UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

IMPLENTACION DE REDES IP MULTICAST

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

ALBERTO GALVAN BALBOA

PROMOCIÓN
1994 - I

LIMA – PERÚ

2008

IMPLEMENTACIÓN DE REDES IP MULTICAST

Dedico este trabajo a:

A mis padres por su dedicada atención en los momentos de flaqueza y necesidad, a ellos les dedico este trabajo por ser los principales motivadores de mi superación.

A mi esposa Luz Elena y mi hija Sol Angie por haberme brindado el apoyo y sacrificio del tiempo en todos los momentos que aun siguen pasando.

A mi abuela Hermógenes en homenaje a su recuerdo.

A mi primo Luis Rolando Cusi por haberme motivado a realizar este trabajo, con sus consejos y atenciones las cuales no olvido.

A mi primo René Vega Pariona que el Dios Todopoderoso lo tenga en su memoria.

SUMARIO

Objetivo General

El presente documento tiene como objetivo general ofrecer una visión detallada del IP multicast, en él se explican las aplicaciones que utilizan la tecnología multicast y los beneficios que proporciona al usuario final, basados en la experiencia de implementar una red multicast en Telefónica del Perú.

Objetivos Específicos:

- Comprobar las ventajas de implementar una red IP multicast en comparación con red unicast tradicional.
- Identificar los criterios de diseño para implementar redes multicast que se ajusten a los requerimientos y necesidades de nuevas aplicaciones multimedia basados en los conceptos básicos del IP multicast.
- Identificar los requerimientos de ancho de banda para brindar los servicios multicast a los usuarios empresariales.

Resumen del Desarrollo

En el marco teórico se definen los conceptos basicos del IP multicast basado en los documentos multicast RFC (Reference Forum Comment), luego se describe la clasificación de direcciones IP clase D de acuerdo al uso particular que será tratado, se dá una explicación detallada de los protocolos asociados al multicast, junto a ello se analizan los comandos de configuración y verificación de redes multicast, también se presentan los criterios de diseño para la implementación de redes IP multicast basados en la experiencia adquirida en Telefónica del Perú.

Finalmente se muestran las conclusiones en base a las pruebas de laboratorio y a la implementación de una red IP multicast.

ÍNDICE

CAPITULO III

PROTOCOLO DE ADMINISTRACIÓN GRUPO INTERNET

CAPITULO IV

PROTOCOLO DE RUTEO MULTICAST

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

PRÓLOGO

Luego de la aparición del Internet a mediados de los año 80 del siglo pasado, los cambios tecnologicos han llevado a cambios constantes en el uso de aplicaciones, desde entonces la demanda de nuevas aplicaciones estan siendo usados en video streaming, video conferencia, distribución de contenidos de video, capacitación en linea y otras formas de aplicaciones de tiempo real han llevado a demandar mayor disponibilidad de ancho de banda para altos volúmenes de tráfico.

En el ámbito profesional tuve la oportunidad de trabajar en este campo, que tiene que ver con la implementación de redes IP Multicast para entidades Bancarias de nuestro medio.

Con tráfico unicast se requiere que el emisor envíe un flujo diferente para cada host destino, esta situación conlleva a que el ancho de banda en la Wan del emisor se dimensionen a la suma total de flujos. De hecho los resultados de los trabajos efectuados con la implementación de redes IP Multicast han resuelto muchos inconvenientes en el uso de recursos de ancho de banda, pues ahora sólo basta que el emisor envíe un frame Multicast para que éste a través de la red llegue hacia todos los destinos del grupo Multicast al que pertenecen.

Actualmente la Empresa de Telefónica del Perú, ha integrado la funcionalidad del IP Multicast en su red MPLS, permitiendo el intercambio de información multicast sobre Redes Privadas Virtuales bajo la modalidad de topología full mesh. Razón por la cual el presente trabajo se considera que está relacionado con los temas de tecnología de punta en las telecomunicaciones, pues contribuye enormemente en la mejora las comunicaciones de las empresas del mercado Peruano.

El informe de suficiencia consiste en realizar el estudio e implementación de redes multicast. Ahora pasamos a describir brevemente algunos rasgos sobresalientes que se desarrollan en cada capítulo.

En el capitulo I se formula el marco teórico necesario para la implementación de una red multicast , se describen los conceptos y las aplicaciones del IP multicast. Las redes deben

ser cuidadosamente diseñados, utilizando nuevos criterios de diseño, en apoyo al IP multicast.

En el capitulo II se refiere a algunos de los conceptos más básicos de IP multicast, en el ambito de direcciones IP clase D, ademas de la clasificacion de direcciones de acuerdo al uso particular que sera tratado, incluye el mapeo de direccionamiento MAC Ethernet en Multicast y como se aborda la relación en Multicast tanto en Capa 2 y Capa 3.

En el capitulo III se describe como IGMP se utiliza sobre la base del mecanismo de señalización para que otros puedan convertirse en miembro de un grupo multicast. Tambien se incluye al IGMPv2 que logra ampliar el mecanismo de señalización.

En el capitulo IV se detalla los diferentes modos de protocolos y categorías de protocolos de ruteo, que sin duda nos permiten entender la forma en que a nivel de ruteo de paquetes son usados para el reenvio de trafico en una red multicast.

En el capitulo V se describe las implicancias de multicast en un red de switches LAN, con el consecuente control de trafico multicast, y el uso eficiente de protocolos como el IGMP Snooping y el CGMP, las mismas que permiten el control en la formación de grupos multicast.

En el capitulo VI se describe los principales comandos que son usados en los routers como parte de implementacion de una red multicast. Es de suma importancia conocer el uso de estos comandos que nos permitiran adecuar nuestra red de acuerdo a las necesidades requeridas con redes multicast.

CAPITULO I
EXPLICACIÓN DEL IP MULTICAST

1.1 Introducción al IP Multicast.

El presente capitulo contempla el ambito del IP Multicast donde se integran las aplicaciones multimedia de sonido, gráficos, animación, texto y vídeo. Este tipo de aplicaciones se han convertido en un medio eficaz de comunicación corporativa. Sin embargo, el envío de más de un combinado de medios campus de la red de datos requiere una gran cantidad de ancho de banda. IP Multicast es una forma eficaz de la entrega de información a muchos terminales a partir de un único flujo IP.

IP multicast incluye un tratamiento estándar, las metodologías para multicast a los usuarios a convertirse en miembros de los grupos, la fuente y árboles compartidos, y los protocolos de enrutamiento multicast. Se puede utilizar Cisco IOS interfaz de línea de comandos (CLI) para aplicar las configuraciones de IP multicast en dispositivos Cisco.

Este documento ofrece una visión general detallada del IP multicast. En él se explican las aplicaciones que utilizan la tecnología multicast y los beneficios que se proporciona al usuario de aplicaciones. Obtendremos la capacidad de ejecutar tareas relacionados con los siguientes:

- Explicación del Multicast
- Explicación del IGMP y Capa 2
- Protocolo de Ruteo Multicast
- Configuración y Verificación Multicast

1.2 Concepto del IP Multicast.

El Multicast consiste en enviar los mismos paquetes de datos a múltiples receptores. Un servidor multimedia envía una copia de cada paquete a una única dirección IP de destino que puede ser recibido por muchas estaciones finales que esperan recibir la dirección multicast.

En la Figura 1.1, el servidor de vídeo transmite un único flujo de datos de vídeo a un conjunto de los dispositivos receptores que admiten una determinada dirección multicast. Sólo 1,5 Mbps del ancho de banda entre el servidor y la red es utilizado, prescindiendo del número de hosts receptores.

Con el envío de los paquetes de datos a múltiples receptores, los paquetes no se duplican para cada receptor, pero se envían en un único stream (flujo de información), donde los routers se encargan de realizar la multiplicación de enviar el mismo flujo hacia otros enlaces en caso sea necesario. Porque el uso del Multicast? Veamos algunas razones:

- Usado cuando se envia la misma data a multiples receptores
- Mejor utilización del ancho de banda
- Menos procesamiento host y router
- Usado cuando los receptores tienen direcciones desconocidos
- Usado cuando la entrega simultanea para un grupo de receptores es requerido (simulticast)

El procesamiento de paquetes en los routers (enruteadores) disminuye porque reciben sólo una única copia del paquete origen.

Debido a que los routers realizan la multiplicación y la entrega de paquetes hacia los receptores, el remitente, o la fuente de tráfico multicast, no tiene que conocer las direcciones unicast del receptor.

Simulcast que consiste en la entrega simultánea de paquetes hacia un grupo de receptores, puede utilizarse para varios propósitos, incluyendo audio o video streaming, noticias y datos similares de entrega, y el despliegue de actualizaciones de software.

Para enviar los datos a múltiples destinos usando unicast, el remitente tiene que enviar el mismo flujo de datos a cada receptor por separado. El remitente tiene que hacer copias de los mismos paquetes y enviarlos una vez por cada receptor.

Algunas tecnologías web por ejemplo, webcasting (difusión por Internet) utilizan el metodo de "envio" para entregar los mismos datos a múltiples usuarios. En lugar de los usuarios hacer clic en un vínculo para obtener los datos, los datos se entregan automáticamente. Los usuarios primero que suscribirse a un canal para recibir los datos, después de esto, los datos periódicamente son enviados al usuario. El problema de la difusión por Internet es que el transporte se sigue haciendo uso de unicast.

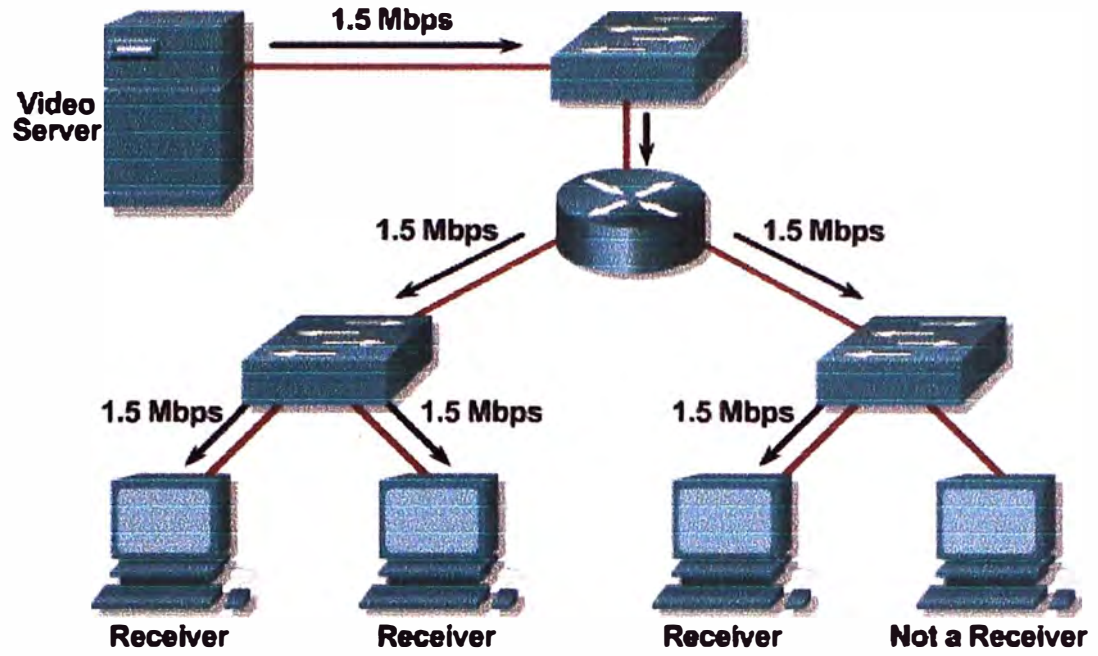


Fig. 1.1 Trafico Multicast

Un servidor de video envia un unico stream de datos a multiples clientes usando una direccion multicast especifica.

1.3 Direccion Unicast versus Multicast.

Una transmisión unicast envía varias copias de datos, una copia para cada receptor.

Un ejemplo del Unicast se grafica en la figura 1.2 donde se muestra a un host que transmite tres copias de datos y una red de transmisión de cada paquete a cada uno de los receptores. El host puede enviar a un solo receptor a la vez, porque tiene que crear un paquete diferente para cada dirección de destino receptor.

Una transmision Multicast envía una única copia de datos a múltiples receptores. Los datos son enviados a los receptores multicast, ya que previamente han sido suscritos para recibirlo.

Un ejemplo del multicast se grafica en la figura 1.3 donde se muestra a un host que transmite una serie de copia de datos y una red que replica el paquete hasta el último tramo de cada receptor. En la red cada paquete es unico. El host puede enviar a varios receptores al mismo tiempo porque es el envío de un solo paquete. Los routers multicast reproducen y envian el paquete de datos a todas las ramas de la red en las que existen receptores multicast.

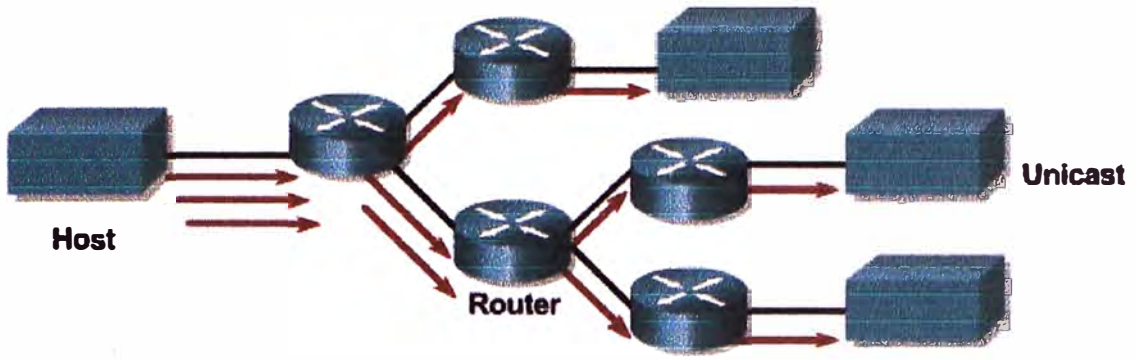


Fig. 1.2 Unicast

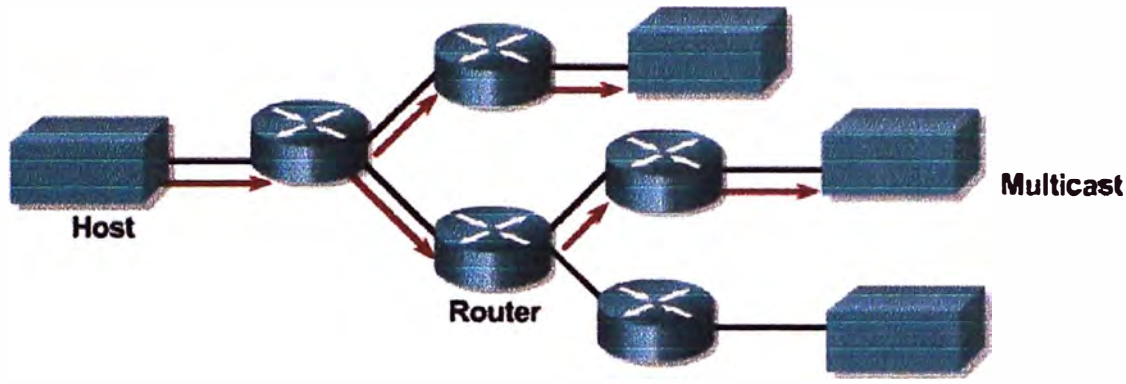


Fig. 1.3 Multicast

Podemos describir brevemente las diferencias entre las direcciones Unicast y Multicast basados en protocolos de transporte:

- TCP es Unicast pero no es Multicast.
  - TCP es un protocolo orientado a la conexión
  - Requiere 03 pasos (handshake) para establecer una sesion TCP
  - Es confiable debido a la secuencia de numeros y confirmación (ack)
  - Posee el mecanismo de Control de Flujo
- UDP es Unicast y Multicast.
  - No es orientado a la conexión
  - No es confiable (la confiabilidad recae el protocolos de aplicación)

  Protocolos Unicast.
  - ARP no es aplicable
  - HSRP no es aplicable

1.4 Ventajas y Desventajas del Multicast.

1.4.1 Ventajas del Multicast

La transmisión Multicast ofrece muchas ventajas sobre unicast, pues la transmisión en el entorno de red es de uno-a-muchos o muchos-a-muchos:

- Eficiencia Mejorada: El consumo de ancho de banda de una red es utilizada de manera más eficiente, porque un gran número de flujos de datos son reemplazados con una única transmisión.
- Ejecución Optimizado: Se requieren menos copias de datos para la transmisión y menos procesamiento. Elimina el trafico redundante.
- Aplicaciones distribuidas: Multiples solicitudes de transmisión que tiene una demanda en crecimiento no será posible atenderlas con unicast, porque la transmisión unicast no es escalable (el nivel de tráfico y aumento de clientes en una tasa de 1:1).

Todos los clientes escuchan el mismo audio de 8 Kbps.

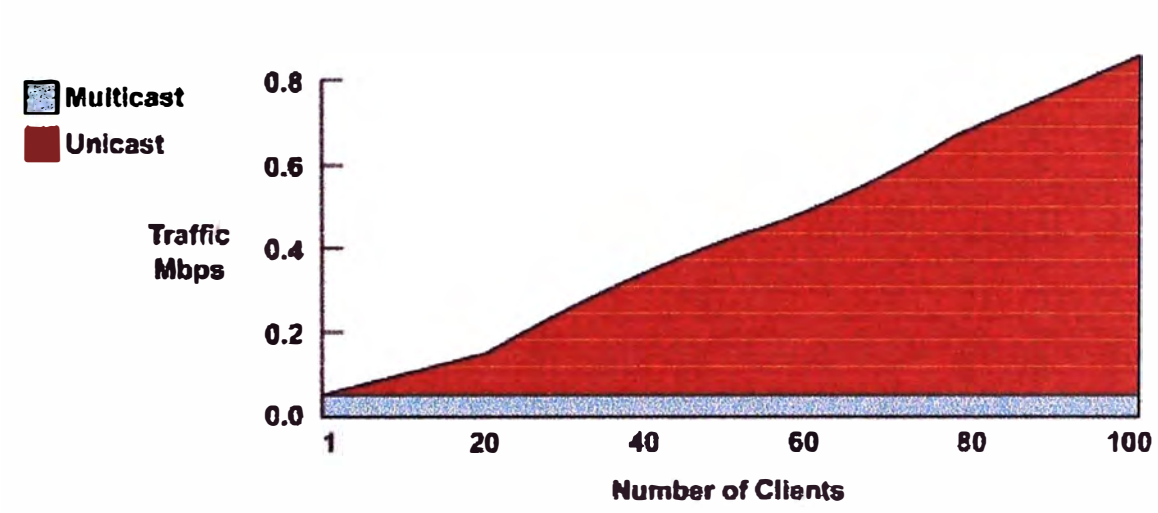


Fig. 1.4 Ejemplo de Audio Streaming

Otras ventajas del Multicast:

- Por la cantidad equivalente de tráfico multicast, el remitente utiliza menos potencia de procesamiento y menor consumo de ancho de banda.
- Los paquetes Multicast no implican un porcentaje tan alto de utilización del ancho de banda como los paquetes unicast, por lo que existe una mayor posibilidad de que lleguen a su destino simultaneamente.

Multicast permite la transmisión de toda una serie de nuevas aplicaciones que no son posibles en unicast (por ejemplo, video bajo demanda).

