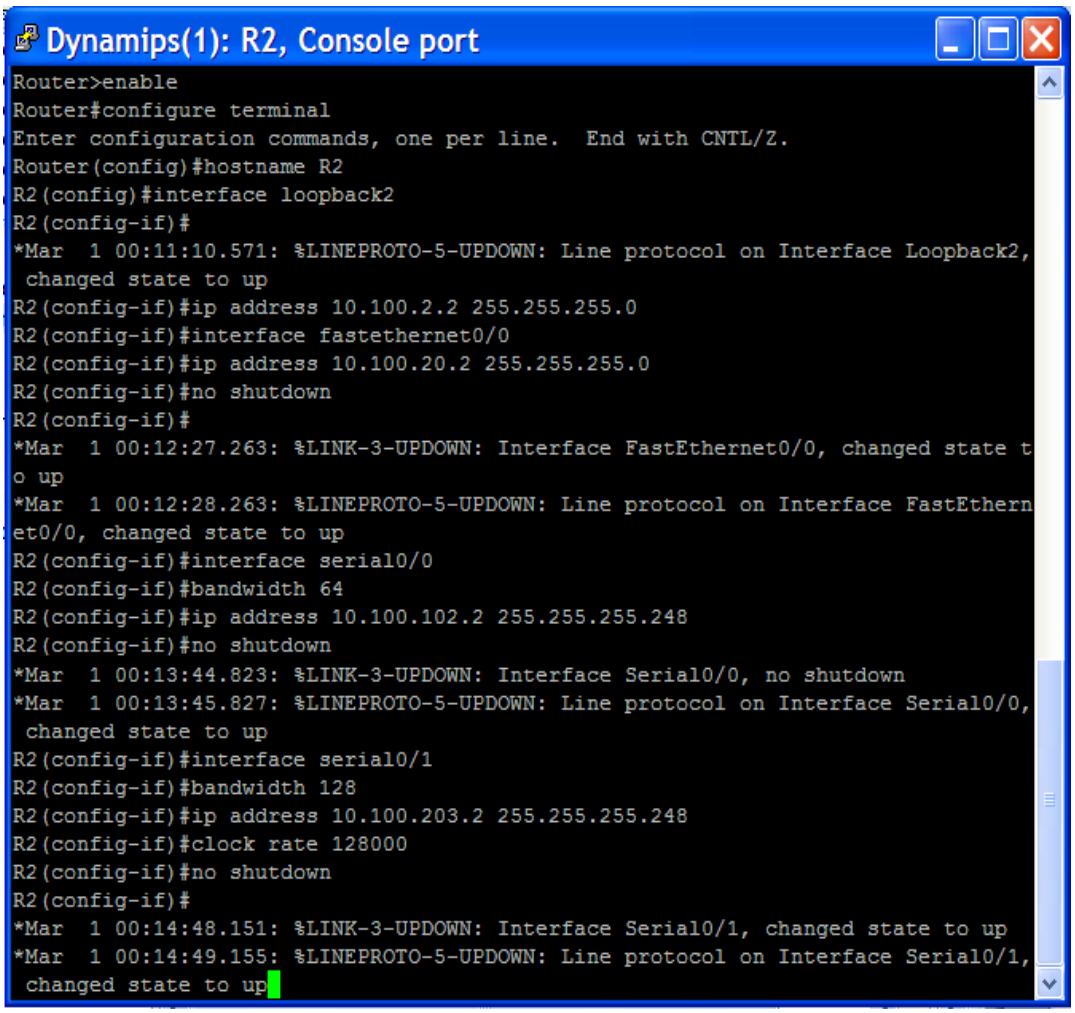
Inicialmente se realizan las configuraciones en los routers:

Figura 319. Configuración de las interfaces en el Router R1



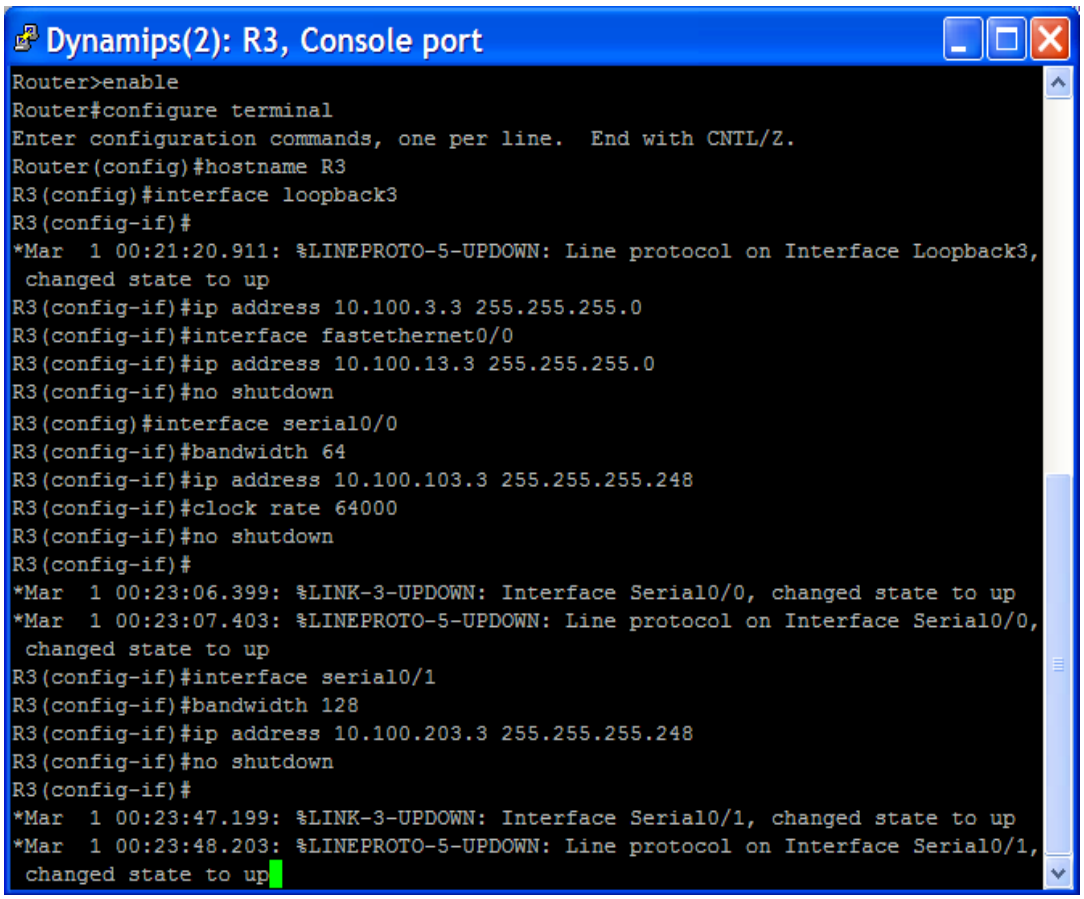
Fuente: Software GNS3.

Figura 320. Configuración de las interfaces en el Router R2



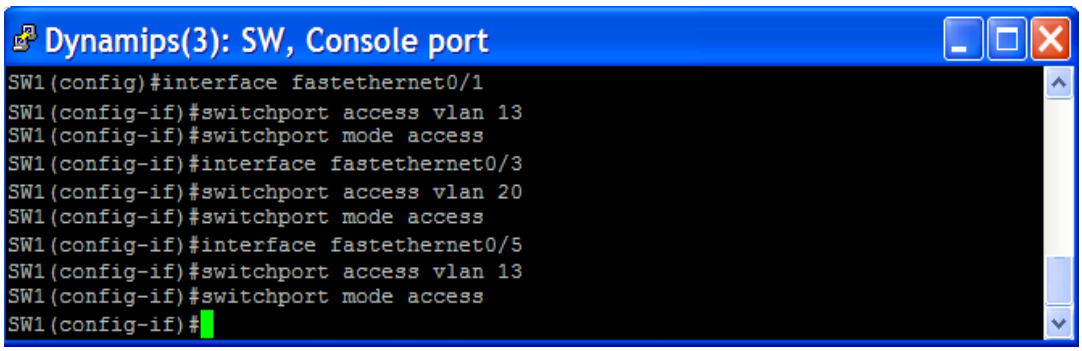
Fuente: Software GNS3.

Figura 321. Configuración de las interfaces en el Router R3



Fuente: Software GNS3.

Figura 322. Configuración de las VLAN en el Switch SW1.

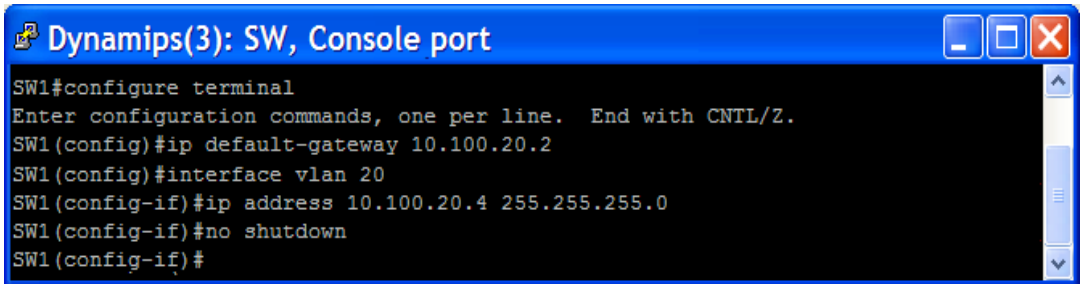


Fuente: Software GNS3.

Se utiliza una interfaz virtual conmutada (SVI: switched virtual interface) en el Switch SW1 para simular una fuente multicast en la subred VLAN20. Esta será utilizada para enviar un ping multicast repetido que simule tráfico multicast mientras se configura la red.

Se asigna la dirección IP 10.100.20.4/24 a SVI con una puerta de enlace por defecto de 10.100.20.2

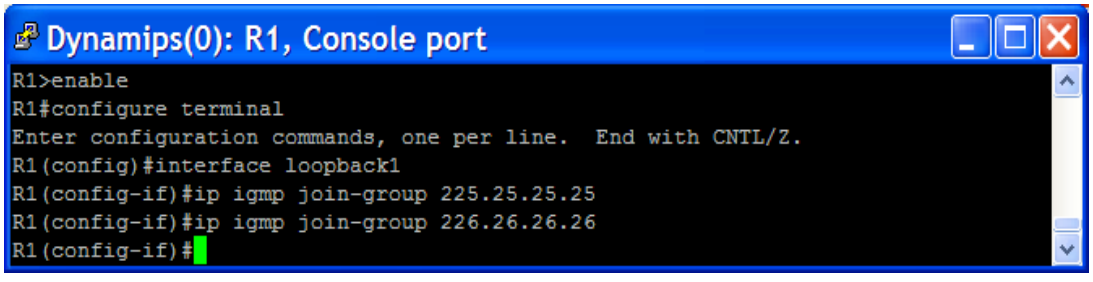
Figura 323. Configuración de SVI en el switch SW1



Fuente: Software GNS3.

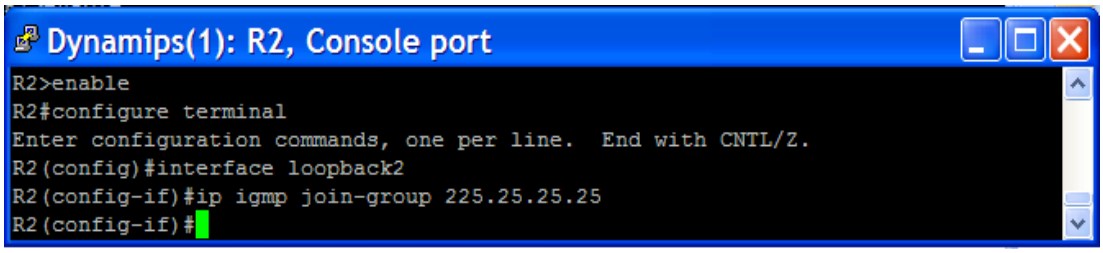
A continuación se utiliza IGMP para suscribir cada una de las interfaces loopback de los routers a los grupos multicast 225.25.25.25. Adicionalmente, se suscriben las loopbacks de R1 y R3 al grupo multicast 226.26.26.26.

Figura 324. Suscripción de loopback1 a grupos multicast en R1



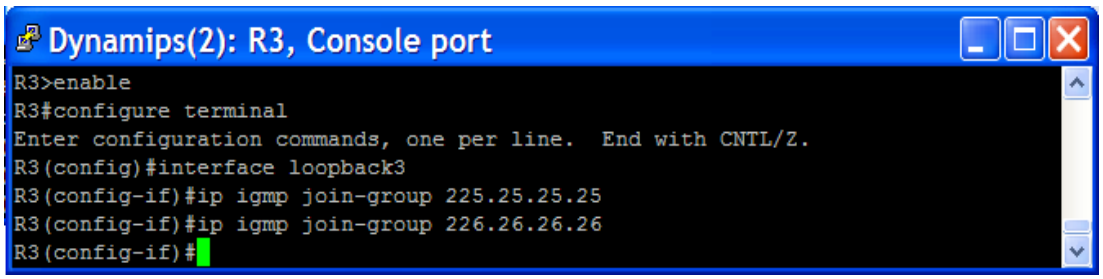
Fuente: Software GNS3.

Figura 325. Suscripción de loopback2 al grupo multicast en R2



Fuente: Software GNS3.

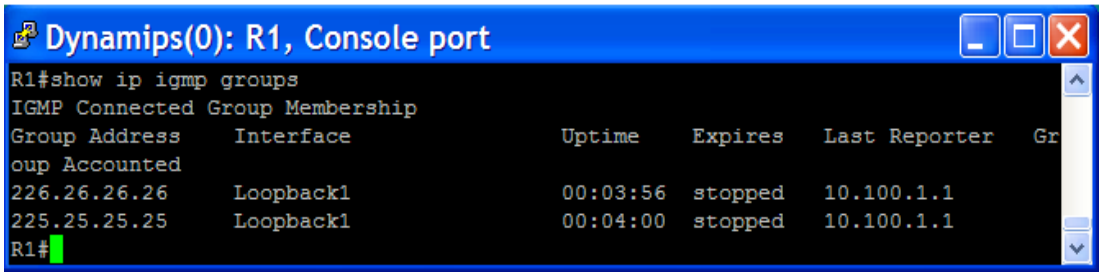
Figura 326. Suscripción de loopback3 a grupos multicast en R3



Fuente: Software GNS3.

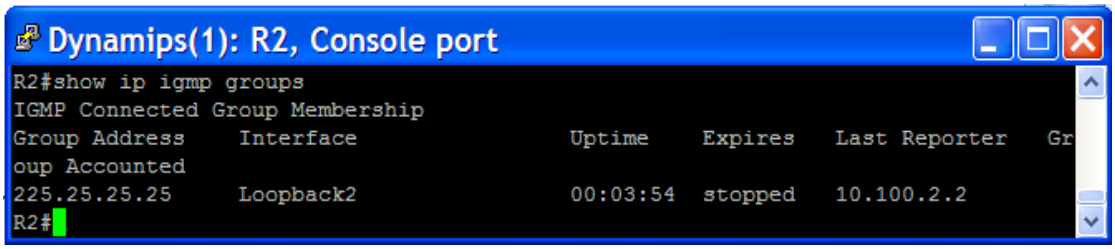
Para verificar que cada una de las interfaces se ha suscrito al grupo multicast se utiliza el comando **show ip igmp groups** en cada router.

Figura 327. Verificación de las interfaces suscritas al grupo multicast en R1



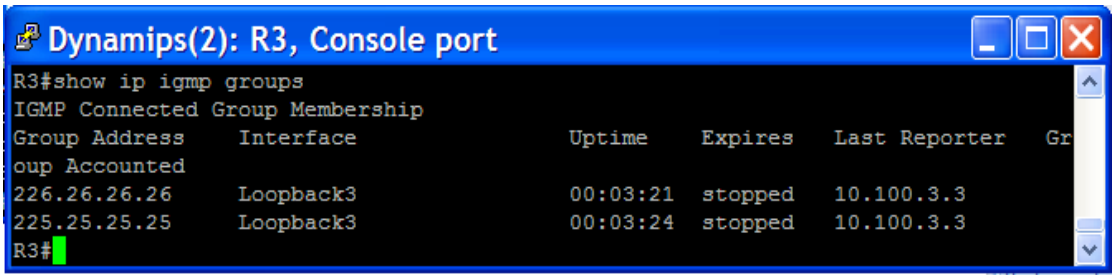
Fuente: Software GNS3.

Figura 328. Verificación de las interfaces suscritas al grupo multicast en R2



Fuente: Software GNS3.

Figura 329. Verificación de las interfaces suscritas al grupo multicast en R3

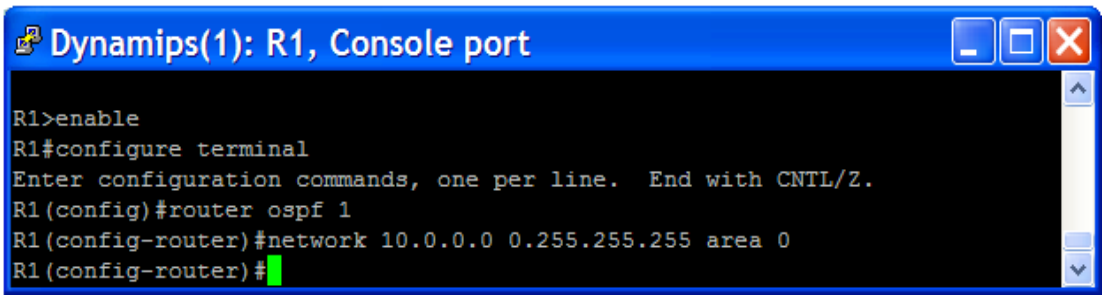


Fuente: Software GNS3.

Configuración OSPF

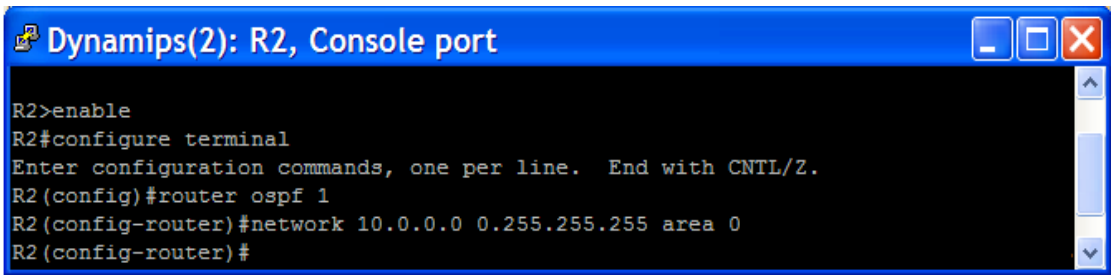
Se configura *OSPF* en cada router como se muestra a continuación:

Figura 330. Creación de un proceso OSPF en R1



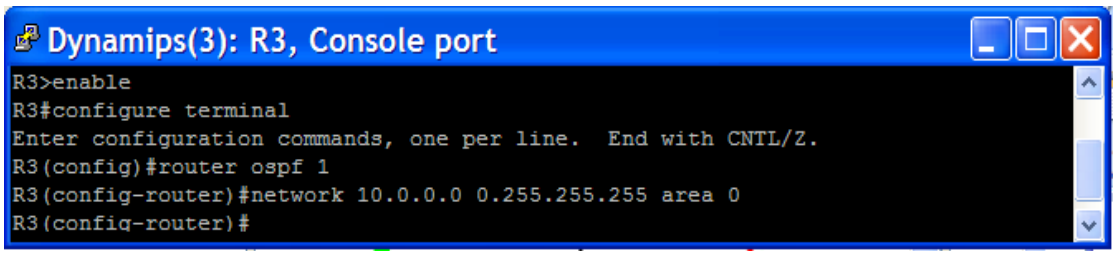
Fuente: Software GNS3.

Figura 331. Creación de un proceso OSPF en R2



Fuente: Software GNS3.

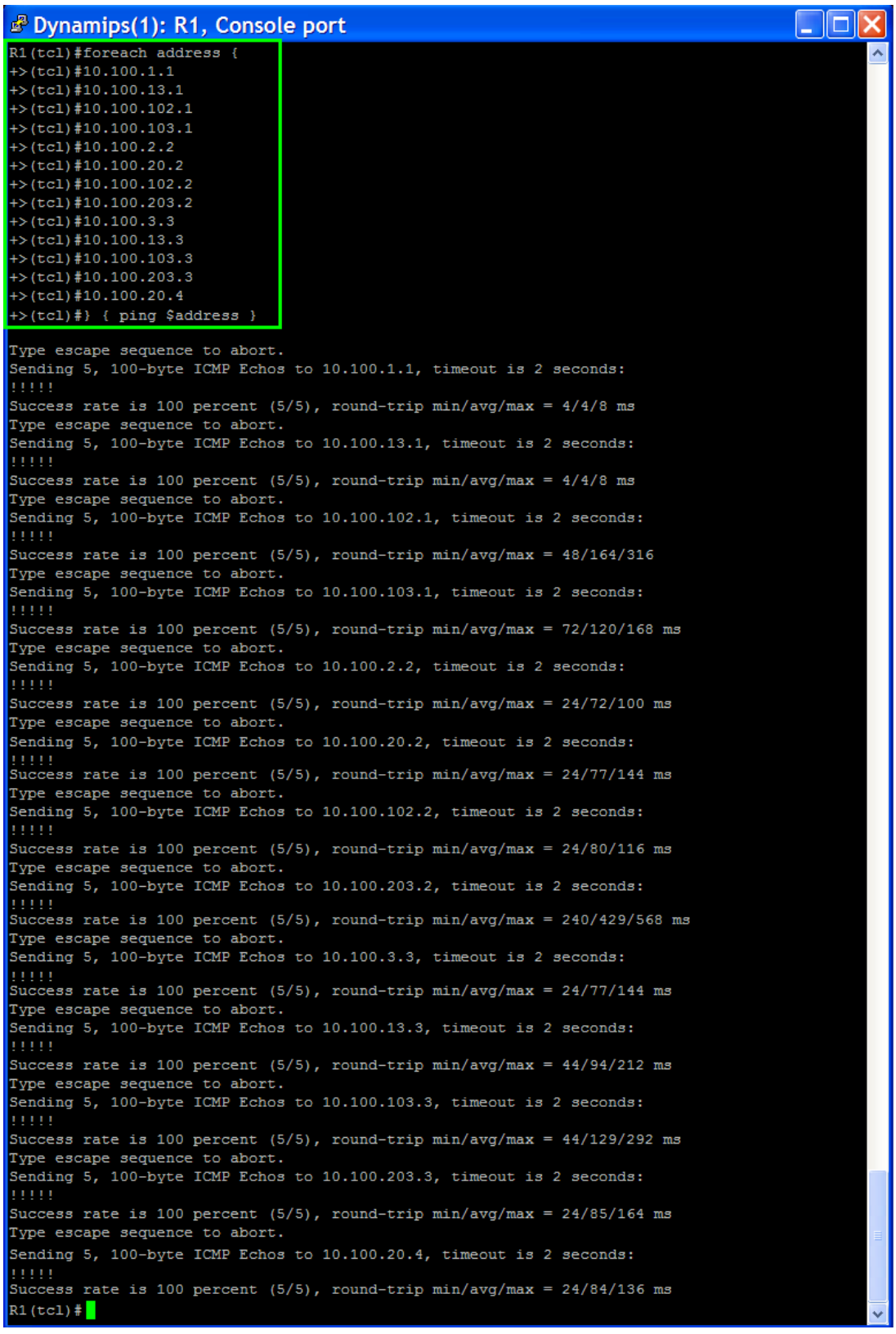
Figura 332. Creación de un proceso OSPF en R3



Fuente: Software GNS3.