1.4.2 Desventajas del Multicast.

Existen también algunas desventajas de multicast que es necesario considerar. La mayoría de las aplicaciones multicast estan basados en protocolos UDP (Unit Datagram Protocol). Estos resultados tienen algunas consecuencias indeseables en comparación con su similar TCP (Transport Control Protocol) aplicaciones unicast. A continuación describiremos algunas desventajas:

- Best-effort (Mejor esfuerzo): es el resultado de entrega de información con algunos paquetes dropeados (perdidos). Muchas aplicaciones multicast operan en tiempo real (por ejemplo, vídeo y audio), estos pueden verse afectados por estas pérdidas, pues si esto ocurre se solicita la retransmisión de los datos perdidos y esto en tiempo real no es viable.

  Dropeos masivos en aplicaciones de voz puede ocasionar intermitencia y degradación en la calidad de voz.

  - Dropeos masivos en aplicaciones de video son perceptibles al ojo humano y aparecer como entrecorte y degradación de la imagen. Sin embargo, algunos algoritmos de compresión pueden ser severamente afectados por los bajos índices de dropeos de paquetes, esto ocasiona que la imagen se "congele" durante varios segundos mientras se recupera el algoritmo de descompresión.
- La falta de control de congestión puede resultar en la degradación general de la red como la presencia en crecimiento de aplicaciones basadas en UDP multicast .
- Duplicar los paquetes en ocasiones puede ser generado por cambio de topologías de red multicast. Las aplicaciones deben aguardar ocasionalmente el arribo de duplicación de paquetes y deben ser destinados según sea el caso.
- La entrega de Fuera de Secuencia de paquetes también pueden dar lugar a cambios en la topología de red u otros eventos que afectan al flujo de corriente de tráfico multicast.
- UDP no tiene mecanismos de fiabilidad, por lo que las cuestiones de fiabilidad deben abordarse dentro de la aplicación multicast cuando la transferencia de datos confiable es necesario.
- La cuestión de la restricción del tráfico multicast sólo a un grupo seleccionado de receptores, aún no ha sido suficientemente resueltas.

- Algunas aplicaciones comerciales son posibles sólo cuando la confiabilidad y la seguridad son cuestiones totalmente resuelto (por ejemplo, suministro de datos financieros).

1.5 Aplicaciones Multicast.

No es frecuente que la gente casi piense en IP multicast y la comunicación del vídeo como la misma cosa. Aunque el primer uso que se utilizará en una red multicast-permitida IP es a menudo comunicación video, el vídeo es solamente uno de muchos usos del IP multicast que puedan agregar valor al modelo del negocio de una compañía. En hecho, después de algunos experimentos iniciales con la comunicación video sobre la red del multicast del IP, muchas compañías encuentran que para la anchura de banda consumida, la imagen del que habla en una videoconferencia típica proporciona poco valor agregado al proceso de la comunicación.

Existen varios tipos de aplicaciones multicast, describiremos tres de los modelos más comunes:

- Uno-a-muchos, en caso de que un remitente envía los datos a muchos receptores.
  - Este tipo de aplicación se puede utilizar para la distribución de audio o vídeo, impulsar los medios de comunicación, anuncios, videovigilancia, etc.
  - Si una aplicación one-to-may necesita información de los receptores, se convierte en una aplicación muchos-a-muchos.
- Muchos-a-muchos, donde un host puede ser un emisor y un receptor, o cuando simultáneamente dos o más receptores también actúan como remitentes.
  - Recibir datos de varias fuentes aumenta la complejidad de las aplicaciones y crea diferentes problemas de gestión.
  - Usando el concepto de many-to-many multicast como principio basico, toda una nueva gama de aplicaciones puede ser construido (por ejemplo, la colaboración, el procesamiento concurrente, y distribuido simulaciones interactivas).
- Muchos-a-uno, donde muchos receptores están enviando datos a un remitente.
  - Usadas por aplicaciones financieras y de redes. Otros usos incluyen el resource discovery (descubrimiento de recursos), data collection (recoleccion de datos), auctions (subastas), y polling (scrutinio).

En la Figura 1.5 se muestra gráficamente muchas de las nuevas aplicaciones multicast que están surgiendo de acuerdo a la demanda, describiremos alguno de ellos:

- Entre las aplicaciones real-time (tiempo real) se incluyen live broadcasts (emisiones en directo), entrega de datos financieros, whiteboard collaboration (colaboración pizarra), y las videoconferencias.
- Las aplicaciones non-real-time (no tiempo real) incluyen la transferencia de archivos, archivos de datos y replicación, y video bajo demanda. La replicación de múltiples imágenes simultáneas en una PC es una aplicación de transferencia de archivos.
- Distribución de información de interes comun, bolsa de valores, anuncios resultados de eventos, noticias.
- Aprendizaje y capacitacion a distancia.
- Distribución de Video.
- Videoconferencia.

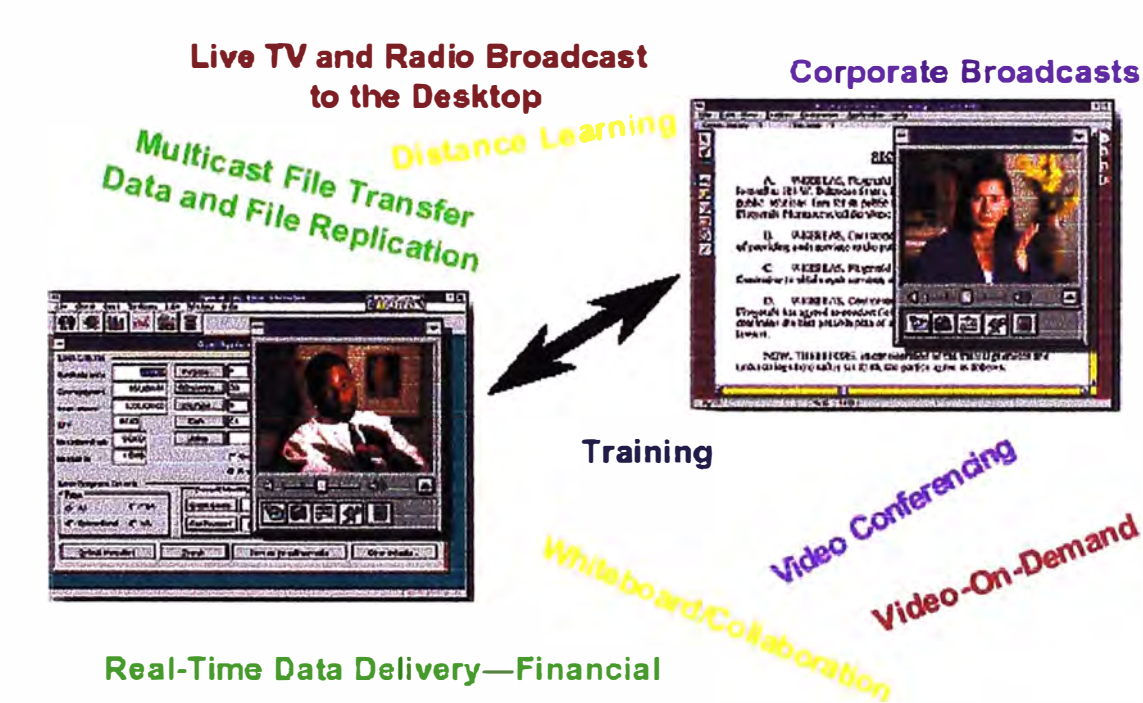


Fig. 1.5 Ejemplo de Aplicaciones Multicast

Algún excelente del IP multicast, como herramienta de comunicación de las multimedias fue desarrollado para el ambiente de UNIX para el uso sobre el MBONE. Estas herramientas (muchas de las cuales recientemente han migrado a las plataformas de Windows 95 y del NT) permiten que una audio conferencia solamente o de audio/video

múltiple ocurra vía el multicast del IP. Además de las herramientas audio y video, una herramienta UNIX-based Whiteboard que permite que los usuarios compartan un electronico whiteboard común. Además de estas herramientas del freeware del MBONE para las redes excesivas del IP multicast de la comunicación de las multimedias, otras compañías ahora están comenzando a ofrecer las formas comerciales de estas herramientas con otras características de valor añadido. Tal como se muetra en la siguiente Figura 1.5:

Fig. 1.6 Videoconferencia

Mucha gente comienza con la comunicación de audio/video porque el vídeo es una nueva manera particularmente emocionante de comunicarse sobre una red. Después de que la novedad del vídeo use apagado y las realidades de los anchos de banda y de las estaciones de trabajo que son consumidos por la comunicación video (particularmente si cada uno en la conferencia es vídeo del origen en el mismo tiempo) llegan a ser evidentes, no es infrecuente ver la comunicación audio-solamente convertirse en el modo normal. Además, si una conferencia audio-solamente se junta con un IP multicast (tal como el uso de Whiteboard mencionado previamente) que permite que los miembros de la conferencia compartan la información de los gráficos, el resultado es una forma extremadamente de gran alcance de comunicación de las multimedias que no consuma mucho ancho de banda.

1.6 Resumen del capitulo.

En este capitulo se visualizado de manera general los conceptos y las aplicaciones del IP multicast. Todavía hay mucho trabajo por hacer antes de que las capacidades del IP multicast capacidades están disponibles para todos los miembros de la Internet. Por otro lado, las redes deben ser cuidadosamente diseñados, utilizando nuevos criterios de diseño, en apoyo al IP multicast.

Se ha mostrado tambien las divergencias existentes entre el trafico Unicast y Multicast y sus respectivas diferencias en funcion al uso de protocolos de transporte.

Es de comprender que la mayoria de las redes existentes en intrente trabajan con csolo Unicast, sin embargo con la incursión del Multicast se pretende proporcionar información necesaria para tomar buenas decisiones de diseño a medida que se modifican las redes de hoy en multicast habilitado para las redes del mañana.

CAPITULO II
MULTICAST BASICO

2.1 Introducción.

Este capítulo describe la traslacion de direcciones IP multicast y direcciones del Media Access Control del multicast (MAC). Ademas trata de conceptos importantes de los árboles de distribución del multicast y del forwarding IP multicast.

2.2 Direcciones IP Multicast.

A diferencia de las direcciones del IP unicast que identifican únicamente un solo host IP, las direcciones del IP multicast especifican a un grupo arbitrario de hosts IP que se han unido al grupo y estan listos para recibir tráfico enviado hacia este grupo. Esta sección explora el formato de las direcciones del IP multicast y cómo se asignan estas direcciones.

2.2.1 Direcciones IP Clase D.

Las direcciones del IP multicast han sido asignadas al espacio de dirección de la clase D por el Internet Autoridad Number Assigned (IANA). Las direcciones en este espacio se denotan con un prefijo binario 1110 en los primeros 4 bits del primer octeto (ver la Fig. 2.1). Así, el IP multicast comprende dentro de rango a partir el 224.0.0.0 a 239.255.255.255.

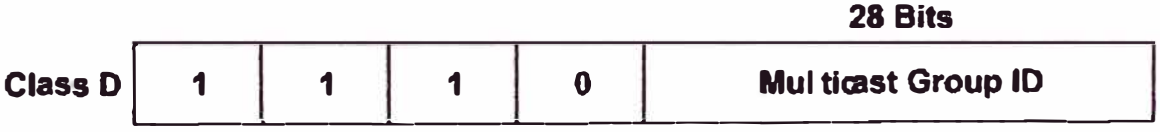


Fig. 2.1 Direccion IP Multicast Basico

Por lo tanto, el rango de direcciones IP multicast es de 224.0.0.0 hasta 239.255.255.255.

Los routers pueden distinguir el tráfico multicast, unicast o broadcast a partir del uso de la Clase D reservada del espacio de direcciones IP. Los dispositivos de la red pueden seleccionar rápidamente la direccion IP multicast clase D en busca de los cuatro bits más importantes, los bits de alto orden, que son siempre 1110. Los siguientes 28 bits se refiere a como el grupo de dirección.

Tabla N° 2.1 Direcciones Multicast Clase D

Class D First Octet								Multicast Addresses
1	1	1	0	0	0	0	0	**224**.0.0.0 – **224**.255.255.255
1	1	1	0	0	0	0	1	**225**.0.0.0 – **225**.255.255.255
1	1	1	0	0	0	1	0	**226**.0.0.0 – **226**.255.255.255
1	1	1	0	...				**227**.0.0.0 – **227**.255.255.255 ... **237**.0.0.0 – **237**.255.255.255
1	1	1	0	1	1	1	0	**238**.0.0.0 – **238**.255.255.255
1	1	1	0	1	1	1	1	**239**.0.0.0 – **239**.255.255.255

Además de las gamas de dirección del multicast descritas previamente, el IANA ha reservado la gama de 239.0.0.0 a 239.255.255.255 como administrativo scoped las direcciones para el uso en dominios privados del multicast. Estas direcciones son similares en naturaleza a las gamas reservadas del unicast del IP, tales como 10.0.0.0/8, definidas en RFC 1918 y el IANA no los asignará a ningún otro grupo o protocolo. Por lo tanto, en teoría, los administradores de la red están libres utilizar direcciones del multicast en esta gama dentro de un dominio sin el riesgo de estar en conflicto con otros a otra parte en el Internet. El uso de administrativo scoped direcciones también ayuda a conservar el espacio de dirección limitado del multicast porque pueden ser reutilizadas en diversas regiones de la red. En realidad, los administradores de la red deben configurar sus routers del multicast para asegurarse de que el tráfico del multicast en esta gama de dirección no se cruza en o fuera de su dominio del multicast.

2.2.2 Direcciones Reservadas por IANA.

Reservado por IANA (Autoridad de Asignacion de Numeros Internet) entidad autorizada para el control y asignación de direcciones IP. El espacio de direcciones IP multicast están separados en los siguientes grupos:

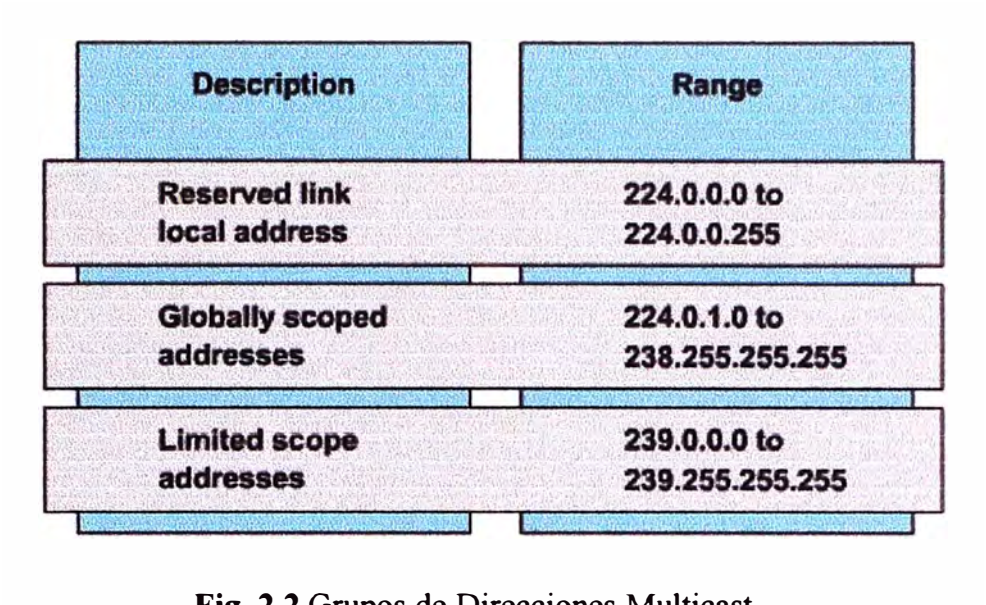


Fig. 2.2 Grupos de Direcciones Multicast

Ahora pasamos a describir cada una de ellas:

a. Direcciones de Alcance local.

- El rango de direcciones es desde 224.0.0.0 hasta 224.0.0.255.
- Este rango de direcciones nunca son enviados fuera de la red Lan, prescindiendo del valor del TTL (Time to Live). Generalmente el TTL está marcado con valor 1.
- Para protocolos de enrutamiento en la subred local.

En la tabla 2.2 se muestra una lista parcial de las direcciones reservadas del multicast tomadas directamente de la base de datos del IANA, donde se enumeran las direcciones reservadas de alcance y la función del protocolo de red a las cuales se han asignado.

Tabla N° 2.2 Direcciones de Alcance Local

Direcciones Reservadas	Asignado en funcion al Protocolo
224.0.0.1	Todos los sistemas (PCs) multicast en una subnet
224.0.0.2	Todos los routers multicast en una subnet
224.0.0.4	Todos los routers Distance Vector Multicast Routing Protocol (DVMRP)
224.0.0.5	Todos los routers OSPF
224.0.0.6	Todos los Ruters Designados OSPF (DRs)
224.0.0.9	Todos los routers RIPv2
224.0.0.10	Todos los routers EIGRP
224.0.0.11	Todos los routers PIMv2

El IANA ha reservado el rango IP de 224.0.0.0 a 224.0.0.255 para el uso por protocolos de red en un segmento local de la red. Los paquetes con una dirección en esta gama son locales en alcance, no son remitidos por los routers de IP (sin importar sus valores de tiempo de vida [TTL]), y por lo tanto van no más lejos que la red local. Los routers que suceden remitir estos multicasts del subnet local son referidas por los administradores de la red como routers multicast.

Por Ejemplo , la dirección del IP multicast de 224.0.0.1 se ha asignado el significado de todos los hosts, y 224.0.0.2 se ha asignado el significado de todas los routers del multicast ambos de esas direcciones del multicast son utilizadas extensivamente por IGMP, que uso de los hosts del multicast de comunicar su deseo de ensamblar un grupo del multicast a una router localmente conectada. El protocolo abierto de la encaminamiento de Expedición Corto de Trayectoria (OSPF), por Ejemplo , emplea direcciones locales del multicast del

subnet. Si usted utiliza el OSPF en su red, usted pudo haber visto los paquetes tratados a la dirección del multicast 224.0.0.5 y 224.0.0.6 en sus redes. Estas direcciones permiten que los routers del OSPF comuniquen datos importantes del OSPF a todas los routers del OSPF o a todas los routers señaladas OSPF respectivamente.

b. **Direcciones de alcance a nivel global (mundial).**

- Estas direcciones son asignadas dinámicamente desde internet.
- El rango de direcciones comprende desde 224.0.1.0 hasta 238.255.255.255.
- El rango 224.2.X.X es usado en aplicaciones del Backbone Multicast (Mbone). Establecido por IETF (Internet Engineering Task Force) para audio multicast and videoconferencias, Mbone es un conjunto de routers en internet que soportan IP multicast sobre el cual diferentes organismos publico o privado envian sus aplicaciones de audio y video.

El IANA asigna típicamente las solas peticiones de la dirección del multicast para los protocolos de red o los usos de la red fuera de la gama de dirección 224.0.1.xxx. Los routers del multicast remitirán a éstos direcciones del multicast, diferente de las direcciones del multicast en la gama de dirección 224.0.0.xxx, que son locales en alcance y nunca son remitidas por los routers.

Tabla 2.3 Otras direcciones multicast reservados

Direcciones Reservadas	**Asignado en funcion al Protocolo**
224.0.1.0	VMTP Managers Group
224.0.1.1	NTP Network Time Protocol
224.0.1.2	SGI Dogfight
224.0.1.79	Tibco Multicast2

c. Alcance de direcciones limitados administrativamente.

- Reservados para el uso dentro de los dominios privados. Similar a la dirección IP privada del espacio que se utiliza dentro de los límites de una sola organización, la limitación de alcance o administrativamente direcciones están limitados a un grupo local u organización.
- El rango de direcciones es desde 239.0.0.0 hasta 239.255.255.255.
- Las organizaciones pueden utilizar direcciones de alcance limitado para aplicaciones multicast a nivel local que no serán transmitidos a través de Internet.

Dentro de un sistema autónomo o de dominio, el rango de direcciones de alcance limitado se pueden subdividir de manera que los límites de multicast local puede definirse. Esta subdivisión es llamado dirección de alcance y permite la reutilización de direcciones entre dominios más pequeños. El espacio de alcance de direcciones multicast limitados administrativamente se divide en los siguientes ámbitos:

- Alcance de Organización ámbito local (239.192.0.0 hasta 239.251.255.255)
- Alcance de Sitio Local (239.255.0.0/16, 239.252.0.0/16, 239.253.0.0/16, y 239.254.0.0/16)

2.3 Direcciones MAC Multicast

La especificación original de Ethernet (ahora estandardizada por el IEEE) hizo las provisiones para la transmisión de el broadcast y/o de los paquetes del multicast. Según lo demostrado en la Figura 2.3, el bit 0 del octeto 0 en un MAC address de IEEE indica si la dirección de destinación es una dirección de broadcast/multicast o una dirección del unicast.

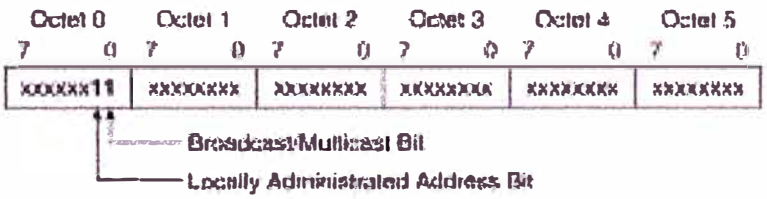


Figura 2.3 Formato MAC Ethernet IEEE 802.3

Si se fija este bit, entonces el marco del MAC es definido para un grupo arbitrario de hosts o todos los hosts en la red (si la dirección de destinación del MAC es la dirección de el

broadcast, 0xFFFF.FFFF.FFFF). El IP multicast en la capa 2 hace uso esta capacidad para transmitir los paquetes del IP multicast a un grupo de hosts en un segmento del LAN.
En la siguiente seccion examinaremos cómo las direcciones del IP multicast de la capa 3 son mapeadas en las direcciones del MAC de IEEE para Ethernet.

2.3.1 Direcciones Multicast Capa 2.

¿Cómo relaciona un router o un switch una dirección IP multicast con una dirección MAC? Normalmente, las tarjetas de interfaz de red (NIC- Network Interface Card) en un segmento de LAN sólo reciben los paquetes con destino a su dirección MAC. Sin embargo, no existe un protocolo de resolución de direcciones (ARP) equivalente al mapeo de direcciones multicast. En lugar de ello, IANA ha definido la porcion del codigo vendor reservado por la Organización Unique Identifier (OUI) cuyo valor permite identificar las direcciones MAC multicast.

2.3.2 Mapeo de Direcciones MAC Ethernet Multicast.

En el caso de Ethernet, el IP multicast enmarca todas las direcciones de la capa del MAC del uso que comienzan con el prefijo 24-bit de 0x0100.5Exx.xxxx. Desafortunadamente, solamente la mitad de estas direcciones del MAC está disponible para el uso por el multicast de IP. Esto deja 23 bits de espacio del MAC address para mapeo direcciones del IP multicast de la capa 3 en direcciones del MAC de la capa 2. Desde todo el IP multicast de la capa 3 las direcciones tienen los primeros 4 de los 32 bits fijados a 0x1110, éste dejan 28 bits de información significativa de la dirección del multicast del IP. Estos 28 bits deben mapeo en solamente 23 bits del MAC address disponible.
Hay una historia interesante en cuanto a porqué el valor de solamente 23 bits del espacio del MAC address fue asignado para el multicast del IP. Detrás en los años 90 tempranos, Steve Deering traía algo de su trabajo de investigación sobre IP multicast a la fruición, y él quiria que el IEEE asignara 16 identificadores únicos de organización consecutivos (OUIs) para el uso como direcciones del MAC del multicast del IP. Porque un OUI contiene 24 valores de los bits del espacio de dirección, 16 OUI consecutivos proveerían un valor completo de 28 bits del espacio del MAC address y permitirían mapeo uno por de las direcciones del IP multicast de la capa 3 a las direcciones del MAC. Desafortunadamente, el precio que iba para un OUI era en ese entonces $1000 y el encargado de Steve, el último Jon Postel, no podía justificar los $16.000 necesarios para comprar el valor completo de 28

bits de las direcciones del MAC. En lugar, Jon estaba dispuesto a pasar $1000 para comprar un OUI fuera de su presupuesto y para dar la mitad de las direcciones (23 bits) a Steve para el uso en su investigación del multicast del IP.

Las direcciones MAC Multicast en el primer octeto siempre comienzan con el mas bajo orden de bit (0x01). Concretamente, el prefijo 0x01005e (además del siguiente bit mas bajo, que es cero) se ha reservado para el mapeo de direcciones IP multicast de la capa 3 dentro de las direcciones MAC de la capa 2. El rango completo de direcciones MAC multicast es desde 0100.5e00.0000 hasta 0100.5e7f.ffff. Este mapeo se muestra gráficamente en la Figura 2.4.

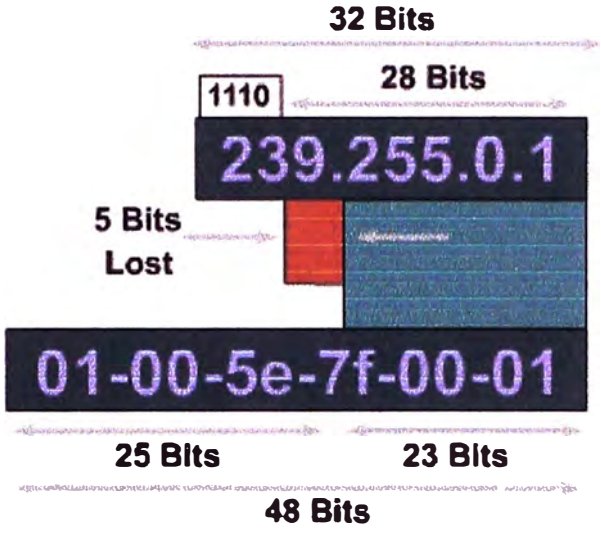


Fig. 2.4 Mapeo de direcciones MAC Ethernet Multicast

Esto hace que los primeros 25 bits de la dirección MAC sean fijos (24 bits más el bit cero) y permite que los últimos 23 bits de la dirección MAC para corresponder a los 23 últimos bits del grupo de direcciones IP multicast. En la Figura.2.5 se muestra la traslacion entre el IP Multicast y la dirección MAC multicast se logra mediante el mapeo de los 23 bits de mas bajo orden del IP (Capa 3) de la dirección multicast dentro de los 23 bits de mas bajo orden de la direccion MAC (Capa 2).

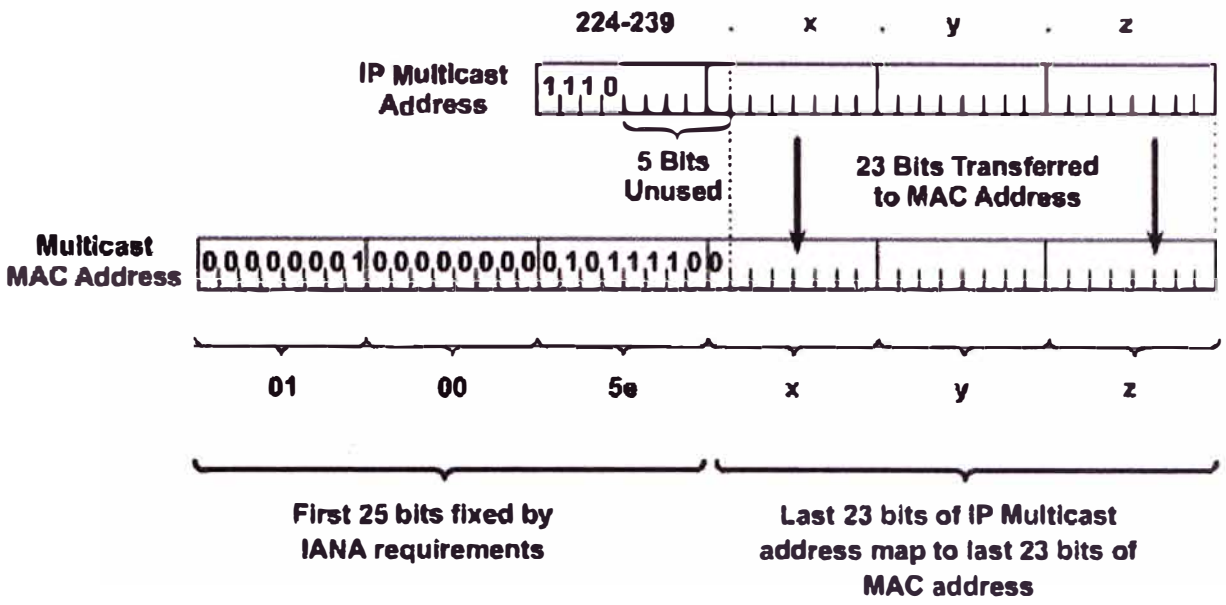


Fig. 2.5 Mapeo del IP Multicast a MAC Multicast

Hay 28 bits unicas del espacio de direcciones para una dirección IP multicast (32 menos de los primeros cuatro bits que contienen el prefijo 1110 Clase D), y hay sólo 23 bits mapeado en la dirección MAC del IEEE. Por lo tanto, cinco bits de la dirección IP no son usados y no son transferidos a la dirección MAC, lo que significa que hay cinco bits de superposición.

El resultado es que dos (o más) diferentes direcciones IP multicast pueden mapearse a la misma dirección MAC multicast. Por ejemplo, 224.1.1.1 y 225.1.1.1 mapea a la misma dirección MAC multicast. Si un usuario suscrito al Grupo A (designado por 224.1.1.1) y el otro usuario suscrito al Grupo B (designado por 225.1.1.1), que ambos reciben flujos de A y B en la Capa 2. En la Capa 3, sin embargo, sólo los paquetes asociados a la dirección IP del grupo multicast seleccionado es visible, debido a que el rango de puertos usados dentro de la dirección es diferente entre los flujos.

Esto da la posibilidad de que 32 diferentes direcciones IP multicast podrían corresponder a una única dirección MAC multicast. Por ejemplo, todas las direcciones IP multicast en la Tabla 2.4 mapea a la misma multicast Capa 2 de 01-00-5e-0a-00-01.

Tabla N° 2.4 Ejemplo de Direcciones Multicast

224.10.0.1	225.10.0.1	226.10.0.1	227.10.0.1	228.10.0.1
229.10.0.1	230.10.0.1	231.10.0.1	232.10.0.1	233.10.0.1
234.10.0.1	235.10.0.1	236.10.0.1	237.10.0.1	238.10.0.1
239.10.0.1	224.138.0.1	225.138.0.1	226.138.0.1	227.138.0.1
228.138.0.1	229.138.0.1	230.138.0.1	231.138.0.1	232.138.0.1
233.138.0.1	234.138.0.1	235.138.0.1	236.138.0.1	237.138.0.1
238.138.0.1	239.138.0.1			

Los administradores de red deben considerar esto cuando se asignen la direccion IP multicast.

2.3.3 Impacto en el Mapeo de Direcciones MAC.

Porque los 28 bits de la información de la dirección del IP multicast de la capa 3 no se pueden mapear en los 23 bits disponibles del espacio del MAC address, 5 bits de información de la dirección se pierden en el proceso mapeo. Esto da lugar a ambigüedad de la dirección de 25 o de 32:1 cuando una dirección del IP multicast de la capa 3 mapea a un MAC address de IEEE de la capa 2. Esto significa que cada MAC address del IP multicast de IEEE puede representar 32 direcciones del multicast del IP, según lo demostrado en la Figura 2.7.

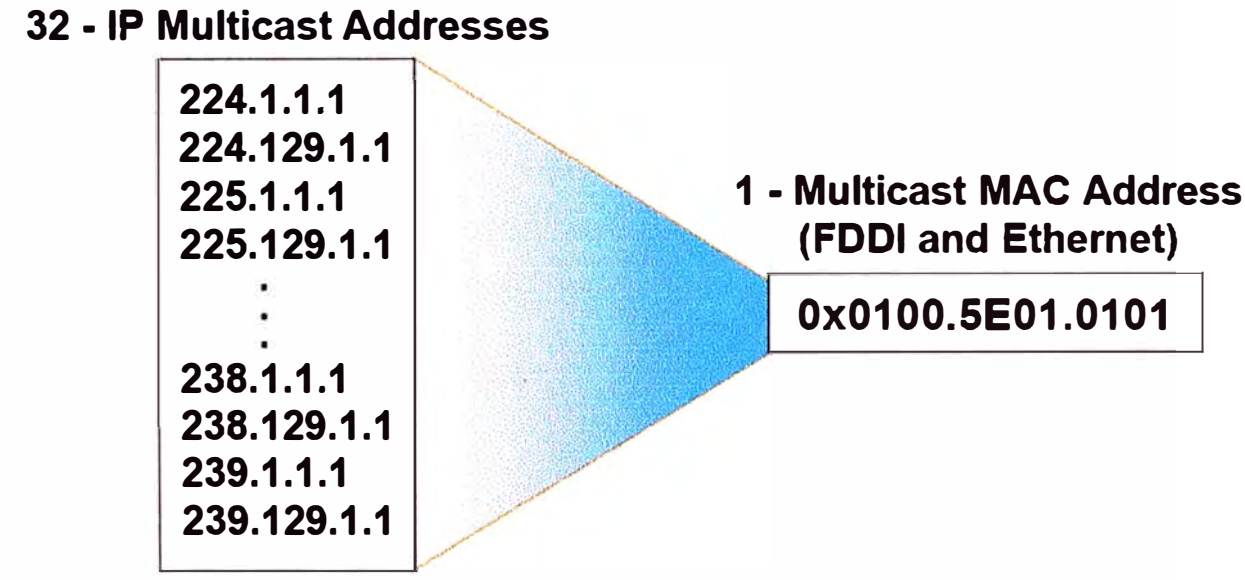


Fig. 2.6 Ambiguedades de direcciones MAC

Debe ser obvio que esta ambigüedad de la dirección de 32:1 puede causar algunos problemas. Por Ejemplo, un host que desea recibir el grupo 224.1.1.1 del multicast programará los registros de hardware en la tarjeta de interfaz de la red (NIC) para interrumpir la CPU cuando un marco con un MAC address del multicast de la destinación de 0x0100.5E00.0101 se recibe. Desafortunadamente, este mismo MAC address del multicast también se utiliza para 31 otros grupos del multicast del IP. Si cualesquiera de estos 31 otros grupos son también activos en el LAN local, la CPU del host recibirá interrupciones cualquier momento un marco se recibe para cualesquiera de estos otros grupos. La CPU tendrá que examinar la porción del IP de cada bastidor recibido para determinarse si es el grupo deseado, es decir, 224.1.1.1. Esto puede tener un impacto en la energía disponible de la CPU del host si es la cantidad suficiente de tráfico "falso" del grupo asignado.

2.4 Sesiones Multicast.

Siempre que una aplicacion multicast se inicia en un receptor, la aplicación tiene que saber a que grupo multicast va a participar. La aplicación tiene que aprender acerca de la disponibilidad de sesiones o flujos, que suelen mapear a uno o más grupos IP multicast.

Hay varias maneras en que las aplicaciones pueden aprender sobre los períodos de sesiones multicast:

- Las aplicaciones se suman a un well-known (bien-conocido) grupo predefinido que estan disponibles en los flujos de sesiones multicast.
- Las aplicaciones se comunican con un directory server (servidor de directorio).
- La aplicación es activado de una a partir de una página web en la que los períodos de sesiones figuran en la lista de URLs, incluso el correo electrónico puede ser utilizado.
- Un usuario puede configurar manualmente la IP multicast dentro de la aplicacion a fin de sensar la sesion multicast presente.

The session directory (sd) application acts as a guide and displays multicast content. A client application runs on a PC and lets the user know what content is available. This directory application uses either Session Description Protocol (SDP) or Session Announcement Protocol (SAP) to learn about the content.

Las aplicaciones de sesiones de directorio (sd) actúa como una guía y muestra el contenido del multicast. Una aplicación de cliente se ejecuta en una PC y permite al usuario saber qué contenido está disponible. Este aplicación de directorio utiliza ya sea Protocolo de

Descripción de Sesión (SDP) o Protocolo de Anuncio de Sesión (SAP) para obtener más información sobre el contenido.

Nota:

Tanto la aplicacion sd y el SDP son algunas veces llamado SDR o sdr. En la documentación de Cisco, SDP / SAP se denomina sdr.

La aplicacion original sd sirve como un medio para anunciar sesiones disponibles y asistir en la creación de nuevos períodos de sesiones. El primer instrumento sd fue revisado, lo que resulto en la herramienta SDP (denominado como SDR), que es una aplicación que permite lo siguiente:

- Periodo de sesiones y sus anuncios
- Transporte de anuncio de sesiones via well-known grupo multicast (224.2.127.254)
- Creacion of nuevas sesiones

On the receiver side, SDR learns about available groups or sessions. If a user clicks an icon describing a multicast stream listed via SDR, a join to that multicast group is initiated.

En el lado receptor, el SDR aprende acerca de la disponibilidad de grupos o sesiones. Si un usuario hace clic en un icono que describe un flujo multicast listados via SDR, se da inicio un join (union) a un grupo multicast.

Cuando SDR es usado en el lado remitente, crea nuevas sesiones y evita los conflictos de direcciones. Los remitentes en el momento de la creación de sesiones consultan con sus respectivos cache SDR (los remitentes son también receptores) y eligen una de las direcciones de multicast no utilizados. Cuando se crean las sesiones, los remitentes empiezan a anunciarse con toda la información que es requerido por los receptores para unirse satisfactoriamente a las sesiones.

RFC 3266, referido al SDP, se define el conjunto de variables estandar que describen las sesiones. La mayoría de las variables fueron heredadas de la herramienta SDR. El transporte en sí mismo no está definido en esta RFC. Los paquetes que describen las sesiones son transportados a través de la red multicast habilitados via varios mecanismos:

- SAP, definido en la RFC 2974, que transporta la informacion de sesion.
- Protocolo de Iniciación de Sesión (SIP), que es definido en el RFC 2543, es un protocolo de señalización usado para conferencias en Internet, telefonía, notificación de eventos y mensajería instantánea.

  Real Time Streaming Protocol (RTSP), que definido en el RFC 2326, sirve principalmente como un protocolo de control en un entorno multimedia. RTSP

permite al igual que los controles VCR (seleccionar, de avanzar, retroceder, pausa, stop, etc) y también lleva información en una sesion.

- E-mail (en formato Multipurpose Internet Mail Extensions [MIME]) tambien lleva paquetes SDR que describe las sesiones.
- Las paginas Web proporcionan la descripcion de sesiones en formato estandarizado SDR.

La Figura 2.8 muestra un ejemplo de los mecanismos del SDR en un Cisco IP/TV. El Cisco IP/TV en general tiene tres componentes: el servidor (la fuente), el gestor de contenidos (en el servidor), y el visualizador (el receptor).