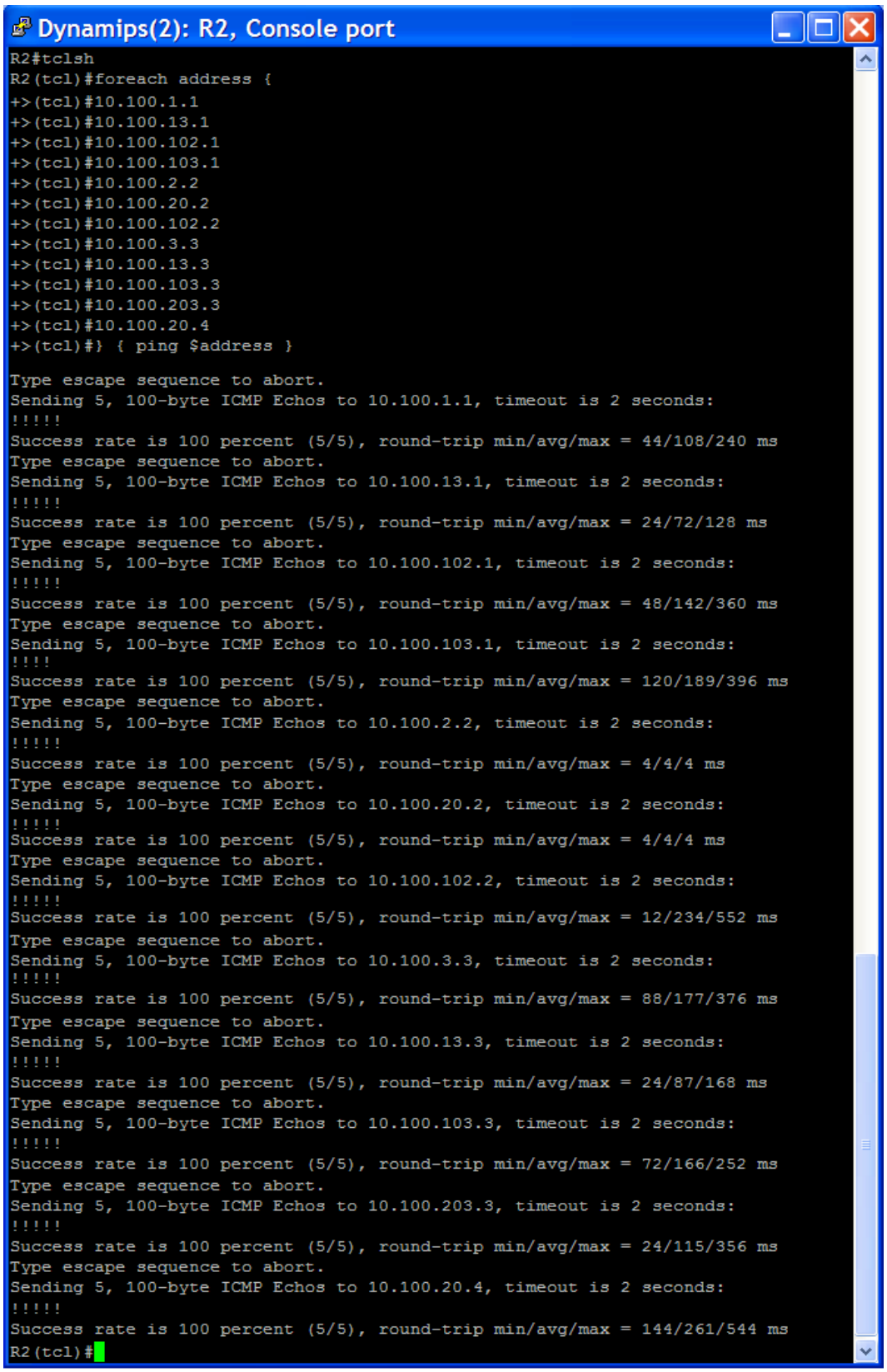
Despues de realizar esta configuración y las adyacencias OSPF, se ejecuta el siguiente script TCL en todos los routers para verificar si hay una completa conectividad unicast.

Figura 333. Verificación de conectividad unicast en R1



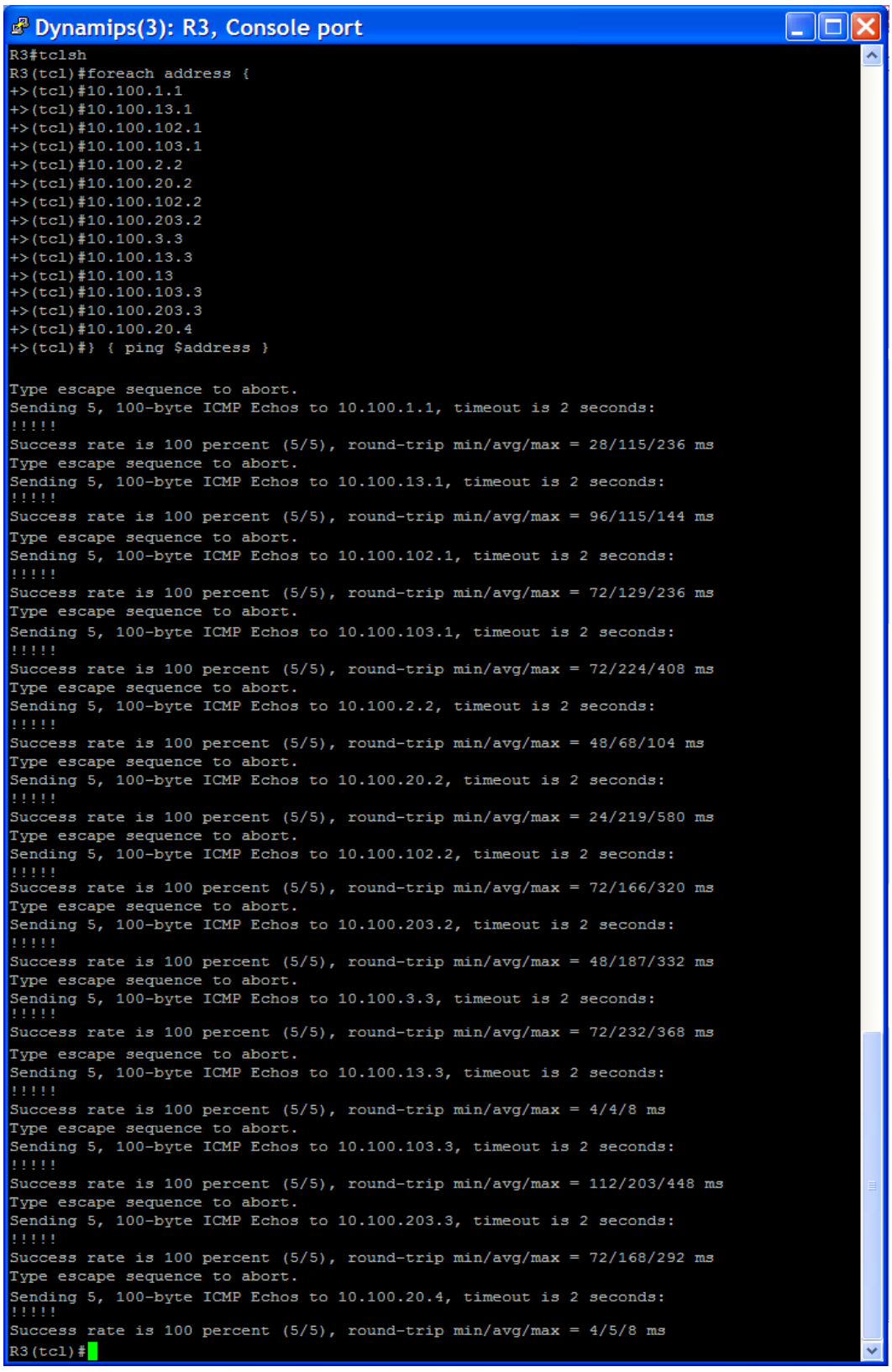
Fuente: Software GNS3.

Figura 334. Verificación de conectividad unicast en R2



Fuente: Software GNS3.

Figura 335. Verificación de conectividad unicast en R3



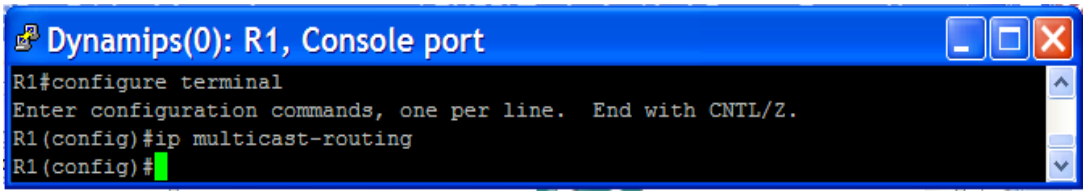
Fuente: Software GNS3.

Se observa que todos los pings son exitosos y que se obtienen respuestas ICMP de la interfaz SVI (10.100.20.4/24) en el switch SW1. Si el switch SW1 tiene una puerta de enlace (por defecto) *"alcanzable"* de la interfaz fastEthernet0/0 de R2 y si todos los routers tienen completa conectividad entre todas las subredes, se puede hacer ping a la dirección de SVI y recibir todas las respuestas.

Implementación de PIM Sparse-Dense Mode

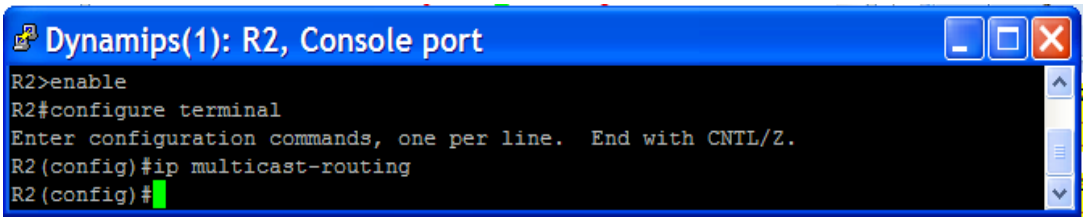
Se habilitan los routers para que ejecuten IP multicast usando el comando **ip multicast-routing** en modo global de configuración.

Figura 336. Habilitación de enrutamiento ip multicast en el Router R1



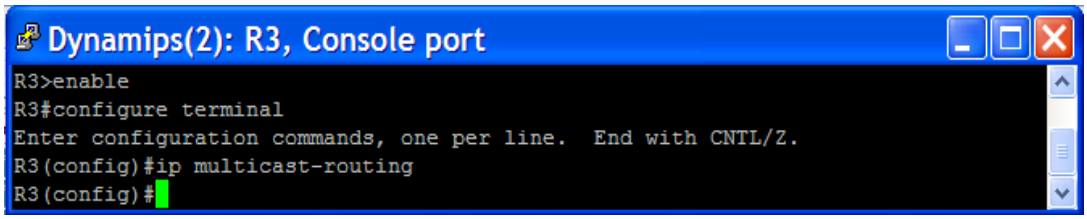
Fuente: Software GNS3.

Figura 337. Habilitación de enrutamiento multicast en el Router R2



Fuente: Software GNS3.

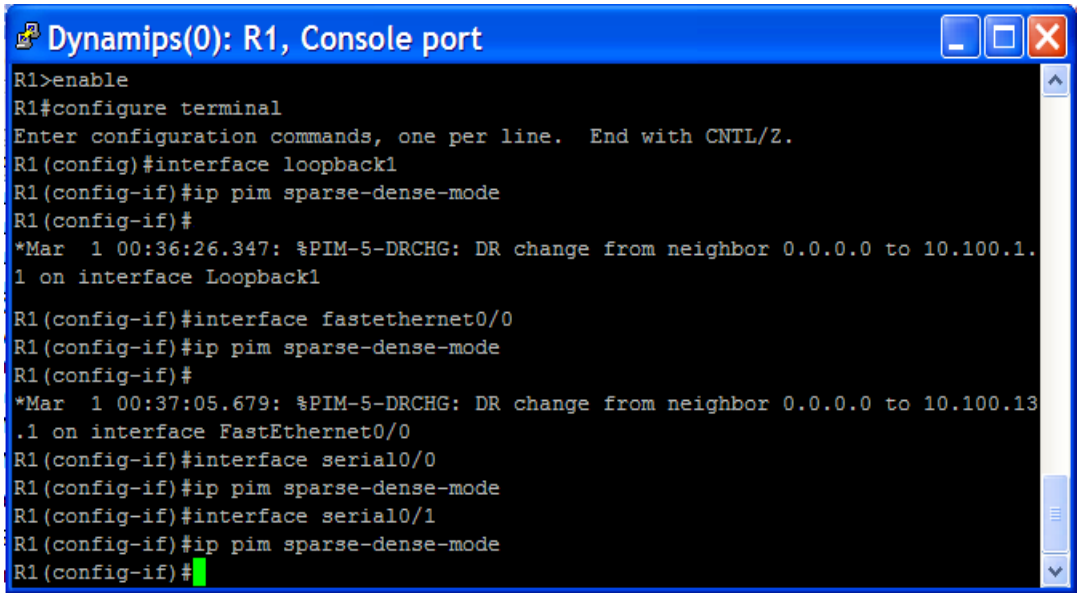
Figura 338. Habilitación de enrutamiento multicast en el Router R3



Fuente: Software GNS3.

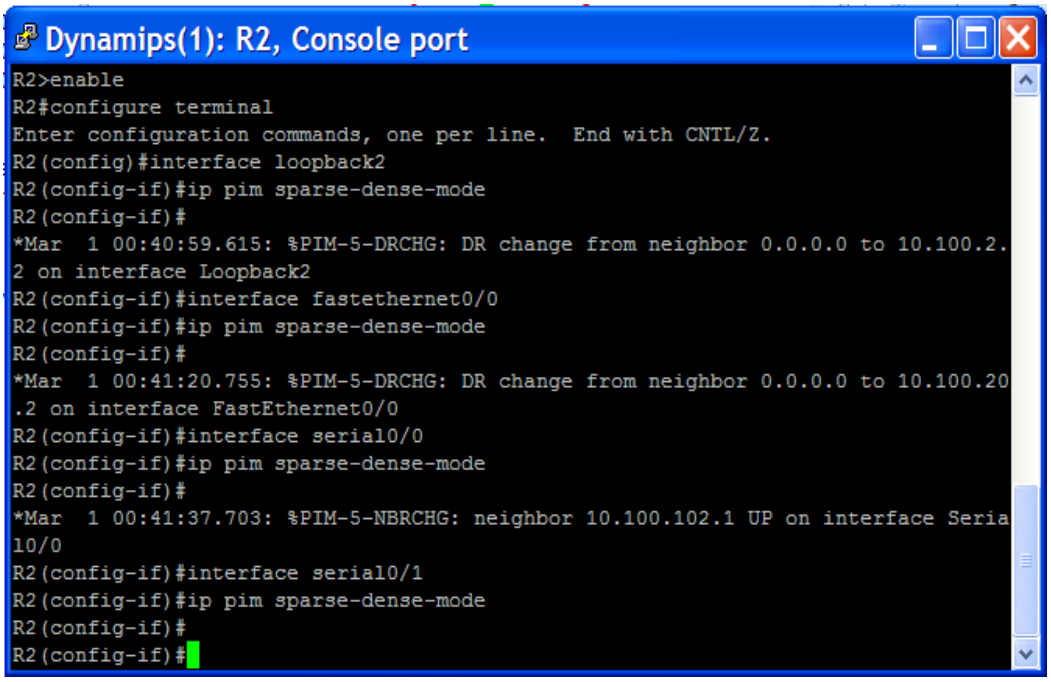
A continuación se activa el modo PIM sparse-dense en todas las interfaces de cada uno de los routers usando el comando **ip pim sparse-dense-mode** en modo de configuración en la interfaz.

Figura 339. Activación de modo Sparse-dense en las interfaces de R1



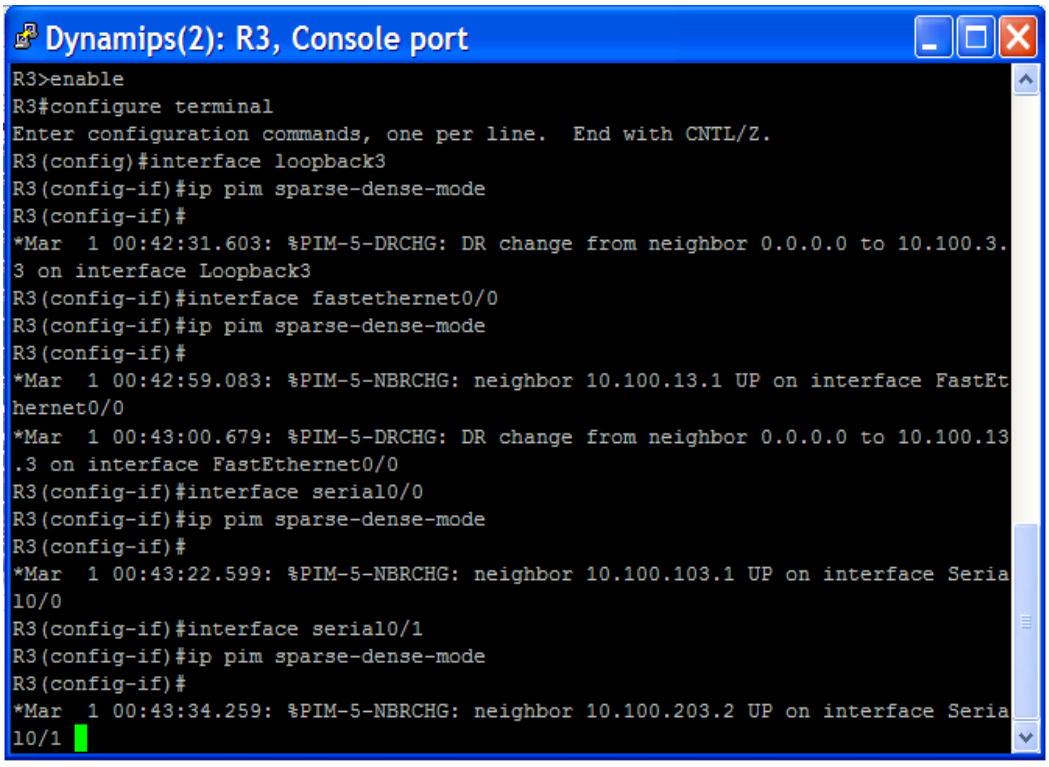
Fuente: Software GNS3.

Figura 340. Activación de modo Sparse-dense en las interfaces de R2.



Fuente: Software GNS3.

Figura 341. Activación de modo Sparse-dense en las interfaces de R3



Fuente: Software GNS3.

A continuación se mencionan algunos conocimientos adquiridos en el laboratorio PIM-SM (desarrollado anteriormente), que serán útiles para comprender el funcionamiento de PIM-SDM

- El propósito del RP en PIM-SM es recibir los paquetes multicast de la fuente y luego reenviarlos a los destinos del grupo a través de un árbol de distribución compartido.
- Si no hay un RP alcanzable en una red PIM-SM las multidifusiones no serán enviadas mediante los mensajes de registro PIM hasta el punto de encuentro y los grupos registrados no serán capaces de recibir las multidifusiones desde las fuentes a través del árbol compartido.
- Si se implementa PIM-SM con un RP estático cada router identificará estáticamente el RP y los grupos que usará para cada RP.
- Existen otras formas para configurar un RP en *sparse mode* y *sparse-dense mode*:

    a. Se puede asignar un RP dinámicamente a través del mecanismo auto-RP. Esto permite que el RP sea asignado dinámicamente.

    b. El uso de un Bootstrap router (BSR) o RP Anycast. BSR permite a los agentes de mapeo ser elegidos como RP. Anycast RP permite que una dirección ip establecida sea publicada desde multiples puntos en una red. Cada uno de estos procesos permite asignación dinámica de RP o agentes de mapeo.