Los visualizadores realizan cualquiera de estas dos acciones:

- Contactarse en forma directa con el gestor de contenidos (por unicast) y solicitar la lista de programas disponibles (sesiones, flujos) del servidor.
- Escuchar los anuncios periodicos SAP.

Cisco IP/TV utiliza SAP para el transporte de sesiones SDR hacia el visualizador (espectador). El formato estándar de SDR es usado para la descripción de sesiones.

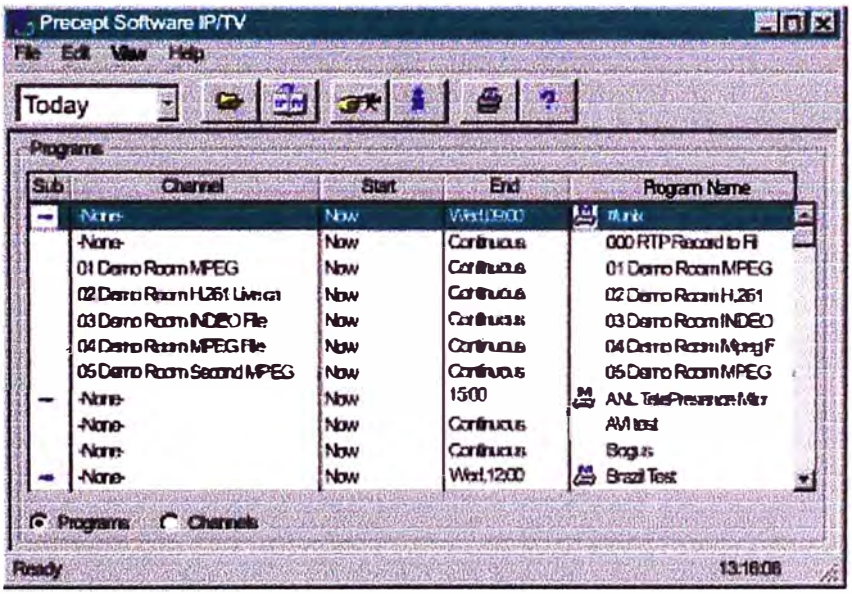


Fig.2.7 Ejemplo de Cisco IP/TV

2.5 Resumen del capitulo.

En este capitulo se refiere a algunos de los conceptos más básicos de IP multicast, en el ambito de direcciones IP clase D se ha presentado la clasificacion de direcciones de acuerdo al uso particular que sera tratado, ademas incluye el mapeo de direccionamiento MAC Ethernet en Multicast y como se aborda la relación en Multicast tanto en Capa 2 y Capa 3, finalmente se describe las características en el proceso de las sesiones de aplicación con multicast y la disponibilidad de sesiones o flujos, que suelen mapear a uno o más grupos IP multicast.

Estos temas son la base sobre la que un buen entendimiento de IP multicast se construye. Conviene tomarse el tiempo para conocer a fondo estos fundamentos para construir una red multicast.

CAPITULO III
PROTOCOLO DE ADMINISTRACIÓN GRUPO INTERNET (IGMP)

3.1 Introduccion al IGMPv2.

El Internet Group Management Protocol (IGMP) ha evolucionado a través de tres versiones (1, 2 y 3). La comprensión de este protocolo es fundamental en la definición de la pertenencia a unirse a un grupo multicast y el proceso de salida, que es una función necesaria del multicasting.

Sin control, los paquetes de multicast se inundan como frames unicast desconocidos por un Ethernet switch. El IGMP snooping y Cisco Group Management Protocol (CGMP) resuelven este problema.

IGMP es un protocolo host-a-router utilizado cuando los hosts quieren unirse a un grupo de multicast. Con IGMPv1, los routers envian consultas periódicas a miembros multicast a la dirección 224.0.0.1. Los hosts envian informes a los miembros del grupo dirección multicast que deseen asociarse. Los hosts silenciosamente pueden dejar el grupo multicast.

La mayoría de los cambios entre IGMPv1 y IGMPv2 principalmente las cuestiones de latencias de unirse y salidas y las ambigüedades de dirección en la especificación original del protocolo. Algunos de los importantes cambios introducidos son los siguientes:

- Grupo de consultas específicas
- Mensaje de salida del grupo
- Mecanismo de consulta de elección
- Consulta de intervalo del tiempo de respuesta

Un grupo de consulta específica que se añadió en IGMPv2 permite al router hacer consultas a un solo grupo en lugar de todos los grupos, que es una forma optimizada para averiguar si algunos miembros se quedan en un grupo sin preguntar a todos los grupos de un reporte. La diferencia entre el grupo de consulta específica y los miembros de consulta es que una consulta es la adhesión a la dirección multicast de todos los hosts (224.0.0.1),

en tanto que un grupo específico de consultas es multicast sólo hacia la dirección del grupo multicast.

Un grupo de mensaje de salida permiten a los hosts comunicar al router que abandonan el grupo. Esta información reduce la latencia de salida del segmento cuando el miembro que está saliendo es el último miembro del grupo. El estandar define que en el momento del abandono debe enviarse el grupo de mensaje de salida.

El tiempo de respuesta del intervalo de consulta se añadió al control de reportes. Esta vez se fijan las consultas para transmitir a los miembros de cuánto tiempo tienen que responder a una consulta con un reporte. IGMPv2 es compatible hacia atrás con IGMPv1.

3.2 Mensaje de Grupo de union y Grupo de salida IGMPv2

Los miembros a unirse a un grupo multicast no tienen que esperar para una consulta de union. Ellos envian un reporte no solicitado indicando su interés. Este procedimiento reduce la latencia para unirse al final del sistema en caso de que no estén presentes los otros miembros.

En la Figura 3.1, después de que el host H2 envía el mensaje de grupo para unirse al grupo 224.1.1.1, la dirección multicast 224.1.1.1 se activa la interfase Ethernet0 del router.

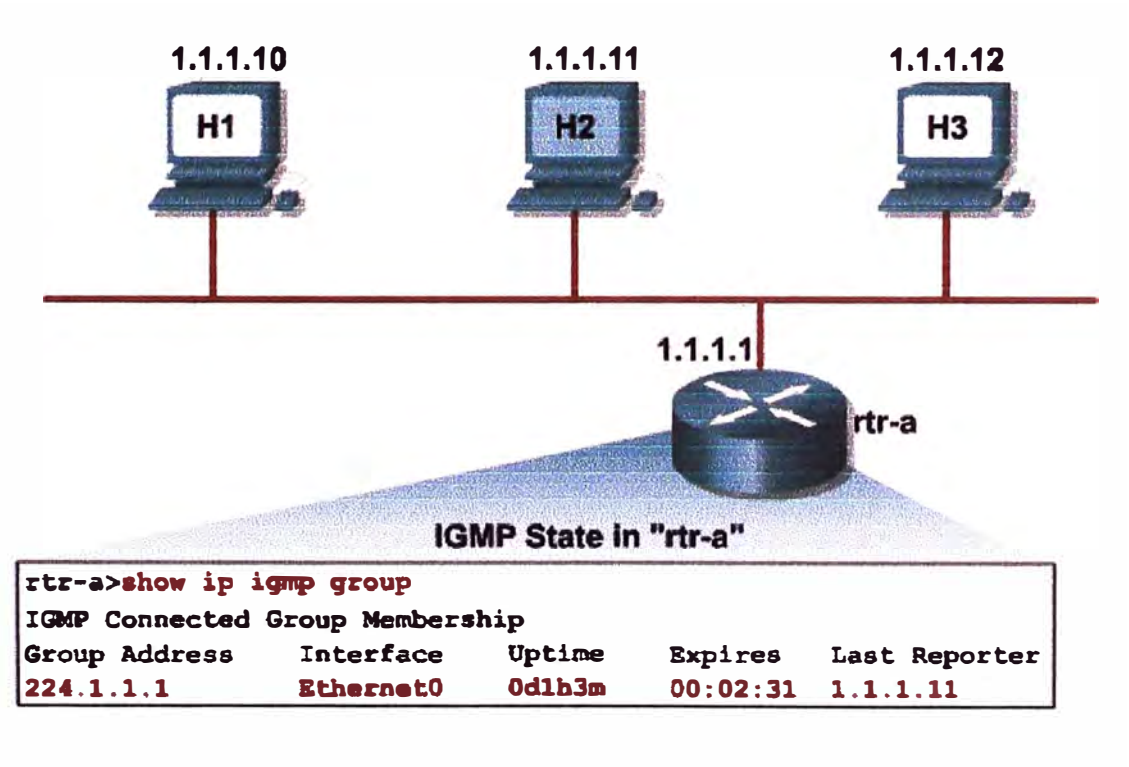


Fig. 3.1 Union a un Grupo IGMPv2

Usando el comando **show ip igmp group** revela lo siguiente:

- Group 224.1.1.1 ha sido activado en esta interfase por 1 hora y 3 minutos.
- Group 224.1.1.1 expira (y se suprime) en 2 minutos y 31 segundos si un reporte de host IGMP de miembros de este grupo no se escucha en ese momento
- El último reporte de host a los miembros de grupo fue 1.1.1.11 (H2).

Cuando hay dos routers (enrutadores) IGMP en el mismo segmento Ethernet (dominio de broadcast), el router es designado Querier con la más alta dirección IP.

En IGMPv1, los hosts abandonan el segmento pasivamente. Ellos explícitamente no dicen que están dejando, dejan de presentar reportes a sus miembros por no responder a las consultas de los miembros del grupo. El IGMPv2, sin embargo, el host que abandona el grupo explícitamente debe dejar mensajes de salida del grupo.

Cuando el router IGMPv2 recibe un mensaje de salida, este responde con el envío de un grupo de consulta específica para los asociados del grupo para ver si hay otros hosts interesados en recibir tráfico para el grupo. Este proceso ayuda a reducir la latencia de salida.

En la Figure 3.2, los hosts H2 y H3 son miembros del grupo multicast 224.1.1.1. En un momento dado, el host H2 sale del grupo y anuncia su salida mediante el envío de un mensaje al grupo multicast 224.0.0.2 (todos los routers multicast).

El router recibe el mensaje de salida y envía un grupo de consulta específica para ver si cualquier otro grupo de los miembros están presentes. El host H3 no ha abandonado el grupo multicast 224.1.1.1 aún, por lo que responde con un mensaje de reporte. Esta respuesta indica al router para mantener el envío de multicast para 224.1.1.1, porque por lo menos un miembro todavía está presente.

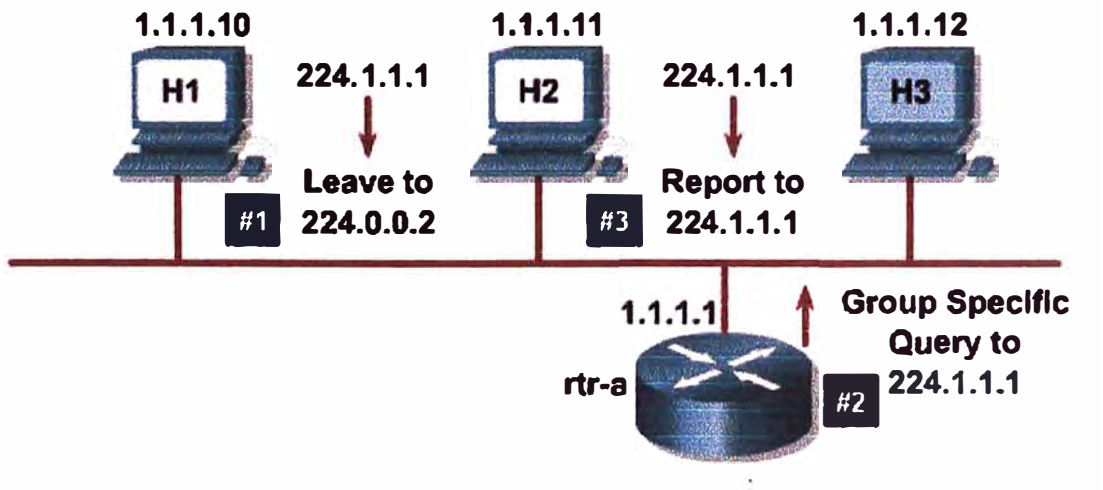


Fig. 3.2 Salida de un Grupo IGMPv2

En la Figura 3.3, el grupo de multicast 224.1.1.1 esta todavía activo. Sin embargo, la información IGMP muestra que el host H3 es el último host para enviar un reporte IGMP de pertenencia al grupo.

Después de recibir un mensaje de salida del host H3, el router envía una consulta de grupo específico para ver si otros miembros del grupo están presentes.

Porque el host H3 fue el último miembro del grupo multicast 224.1.1.1, ningún reporte de miembro IGMP es recibido para el grupo 224.1.1.1, ni el grupo de tiempo de espera. Esta actividad suele tardar de 1 a 3 segundos, desde el momento en que el mensaje de salida se envía hasta que el grupo de consulta específica se detiene y deje de fluir el tráfico multicast para ese grupo.

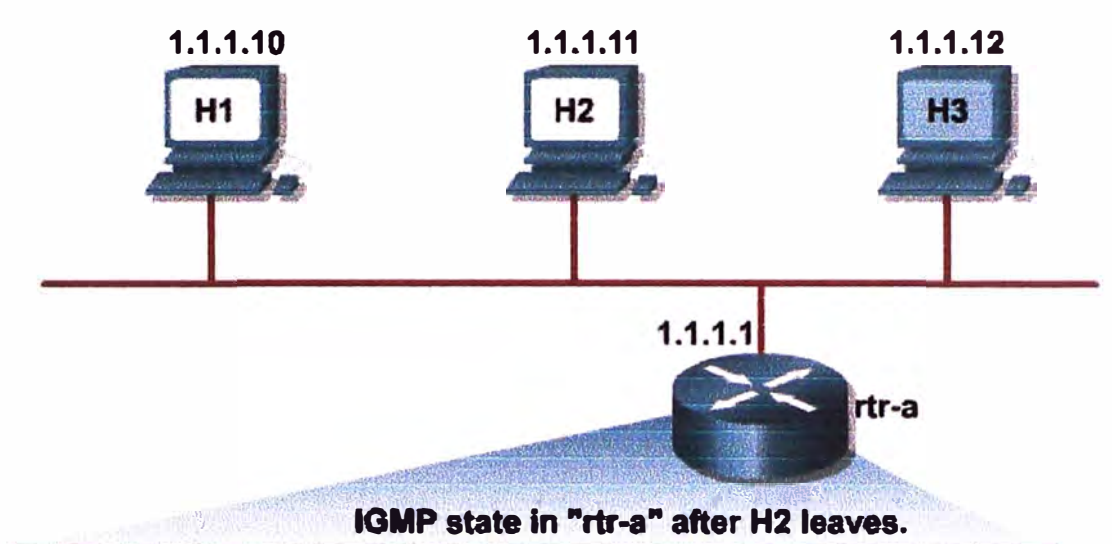


Fig. 3.3 Salida de un Grupo (continuacion)

En la Figura 3.4, todos los hosts 224.1.1.1 han abandonado el grupo en Ethernet0. Esta condición se indica en la salida del comando **show ip igmp group**

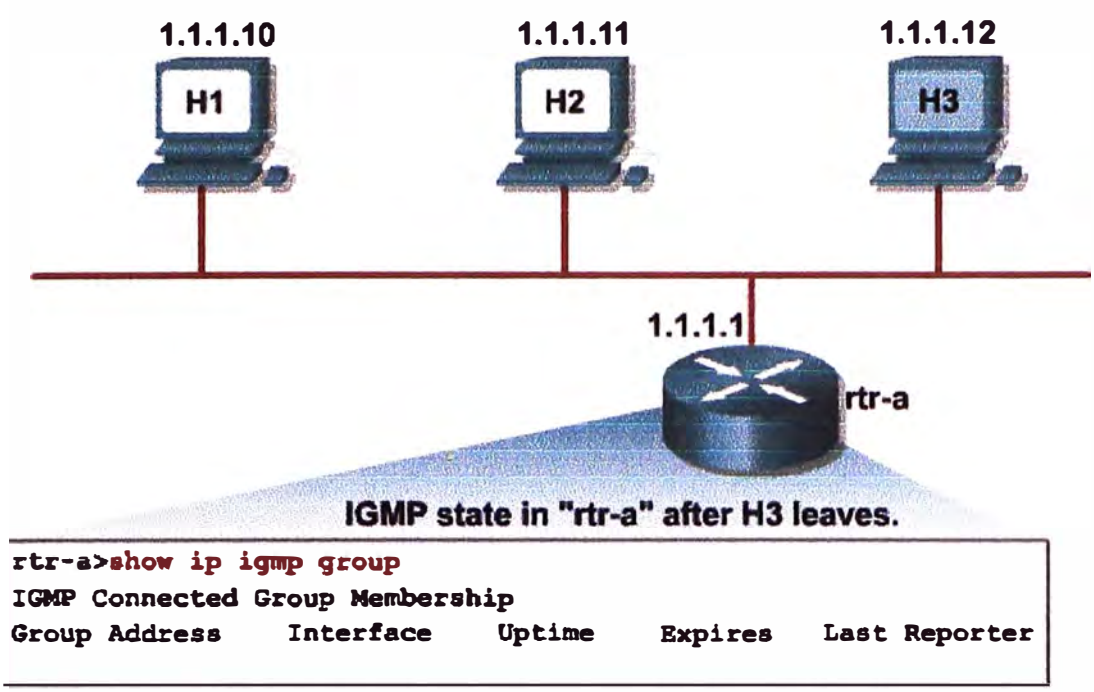


Fig. 3.4 Salida de un Grupo (continuacion)

3.3 Introduccion del IGMPv3

La principal intención del IGMPv3, definido en el RFC 3376, es permitir a los hosts para indicar que se desea recibir sólo el tráfico particular cuya fuente esta dentro de un grupo multicast. IGMPv3 añade la capacidad para filtrar multicasts basado en la fuente multicast. Esto se muestra en la Figura 3.5, donde miembros de union envian reportes IGMPv3 luego de ingresar al grupo:

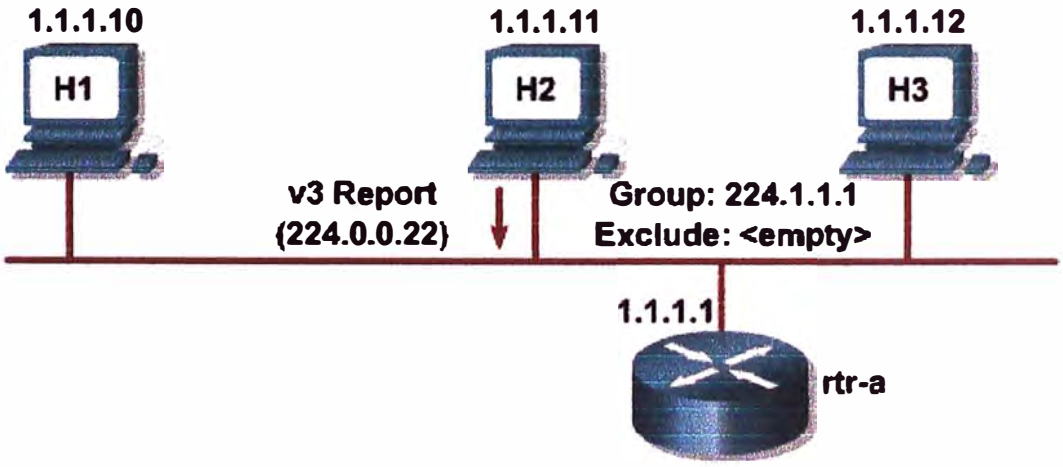


Fig. 3.5 Uniendo a un Grupo con IGMPv3

Esta mejora hace que la utilización de los recursos de rutas más eficientes.

La figura 3.6 muestra una operacin IGMPv3. El host H3 envía un mensaje de union con una solicitud explícita de unirse a las fuentes de la lista fuente. IGMPv3 utiliza una fuente de la lista de fuente con filtros, que permite a un sistema que reporte interés en la recepción de los paquetes sólo de las direcciones específicas de origen o de fuente específica, pero todas las direcciones que se envían a una dirección de multicast. Los protocolos de enrutamiento multicast puede utilizar esa información para evitar la entrega de los paquetes multicast de fuentes específicas a las redes donde no hay receptores interesados.

En IGMPv3, los reportes se envían a 224.0.0.22 en lugar de 224.0.0.2.

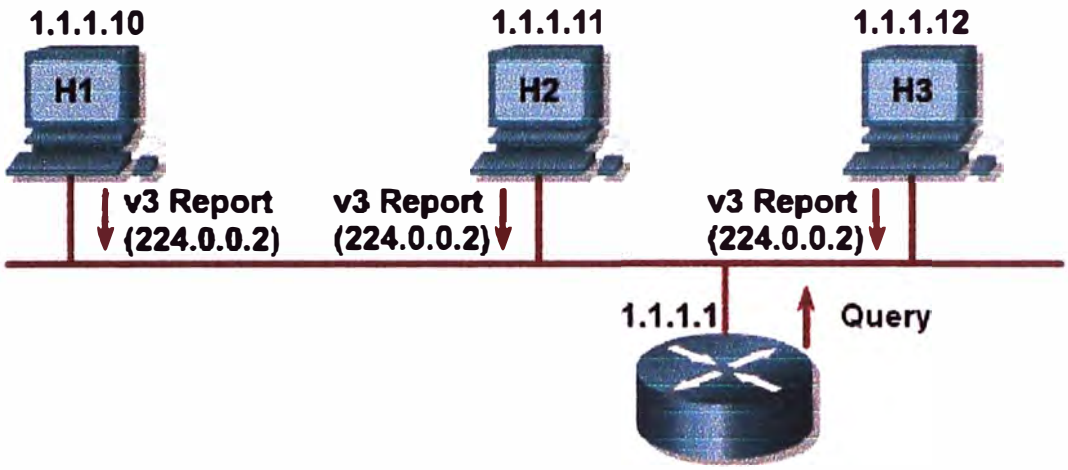


Fig. 3.6 Estado de Mantenimiento IGMPv3

3.4 Interoperatividad entre IGMPv2 y IGMPv3

Utilice el comando **show ip igmp interface** para determinar que versión del IGMP está activo actualmente en una interface. En la Figura 3.7 se visualiza la versión que esta trabajando:

En el ejemplo, la versión del IGMP es la línea que dice "Current IGMP host version is 2" and "Current IGMP router version is 2".

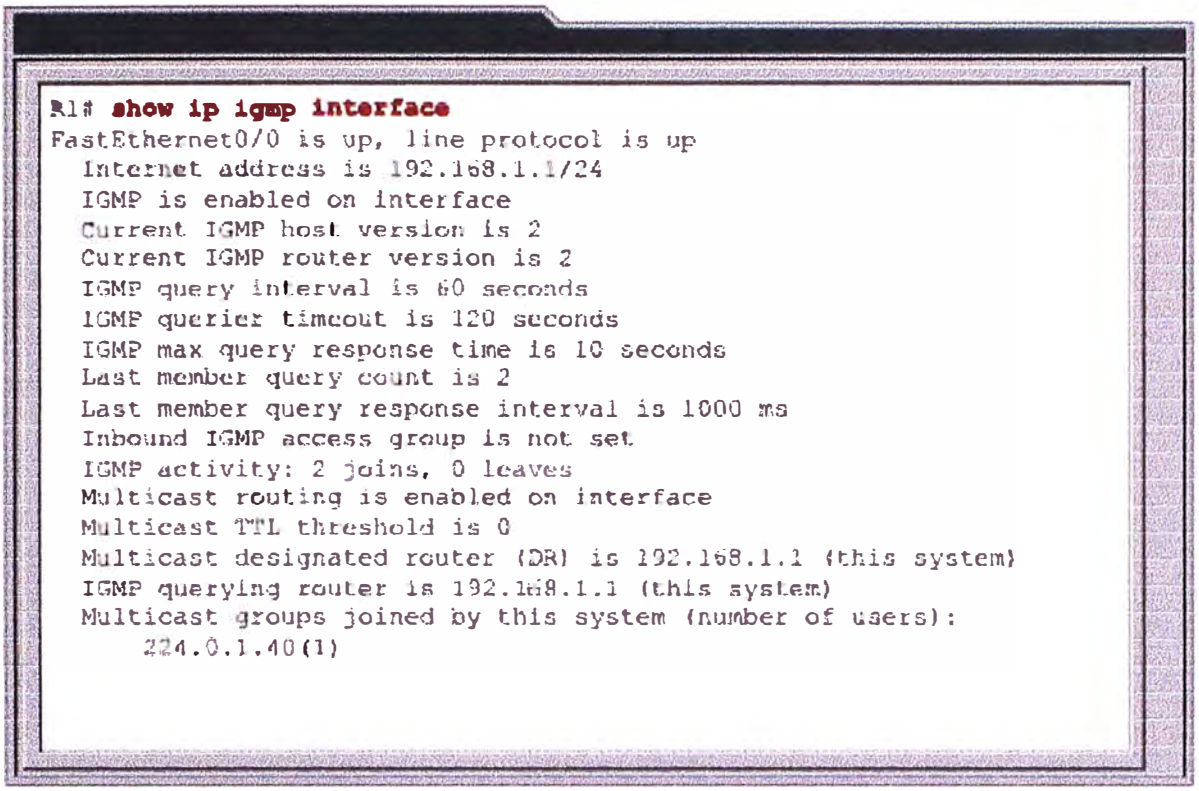


Fig. 3.7 Verificando la version IGMP

3.5 Multicast en Entorno Switch Capa 2

Para la mayoría de los switches Capa 2, el tráfico multicast es normalmente tratada como un desconocido dirección MAC o frame broadcast que hace que se inundan todos los puertos dentro de una VLAN. Este tratamiento es aceptable para broadcast, pero, como se señaló anteriormente, los hosts con IP multicast pueden unirse y estar interesado sólo en grupos específicos de multicast. En la mayoría de los switches Capa 2, este tráfico se reenvía a todos los puertos, lo que resulta en desperdicio de ancho de banda en la red y en las estaciones finales. En la Figura 3.8 se muestra gráficamente:

Fig. 3.8 Frame Switching Multicast Capa 2

Uno de los métodos que utilizan los switches Cisco Catalyst para eludir este impase es permitir al administrador que configure el switch manualmente para asociar una dirección MAC multicast con varios puertos.

Por ejemplo, el administrador configura los puertos 5, 6, y 7 de modo que son los únicos que reciben la multicast el tráfico destinado a los grupos de multicast. Este método funciona, pero no es escalable. Los hosts con IP multicast dinámicamente deben unirse y salirse de los grupos que utilizan IGMP multicast para indicar al router. La configuración dinámica de la tabla de reenvio es más eficaz y reduce la administración de los usuarios.

3.6 Soluciones Multicast en Capa 2.

Muchas soluciones de switching multicast se han desarrollado para mejorar el comportamiento de los switches, cuando reciban los frames multicast, como los siguientes:

- CGMP
- IGMP snooping

CGMP es un protocolo propietario de Cisco System que se ejecuta entre un router multicast y un switch. Este protocolo permite al Cisco multicast informar sobre el cambio de la información contenida en el paquete IGMP después de que recibe los mensajes IGMP enviados por los hosts.

Con IGMP snooping, un switch multicast debe examinar cada paquete de datos para determinar si contiene cualquier información de control pertinente IGMP y actualizar la tabla de MAC como corresponde. IGMP snooping llevarán a cabo en un switch de baja

performance con un CPU lento podría tener un impacto de grave rendimiento cuando los datos se envían a altas velocidades.

La solución es implementar IGMP snooping en switches de alto rendimiento, con la especial aplicación específica de los circuitos integrados (ASIC), que puede realizar el control IGMP en hardware. CGMP es una mejor opción para el bajo rendimiento de switches, no se requiere hardware especial.

3.7 Cisco Group Management Protocol (CGMP).

CGMP es el más común solucion switching multicast, y que fue implementado por primera vez por Cisco.

CGMP se basa en el modelo cliente / servidor, donde el router es considerado como un servidor CGMP y el switch asume el papel de cliente. Hay componentes de software que se ejecutan en ambos dispositivos, con el enrutador se traducen los mensajes IGMP en comandos CGMP, que luego son procesados en los switches y son usados para rellenar la tabla de reenvio Capa 2 con las correctas entradas multicast. En la figura 3.9 se visualiza el principio basico del CGMP:

Fig. 3.9 Frame Switching CGMP Multicast Capa 2

El principio basico del CGMP es que el router IP multicast ve a todos los paquetes IGMP e informa al switch cuando los hosts específicos se unen o salen de los grupos multicast. Routers usan el web-known CGMP direcciones MAC de multicast para enviar paquetes de control CGMP hacia el switch. El switch luego usa esta información para programar la tabla de reenvio (forwarding table).

Cuando el router vea un paquete de control IGMP, se crea un paquete CGMP que contiene el tipo de solicitud (de union o salida), la dirección MAC multicast Capa 2, y la actual dirección MAC del cliente.

Este paquete es enviado hacia el bien-conocido (well-known) CGMP dirección MAC multicast 0x0100.0cdd.dddd que todos los switches CGMP detectan. El mensaje de control

CGMP va a ser interpretado, y las respectivas entradas se crean en la tabla de cambio de contenido de memoria direccionable (CAM) – content-addressable memory para obligar la transmisión de tráfico multicast para este grupo.

3.8 IGMP Snooping.

La segunda solucion multicast switching es el IGMP snooping. Como su nombre lo indica, los switches llegan a ser IGMP-aware y sensan las conversaciones sobre el IGMP entre los hosts y routers.

This activity requires the processor in each switch to identify and intercept a copy of all IGMP packets flowing between routers and hosts and vice versa. It includes these IGMP packets:

Esta actividad requiere el procesador en cada switch para identificar e interceptar una copia de todos los paquetes IGMP que fluyen entre los routers y hosts, y viceversa. Estos incluyen paquetes IGMP:

- IGMP membership reports
- IGMP leaves

If care is not taken as to how IGMP snooping is implemented, a switch may have to intercept all Layer 2 multicast packets to identify IGMP packets. This action can have a significant impact on switch performance. Proper designs require special hardware (Layer 3 ASICs) to avoid this problem, which may directly affect the overall cost of the switch. Switches must be Layer 3-aware to avoid serious performance problems because of IGMP snooping. (ver Figura 3.10)

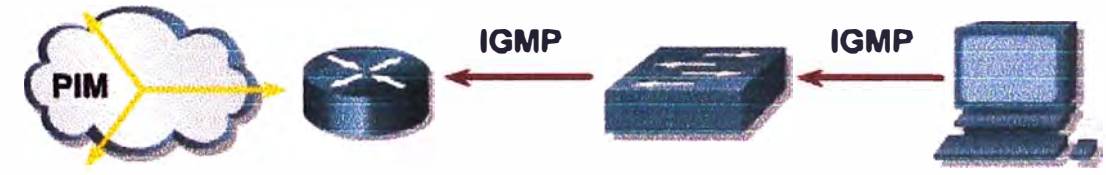


Fig. 3.10 Frame Switching IGMP Snooping Multicast Capa 2

Si no se tiene cuidado en cuanto a como el IGMP snooping es implementado, un switch podra interceptar a todos los paquetes multicast de Capa 2 para identificar los paquetes IGMP. Esta acción puede tener un impacto significativo en el rendimiento del switch. Para evitar este problema los correctos diseños requieren hardware especial (ASICs Capa 3), el

cual puede afectar directamente en el costo del switch. Los switches Capa 3-aware a fin de evitar serios problemas de rendimiento debido al IGMP snooping.

3.9 Resumen del capitulo.

En este capítulo, se ha visto cómo IGMP se utiliza como base el mecanismo de señalización para informar a los routers en una subred de un anfitrión del deseo de convertirse en miembro de un grupo de multidifusión. IGMPv2 amplió este mecanismo de señalización para permitir que alberga a la señal cuando ya no quería pertenecer a un grupo de multidifusión. Esta extensión del protocolo ha reducido significativamente la latencia de la licencia que, a su vez, permite que los routers y conmutadores para responder rápidamente y cierre el flujo de tráfico multicast innecesarios a las partes de las redes en las que ya no es necesario.

Por último, es importante recordar que IGMP es el único mecanismo de acogida puede utilizar para routers señal de su deseo de recibir tráfico de multidifusión para un grupo específico. Ejércitos no son ni conoce, ni en caso de que se ocupa, que es el protocolo de enrutamiento en uso por los routers en la red. En lugar de ello, los routers de la red es responsable de conocer y entender el protocolo de enrutamiento multicast en uso, así como de asegurarse que el tráfico multicast se entrega a los miembros del grupo a través de la red.

CAPITULO IV
PROTOCOLO DE RUTEO MULTICAST

4.1 Introducción.

La necesidad de implementar una red multicast requiere comprender previamente aspectos importantes de cómo aprender la presencia de los routers vecinos que conozcan de multicast, para ello el presente capitulo nos va a detallar los pormenores de las categorías protocolos de ruteo usados en redes multicast. Tambien examinaremos los diferentes modos de protocolos, distribución de arboles y los procedimientos existentes para el reenvio de trafico; para su eficaz uso en la implementacion de redes multicast.

4.2 Protocolos usados en Multicast.

Para entender el modelo del multicast del IP, usted debe tener un buen conocimiento de trabajo de los árboles de la distribución del multicast. En el modelo del unicast, el tráfico se encamina a través de la red a lo largo de una sola trayectoria de la fuente al host de la destinación. En el modelo del multicast, sin embargo, la fuente está enviando tráfico a un grupo arbitrario de los hosts que son representados por una dirección del grupo del multicast.

Para entregar tráfico del multicast a todos los receptores, los árboles de la distribución del multicast se utilizan para describir la trayectoria que el tráfico del IP multicast toma a través de la red. Los dos tipos básicos de árboles de la distribución del multicast son árboles de la fuente y los árboles compartidos.

Lo arboles de distribucion multicast definen la trayectoria desde la fuente (origen) hacia los receptores sobre el cual fluye el trafico multicast. Existen 02 tipos de arboles de distribución multicast:

- Source trees (arbol origen)
- Shared trees (arbol compartido)

4.2.1 Arbol Origen.

Con un source tree, cada tree (arbol) es construido para cada una de los sources (fuentes) a todos los miembros de su grupo. Debido a que el source tree toma el camino más corto de la fuente a sus receptores, esto también es llamado un árbol de camino más corto (SPT-shortest path tree). Cada par de source/group necesita su propia información de estado. Para los grupos que tienen un gran número de fuentes, o las redes que tienen un gran número de grupos con un gran número de fuentes de cada grupo, los source trees pueden dar enfasis en la capacidad de almacenamiento de los routers.

Nota:

Los source trees son también referidos como el source-based trees o source-root trees.

La forma más simple de un árbol de distribución del multicast es un árbol deorigen raíz que es la fuente del tráfico del multicast y que ramas forman un árbol que atraviesa a través de la red a los receptores. Porque este árbol utiliza la trayectoria más corta a través de la red, también se refiere con frecuencia como árbol más corto de la trayectoria (SPT).

La Figura 4.1 muestra un ejemplo de un SPT para el grupo 224.1.1.1 arraigado en la fuente, recibe A, y conecta dos receptores, hosts B y C.

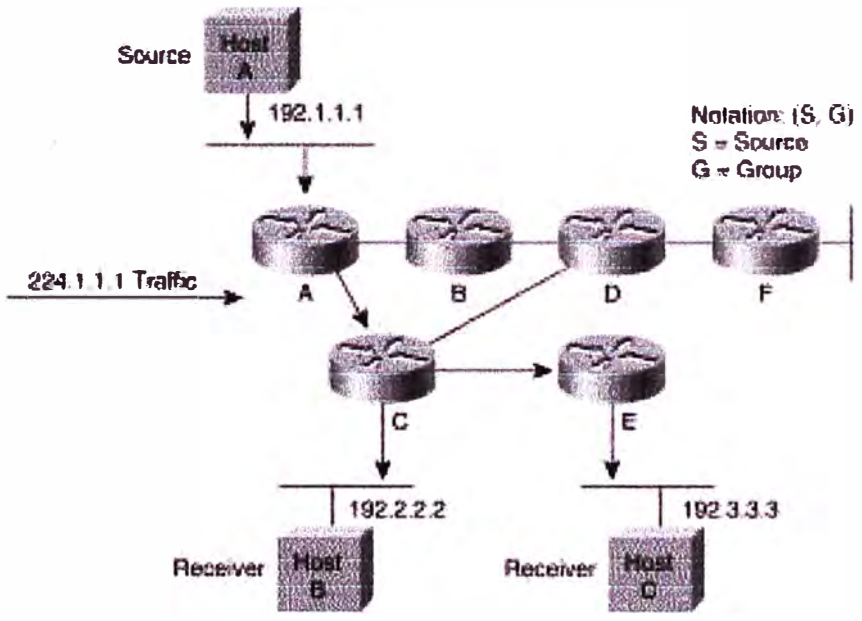


Fig. 4.1 Host A Shortest Path Tree

La connotación especial de (S, G), pronunciada la "coma G de S", enumera un SPT donde está el IP address S de la fuente y G es la dirección del grupo del multicast. Usando esta notación, el SPT para el ejemplo en la Figura 2-8 sería escrito como (192.1.1.1, 224.1.1.1).

Note que esta notación implica que un SPT separado existe para cada fuente individual que envía a cada grupo, que es exacto qué sucede. Por lo tanto, si el host B también está enviando tráfico al grupo 224.1.1.1 y recibe A y C es receptores, entonces un separado (S, G) SPT existiría con una notación de (192.2.2.2, 224.1.1.1) según lo demostrado en la Figura 4.2.