Como se mostró anteriormente en el laboratorio PIM-SM, es importante situar RPs en ubicaciones *"alcanzables"* a través de un protocolo de enrutamiento unicast cuando esté disponible. En este laboratorio se configuran los dos candidatos RP para el grupo multicast 225.25.25.25. y se permitirá solo a R1 ser elegido como el RP para el grupo

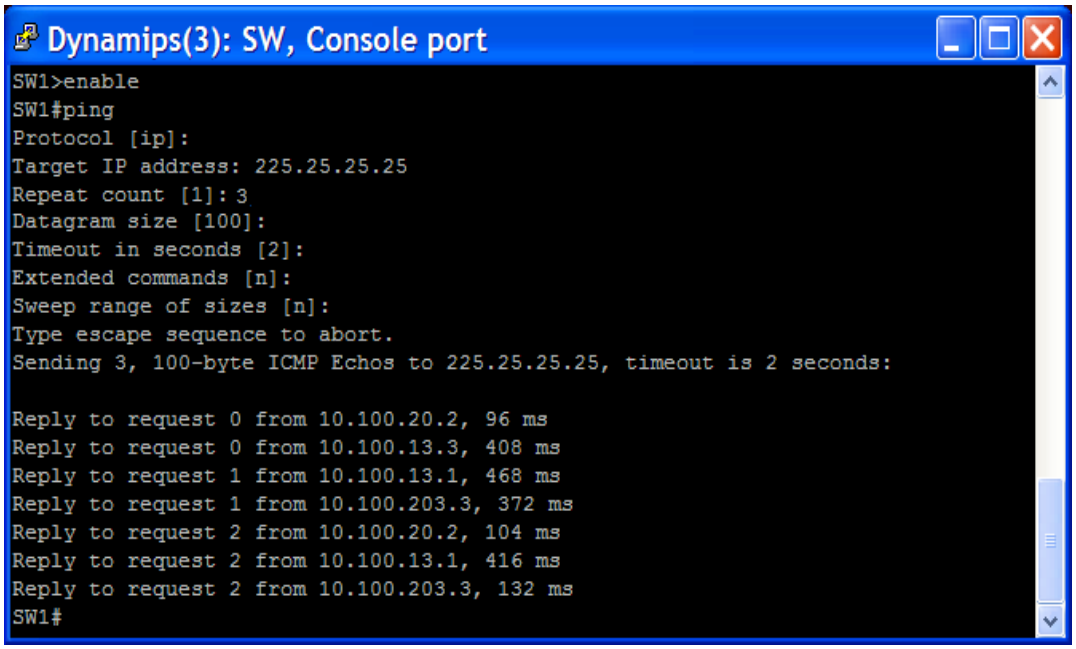
226.26.26.26, pero se descubrirán dinámicamente todos los candidatos RP. Se utiliza *PIM sparse-dense mode* y *Auto-RP* para lograr esta funcionalidad.

PIM sparse-dense mode maneja grupos multicast dinámicamente entre *sparse mode* y *dense mode. Sparse-dense mode* aplica procesos y algoritmos *sparse mode* para cualquier grupo multicast para los cuales puede descubrir un RP por medio de una configuración estática, *Auto-RP,* o el proceso más avanzado *Bootstap Router (BSR).* Los grupos multicast que corren sobre un router *sparse-dense mode* no pueden descubrir un RP que corra en *PIM-DM*.; esto aplica también para redes PIM-SM. Este proceso es referenciado como *dense mode fallback* y puede ser deshabilitado con el comando **no ip pim dm-fallback** en modo de configuración global.

Sin una configuración adicional los grupos multicast 225.25.25.25 y 226.26.26.26 funcionarán en modo denso hasta que un RP pueda ser localizado. Debido a que el router más cercano a las fuentes multicast no puede encontrar el RP, este no puede encapsular los paquetes de multicast en paquetes unicast. Por lo tanto, esto simplemente inunda los multicast a todas las interfaces de multicast conectados en modo denso.

Si se realizara un ping de SW1 al grupo 225.25.25.25 se debería recibir alguna respuesta debido a que el grupo estará funcionando en modo denso hasta que un RP sea encontrado. A continuación se realiza una serie de pings multicast desde SVI en SW1 para generar el estado (S, G) en sus routers.

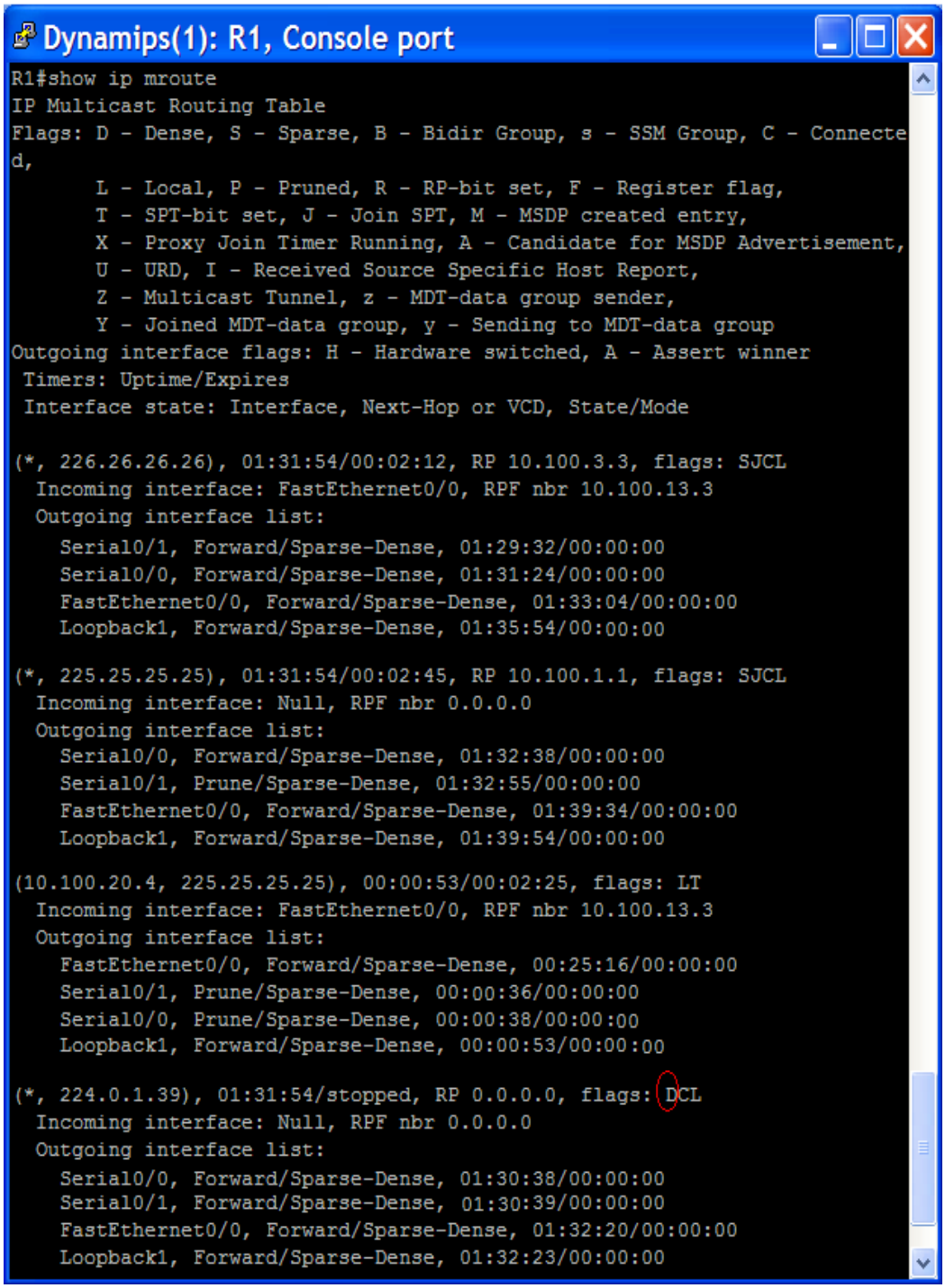
Figura 342. Pings multicast en el switch SW1



Fuente: Software GNS3.

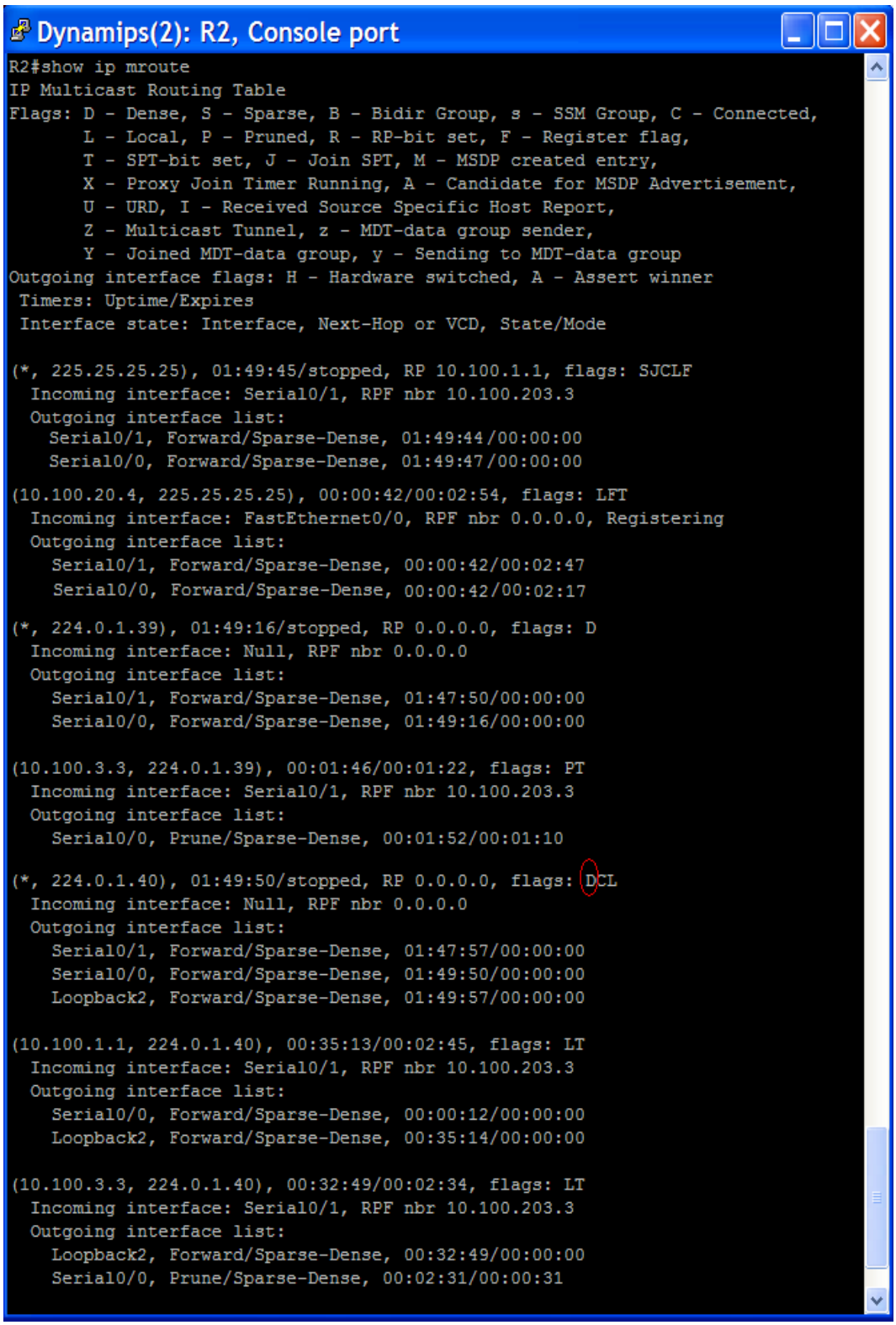
Seguidamente se muestra la tabla de enrutamiento multicast en cada router con el comando **show ip mroute.**

Figura 343. Tabla de enrutamiento Multicast en el router R1.



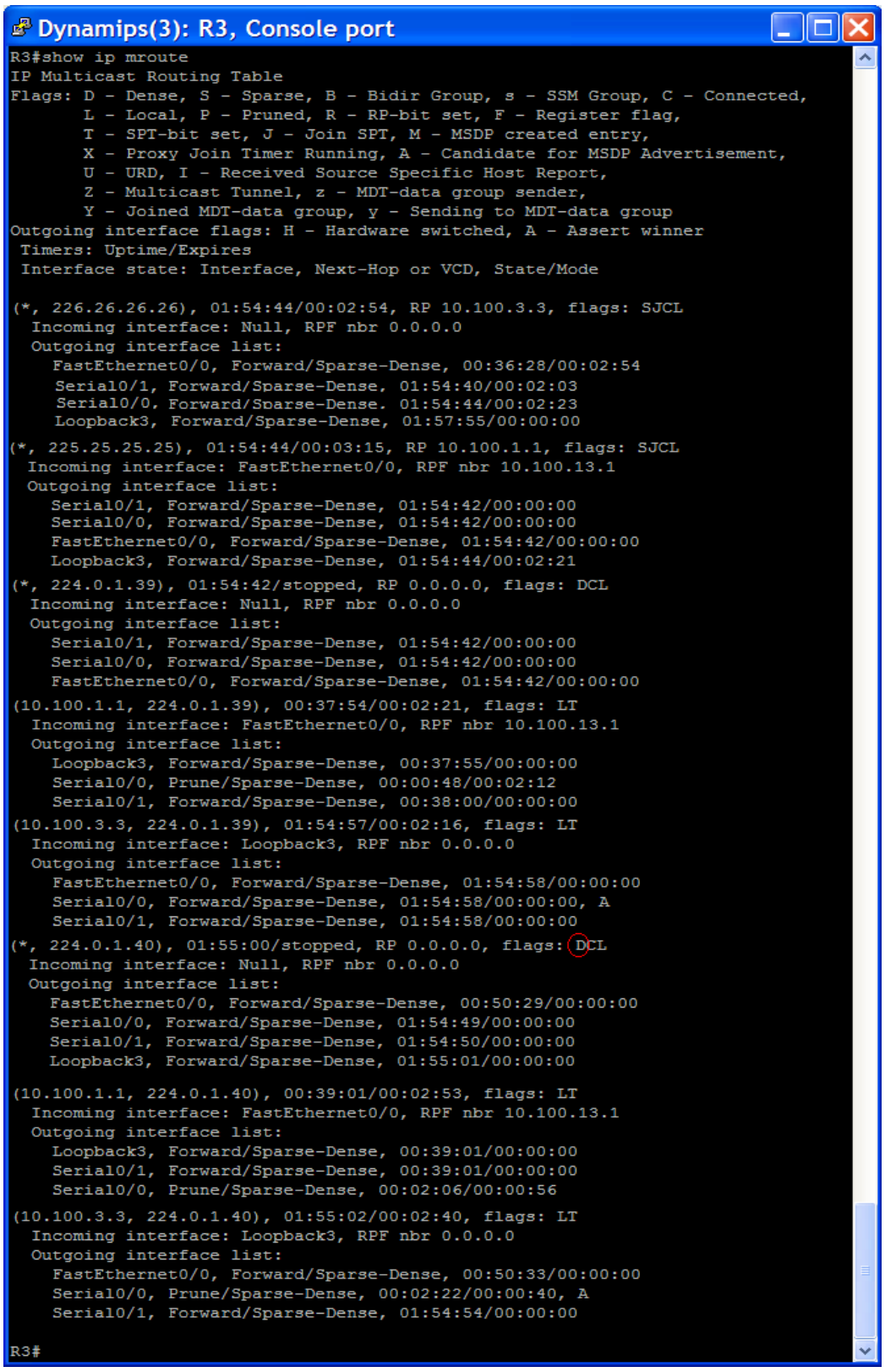
Fuente: Software GNS3.

Figura 344. Tabla de enrutamiento Multicast en el router R2.



Fuente: Software GNS3.

Figura 345. Tabla de enrutamiento Multicast en el router R3.

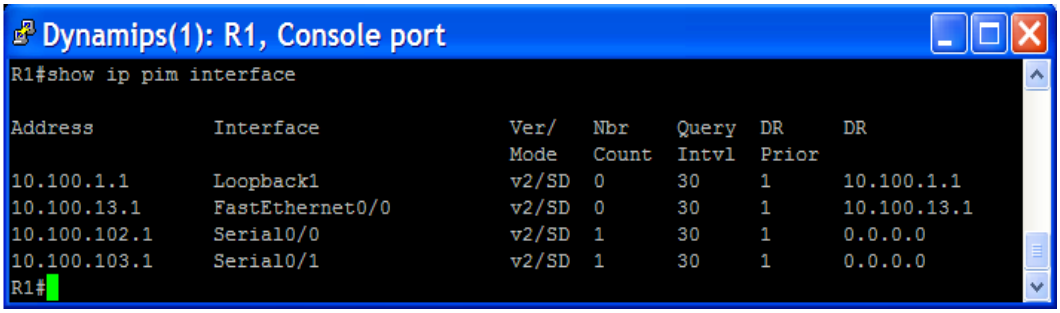


Fuente: Software GNS3.

De la salida anterior se puede comprobar que PIM está funcionando en modo denso debido a que el RP no ha sido localizado. Esto se indica en las tablas de enrutamiento multicast por medio de la bandera *"D"* en cada entrada en el árbol de enrutamiento multicast.

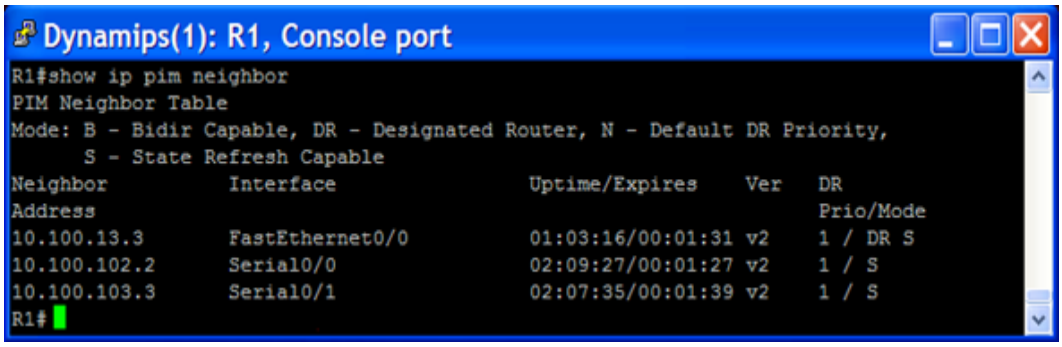
Para verificar que se haya configurado correctamente PIM sparse-dense mode en todas las interfaces se utiliza el comando **show ip pim interface.** Y para asegurarse de que todas las adyacencias PIM están activas se utiliza el comando **show ip pim neighbor.**

Figura 346. Verificación de PIM sparse-dense en R1.



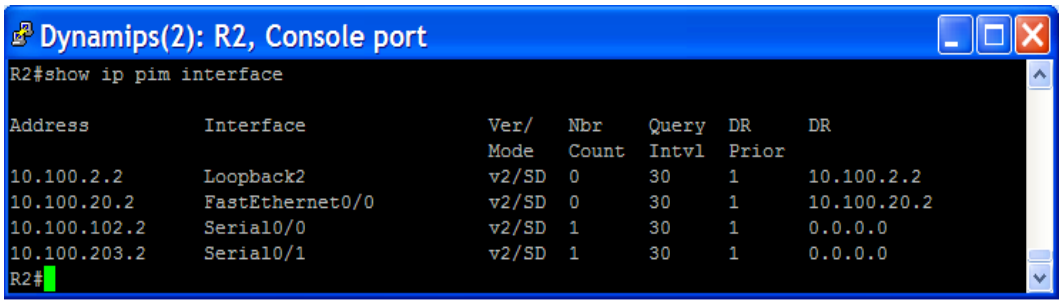
Fuente: Software GNS3.

Figura 347. Verificación de las adyacencias PIM activas en el router R1.



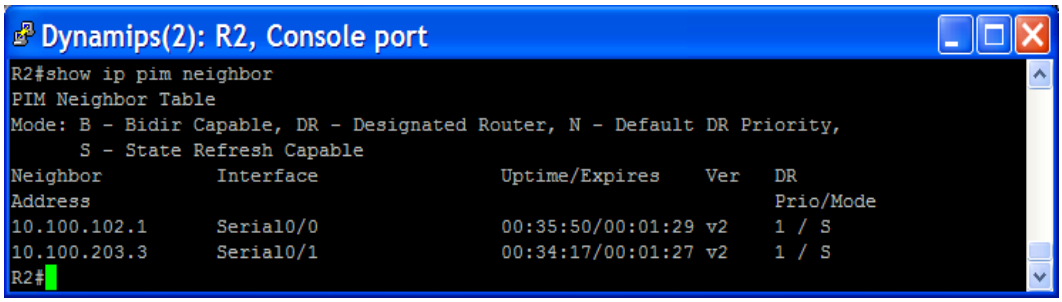
Fuente: Software GNS3.

Figura 348. Verificación de PIM sparse-dense en R2.



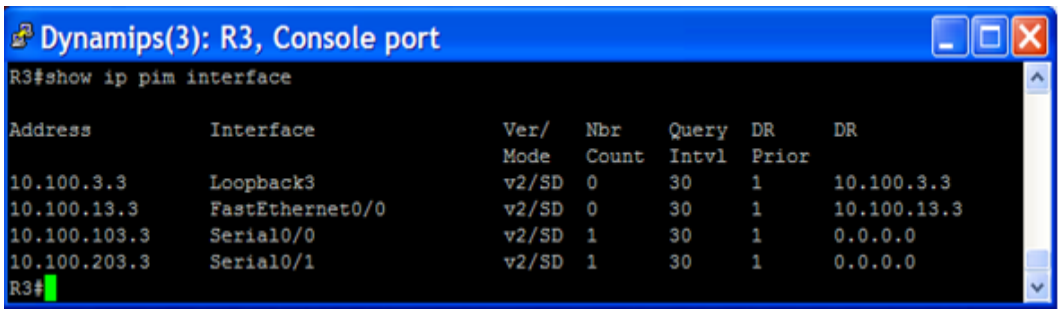
Fuente: Software GNS3.

Figura 349. Verificación de las adyacencias PIM activas en el router R2.