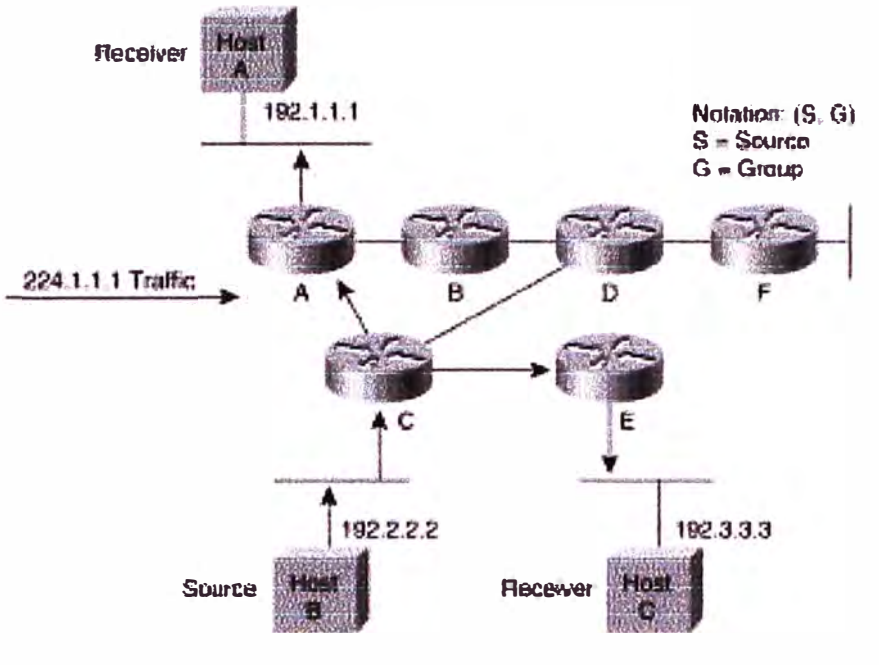


Fig. 4.2 Host B Shortest Path Tree

4.2.2 Arboles Compartidos.

Los protocolos shared tree crean caminos de transmisión multicast que se basan en un router como núcleo central que sirve de punto de encuentro (RP- rendezvous point) entre las fuentes y los destinos multicast. Las fuentes inicialmente envian sus paquetes multicast a la RP, que a su vez envía los datos a través de un shared tree (arbol compartido) a los miembros del grupo. Un árbol compartido es menos eficiente que un SPT (caminos entre la fuente y los receptores no son necesariamente el más corto), pero es menos exigente en routers (memoria, CPU).

Hay básicamente dos tipos de protocolos de enrutamiento multicast: dense mode (modo denso) y sparse mode (modo esparcido):

a. Protocolo Modo Denso.

Consiste en la inundación (flood) de trafico multicast a todas partes de la red y corte de flujos donde no hay receptores, usando el mecanismo periodico flood-and-prune.

b. Protocolo Modo Esparcido.

Usa un explicito mecanismo de union (join), donde la distribucion de arboles (distribution tree) se basan en la demanda explicita por unirse a los mensajes enviados por los routers que se han conectado directamente los receptores.

Diferente de los árboles de la fuente que tienen sus raíces en la fuente, los árboles compartidos utilizan una sola raíz común puesta en un cierto punto elegido en la red. Dependiendo del protocolo de la encaminamiento del multicast, esta raíz se llama a menudo un Punto Pendezvous (RP) o la base, que se prestan a otros nombres del campo común de los árboles compartidos: Árboles del RP (RPT).

La Figura 4.3 muestra un árbol compartido para el grupo 224.2.2.2 con la raíz situada en el router D. Al usar un árbol compartido, las fuentes deben enviar su tráfico a la raíz para que el tráfico alcance todos los receptores.

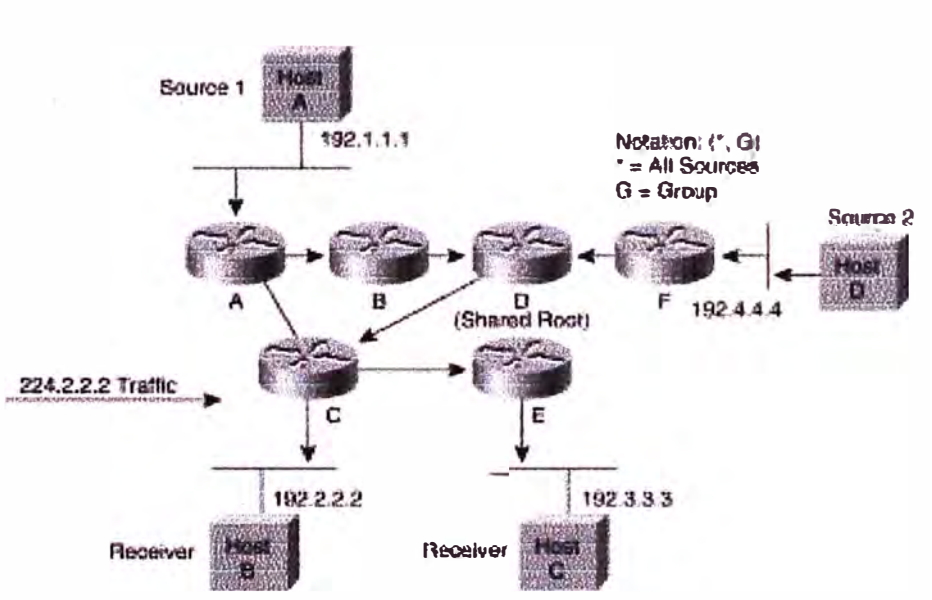


Fig. 4.3 Distribucion de arbol Compartidos

En este ejemplo, el tráfico del grupo del multicast de la fuente recibe A y D viaja a la raíz (router D) y entonces abajo del árbol compartido a dos receptores, hosts B y C. Porque todas las fuentes en el grupo del multicast utilizan un árbol compartido común, una

notación del comodín escrita como (*, G), representa el árbol. En este caso, * los medios todas las fuentes, y el G representa el grupo del multicast. Por lo tanto, el árbol compartido demostrado en La Figura 4.3 sería escrito, (*, 224.2.2.2).

4.2.3 Categorias de Protocolo de Ruteo.

Los actuales protocolos del multicast se pueden subdividir en tres categorías básicas:

- Los protocolos modo denso (DVMRP y PIM-DM)
- Los protocolos modo esparcido (PIM-SM y CBT)
- Los protocolos en modo de enlace de estado (MOSPF)

Algunos protocolos, tales como PIM, son capaces del funcionamiento en modo denso o escaso dependiendo de cómo se configura la router . Es también posible configurar los router Cisco PIM para tomar la decisión de sparse/dense dinámicamente en una base del grupo del multicast.

a. Protocolo Modo Denso.

Los protocolos densos del modo tales como DVMRP y PIM DM emplean solamente SPTs para entregar (S, G) tráfico del multicast usando un principio del empuje. El principio del empuje asume que cada subnet en la red tiene por lo menos un receptor de (S, G) tráfico del multicast, y por lo tanto el tráfico se empuja o se inunda a todos los puntos en la red. Este proceso es análogo a una radio o a el broadcast de TV que se transmitan sobre el aire a todos los hogares dentro del área de la cobertura. Los receptores necesitan simplemente templar adentro a el broadcast para recibir el programa.

b. Protocolo Modo Esparcido.

Los protocolos escasos del modo hacen uso árboles compartidos y de vez en cuando, como en el caso de PIM-SM, SPTs para distribuir tráfico del multicast a los receptores del multicast en la red. En vez de usar un modelo del empuje, sin embargo, los protocolos de modo esparcidos hacen uso un modelo del tirón en el cual el tráfico del multicast se tire hacia abajo a los receptores en la red. El modelo del tirón por lo tanto asume que el tráfico del multicast no está deseado a menos que se solicite específicamente usando un explícito ensamble el mecanismo. Usando la analogía de la TV otra vez, este modelo es como un acontecimiento de la pagar por vista que no se envíe al receptor a menos que esté solicitado específicamente.

Mensaje de arbol de Uniones Compartidos.

Para tirar hacia abajo el tráfico del multicast a un receptor en una red escasa del modo, un rama compartido del árbol se debe construir del nodo de la raíz (el RP en PIM-SM o de la base en el CBT) al receptor. Para construir este rama compartido del árbol, una router envía un árbol compartido ensambla el mensaje hacia la raíz del árbol compartido. Esto ensambla el router de los recorridos del mensaje por el router hacia la raíz, construyendo un rama del árbol compartido mientras que va. La Figura 4.4 demostraciones ensambla ser enviado encima del árbol compartido a la raíz. En este Ejemplo , el router E tiene un receptor localmente conectado y por lo tanto envía un mensaje del unido (representado por la flecha rayada) hacia la raíz vía el router C. El mensaje viaja salto por el salto hasta que alcanza la raíz y construye un rama del árbol compartido (según lo mostrado por las flechas sólidas).

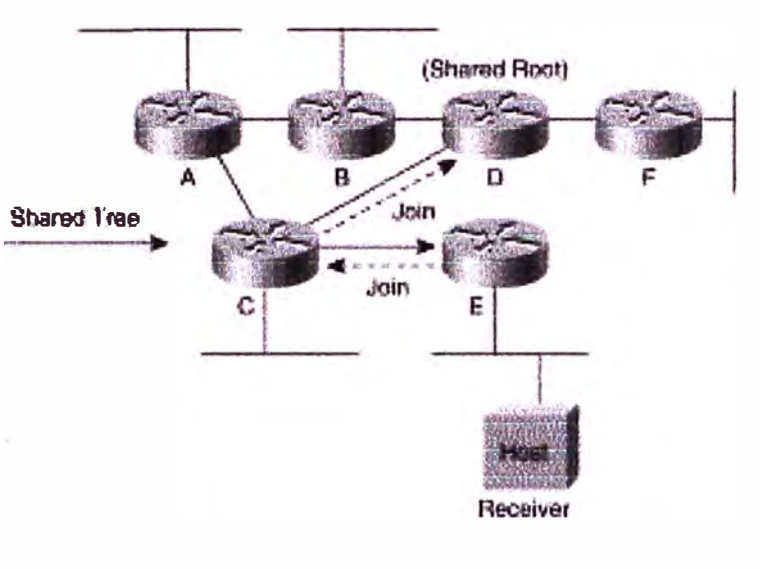


Fig. 4.4 Shared Tree Join Message

En algunos casos (PIM-SM, por Ejemplo), los SPT ensamblan mensajes se pueden también enviar en la dirección de la fuente para construir un SPT de una fuente individual del multicast a los receptores en la red. SPTs permite a los routers que han conectado directamente receptores con el corte a través la red y puentea el nodo de la raíz para poder recibir tráfico del multicast de una fuente vía una trayectoria más directa.

La Figura 4.5 representa un SPT que es el usar construido ensambla los mensajes enviados hacia una fuente específica del multicast. En este Ejemplo , el router E envía un SPT ensambla el mensaje (demostrado por las flechas rayadas) hacia la fuente vía el router C.

Los SPT ensamblan recorridos saltan por el salto hasta que alcanzan el router A, construyendo el SPT (demostrado por las flechas sólidas) como va.

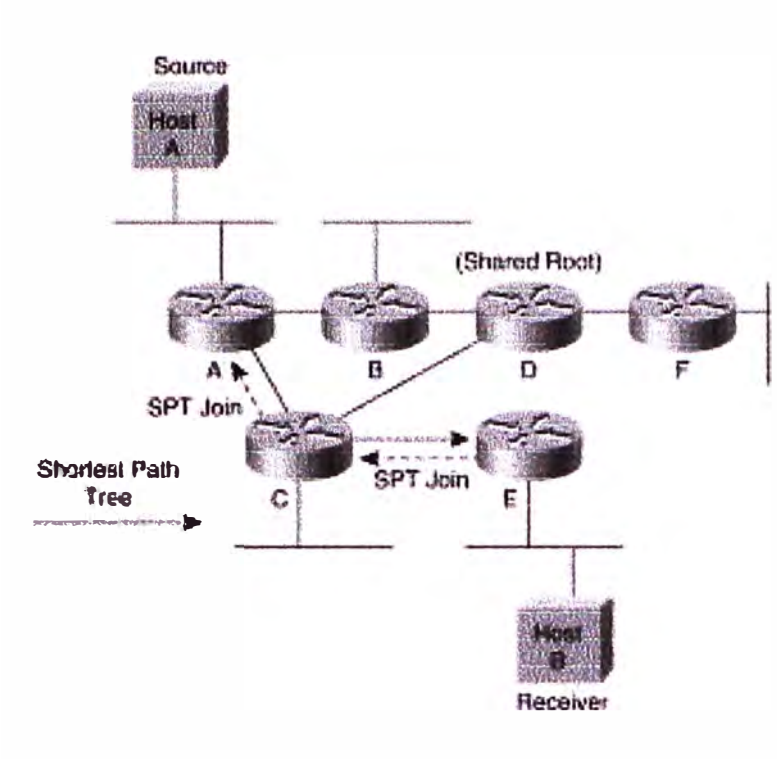


Fig. 4.5 Mensajes SPT Join

Es importante observar que si los ramas de los árboles de la distribución en una red escasa del modo (los árboles compartidos o SPTs) no se restauran, medirán el tiempo hacia fuera y serán suprimidos, de tal modo parando la circulación abajo del rama del árbol compartido. Para evitar este problema, los ramas de los árboles escasos de la distribución del modo son mantenidos por una cierta forma de periódico ensamblan restauran el mecanismo que los routers envían a lo largo del rama. Algunos protocolos (PIM-SM, por Ejemplo) manejan la restauración volviendo a enviar el mensaje del unido encima del árbol para restaurar el rama periódicamente.

c. Protocolos de Estado de Enlace.

Los protocolos de acoplamiento-estado por Ejemplo la función de MOSPF como protocolos densos del modo en que ambos utilizan SPTs para distribuir tráfico del multicast a los receptores en la red. los protocolos del Acoplamiento-estado, sin embargo, no utilizan la inundación y no podan el mecanismo que se utiliza en DVMRP o PIM-DM. En lugar, inundan multicast especial, la información del acoplamiento-estado que identifica

el lugar de los miembros del grupo (es decir, receptores) en la red. Todas los routers en la red utilizan esta información de la calidad de miembro de grupo para construir los árboles más cortos de la trayectoria de cada fuente a todos los receptores en el grupo.

4.3 Multicast Distribution Trees.

La Figura 4.6 muestra un SPT entre la fuente 1 y receptores 1 y 2. Esto es apropiado pues la ruta entre la fuente y los receptores sobre los routers A, C, y E es el camino con mas bajo costo.

Los paquetes se envían de acuerdo a la fuente y par de dirección de grupo. El reenvío de estado asociado con el SPT es a la que se refiere por la notación (S, G), en donde S es la dirección IP de la fuente, y G es la dirección de grupo multicast.

La Figura 4.7 muestra otro ejemplo de SPT, en donde la fuente 2 esta activa y esta enviando paquetes multicast a los receptores 1 y 2. Un SPT está diseñado para este fin, esta vez con la fuente 2 en la raíz del SPT. El punto principal es que el SPT se construye por separado para cada fuente S enviando al grupo G.

La Figura 4.8 muestra un árbol de distribución compartida. Router D es la raíz (root) de este árbol compartido, que se construye a partir del router D a los routers C y E hacia los receptores 1 y 2. En el Protocolo Multicast Independiente (PIM), la raíz del árbol compartido es un RP.

Los paquetes se envían por el árbol de distribución compartida hacia los receptores. El valor por defecto para el reenvío de estado del árbol compartido es identificado por la notación (*, G), donde el asterisco (*) es un comodín de entrada, que representa a cualquier fuente, y G es la dirección de grupo multicast.

En la Figura 4.9, las fuentes 1 y 2 envian paquetes multicast hacia un RP vía SPTs, y desde el RP, los paquetes multicast están fluyendo a través de un árbol de distribución compartida hacia los receptores 1 y 2.

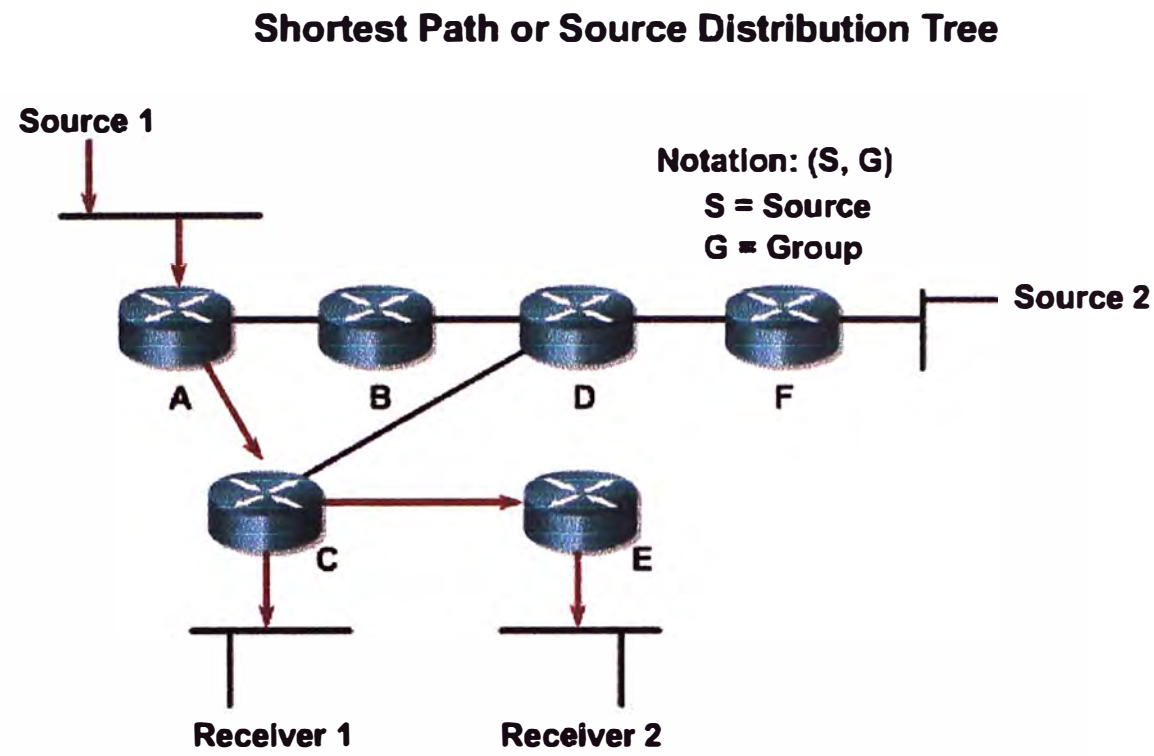


Fig. 4.6 Shortest Path Trees

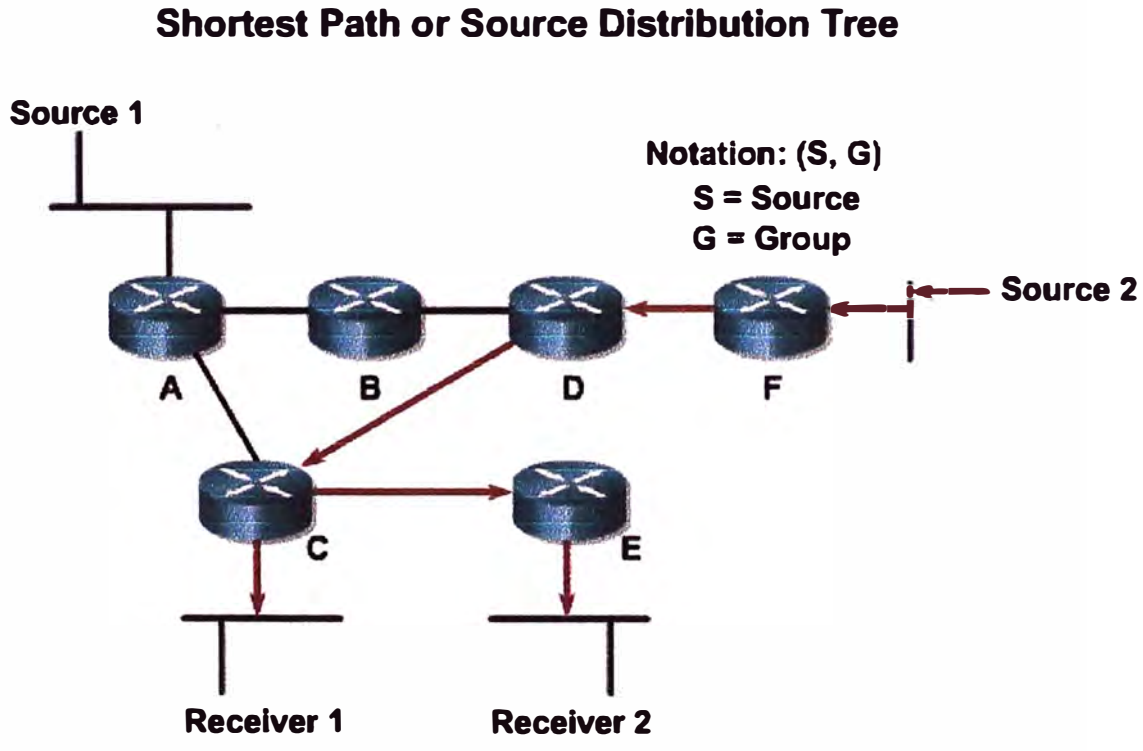


Fig. 4.7 Shortest Path Trees (Cont.)

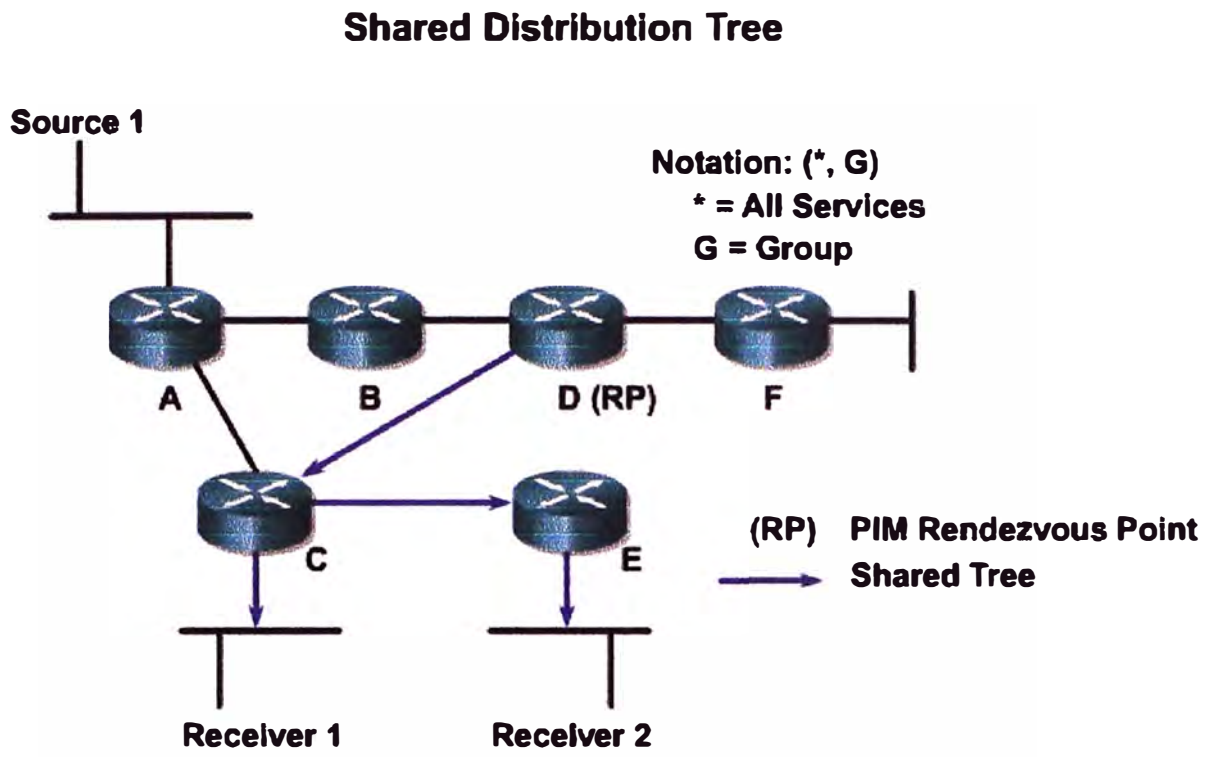


Fig. 4.8 Shared Distribution Trees

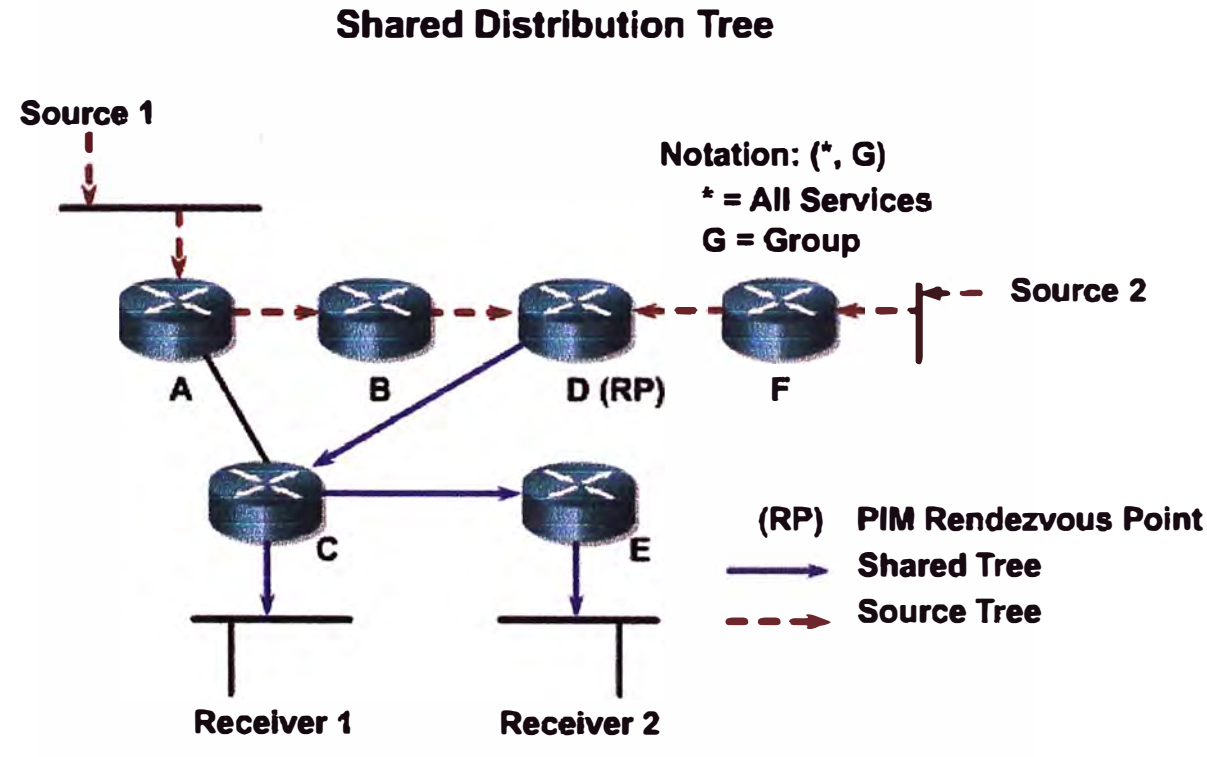


Fig. 4.9 Shared Distribution Trees (Cont.)

4.4 Identificación del Multicast Distribution Trees.

El reenvío de entradas multicast que aparecen en las tablas de reenvío multicast son leidos de la siguiente manera:

- **(S, G):** Por la fuente S se envian al grupo G. Estas entradas suelen reflejar la SPT, pero también pueden aparecer en un árbol compartido.
- **(*, G):** Para cualquier fuente de origen (*) se envian al grupo G. Estos entradas reflejan el árbol compartido, pero también son creadas (en routers Cisco) para cualquier entrada existente (S, G).

El estado de entradas SPT usa mayor recursos de memoria porque hay una entrada para cada remitente y grupo de pares, pero el tráfico se envía a través de la ruta óptima para cada receptor, de este modo se minimiza la demora en la entrega de paquetes.

El estado de entradas de Shared distribution tree consume menos recursos de memoria, pero puede trazar caminos menos optimos de una fuente a los receptores, consecuentemente esto nos lleva a un retrazo adicional en la entrega de paquetes.

4.5 IP Multicast Routing.

En enrutamiento unicast, cuando el router recibe un paquete, la decisión sobre a donde enviar el paquete depende de la dirección destino del paquete. En enrutamiento multicast, la decisión sobre a donde enviar los paquetes multicast depende de donde provenía el paquete.

Los routers multicast deben saber el origen de los paquetes en lugar de su destino. Con el origen del multicast, la dirección IP se refiere a la conocida fuente, y la dirección IP de destino se refiere a un grupo de receptores desconocidos.

El enrutamiento multicast utiliza un mecanismo denominado Reverse Path Forwarding (RPF) para evitar el reenvío de bucles y para asegurar el camino más corto desde la fuente hasta los receptores.

4.5.1 Reenvio del IP Multicast.

En el modelo del unicast, los routers remiten tráfico a través de la red a lo largo de una sola trayectoria de la fuente al host de la destinación que IP address aparece en el campo de dirección de destinación del paquete del IP. Cada router a lo largo de la manera toma una decisión de la expedición del unicast, usando el IP address de la destinación en el paquete, mirando encima de la dirección de destinación en la tabla y entonces la expedición de la

ruta del unicast el paquete al salto siguiente vía el interfaz indicado hacia la destinación.
En el modelo del multicast, la fuente está enviando tráfico a un grupo arbitrario de hosts representados por una dirección del grupo del multicast en el campo de dirección de destinación del paquete del IP. En contraste con el modelo del unicast, el router del multicast no puede basar su decisión de la expedición en la dirección de destinación en el paquete; estas routers tienen que remitir típicamente el paquete del multicast fuera de los interfaces múltiples para que alcance todos los receptores. Este requisito hace el proceso de la expedición del multicast más complejo que el que esta' usado para la expedición del unicast.
Esta sección examina el concepto de la expedición reversa de la trayectoria (RPF), que es la base del proceso de la expedición del multicast en la mayoría de los protocolos de la encaminamiento del multicast. Esta sección también presenta la información sobre los escondrijos de la expedición del multicast, umbrales de la TTL, y administrativo límites demarcados.

4.5.2 Reenvio en trayectoria Inverso (RPF).

Virtualmente todos los protocolos de la encaminamiento del IP multicast hacen uso una cierta forma de RPF o de cheque entrante del interfaz como el mecanismo primario para determinarse si remitir o caer un paquete entrante del multicast. Cuando un paquete del multicast llega una router , el router realiza un chequeo del RPF en el paquete. Si el cheque del RPF es acertado, se remite el paquete; si no, se dropea.
Para el tráfico que fluye abajo de un árbol de la fuente, el mecanismo del cheque del RPF trabaja como sigue:

1. El router examina la dirección de la fuente del paquete del multicast que llega para determinarse si el paquete llegó vía un interfaz que está en la trayectoria reversa de nuevo a la fuente.
2. Si el paquete llega en el interfaz que conduce de nuevo a la fuente, el cheque del RPF es acertado y se remite el paquete.
3. Si el chequeo del RPF falla, se descarta el paquete.

Cómo una router del multicast se determina qué interfaz está en la trayectoria reversa de nuevo a la fuente depende del protocolo de la encaminamiento en uso. En algunos casos, el protocolo de la encaminamiento del multicast mantiene una tabla de encaminamiento separada del multicast y la utiliza para este cheque del RPF. Un buen Ejemplo de esto es

el protocolo de la encaminamiento del multicast del vector de la distancia (DVMRP), llamado "el protocolo de la encaminamiento del multicast del vector de la distancia." En otros casos, el protocolo del multicast utiliza la tabla de encaminamiento existente del unicast para determinar el interfaz que está en la trayectoria reversa de nuevo a la fuente.

La Figura 4.10 ilustra el proceso del cheque del RPF. Este Ejemplo utiliza una tabla de encaminamiento separada del multicast, aunque el concepto es igual si se utiliza la tabla de encaminamiento del unicast o un poco de otra tabla del reachability.

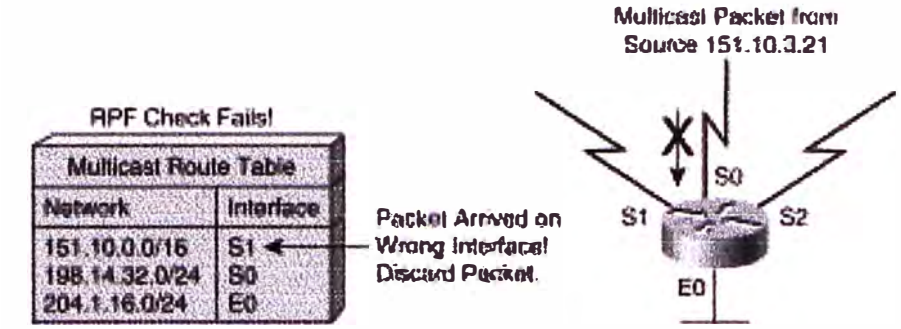


Fig. 4.10 Chequeo de Fallas del RPF

Un paquete multicast de la fuente 151.10.3.21 se recibe en el interface S0. Un chequeo de la tabla de encaminamiento del multicast muestra que el interfaz en la trayectoria reversa de nuevo a la fuente es S1, no S0. Por lo tanto, el chequeo del RPF falla, y se descarta el paquete. La Figura 4.11 es otro ejemplo de un paquete del multicast de la fuente 151.10.3.21 que llega la router , este vez vía el interface S1.

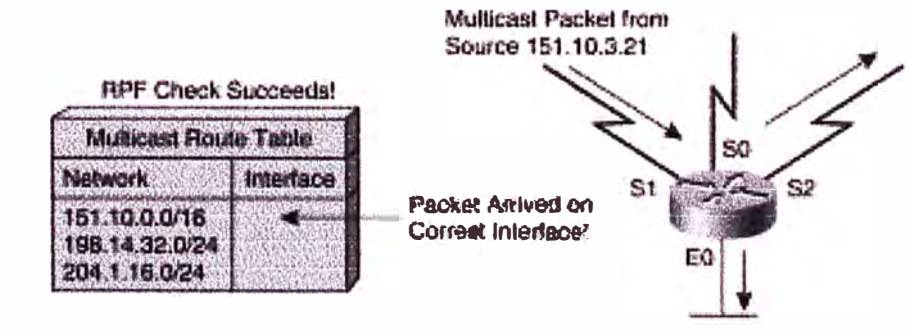


Fig. 4.11 RPF Check Succeeds

En este caso, el cheque del RPF tiene éxito mientras que el interfaz S1 está en la trayectoria reversa de nuevo a la fuente, y por lo tanto el paquete se remite a todos los

interfaces en la lista saliente de la interface. (aviso que los interfaces salientes no tienen que necesariamente incluir todos los interfaces en la router).

4.5.3 Cache de Reenvio Multicast.

La sección "árboles de la distribución del multicast", anterior en este capítulo se discutió el concepto de los árboles de la distribución del multicast del edificio que se utilizan para remitir tráfico del multicast a través de la red a todos los receptores. Desde el punto de vista de la router , cada SPT o árbol compartido se puede representar en una entrada del escondrijo de la expedición del multicast (designada a veces una entrada de la tabla de la ruta del multicast) como interfaz entrante asociado interfaces cero o más saliente. Observe que los árboles compartidos bidireccionales modifican este proceso levemente, pues no hacen una distinción entre los interfaces entrantes y salientes porque el tráfico puede fluir arriba y abajo del árbol.

Realizando el RPF compruebe en resultados entrantes de cada paquete del multicast en una pena substancial del funcionamiento en la router . Por lo tanto, es común para que una router del multicast determine el interfaz del RPF cuando se crea el escondrijo de la expedición del multicast. El interfaz del RPF entonces se convierte en el interfaz entrante de la entrada del escondrijo de la expedición del multicast. Si un cambio ocurre en la tabla de encaminamiento usada por el proceso del cheque del RPF, el interfaz del RPF debe ser recomputed y la entrada del escondrijo de la expedición del multicast puesta al día para reflejar esta información. Observe que los interfaces salientes están determinados de varias maneras dependiendo del protocolo de la encaminamiento del multicast en uso.

Tabla Nº 4.1 Cisco Multicast Routing Tabla Entry

(151.10.3.21/32, 224.2.127.254), 00:04:15/00:01:10, flags: T
Incoming interface: Serial1, RPF nbr 171.68.0.91
Outgoing interface list:
Serial2, Forward/Sparse, 00:04:15/00:02:17
Ethernet0, Forward/Sparse, 00:04:15/00:02:13

Este (S, G) entrada describe (151.10.3.21/32, 224.2.127.254) el SPT. De esta información usted puede ver que la entrada tiene un interfaz entrante, Serial1, y dos interfaces salientes, Serial2 y Ethernet0.

4.6 Protocol-Independent Multicast: Descripcion del PIM-DM.

PIM dense mode (PIM-DM) inicialmente inunda de tráfico a todos las interfaces no-RPF donde hay otro PIM-DM vecino o conectado en forma directa a los miembros del grupo.

En la Figura 1, el tráfico multicast son enviados por la fuente y se propaga a toda la red. Como cada router recibe el tráfico multicast a través de su interface RPF (la interface en la dirección de la fuente), que dirige el tráfico multicast a todos sus PIM-DM vecinos.

Esto da lugar a que algunos tráficos llegan a través de una interface no-RPF, al igual que con los dos routers en el centro y extremo derecho de la figura. Los paquetes que llegan a través de la interface del no-RPF no son descartados. Estos flujosno-RPF son normales para la formación inicial de inundaciones de datos y son corregidos por el normal mecanismo de poda (pruning).

En la Figura 2, los mensajes prune PIM-DM son envíados (señalados con flechas de guiones) para detener el tráfico no deseado.

Los mensajes prune se envían también a las interfaces no-RPF para cerrar el flujo de tráfico multicast, ya que se trata de llegar a través de una interface que no está en el camino más corto hacia la fuente. El ejemplo de mensajes prune enviados a una interface no-RPF se puede ver en los enrutadores en el centro y extremo derecho de la figura.

Los mensajes prune son enviados a una interface RPF sólo cuando el router no tiene trafico multicast a los receptores.

La Figura 3 muestra el resultado del SPT a partir del pruning (poda) de tráfico multicast no deseado en la red.

Aunque el flujo de tráfico multicast ya no es llegar a la mayoría de los routers en la red, el (S, G) sigue siendo el estado de todas ellas y se mantendrá hasta que se detiene la fuente de origen.

En PIM-DM, todos los mensajes prune expiran en 3 minutos. Después de eso, el tráfico multicast se inunda de nuevo a todos los routers. Este comportamiento periodico de flood-and-prune (inundar y cortar) es normal y se debe tener en cuenta cuando la red está diseñada para usar el PIM-DM.