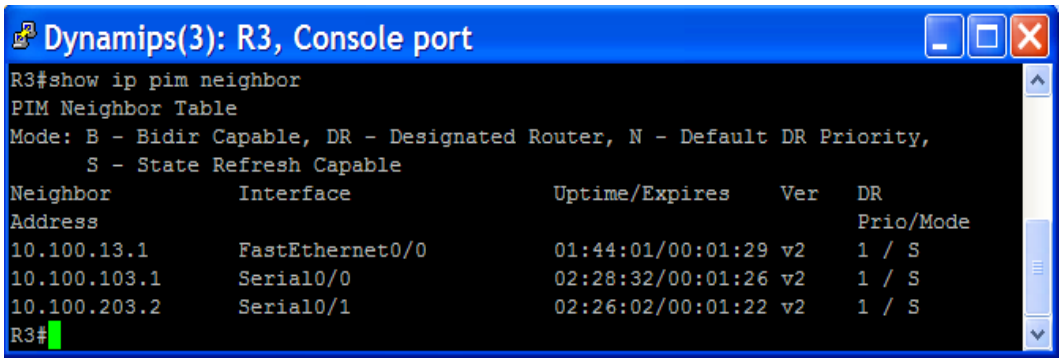
Fuente: Software GNS3.

Figura 350. Verificación de PIM sparse-dense en R3.



Fuente: Software GNS3.

Figura 351. Verificación de las adyacencias PIM activas en el router R3.



Fuente: Software GNS3.

Configuración de PIM Auto-RP

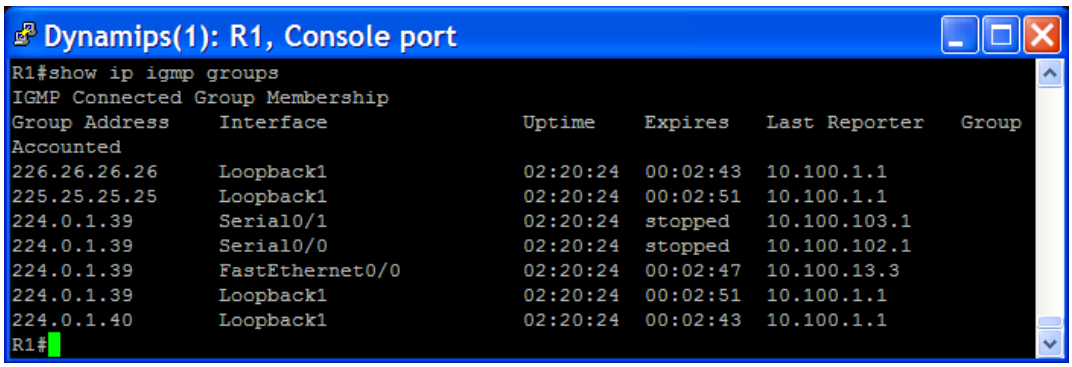
Aunque PIM opera de manera exitosa, se pueden configurar los routers para que utilicen el ancho de banda de manera eficiente, forzando a los grupos multicast a usar PIM-SM.

Los RP en PIM-SM introducen fuentes multicast actuando como una red receptora que conoce la ubicación de todas las fuentes multicast para grupos específicos.

PIM-SM crea árboles de distribución compartidos para grupos multicast representados por (*, G) en cada tabla de enrutamiento multicast. Este árbol compartido es calculado usando la interfaz upstream RPF para el RP para ese grupo. De esta manera, el árbol compartido es escencialmente el árbol de camino más corto a la dirección del RP.

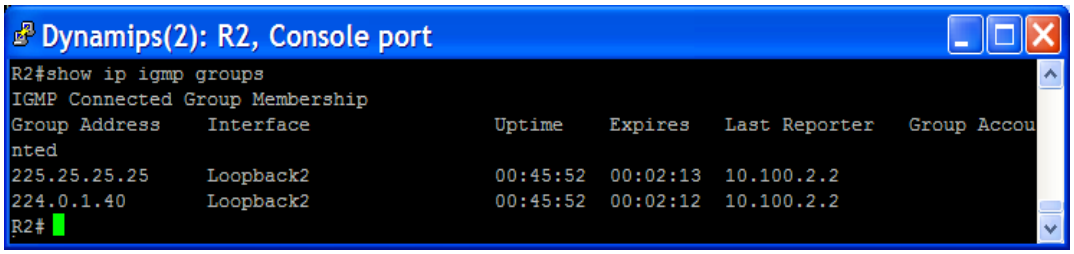
Cuando se configuran interfaces en *sparse-dense mode* cada router se suscribe implícitamente al grupo *RP Discovery* 224.0.1.40 y 224.0.1.39. Esto se puede verificar utilizando el comando **show ip igmp groups**. Cada router aplica la información que recibe acerca de las asignaciones *group-to-RP* por el grupo *RP Discovery* a sus entradas de la tabla de enrutamiento multicast.

Figura 352. Verificación de grupos multicast suscritos en el router R1.



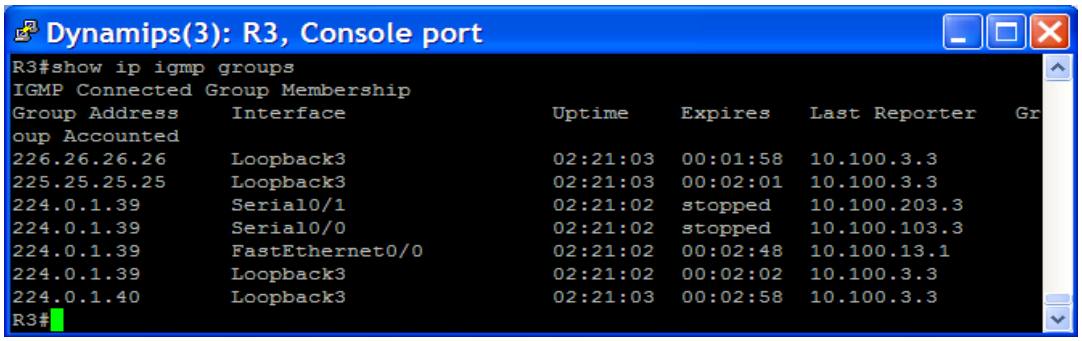
Fuente: Software GNS3.

Figura 353. Verificación de grupos multicast suscritos en el router R2.



Fuente: Software GNS3.

Figura 354. Verificación de grupos multicast suscritos en el router R3.

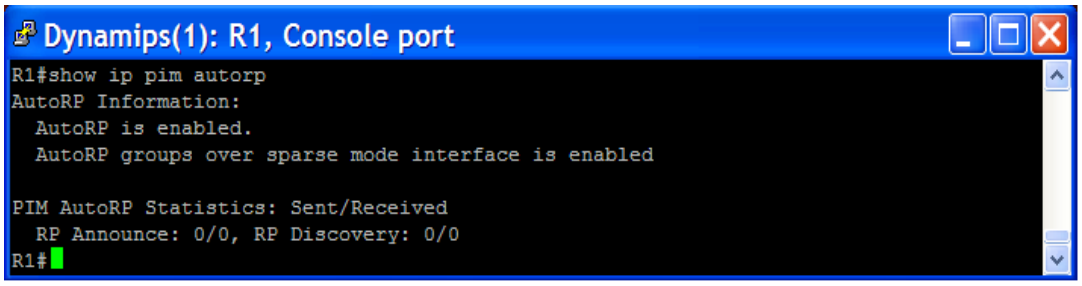


Fuente: Software GNS3.

Si se configuran las interfaces para que corran solo PIM-SM, también se necesita aplicar el comando **ip pim autorp listener** a cada interfaz sparse-mode. Este comando permite que los mensajes de mapeo RP puedan ser leidos por routers multicast y propagados a través de la red en forma de modo denso. Debido a que *sparse-dense mode* actúa en una forma PIM-DM sin un RP para el grupo, se puede obtener la misma funcionalidad sin aplicar el comando.

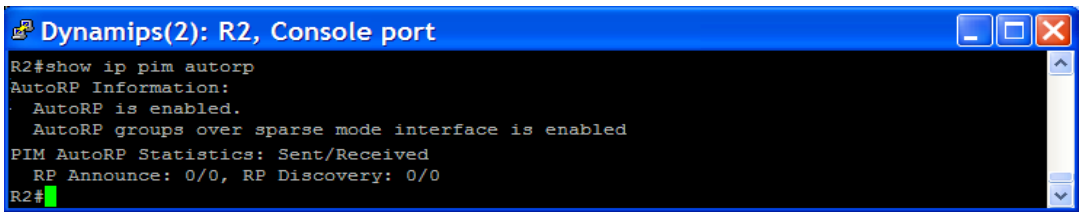
Por defecto, sparse-dense mode también habilita la instalación de información de mapeo RP dentro de la tabla de enrutamiento multicast. Esto se puede verificar con el comando **show ip pim autorp** en los routers.

Figura 355. Información RP mapping en R1.



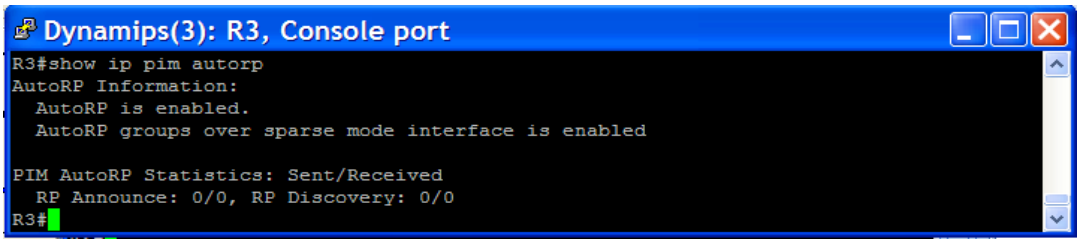
Fuente: Software GNS3.

Figura 356. Información RP mapping en R2.



Fuente: Software GNS3.

Figura 357. Información RP mapping en R3.

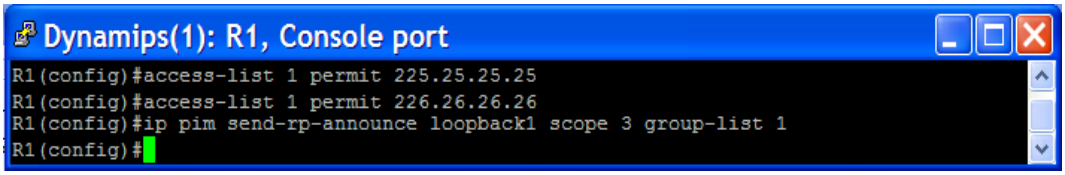


Fuente: Software GNS3.

Luego se habilita la publicación de información de Auto-RP para los grupos especificados en R1 y R3. Además de configurar a R1 como candidato a RP para ambos grupos. R3 debe ser candidato sólo para el grupo 226.26.26.26, y se configuran las listas de acceso para controlar los grupos a los cuales se envía información Auto-RP. Por último se aplican estas listas de acceso con el comando **ip pim send-rp-announce** {*interface-type interfacenumber* | *ip-address*} **scope** *ttl-value* [**group-list** *access-list*].

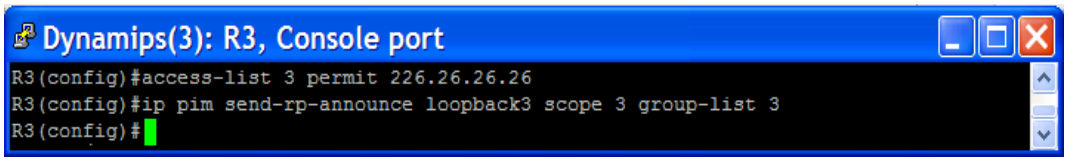
Los candidatos a RP deberían ser las interfaces loopback en R1 y R3. Se utiliza un TTL (time-to-live) de 3 para que las publicaciones RP no sean descartadas en cualquier parte de la red existente. El ***scope*** determina el número de veces que un paquete multicast es enrutado en capa 3 antes de ser descartado porque el TTL ha alcanzado 0.

Figura 358. Configuración de scope en el router R1.



Fuente: Software GNS3.

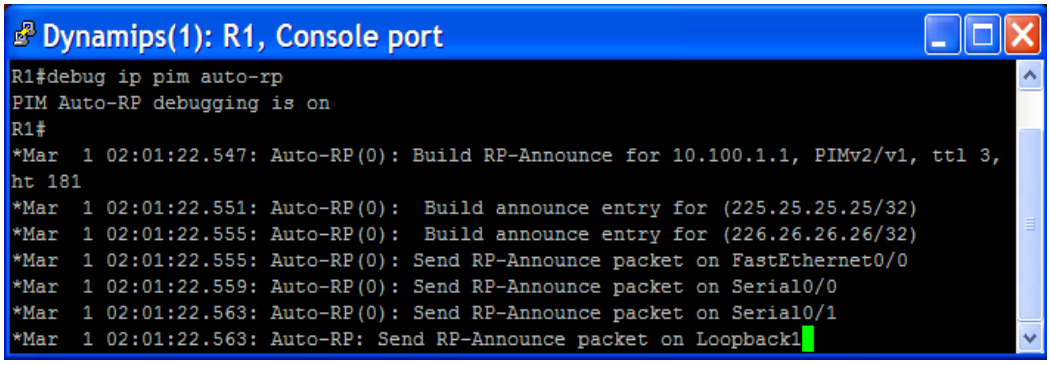
Figura 359. Configuración de scope en el router R3.



Fuente: Software GNS3.

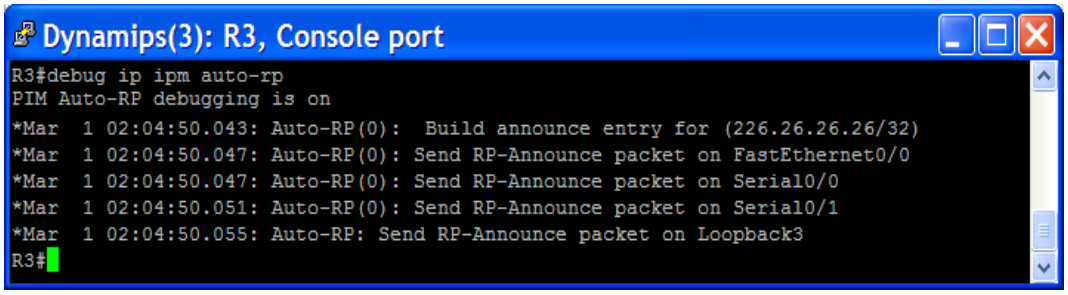
Enseguida se habilita la depuración de PIM Auto-RP con el comando **debug ip pim auto-rp** en R1 y R3. Las publicaciones Auto-RP son enviadas periódicamente, como se muestra a continuación, indicando que las publicaciones están siendo inundadas desde el router local.

Figura 360. Habilitación de la depuración de PIM Auto-RP en el router R1.



Fuente: Software GNS3.

Figura 361. Habilitación de la depuración de PIM Auto-RP en el router R3.



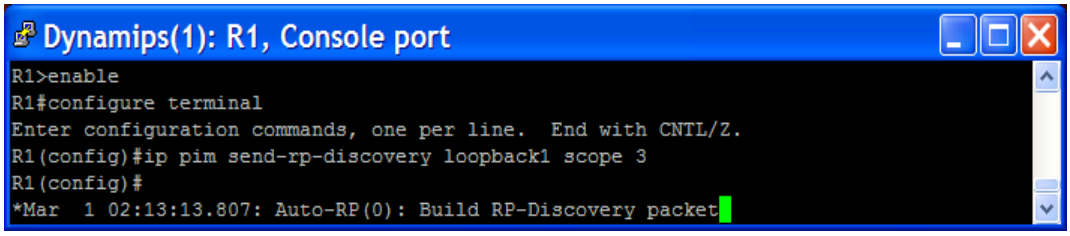
Fuente: Software GNS3.

Se continúa con la depuración de mensajes Auto-RP mientras que se configura el agente de mapeo.

Las redes PIM-SM que usan Auto-RP también necesitan uno o más agentes de mapeo para informar a los routers que están escuchando al grupo Auto-RP de las asignaciones *group-to-RP*.

Se configura el router R1 como el agente de mapeo para esta red usando el comando **ip pim send-rp-discovery** [*interface-type interface-number*] **scope** *ttl-value* para que genere mensajes de mapeo group-to-RP desde R1.

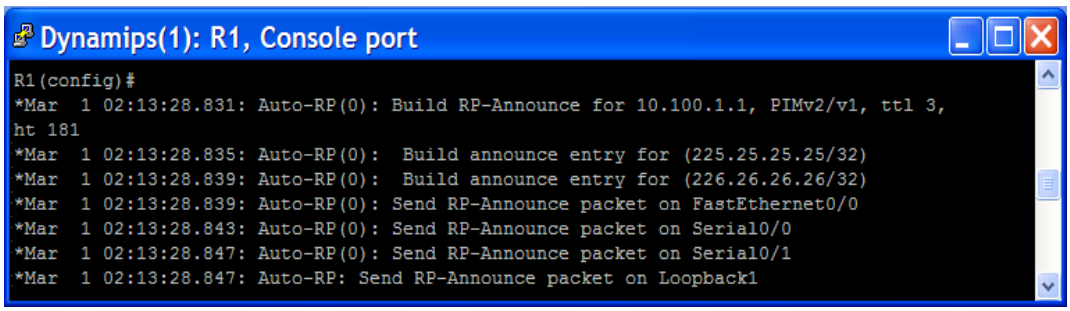
Figura 362. Configuración del agente de mapeo en el router R1.



Fuente: Software GNS3.

Se obtiene la siguiente salida:

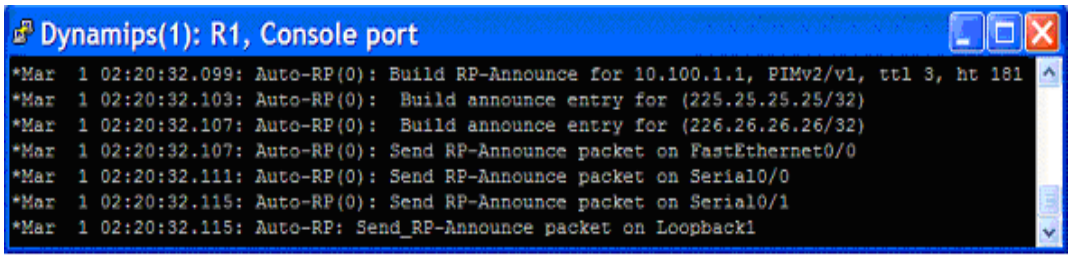
Figura 363. Depuración de configuración del agente de mapeo en R1.



Fuente: Software GNS3.

Debido a que previamente se ha configurado a R1 como candidato RP, éste se anuncia a sí mismo como un RP para los grupos 225.25.25.25 and 226.26.26.26. Sin embargo, ningún router seleccionará a R1 como el RP confirmado para estos grupos hasta que no lo escuche del agente de mapeo. R1 continúa con sus anuncios multicast de candidatura RP a todas las interfaces como se muestra en la siguiente figura.

Figura 364. Anuncios multicast de candidatura RP desde R1 (I).

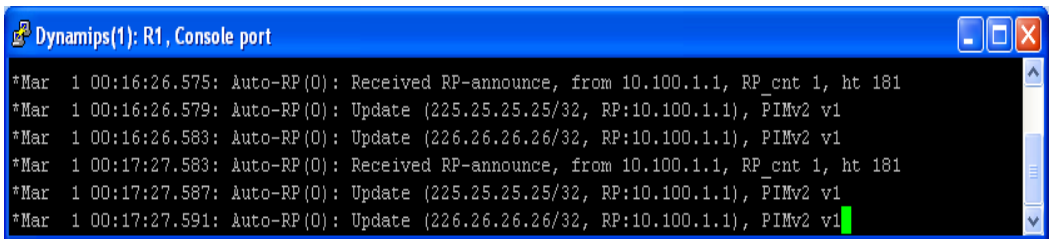


Fuente: Software GNS3.

El router que actua como agente de mapeo, que en este caso es el router R1, recibe el anuncio de candidatura que el proceso Auto-RP en R1 envió al grupo 224.0.1.39. (*Auto-RP announcement*).

R1, actuando como agente de mapeo RP elige a R1 como el RP para ambos grupos debido a que no ha recibido ningún otro anuncio RP de una fuente con una dirección IP más alta. El agente de mapeo envía las dos asignaciones *group-to-RP* por medio multicast a todos los oyentes Auto-RP en la red. Las asignaciones son enviadas al grupo de descubrimiento Auto-RP 224.0.1.40.

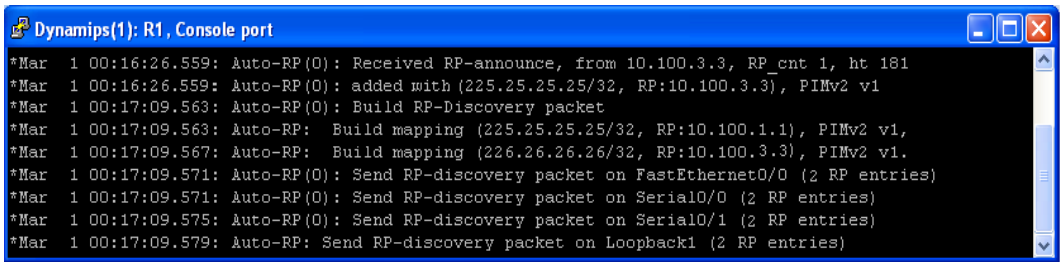
Figura 365. Anuncios multicast de candidatura desde R1 (II)



Fuente: Software GNS3.

Los mesajes Auto-RP que R1 envió previamente son recibidos de nuevo en diferentes interfaces debido a la inundación *dense-mode* a través de la red. R1 simplemente instala nuevamente las asignaciones *group-to-RP* en su tabla.

Figura 366. Salida configuración del agente de mapeo en R1.



Fuente: Software GNS3.

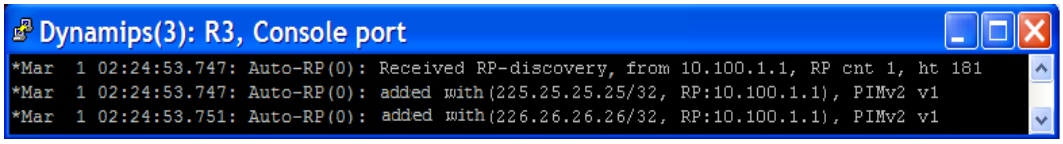
Dentro de poco tiempo, R3 envía su anuncio de candidatura para el grupo multicast 226.26.26.26. R1 recibe este paquete y, actuando como el agente de mapeo RP, lo evalúa contra el RP actual. Debido a que la dirección IP de 10.100.3.3 es mayor que 10.100.1.1, el agente de mapeo elige a R3 como el RP para 226.26.26.26. R1 continúa siendo el RP para el grupo 225.25.25.25.

R1 envía notificación de los ganadores de las elecciones *group-to-RP* para el grupo de descubrimiento 224.0.1.40. Todos los routers multicast

que funcionan con PIM-SM o PIM-DM han sido suscritos implícitamente a este grupo y guardan esta información en sus tablas de enrutamiento.

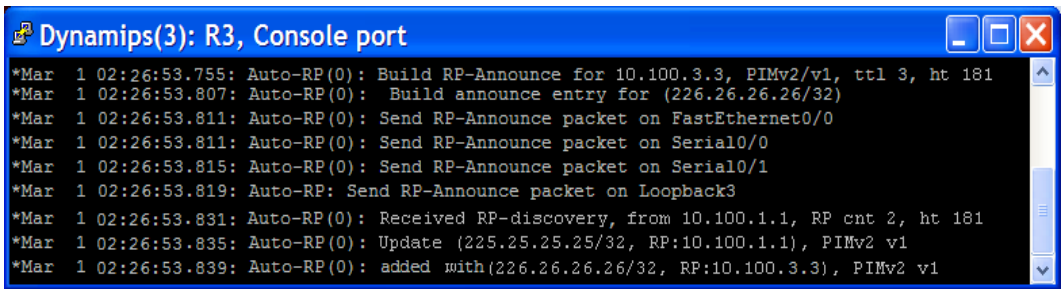
Durante este tiempo, el protocolo PIM que funciona en R3 ha registrado la siguiente salida.

Figura 367. Salida configuración del agente de mapeo en R3.



Fuente: Software GNS3.

Figura 368. Salida configuración del agente de mapeo en R3.

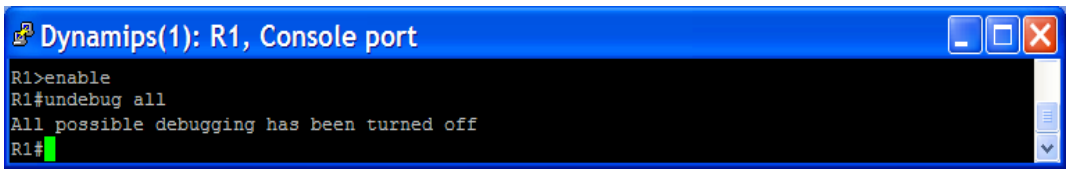


Fuente: Software GNS3.

De acuerdo a lo anterior, cuando R1 inunda el primer paquete de descubrimiento RP, el agente de mapeo aún no ha recibido un paquete de anuncio Auto-RP de R3. Después que R3 envía el anuncio, el agente de mapeo compara las direcciones IP de los dos candidatos para la red 226.26.26.26 y elige a R3 como el RP.

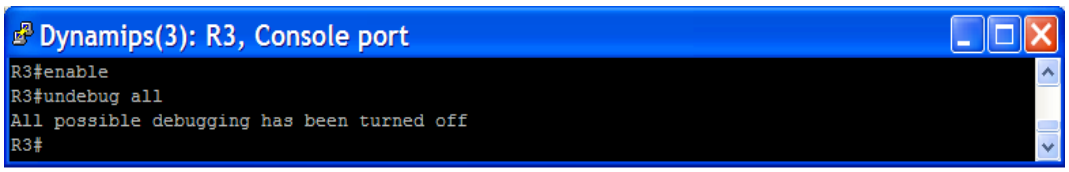
Para detener la ejecución de eventos *PIM Auto-RP* se utiliza el comando **undebug all.**

Figura 369. Detención de la ejecución de eventos de PIM Auto-RP en R1.



Fuente: Software GNS3.

Figura 370. Detención de la ejecución de eventos de PIM Auto-RP en R3.

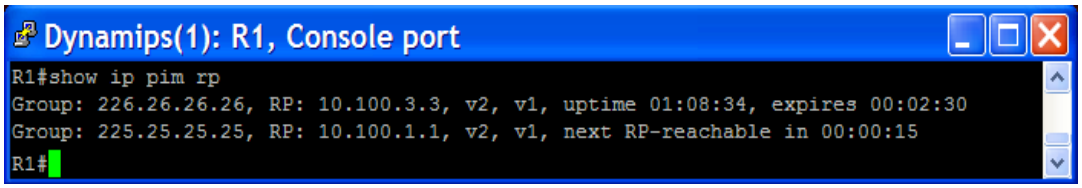


Fuente: Software GNS3.

Verificación de asignaciones RP

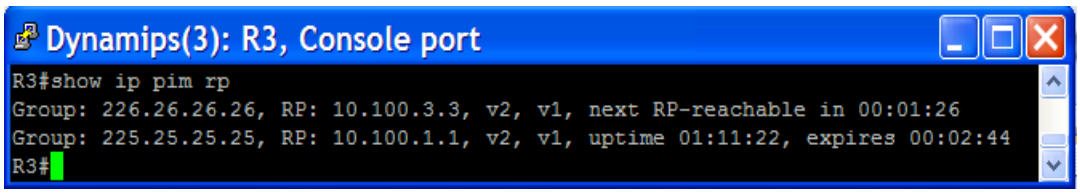
Se utiliza el comando **show ip pim rp** en los routers Auto-RP para ver las asignaciones RP para cada grupo.

Figura 371. Verificación del grupo RP en el router R1.



Fuente: Software GNS3.

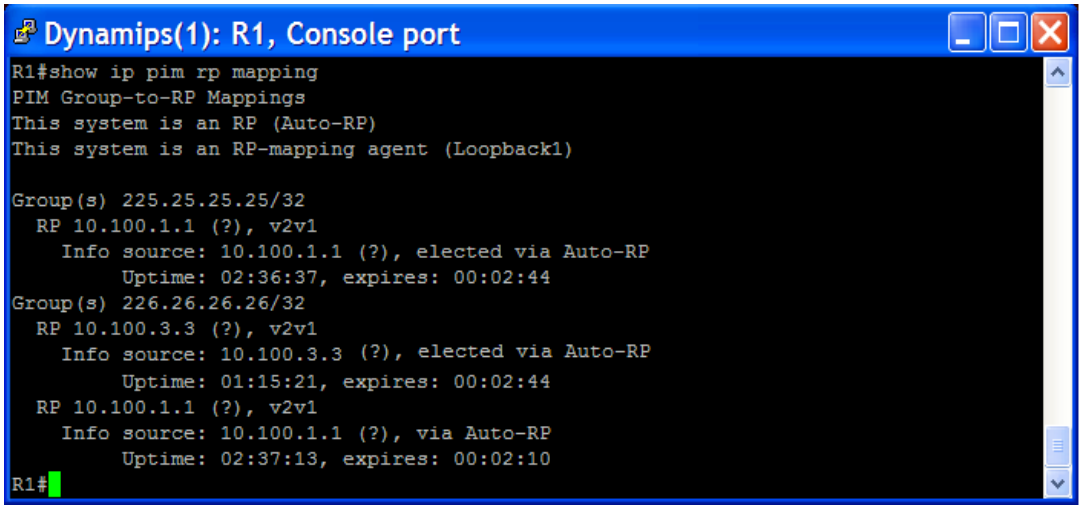
Figura 372. Verificación del grupo RP en el router R3.



Fuente: Software GNS3.

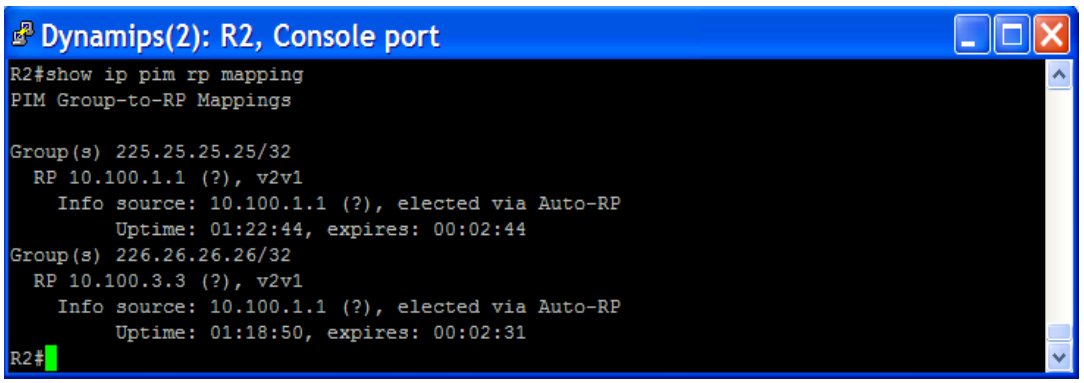
Para obtener una visión completa de las asignaciones RP de los grupos se utiliza el comando **show ip pim rp mapping** en todos los routers. Este comando muestra cómo fue elegido el RP y cuál router realizó el mapeo. Es muy útil en la depuración de elecciones Auto-RP.

Figura 373. Elección del RP y que router realizó el mapeo en R1.



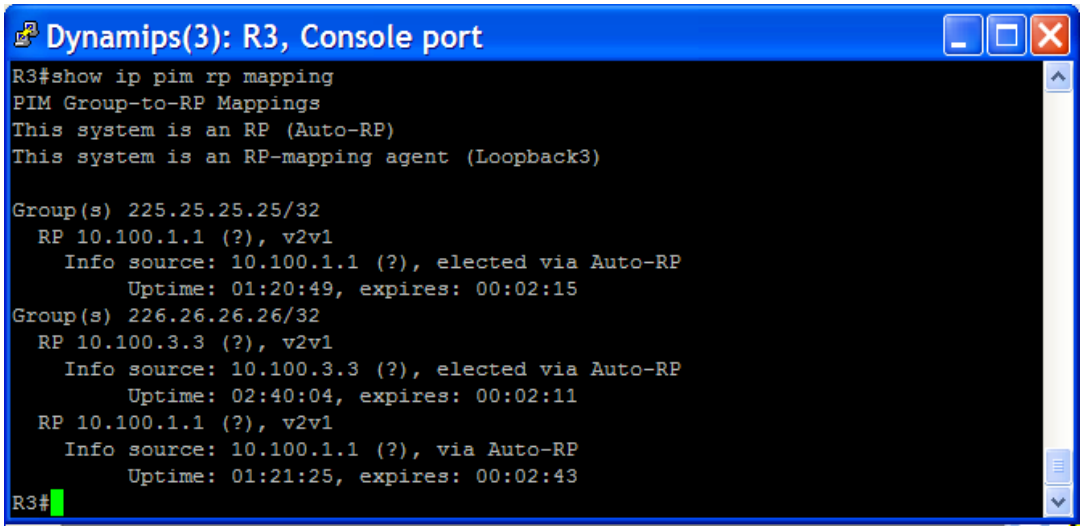
Fuente: Software GNS3.

Figura 374. Elección del RP y que router realizó el mapeo en R2.



Fuente: Software GNS3.

Figura 375. Elección del RP y que router realizó el mapeo en R3.



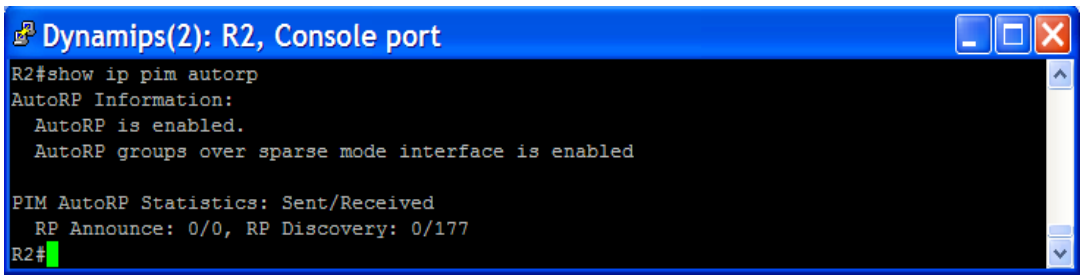
Fuente: Software GNS3.

Cada router aprende sobre estos mapeos escuchando al grupo 224.0.1.40 al cual los agentes de mapeo Auto-RP envían asignaciones al grupo RP. Las asignaciones deben ser ingresadas en la tabla de mapeo de cada router.

Debido a que R1 se configuró como agente de mapeo, los routers PIM que no son elegidos como Auto-RP monitorean el número de mensajes

de descubrimiento RP recibidos. Lo anterior se verifica con el comando **show ip pim autorp** en R2.

Figura 376. Monitoreo de mensajes de descubrimiento RP recibidos en R2.

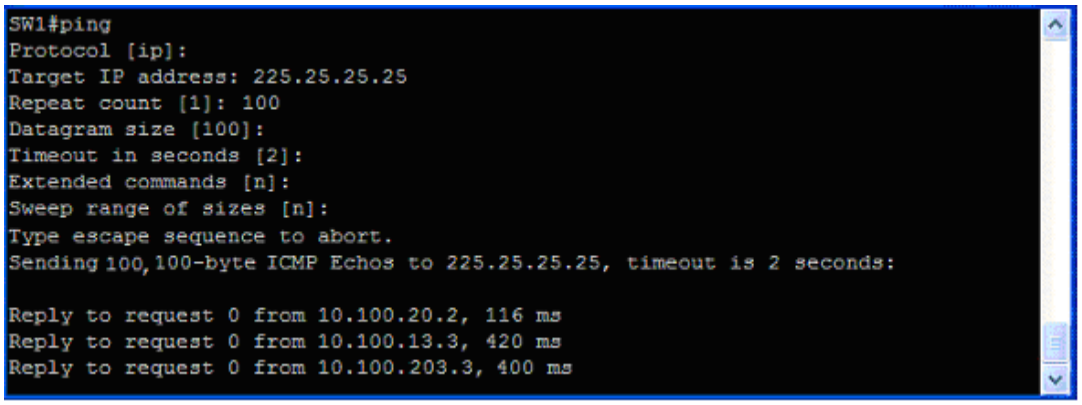


Fuente: Software GNS3.

Verificación del funcionamiento multicast

Se emiten pings multicast para generar el estado (S, G) en la red multicast. Se utiliza un número de repeticiones de 100 para generar un flujo de paquetes multicast que circulen a través de la red.

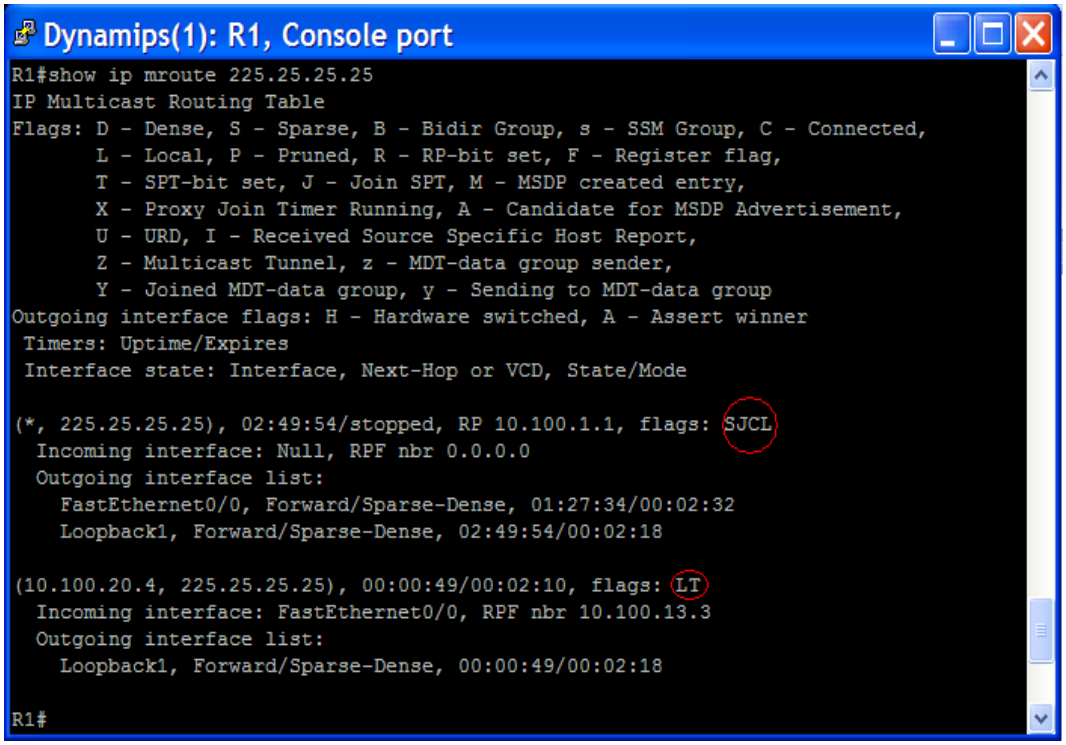
Figura 377. Ping para generar un flujo de paquetes multicast en SW1.



Fuente: Software GNS3.

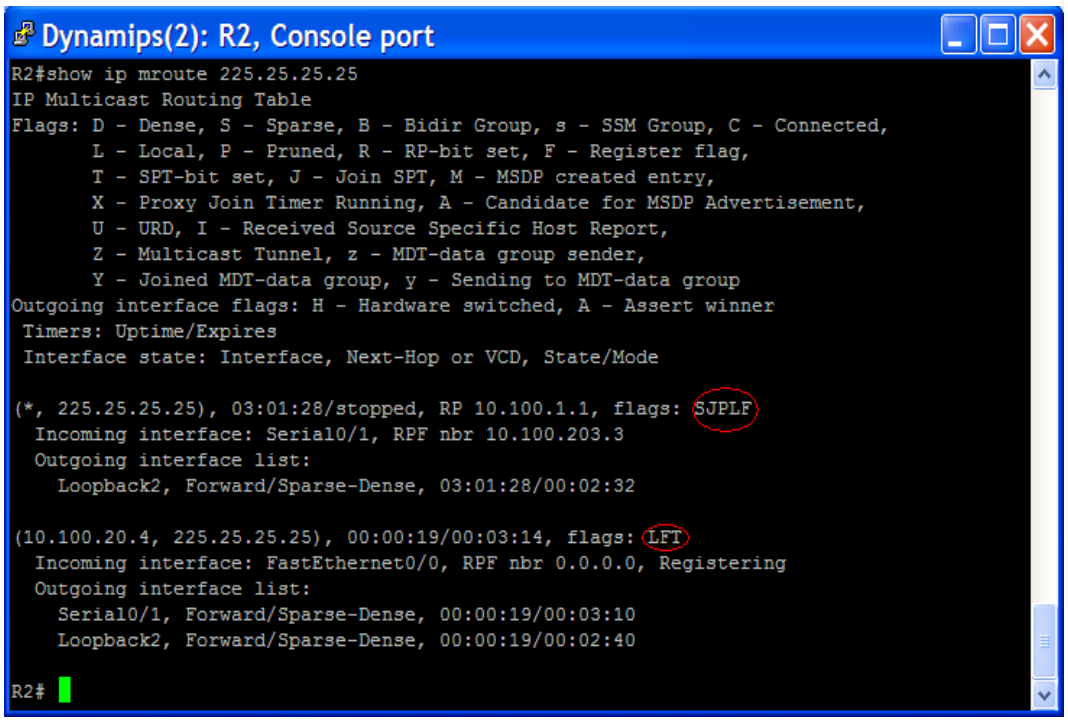
A continuación se muestra la tabla de enrutamiento multicast para el grupo 225.25.25.25 en cada router utilizando el comando **show ip mroute** *group-address*

Figura 378. Enrutamiento multicast para 225.25.25.25 en R1.



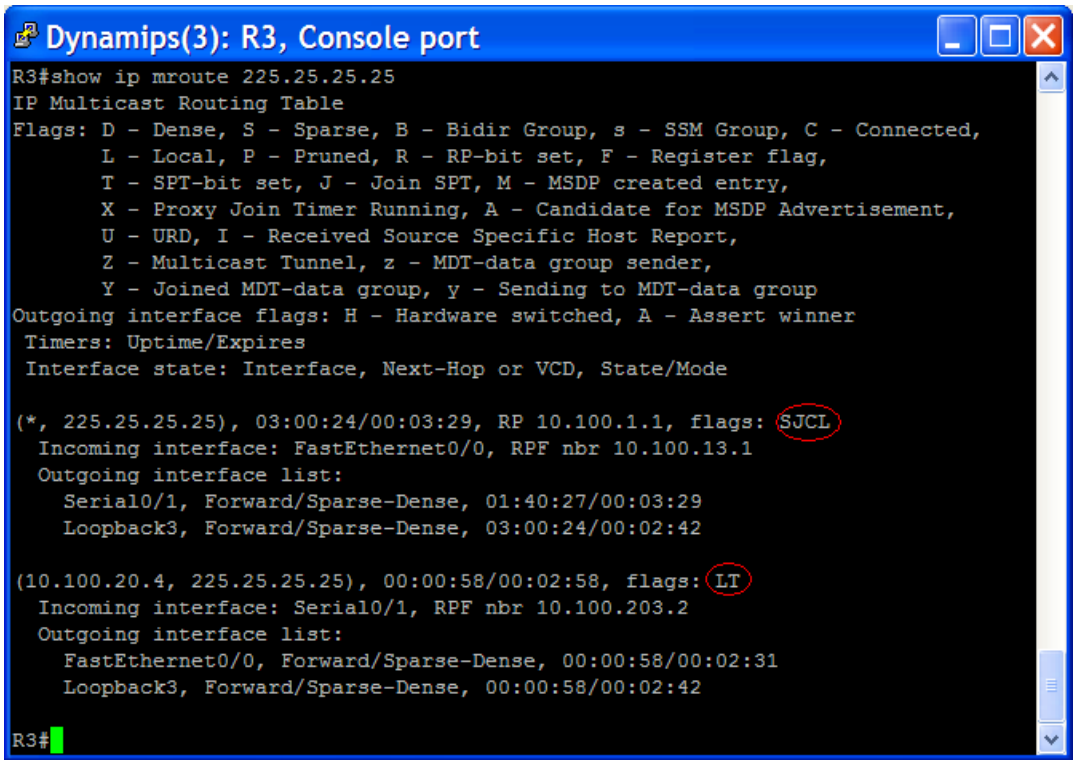
Fuente: Software GNS3.

Figura 379. Enrutamiento multicast para 225.25.25.25 en R2.



Fuente: Software GNS3.

Figura 380. Enrutamiento multicast para 225.25.25.25 en R3.



Fuente: Software GNS3.

De acuerdo a la salida anterior se puede determinar que el grupo 225.25.25.25.25 está operando en modo *PIM SM*, porque la bandera en el grupo multicast muestra una "*S*".

Los mensajes de registro PIM que enviará R2 a los grupos multicast se enviarán a sus respectivos RPs. Es decir, los mensajes de registro del grupo 225.25.25.25 se enviarán a 10.100.1.1 y los mensajes de registro del grupo 226.26.26.26 se enviarán a 10.100.3.3.

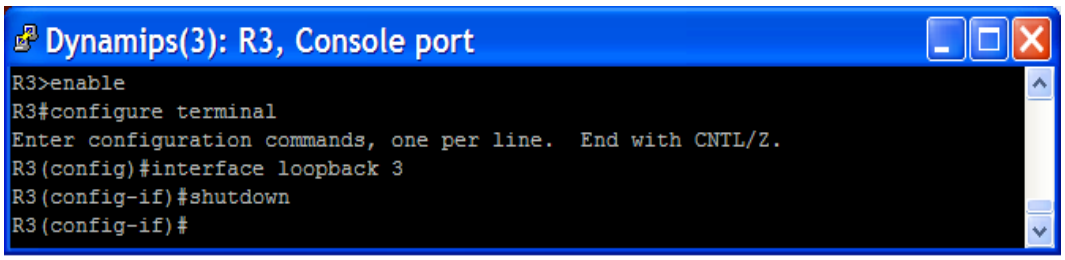
Funcionamiento de Auto-RP con *PIM-SDM*

Para explorar el funcionamiento de Auto-RP se habilita la depuración Auto-RP en el router R1 utilizando el comando **debug ip pim auto-rp** y se baja (Shut down) la interfaz Loopback3 en el router R3.

Figura 381. Activación de la depuración Auto-RP en R1.

Fuente: Software GNS3.

Figura 382. Bajar (Shut down) la interfaz Loopback3 en el Router R3.

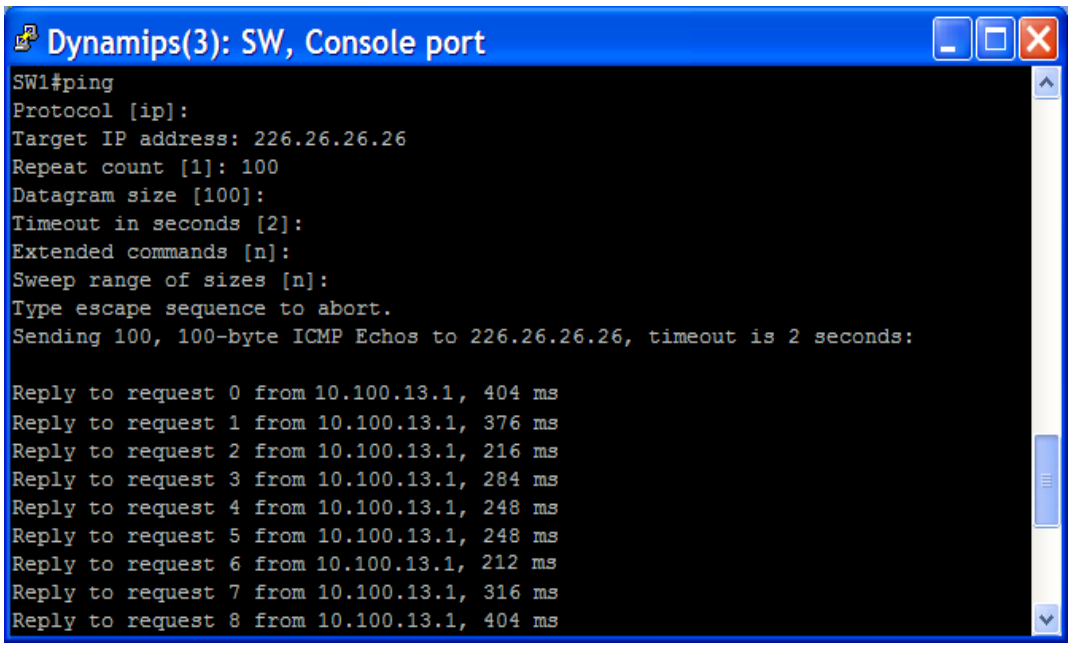


Fuente: Software GNS3.

Si la corriente del RP para el grupo 226.26.26.26 se convierte en inalcanzable, entonces otro RP debe ser elegido a través de AutoRP, o el o el grupo caerá nuevamente en el modo denso. En este caso, el grupo elegirá la interfaz loopback1 del router R1 como el nuevo RP para el grupo 226.26.26.26. Hasta el descubrimiento de la información sobre el RP en el tiempo de espera de R2, R2 seguirá enviando mensajes de Registro PIM al router R1.

Se emiten pings multicast repetidos para generar el estado (S,G) en los routers antes que R1 asuma ser el RP para el grupo 226.26.26.26.

Figura 383. Emisión de pings multicast repetidos en el switch SW1.

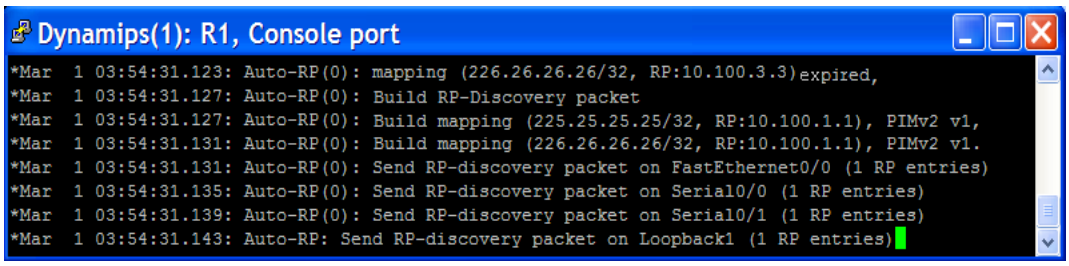


Fuente: Software GNS3.

Si se caen varios pings antes de alcanzar las interfaces loopback IGMP suscritas en R1 y R3 se debe a que la información RP debe cumplir un tiempo de espera en el agente de mapeo, y el nuevo RP debe ser elegido. Todos los routers que han sido informados de que la interfaz loopback de R3 es el RP para 226.26.26.26 deben esperar que su información cumpla un tiempo de espera antes de enviar multicast en modo denso. El número de pings caidos indica la duración del tiempo que tarda el periodo de espera de la información RP en ser excedida. Esto afecta el enrutamiento multicast haciéndolo ineficaz para el grupo 226.26.26.26 mientras que el RP para ese grupo sea inalcanzable. Mensajes de Registro PIM no se enviarán, por lo que los suscriptores IGMP a ese grupo no recibirán ningún dato.

Si la depuración de *Auto-RP* esta habilitado, se obtiene la siguiente salida en el agente de mapeo después de algunos minutos.

Figura 384. Activación de la depuración Auto-RP en R1.

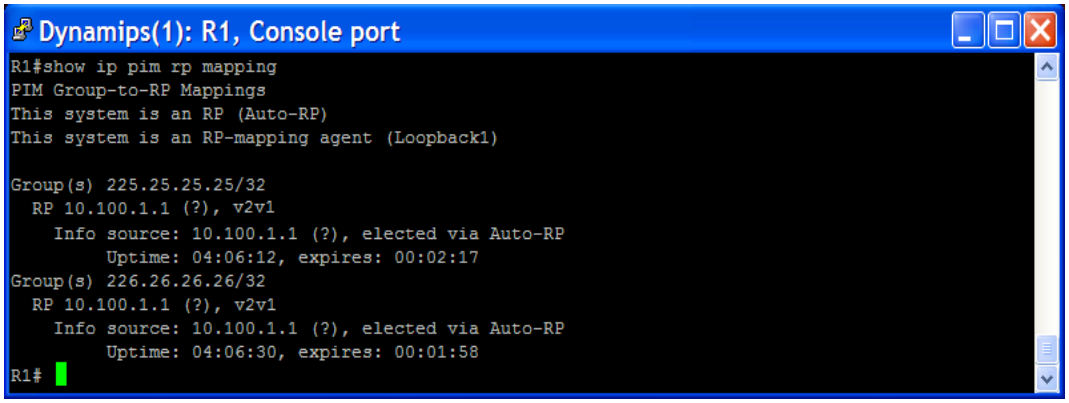


Fuente: Software GNS3.

En la salida anterior, el primer mensaje indica que desde que no se han recibido notificaciones RP para el periodo de espera, el agente de mapeo ha liberado a R3 como el RP para el grupo 226.26.26.26. El agente de mapeo elige a R1 como el nuevo RP para el grupo y envía el mensaje de descubrimiento RP a todos los routers PIM.

Se pueden chequear las asignaciones de RPs a los grupos multicast usando el comando **show ip pim rp mapping.**

Figura 385. Chequeo de mapeos del group-to-RP en R1.



Fuente: Software GNS3.

Auto-RP permite configurar RPs de respaldo (*backup RPs)* en una red *Sparse Mode* o *Sparse-Dense Mode.* Si se configurara un RP estático y después se volviera inalcanzable, los receptores no podrían usar el árbol compartido para recibir datos. Auto-RP provee una capa de redundancia en redes *Sparse Mode* usando agentes de mapeo para delegar roles RP a candidatos RP.

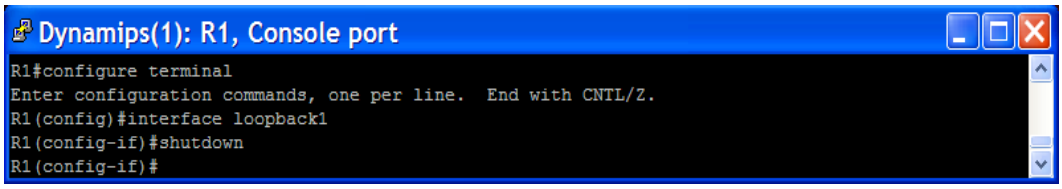
Operación de Dense-Mode Fallback

Dense-Mode Fallback describe el cambio de modo *PIM SM* (el cual requiere un RP) a *PIM DM* (que no requiere RP), este fallback se produce cuando se pierde la información del RP. Por defecto se encuentra habilitado en *PIM SDM*; para deshabilitarlo se utiliza el comando **no ip pim dm-fallback** el cual permitirá que en ausencia de un RP se continúe operando en modo *PIM-SM* asignando como RP a la dirección 0.0.0.0.

En este laboratorio se continuará con la configuración por defecto de PIM DSM con el *fallback* habilitado.

Si se baja la interfaz loopback en el router R1 el estado de los RPs para ambos grupos será inalcanzable.

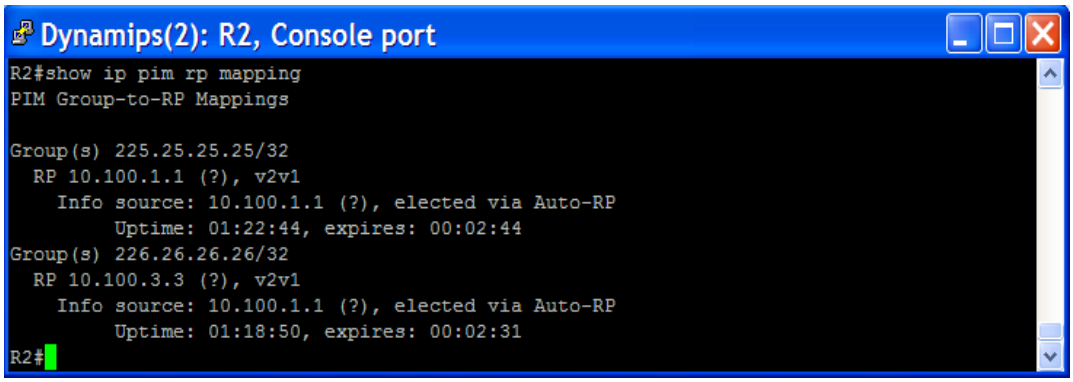
Figura 386. Bajar (shut down) la interface loopback1 en el router R1.



Fuente: Software GNS3.

El cambio a RPs inalcanzables no se refleja inmediatamente en los grupos multicast.

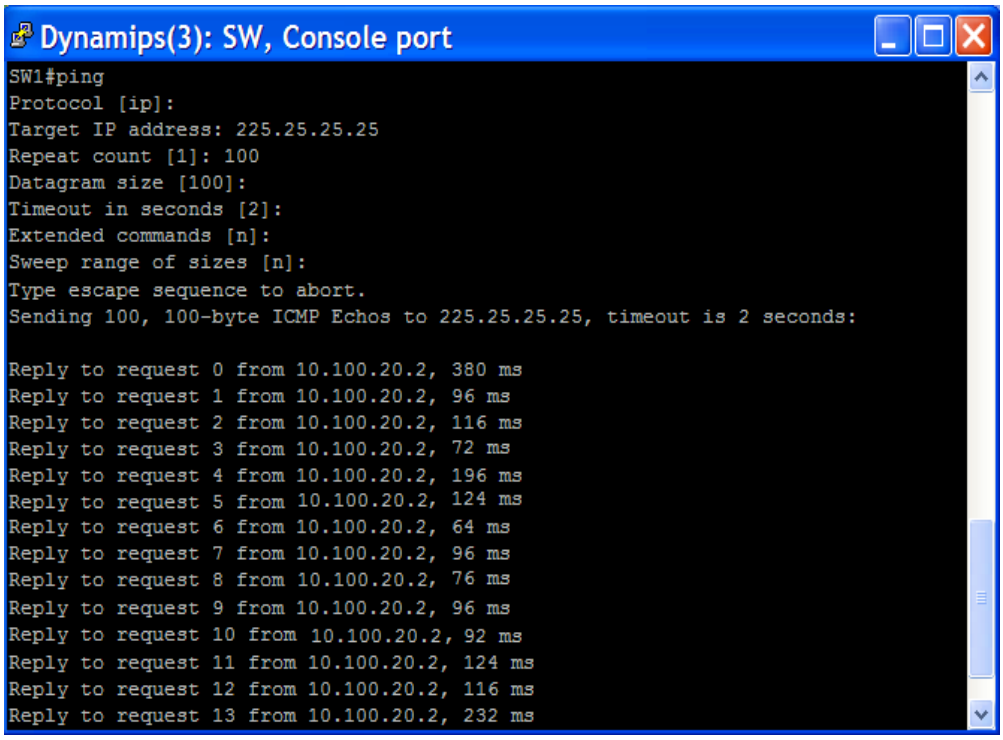
Figura 387. Chequeo de asignaciones RP en los grupos multicast en R2.



Fuente: Software GNS3.

Después de algunos minutos el router PIM será informado de que no hay RP para ninguno de los grupos y volverán a caer al modo denso (fallback). Esto se verifica utilizando los comandos **show ip pim rp mapping** y **show ip mroute** antes de que termine el mapeo.

Figura 388. Emisión de pings multicast en el switch SW1.

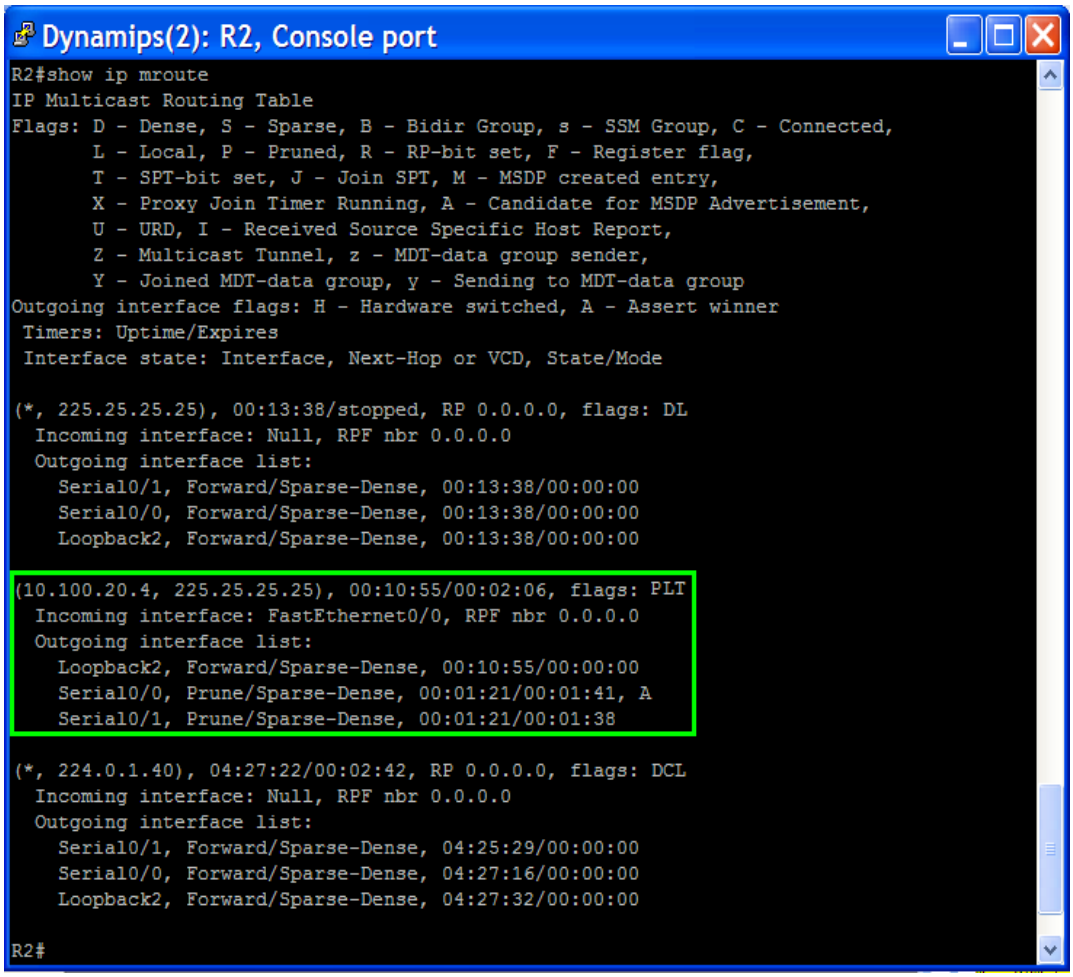


Fuente: Software GNS3.

Figura 389. Chequeo de asignaciones RP en los grupos multicast enR2

Fuente: Software GNS3.

Figura 390. Tabla de enrutamiento multicast en R2.

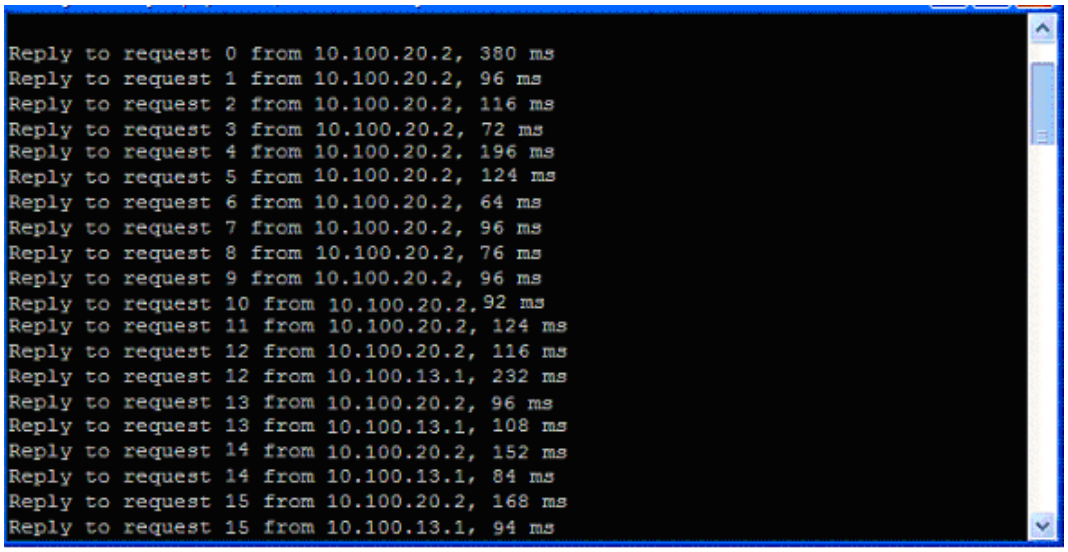


Fuente: Software GNS3.

Cuando las asignaciones *group-to-RP* expiran en R2, PIM nota que ya no hay un RP para los grupos 225.25.25.25 y 226.26.26.26 y convierte estos grupos a funcionar en modo denso. Cuando esto ocurre, PIM inunda de datos multicast a todas las interfaces y después poda a R2 debido a que no hay otros receptores del grupo 225.25.25.25

Se realiza nuevamente un ping desde SW1 y después se habilitan las interfaces loopback que se bajaron en el router R1 y R3.

Figura 391. Pings repetidos multicast en SW1 al grupo 225.25.25.25.



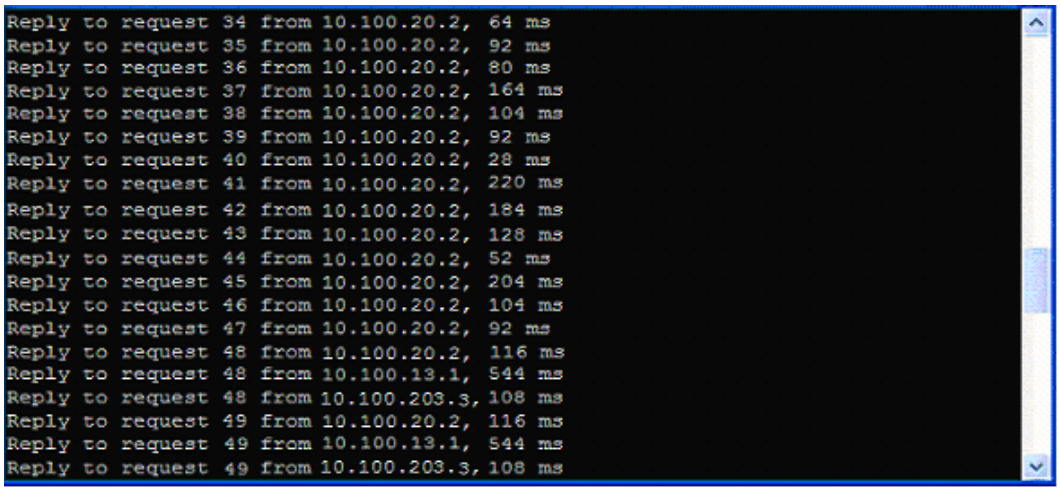
Fuente: Software GNS3.

El agente de mapeo no envió ningún RP para estos grupos a R2, por lo que continúa empleando un comportamiento *PIM-DM flood-and-prune.*

R2 escucha el anuncio Auto-RP de R1 al grupo 224.0.1.40. Debido a que ahora hay RPs en la red, R2 convierte el estado 225.25.25.25 y 226.26.26.26 a usar *PIM-SM.* R2 no empieza a enviar datos al RP debido a que el agente de mapeo aún no ha elegido un RP para el grupo 225.25.25.25. R2 espera a recibir la dirección RP del agente de mapeo

antes que comience a encapsular datos multicast como unicast para R1, el RP.

Figura 392. Pings repetidos multicast en SW1 al grupo 225.25.25.25.



Fuente: Software GNS3.

Request 48 es el primer paquete que R2 encapsula en un paquete unicast y envía al RP. R1, el RP, envía tráfico multicast al árbol compartido a todos los suscriptores del grupo 225.25.25.25.

Cuando R2 convierte un grupo a un modo diferente, los paquetes multicast inevitablemente se pierden antes de alcanzar los receptores. Aunque *sparse-dense mode* tiene un alto nivel de resistencia comparado con *sparse mode*, los paquetes aún se pierden durante la transición y el recobro del *fallback dense-mode*

Los anteriores laboratorios en multicast proporcionaron los fundamentos para entender sparse-dense mode. A continuación se explican como los conceptos de estos laboratorios conducen a un profundo entendimiento de PIM sparse-dense mode.

PIM-SDM es un modo híbrido en el cual el modo para los grupos por defecto es PIM-DM si un RP no se puede encontrar.

IGMP permite a los hosts y routers suscribirse a grupos de multicast. IGMP snooping evita que multidifusiones en la capa 2 actúen como broadcast.

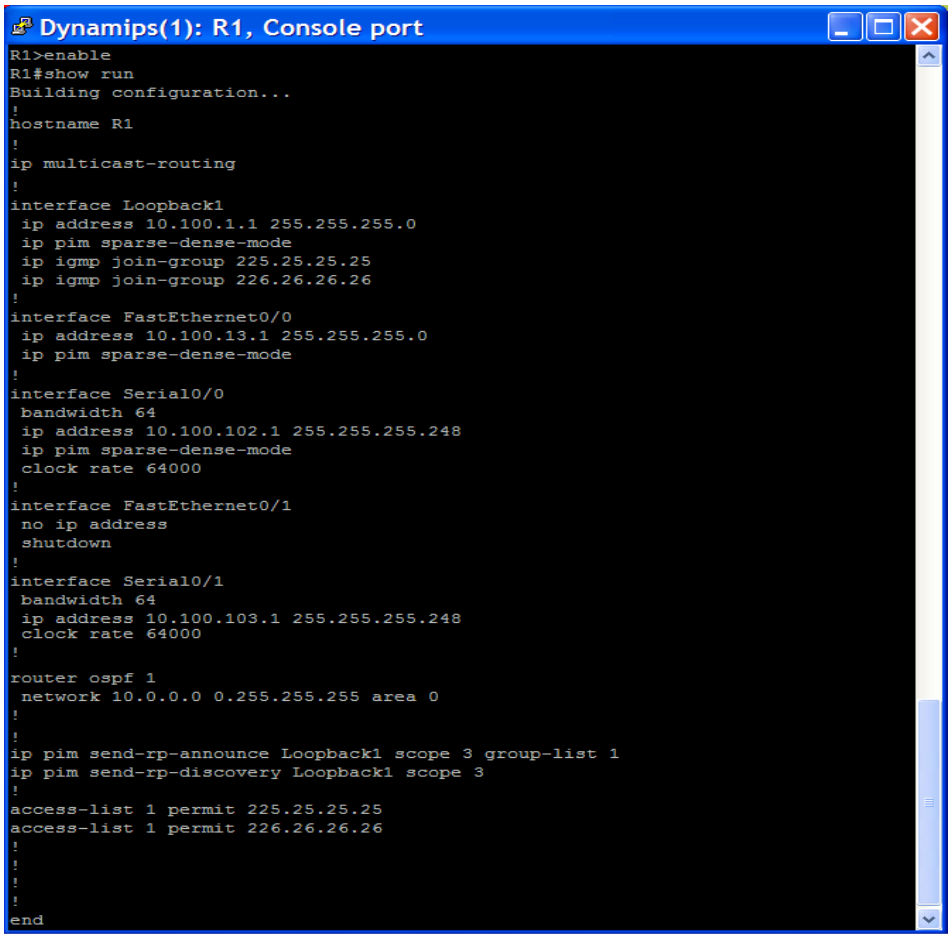
PIM-DM es un protocolo muy simple de implementar, pero requiere alto consumo de ancho de banda y sobrecarga de memoria.

PIM-SM proporciona mecanismos para crear una red multicast con bajo consumo de ancho de banda y de memoria.

Configuración Final

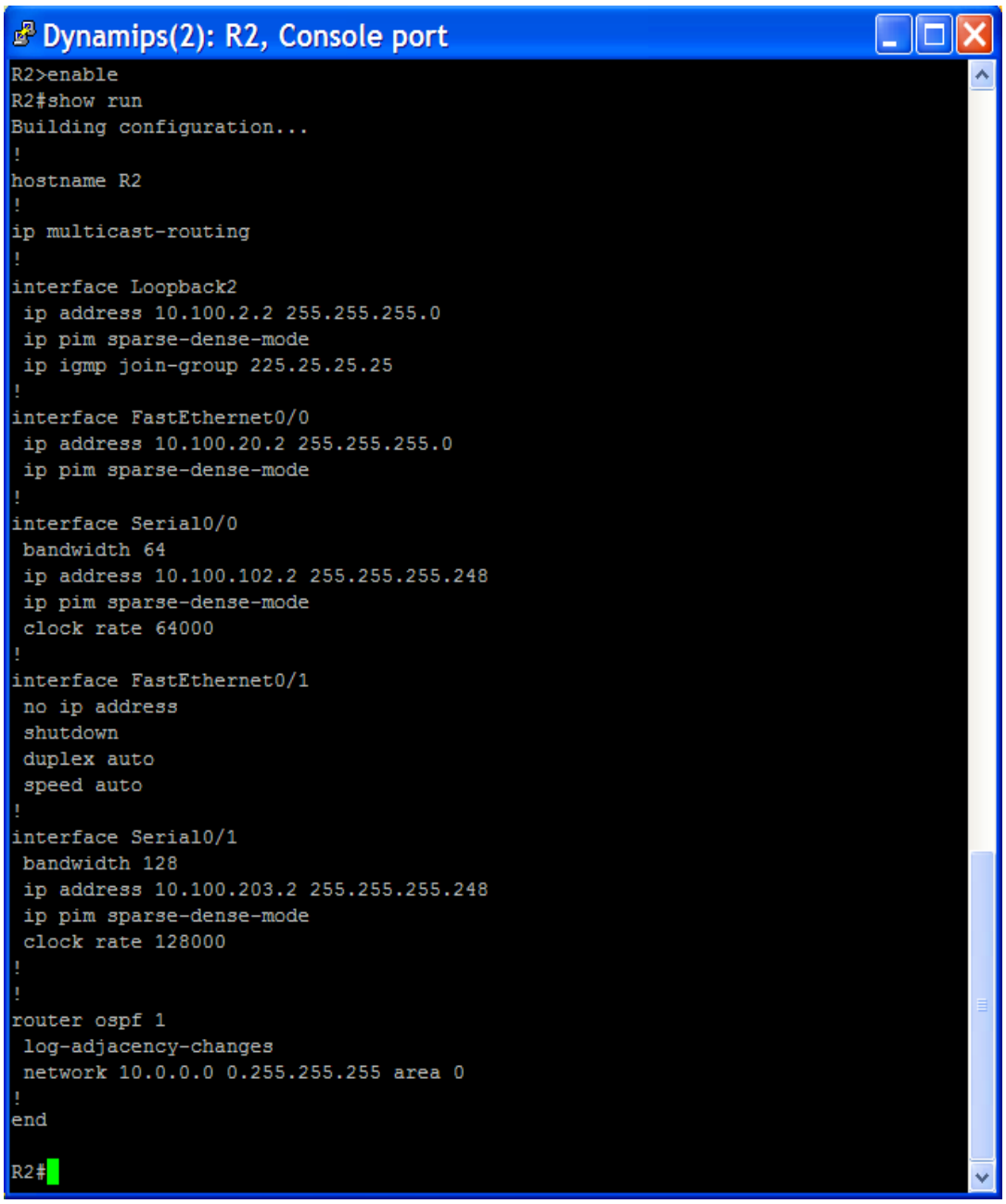
Finalmente se verifica la configuración final de las interfaces en todos los dispositivos con el comando **show run** como se muestra a continuación.

Figura 393. Configuración final del router R1.



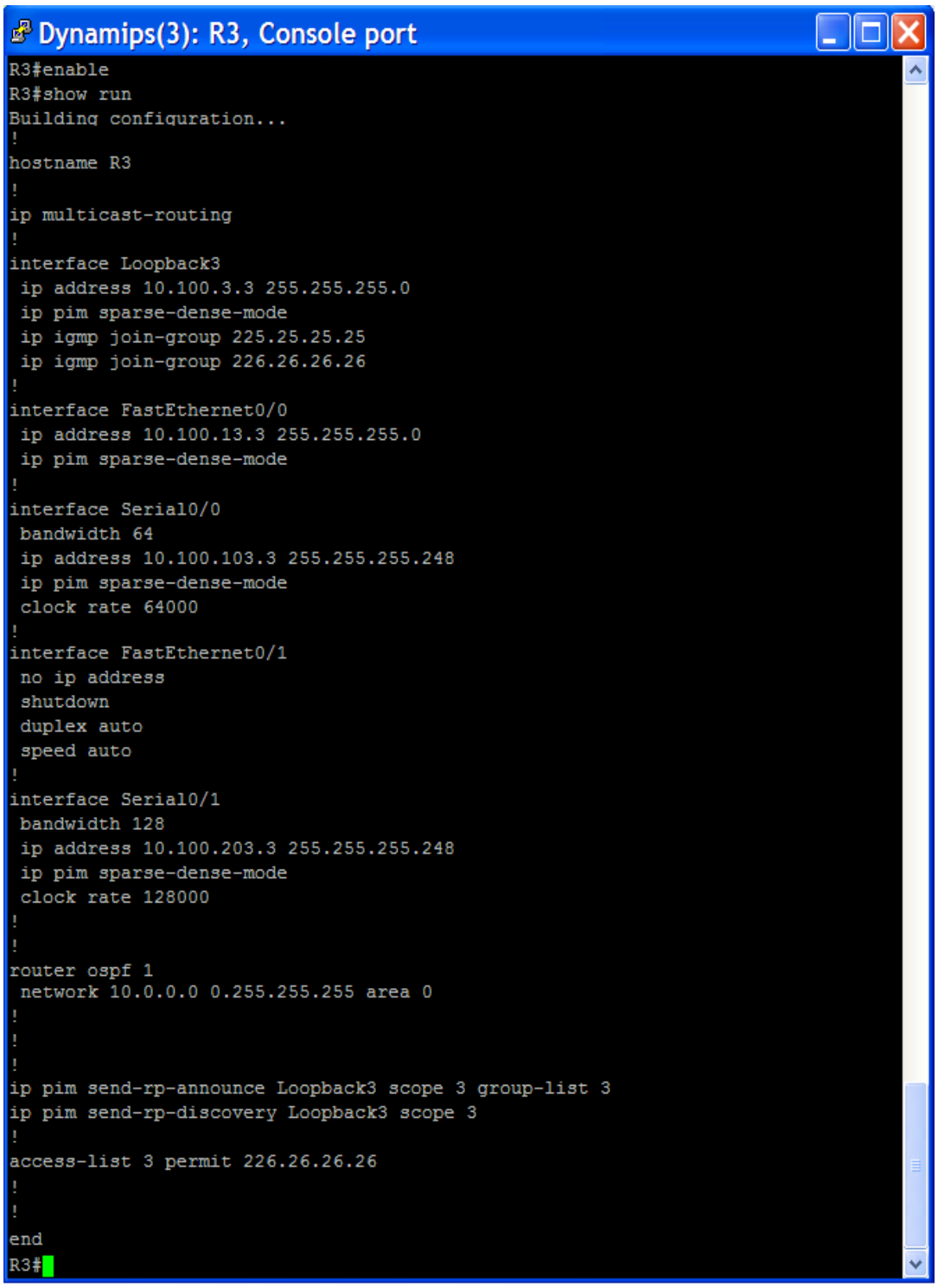
Fuente: Software GNS3.

Figura 394. Configuración final del router R2.



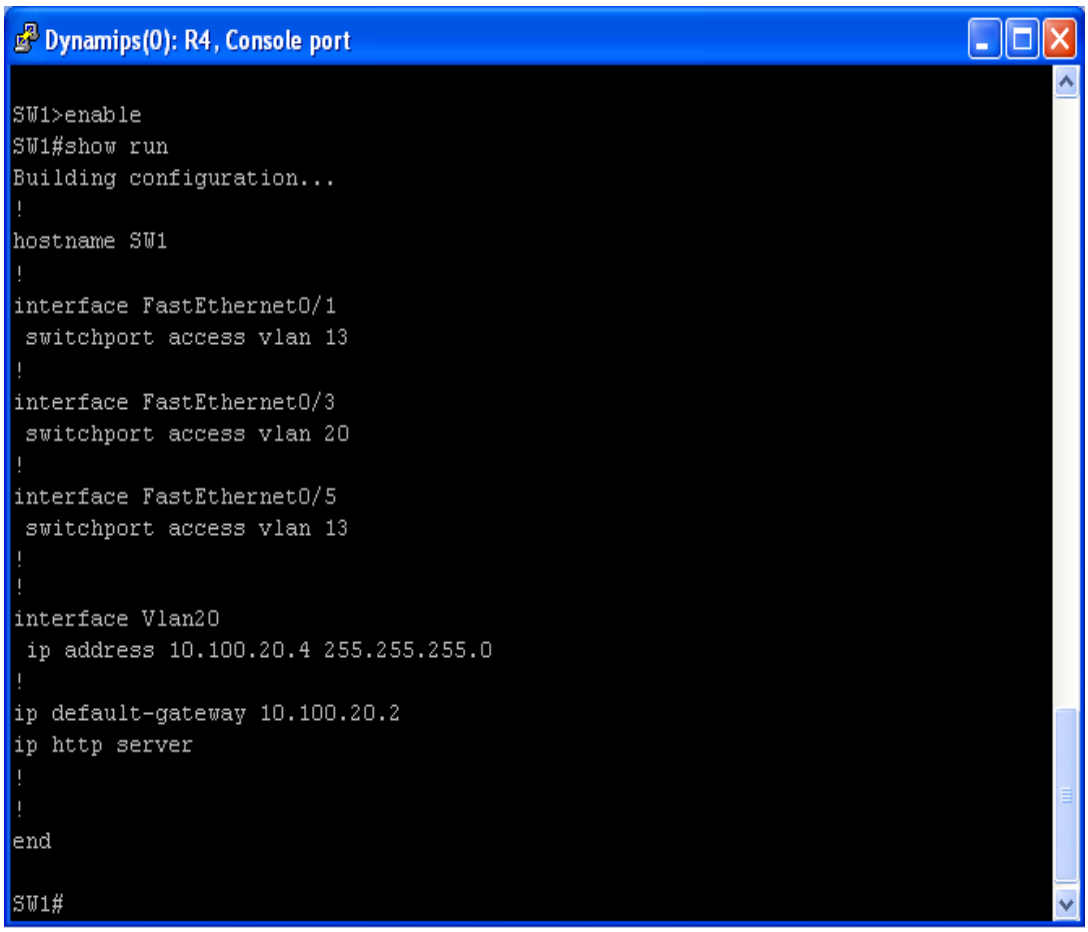
Fuente: Software GNS3.

Figura 395. Configuración final del router R3.



Fuente: Software GNS3.

Figura 396. Configuración final del Switch SW1.



Fuente: Software GNS3.

6. CONCLUSIONES

1. IP Multicast presenta un modelo conceptual interesante en cuanto al manejo eficiente de recursos en distribuciones simultáneas a múltiples usuarios. Esta tecnología está siendo cada vez más utilizada en intranets y en algunas comunidades dentro de internet (como la RNP[8]). Sin embargo su implantación en redes con millones de puntos o grupos multicast (internet) no ha tenido suficiente acogida debido a que además de requerir una gran inversión en recursos y equipos, demanda el consenso en políticas de gestión por parte de los operadores de red implicados.

2. EIGRP es un protocolo híbrido que toma lo mejor de los protocolos de vector distancia y de estado de enlace y se presenta como una buena opción para configurar grandes redes multiprotocolo, el hecho de tener su propio protocolo de transporte confiable (RTP) permite rápida convergencia y mayor confiabilidad en el transporte de tráfico, sin embargo por ser un protocolo propietario limita a que solo funcione en redes con dispositivos Cisco y que sus costos de operación incrementen, a diferencia del protocolo OSPF que es de distribución gratuita y que no discrimina entre los fabricantes de dispositivos pero que no resulta tan confiable ya que por ser de libre distribución requiere implementaciones adicionales de seguridad.

3. Los protocolos de enrutamiento OSPF y EIGRP mantienen la información de ruta y topología en tres tablas: la tabla de vecinos (enumera los routers adyacentes), la tabla de topología (integrada por todas las tablas de enrutamiento) y la tabla de enrutamiento (contiene

[8] RNP: Red Nacional de Enseñanza e Investigación. http://www.rnp.br/es/multicast/index.html.

las mejores rutas hacia un destino) con el fin de reaccionar ante cambios en la topología de la red.

4. El protocolo PIM-SM es más eficiente que PIM-DM ya que solo almacena información de enrutamiento multicast acerca de los árboles compartidos y los árboles fuentes para los cuales se ha hecho alguna solicitud. PIM-SM también es más eficiente que PIM-DM porque no utiliza la cantidad de ancho de banda en ramas de la red que no están interesadas en el tráfico multicast.

5. Los simuladores de redes permiten diseñar redes de datos y estudiar su comportamiento, permitiendo configurar los equipos (switches, routers, etc.) simulados de forma similar a como se configuran en la realidad. El simulador Packet Tracer ofrece la facilidad del manejo y permite realizar configuraciones avanzadas de protocolos como OSPF y EIGRP sin embargo es bastante restringido en cuanto a instrucciones propias del enrutamiento multicast, pues sus routers no aceptan muchos de los comandos de configuración multicast debido a su limitado IOS, a diferencia del software GNS3 que gracias a las diversas IOS de los routers permite completa configuración multicast, sin embargo la configuración de este último requiere un trabajo adicional ya que en ocasiones ocupa el 100% de la CPU y bloquea el equipo de trabajo.

7. GLOSARIO

A

ABR - *Area Border Router***:** es un router que conecta una o más áreas a la red backbone principal. Es considerado miembro de todas las áreas a las que está conectado. Un ABR guarda en memoria múltiples copias de la base de datos de estado de enlace, una para cada área a la cual ese router está conectado.

ACK: paquete Hello sin datos. Se trata de una aceptación.

Active: estado de la ruta cuando hay un cambio en la red y no se encuentra un FS. La ruta se establece en modo Active, y el router pregunta por rutas alternativas.

Adyacencia: se forma cuando dos routers vecinos han intercambiado información de enrutamiento y han sincronizado sus tablas. Ambos routers están en la misma red.

Adyacencia Completa: se produce en el momento que dos vecinos tienen totalmente sincronizadas la visión de la red (tienen exactamente la misma visión de la red).

AD - *Advertised Distance*: distancia notificada. El costo del camino a una red remota desde el vecino (por ejemplo La métrica del vecino).

Agente de mapeo (*mapping agent):* dispositivo que se encarga de distribuir información sobre todos los de la RPs en toda la red.

Algoritmo de Dijkstra: algoritmo que permite determinar el camino más corto dado un vértice origen al resto de vértices en un grafo dirijido y con pesos en cada arista. En este algoritmo se van explorando todos los

caminos más cortos que parten del origen y llevan a los demás vértices, cuando se obiente el camino más corto al resto de vértices el algoritmo se detiene.

Árbol de distribución multicast: definen el camino por el que los datos fluyen desde la fuente (S) a los receptores (R). Son dinámicos debido a que la fuente y los participantes varían en el tiempo. Son de dos tipos SPT y RPT.

Árbol SPF: árbol de la red topológica. El algoritmo elimina del árbol aquellos enlaces alternativos que pueden crear bucles. Cada router es el punto central de la red.

Área: grupo de routers con el mismo ID de área. Los routers en un área comparten la misma tabla topológica. El área se describe por interfaz en base a la configuración.

AS- *Autonomous System:* es un conjunto de redes bajo una administración común, las cuales comparten una estrategia de enrutamiento común. Para el mundo exterior, el AS es una entidad única.Puede ser administrado por uno o más operadores, a la vez que presenta un esquema unificado de enrutamiento hacia el mundo exterior.

ASBR - *Autonomous System Boundary Router:* es un router que está conectado a más de un SA y que intercambia información de enrutamiento con otros routers en otros sistemas autónomos. ASBR generalmente ejecuta protocolos de enrutamiento exterior y/o usa rutas estáticas.

B

BDR - *Backup Designated Router*: router que asume las funciones del DR en caso de que este falle.

Broadcast: modo de transmisión en el que un emisor envía información a múltiples nodos de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.

C

CGMP - *Cisco Group Management Protocol***:** protocolo de Cisco que corre entre un router multicast y un switch.

Conmutación: conexión que realizan los diferentes nodos que existen en distintos lugares y distancias para lograr un camino apropiado para conectar dos usuarios de una red. La conmutación permite la descongestión entre los usuarios de la red disminuyendo el tráfico y aumentando el ancho de banda.

Costo: es el valor asignado a un enlace. Los protocolos de estado de enlace asignan un costo a un enlace, a base del ancho de banda del enlace o la velocidad de transmisión. Esto se usa en lugar de los saltos.

D

Datagrama: paquete de datos que se transfiere en una conexión.

Descriptor de la Base de Datos: descrito como DBD - *Data Base Descriptor* o como DDPs - *Database Description Packets*. Estos paquetes son intercambiados entre vecinos durante el estado *exchange*.

Dijkstra: algoritmo complejo utilizado por los routers que utilizan protocolos de enrutamiento de estado del enlace, para encontrar el camino más corto al destino.

Dirección loopback: es una interfaz virtual y se encuentra en estado *up* en forma automática cuando está configurada. La ventaja de utilizar una interfaz loopback es que, a diferencia de las interfaces físicas, ésta no puede fallar. No hay cables ni dispositivos adyacentes reales de los que dependa la interfaz loopback para encontrarse en estado *up*. Por lo tanto, la utilización de una dirección de loopback para el ID del router ofrece estabilidad al proceso OSPF.

DDPs - *Database Description Packets:* paquetes de descripción de la base de datos.

DM - *Dense Mode:* modo Denso. Modo de operación de los protocolos de enrutamiento ip multicast. Se caracteriza por utilizar para la construcción de los árboles de distribucón multicast inundaciones periodicas y podas, árboles basados en el origen.

DR - *Designated Router:* router Designado. El DR es el router responsable de establecer las adyacencias entre todos los vecinos de una red de multiacceso. Un DR lleva a cabo tareas de envío y sincronización y se asegura que todos los routers tengan una base de datos topológica idéntica.

DUAL - *Diffusing Update Algorithm*: algoritmo de actualización difusa. Es un algoritmo de vector-distancia utilizado por EIGRP, que garantiza una operación sin bucles durante todo el cálculo de rutas, lo que permite la sincronización simultánea de todos los routers involucrados en cambio de topología.

E

Enrutamiento: capacidad de transmitir datos entre redes interconectadas

Estado de enlace: algoritmo que aplican los routers para calcular rutas óptimas a cada destino. Cada router recibe información sobre el estado de los enlaces de la red y la emplea para un cálculo de trayectoria más corta.

Estado Exchange: estado en el cual dos vecinos descubren el mapa de la red. Cuando estos routers sean adyacentes, intercambiarán DDPs para asegurarse que tienen la misma base de datos topológica.

Estado Exstart: estado en el cual dos vecinos determinan los números de secuencia de los DDPs y establecen su relación maestro/esclavo.

Estado Init: estado en el cual se ha enviado un paquete *Hello* y se está esperando una respuesta para entrar en comunicación *two-way*.

Estado Loading: estado en el cual el router receptor solicita más información durante el proceso en el cual dos routers están creando la adyacencia. Si se necesita más información se enviará un LSR al que se responderá con un LSU.

Estado Two-Way: estado durante el proceso de crear la adyacencia. El router ve su propio ID en un paquete *Hello* recibido de otro router. Este es el punto anterior a que la información de routing sea intercambiada.

F

Fallback dense-mode: describe el cambio de modo PIM de *SM* (el cual requiere un RP) a *DM* (que no requiere RP), este fallback se produce cuando se pierde la información del RP.

FC - *Feasible Condition*: condición de factibilidad. Cuando un router tiene una AD más pequeña que su FD.

FD - *Feasible Distance*: distancia factible. La métrica más baja a una red remota.

Flood (Flooding): inundación. La información de la red se envía a todos los dispositivos del dominio por inundación.

FS - *Feasible Successor*: sucesor factible. Si un vecino reporta una AD más pequeña que la FD, entonces el vecino se convierte en Feasible Successor.

Forwarder: router PIM con la menor distancia administrativa y métrica a la fuente.

Frame: bloque fijo de datos transmitidos como una sola entidad. También llamado packet (paquete).

G

Grupo multicast: es un conjunto de destinatarios interesados en recibir un flujo de datos en particular. Este grupo no tinene limites físicos ni geográficos (los hosts pueden estar ubicados en cualquier punto de internet o red privada).

H

Hello: mensajes utilizados para encontrar y mantener vecinos en la tabla topológica.

Holdtime: valor configurado en el paquete Hello. Determina cuanto tiempo se va a esperar para recibir Hellos de un vecino antes de declararlo no disponible.

I

IGMP - *Internet Group Management Protocol***:** protocolo de red que establece un mecanismo para el intercambio y actualización de información sobre la pertenencia de nodos de un segmento a un grupo multicast.

IGMP Snooping: proceso de escuchar tráfico IGMP. Permite al switch escuchar tráfico IGMP entre host conectados al switch y routers multicast en la red.

Internetwork: agrupamiento de redes interconectadas por routers y otros dispositivos que funciona (en general) como una sola red. A veces denominada una internet, que no se debe confundir con la Internet.

Inundación: también conocido como *Flooding*. La información de la red se manda a todos los dispositivos del dominio por inundación.

J

Join: mensaje (de unión) que envía un posible miembro multicast al DR del grupo al cual desea unirse.

L

LSA - *Link-State Advertisement*: notificaciones de estado de enlace. Paquete que describe los enlaces del router. Existen diferentes tipos de LSAs.

Link-State Database: también conocido como mapa topológico. Mapa con todos los routers, sus enlaces y estado de sus enlaces.

LSR - *Link-State Request*: cuando un router recibe la DDP completa con LSAs parciales los compara la base de datos topológica, si encuentra algún LSA que no esté presente o con una entrada más antigua que la de la DDP, envía una petición (LSR) con más información.

LSU - *Link-State Update*: respuesta a un LSR. Es un LSA con la información solicitada.

M

Métrica: método mediante el cual un algoritmo de enrutamiento determina que una ruta es mejor que otra. Esta información se guarda en tablas de enrutamiento. Las métricas incluyen ancho de banda, costo de la comunicación, retraso, número de saltos, carga, MTU, costo de la ruta y confiabilidad.

Multicast: método de transmisión uno a muchos que realiza el envio de datos a múltiples destinos simultáneamente.

MVPN-*multicast virtual prívate network:* permite a un proveedor de servicios configurar y soportar el tráfico multicast en una conmutación de etiquetas multiprotocolo (MPLS) entorno de red privada virtual (VPN). Esta función admite enrutamiento y envio de paquetes de multicast para cada individuo VPN de enrutamiento y el reenvio de la instancia (VRF), y proporciona un mecanismo para el transporte de paquetes de multicast VPN a través de la columna vertebral de proveedor de servicios

MVRF- Multicast Virtual Route Forwarding: es la tabla de enrutamiento multicast para un VRF.

N

Nodo: punto de interconexión en la red.

O

OSPF - *Open Shortest Path First*: protocolo de enrutamiento de estado de enlace.

P

Passive: una ruta operacional es pasiva. Si no se ha perdido el camino, el router examina la tabla topológica en busca de un FS. Si existe un FS se añade a la tabla de routing, si no, el router pregunta a los vecinos y la ruta se queda en modo active.

Prioridad: herramienta de Cisco con la cual se puede escoger el DR, o incluso decidir que router nunca llegará a ser DR o BDR.

Q

Query: consulta enviada por el router cuando pierde el camino a una red. Si no existe una ruta alternativa (feasible successor), envía la query a los vecinos preguntando si tienen un feasible successor. Esto hace que la ruta pase a estado *active*.

Query Scoping: diseño de red para limitar el ámbito del rango de peticiones, es decir, a qué distancia se permite que se busque un feasible

successor. Esto es necesario para prevenir SIA, lo cual puede provocar problemas en la red.

R

Reply: respuesta a una query, si el router no tiene información para devolver entonces pregunta a todos sus vecinos. El Reply se envía por unicast.

RTO - *Retransmission Timeout*: tiempo calculado en referencia al SRTT. El RTO determina cuánto tiene que esperar el router el ACK antes de retransmitir el paquete.

Router Interno: router que tiene todas las interfaces en la mismo área.

RP - *Rendezvous Point:* punto de encuentro. Los RP's se usan en PIM-SM para proporcionar puntos de unión entre las fuentes multicast y los miembros de un grupo en una red multicast. Los RP's crean un punto común para que los routers multicast instalen árboles compartidos.

RPF - *Reverse Path Forwarding: reenvio de ruta inversa. E*s una técnica utilizada en los routers con el propósito de garantizar el reenvio correcto de tráfico multicast, hace uso de la tabla de enrutamiento unicast existente para determinar los vecinos downstreams, ayuda a garantizar que la distribución del árbol este libre de bucles.

RPT – *Rendezvous Point Tree*: árbol de punto de encuentro o árbol compartido.

RTP- *Reliable Transport Protocol*: mecanismo utilizado para determinar los requerimientos de entrega de los paquetes, asegurando la entrega secuencial de los mismos.

S

Sistema Autónomo: es un conjunto de redes bajo una administración común, las cuales comparten una estrategia de enrutamiento común. Para el mundo exterior, el AS es una entidad única. El AS puede ser administrado por uno o más operadores, a la vez que presenta un esquema unificado de enrutamiento hacia el mundo exterior.

SDM - *Sparse-Dense Mode*: modo esparcido-denso (híbrido)

SIA - *Stuck in Active:* estado de un router que ya ha enviado paquetes y está esperando los ACKs de sus vecinos.

SM - *Sparse Mode**:*** modo Esparcido. Modo de operación que utilizan los protocolos de enrutamientro ip multicast. Se caracterizan por usar árboles compartidos a través de un nodo llamado RP.

SPF- *Shortest Path First*: es básicamente el algoritmo de Dijkstra, utilizado para decidir la(s) mejor(es) ruta(s).

SPT-*Shortest Path Tree:* árbol basado en origen.Es la forma más simple del árbol de distribución multicast, es un árbol fuente con su raíz en el origen y sus ramas formando un spanning tree a través de la red y hacias los receptores.

SRTT - *Smooth Round-Trip Time:* el tiempo que el router espera después de enviar un paquete para oír el acknowledge.

Sucesor: el siguiente router que pasa la FC. Se escoge el que tenga la métrica más baja a un destino de los FS.

T

Tabla de Enrutamiento: lista de las redes disponibles y los mejores caminos.

Tabla de Vecinos: tabla construida con paquetes *Hello*. Los paquetes *Hello* también portan información sobre los vecinos.

Tabla Topológica: tabla que contiene todos los caminos anunciados por los vecinos a todas las redes conocidas.

U

UDP – *User Datagram Protocol* . Protocolo de datagrama de usuario. Al igual que IP, es un protocolo *no orientado a conexión* (no establece una conexión previa con el otro extremo para transmitir un mensaje UDP), lo que ocasiona que los mensajes enviados puedan duplicarse o llegar desordenados al destino. Además es un protocolo *no fiable* lo cual indica que los mensajes UDP se pueden perder.

Unicast: método de transmisión donde el envio de datos se realiza de un único emisor a un único receptor.

Update: paquete EIGRP que contiene información sobre los cambios de la red. Se envían únicamente cuando hay un cambio en la red que afecta a los routers

V

Vecino: router en el mismo enlace físico con el que se comparte información de enrutamiento.

Vector de distancia: método de enrutamiento para cálculo de rutas óptimas a cada destino de la red. Periódicamente, cada router recibe información sobre las rutas de sus vecinos; un router reemplaza una ruta

actual si queda disponible otra de menor costo. Este método es utilizado por los protocolos RIP, IGRP y EIGRP.

VPN- *virtual prívate network*: una VPN es la conectividad de red a través de una infraestructura compartida, como un proveedor de servicios Internet (ISP). Su función es proporcionar a las mismas políticas y el desempeño como una red privada, a un costo reducido de la propiedad, lo que crea muchas oportunidades para el ahorro de costos a través de las operaciones y la infraestructura.

VRF-*virtual routing and forwarding:* es una tecnología que permite que varias instancias de una tabla de enrutamiento puedan coexistir en el mismo router, al mismo tiempo. Tabla de enrutamiento que contiene rutas VPN

BIBLIOGRAFÍA

- CACHINERO POZUELO, Juan Angel. Análisis y modelado de "multicast" interdominio para el soporte de servicios de video. Madrid, 2009, 268 p. Trabajo de grado (Ingeniero de Telecomunicación), Universidad Politécnica de Madrid. Escuela superior de ingenieros de telecomunicación.

- CONLAN, Patrick J. Cisco® Network Professional's Advanced Internetworking Guide. Indianapolis, EUA: Wiley Publishing, Inc. 2009. 823 p. ISBN: 978-0-470-38360-5

- LAWRENCE , Harte. Introduction to Data Multicasting, IP Multicast Streaming for Audio and Video Media Distribution. Althos Publishing. 2008.

- RIGOTTI, Guillermo. Implementación y Análisis de CBTv2 en el medioambiente Ns. Argentina, 1998, 195 p. Trabajo de grado (Magíster en redes de datos), Universidad Nacional de la Plata. Facultad de Ciencias Exactas.

- Williamson, Beau. Developing IP Multicast Networks. Indianapolis, EUA: Cisco Pres. 2000. 568 p. ISBN: 1-57870-077-9

- WITTMANN, Ralph; Zitterbart Martina. Multicast communication: protocols and applications. Morgan Kaufmann Publishers. London, 2001.

- Pragyansmita Paul. Survey of multicast routing algorithms and protocols [Artículo de internet]. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.20.1460. [Consulta: Febrero 12 de 2010]

- Cisco. Internet Protocol IP multicast technology. [Artículo de internet]. http://tools.cisco.com/search/JSP/search-results.get?strQueryText=i p+multicast&Search+All+cisco.com=cisco.com&language=en&country=US&thissection=f&accessLevel=Guest.[Consulta: Febrero 12 de 2010]

- Cisco. Multicast [Indice de contenidos con hipervínculos a artículos generales de multicast].

http://tools.cisco.com/search/JSP/search-results.get?isPagination=true&strQueryText=multicast&strDocsPerPage=10&strSortBy=&strStartDoc=91&strqueryid=1&websessionid=gtO-q4DzQkDrXLEr1JVmDTO&strCurrentSimilarSearchBreadCrumb=&strCurrentSelectedModifierValues=&country=US&language=en&profile=enushomesppublished

ANEXOS

ANEXO A. ALGORITMOS DE ENRUTAMIENTO[9]

Los protocolos de enrutamiento pueden clasificarse en IGP o EGP, lo que describe si un grupo de Routers se encuentra bajo una sola administración o no. Los IGP pueden a su vez clasificarse en protocolos de vector-distancia o de estado de enlace.

En los protocolos de enrutamiento por vector de distancia los routers deben tomar decisiones de rutas preferidas conforme a una distancia o métrica a una red. Un router vector distancia confía en que otro router publique la verdadera distancia hacia la red de destino.

Los protocolos de enrutamiento de estado de enlace tienen un enfoque diferente. Los protocolos de enrutamiento de estado de enlace crean un mapa topológico de la red y cada router utiliza dicho mapa para determinar la ruta más corta hacia cada red. Los routers de estado de enlace utilizan un mapa para determinar la ruta preferida para alcanzar otro destino. Los routers que ejecutan un protocolo de enrutamiento de estado de enlace envían información acerca del estado de sus enlaces a otros routers en el dominio de enrutamiento. El estado de dichos enlaces hace referencia a sus redes conectadas directamente e incluye información acerca del tipo de red y los routers vecinos en dichas redes; de allí el nombre protocolo de enrutamiento de estado de enlace.

El enrutamiento por vector-distancia determina la dirección y la distancia (vector) hacia cualquier enlace en la red. La distancia puede ser el número de saltos hasta el enlace. Los routers que utilizan los algoritmos de vector-distancia envían todos o parte de las entradas de su tabla de enrutamiento a los routers adyacentes de forma periódica. Esto sucede aún si no ha habido modificaciones en la red. Un router puede verificar

[9] **CCNA - Cisco Certified Network Associate**

todas las rutas conocidas y realizar las modificaciones a su tabla de enrutamiento al recibir las actualizaciones de enrutamiento. Este proceso también se llama "enrutamiento por rumor". La comprensión que el router tiene de la red se basa en la perspectiva que tiene el router adyacente de la topología de la red.

Los ejemplos de los protocolos por vector-distancia incluyen los siguientes:

- **Protocolo de información de enrutamiento (RIP):** es el IGP más común de la red. RIP utiliza números de saltos como su única métrica de enrutamiento.
- **Protocolo de enrutamiento de Gateway interior (IGRP):** es un IGP desarrollado por Cisco para resolver problemas relacionados con el enrutamiento en redes extensas y heterogéneas.
- **IGRP mejorada (EIGRP):** esta IGP propiedad de Cisco incluye varias de las características de un protocolo de enrutamiento de estado de enlace. Es por esto que se ha conocido como protocolo híbrido balanceado, pero en realidad es un protocolo de enrutamiento vector-distancia avanzado.

Los protocolos de enrutamiento de estado de enlace se diseñaron para superar las limitaciones de los protocolos de enrutamiento vector distancia. Los protocolos de enrutamiento de estado de enlace responden rápidamente a las modificaciones en la red, enviando actualizaciones sólo cuando se producen las modificaciones. Los protocolos de enrutamiento de estado de enlace envían actualizaciones periódicas, conocidas como renovaciones de estado de enlace a rangos más prolongados; por ejemplo, 30 minutos.

Cuando una ruta o enlace se modifica, el dispositivo que detectó el cambio crea una publicación de estado de enlace (LSA) en relación a ese enlace. Luego la LSA se transmite a todos los dispositivos vecinos. Cada

dispositivo de enrutamiento hace una copia de la LSA, actualiza su base de datos de estado de enlace y envía la LSA a todos los dispositivos vecinos. Se necesita esta inundación de LAS para estar seguros de que todos los dispositivos de enrutamiento creen bases de datos que reflejen de forma precisa la topología de la red antes de actualizar sus tablas de enrutamiento.

Por lo general, los algoritmos de estado de enlace utilizan sus bases de datos para crear entradas de tablas de enrutamiento que prefieran la ruta más corta.

Ejemplos de protocolos de estado de enlace son: Primero la Ruta Libre Más Corta (OSPF) y el Sistema Intermedio a Sistema Intermedio (IS-IS).

ANEXO B. ALGORITMO DUAL

El Algoritmo de actualización por difusión (DUAL) es el algoritmo de convergencia utilizado por EIGRP en lugar de los algoritmos Bellman-Ford o Ford Fulkerson utilizados por otros protocolos de enrutamiento por vector de distancia, como RIP. DUAL está basado en investigaciones realizadas en SRI International, mediante el uso de cálculos propuestos por primera vez por E.W. Dijkstra y C.S. Scholten. El trabajo más destacado con DUAL lo realizó J.J. Garcia-Luna-Aceves.

Los loops de enrutamiento, incluso los temporales, pueden ser extremadamente perjudiciales para el rendimiento de la red. Los protocolos de enrutamiento por vector de distancia, como RIP, impiden loops de enrutamiento con temporizadores de espera y horizontes divididos. A pesar de que EIGRP utiliza ambas técnicas, las usa de manera un tanto diferentes; la forma principal en la que EIGRP impide los bucles de enrutamiento es con el algoritmo DUAL.

El algoritmo DUAL se utiliza para que no se produzcan bucles a cada instante, a lo largo de un cálculo de ruta. Esto permite que todos los routers involucrados en un cambio de topología se sincronicen al mismo tiempo. Los routers que no se ven afectados por los cambios en la topología no se encuentran involucrados en el recálculo. Este método proporciona a EIGRP mayor tiempo de convergencia que a otros protocolos de enrutamiento por vector de distancia.

La Máquina de Estado Finito DUAL realiza todo el proceso de decisión para todos los cálculos de ruta. En términos generales, una Máquina de Estado Finito (FSM) es un modelo de comportamiento compuesto de un número finito de estados, transiciones entre esos estados, y eventos o acciones que crean las transacciones.

FSM DUAL rastrea todas las rutas, utiliza su métrica para seleccionar rutas eficientes y sin bucles, y selecciona las rutas con la ruta de menor costo para insertarla en la tabla de enrutamiento.

Como el recálculo del algoritmo DUAL puede exigir mucho al procesador, es aconsejable evitar el recálculo siempre que sea posible. Por lo tanto, DUAL mantiene una lista de rutas de respaldo que ya ha determinado como sin bucles. Si la ruta principal en la tabla de enrutamiento falla, el mejor camino de respaldo se agrega de inmediato a la tabla de enrutamiento.