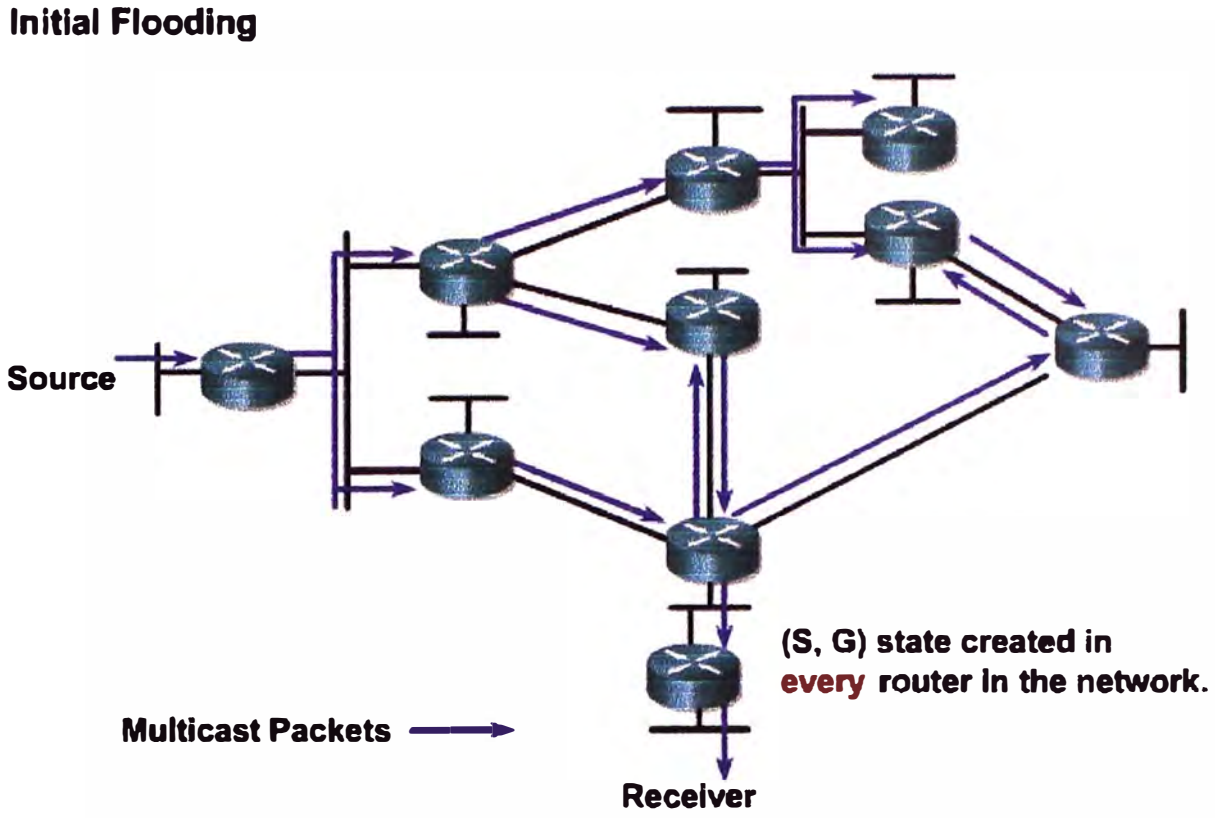


Fig. 4.12 PIM-DM Flood and Prune

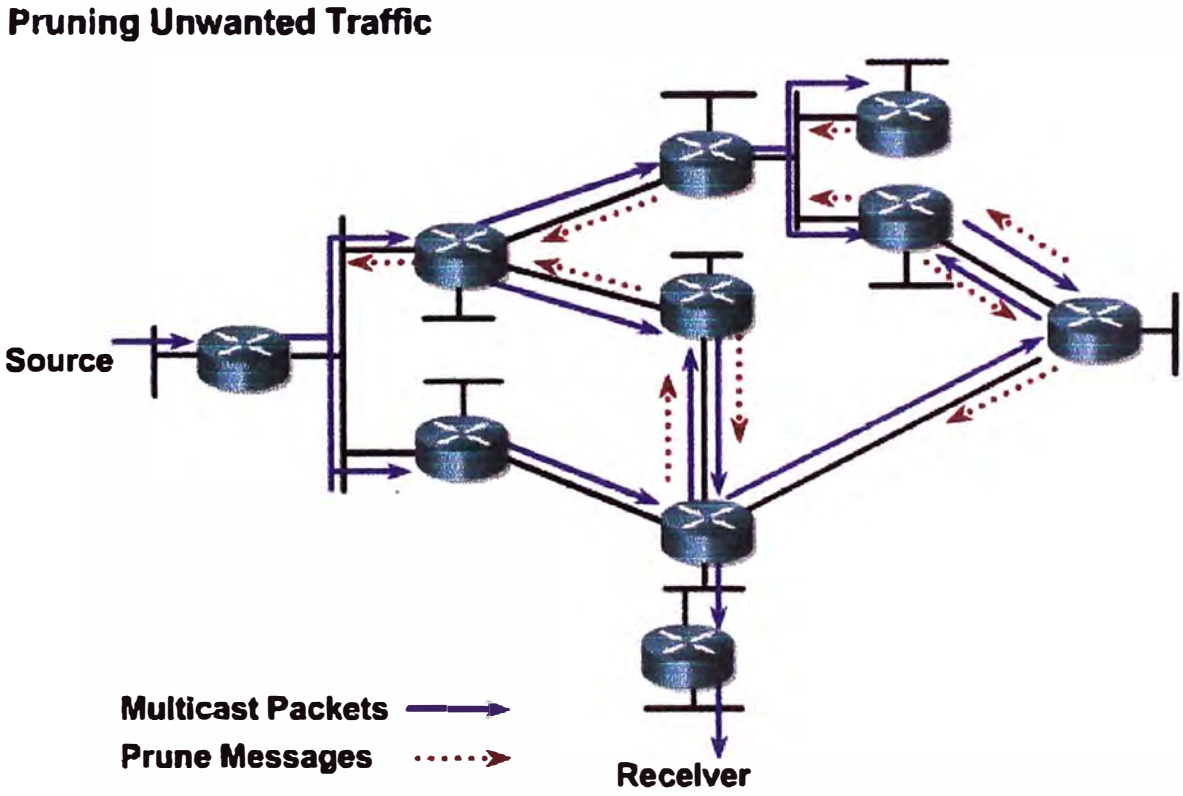


Fig. 4.13 PIM-DM Flood and Prune (Cont.)

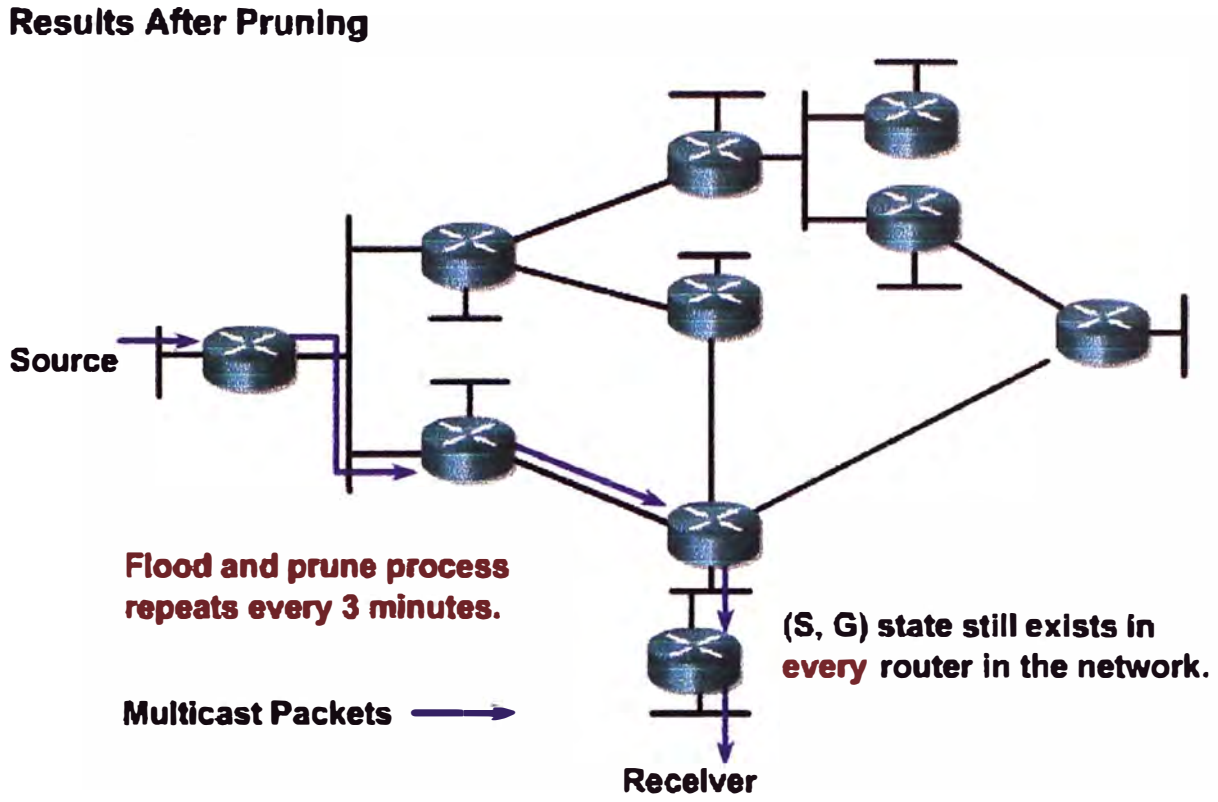


Fig.4.14 PIM-DM Flood and Prune (Cont.)

4.7 Protocol Independiente Multicast: Describiendo el PIM-SM.

El modo PIM sparse (PIM-SM) se describe en el RFC 2362. Al igual que con el PIM-DM, PIM-SM es también independiente de los protocolos unicast subyacentes. PIM-SM utiliza árboles de distribución compartida (shared distribution trees), pero esto también puede cambiar a la SPT.

PIM-SM se basa en un modelo explícito de atracción. Por lo tanto, el tráfico se remite sólo a las partes de la red que lo necesiten.

PIM-SM utiliza un RP a fin de coordinar el reenvío de tráfico multicast de una fuente a los receptores. Los remitentes se registran en el RP y envian una copia unica de datos a través del multicast a los receptores registrados.

Los miembros del grupo se han unido al árbol compartido (shared tree) por sus locales router designado (DR). Un árbol compartido que se construye de esta manera está siempre enraizada en la RP.

En la redes empresariales es apropiado el uso del PIM-SM para el despliegue a gran escala para ambos densely (densamente) y esparsely (escasamente) grupos pobladas. Esta es la

mejor opcion para todas las redes en producción, independientemente de su tamaño y la composición de densidad.

Hay muchas optimizaciones y mejoras en el PIM, incluyendo las siguientes:

- Modo bidireccional PIM, la cual está diseñada para múltiples aplicaciones (es decir, muchos hosts multicasting los unos a los otros).
- Source Specific Multicast (SSM), que es una variante del PIM-SM en que se basa en única source-specific SPTs y no necesita un RP activo para grupos con source-specific (rango de direcciones 232 / 8).

En la Figura 4.15, un receptor activo (que se adjunta a una hoja de router en la parte inferior de la figura) se ha unido al grupo multicast G.

El ultimo (last-hop) router conoce la dirección IP del router RP para el grupo G, y envía una (*, G) para unirse a este grupo hacia el RP.

Esta union (*,G) viaja paso a paso hacia el RP, construyendo una area de clasificacion del arbol compartido (shared tree) que se extiende desde el RP hacia el ultimo (last-hop) router directamente conectado al receptor.

En este punto, los flujos de tráfico del grupo G cae en el árbol compartido para el receptor.

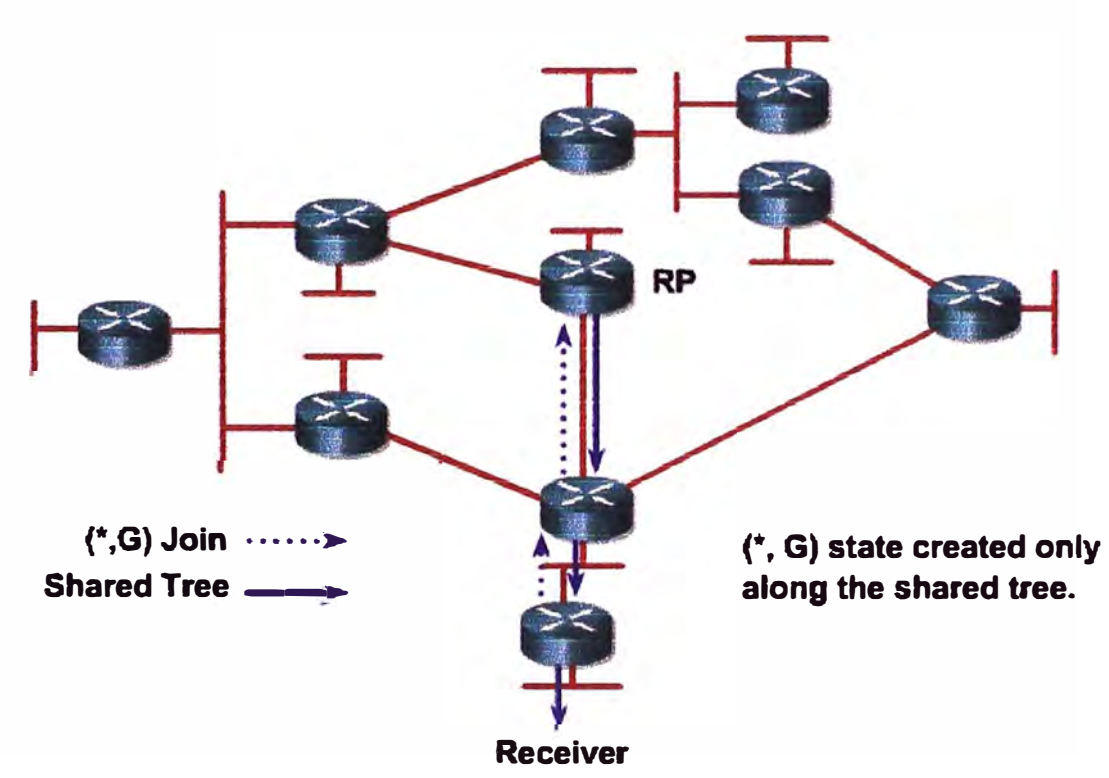


Fig. 4.15 PIM-SM Shared Tree Join

4.8 PIM Sparse-Dense-Mode.

La Figura 4.16 muestra dos fuentes de multicast. Para lograr la máxima eficiencia, se pueden aplicar multiples RPs, en la que cada RP se encuentra en una ubicación óptima. Este diseño es difícil de configurar, administrar y solucionar problemas con el manual de configuración de RPs.

PIM sparse-dense mode soporta la selección automatica de RPs para cada multicast. El router A en la figura podría ser el RP para el source 1, y el router F podría ser el RP para el source 2.

PIM sparse-dense mode es la solución recomendada por Cisco para IP multicast, porque el PIM-DM no es escalable y requiere gran parte de recursos del router, y PIM-SM ofrece limitadas opciones de configuración para el RP.

Si no se descubre la RP para el grupo multicast o ninguno está configurado manualmente, PIM-sparse dense mode opera en modo denso. Por lo tanto, debe aplicar el descubrimiento automático del RP con el PIM sparse-dense mode.

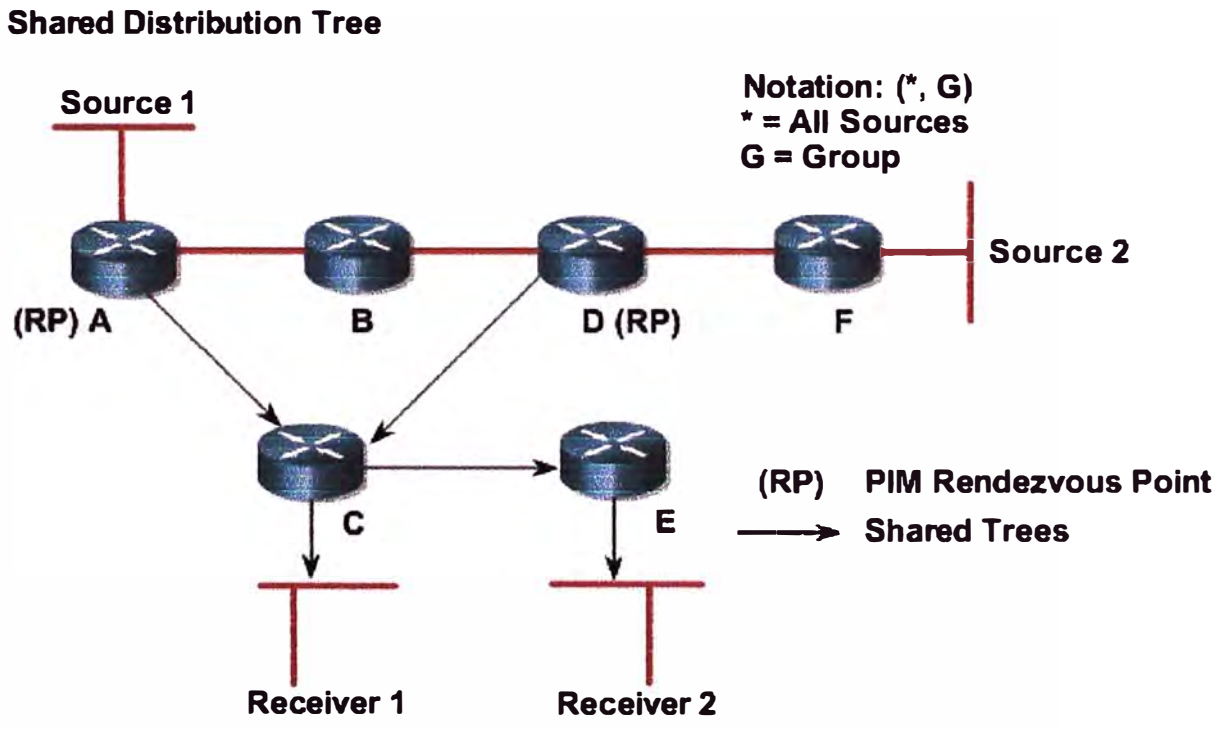


Fig. 4.16 Multiples RPs con Auto RP

4.9 Resumen del capitulo.

En el presente capitulo se ha detallado los diferentes modos de protocolos y categorías de protocolos de ruteo, que sin duda nos permiten entender la forma en que a nivel de ruteo de paquetes son usados para el reenvio de trafico en una red multicast.

Hoy los ingenieros deberían comprender el uso de protocolos de ruteo para su uso en sus redes de la misma manera como se utiliza RIP para redes unicast.

Sin una razón de peso, como para ofrecer compatibilidad con versiones anteriores, la mayoría de ingenieros de redes ni siquiera piensan en el despliegue de una red unicast basadas en RIP. Multicast redes no debe ser diferente. DVMRP deben ser empleados en los nuevos diseños de red sólo cuando sea necesario para la interface con las infraestructuras existentes DVMRP y, a continuación, hasta que la red sólo puede ser migrado a algún otro protocolo multicast más eficientes.

CAPITULO V
MULTICAST SOBRE CAMPOS DE REDES

5.1 Introducción.

Sobre los últimos años, los equipos switching en layer 2 LAN ha ido de una tecnología costosa, marginal que fue desplegada solamente en la espina dorsal de la red a una tecnología relativamente madura.

Esto ha conducido a contar con switching LAN con topologías algo grandes que eran construidas donde un número de switches LAN se interconectan vía trunks de VLANs de alta velocidad para formar un subnet solo, grande, cambiado.

Este capítulo explora algunas de las ediciones con IP multicast en estas topologías de la conmutación del LAN y hecha una ojeada algunos de la corriente y de los métodos propuestos para ocuparse de ellos.

5.2 Caracteristicas de Switches LAN.

Pues usted está probablemente ya enterado, las diferencias entre un bridge y un switch son básicamente velocidad y número de puertos. Como un puente, un switch remite un marco entrante del Media Access Control (MAC) mirando encima del MAC address de la destinación en una tabla de la expedición del MAC address a determinarse fuera de qué puerto debe ser remitido el marco. Para que un switch pueble su tabla de la expedición, el switch debe aprender las direcciones del MAC de la capa 2 de las estaciones y de los puertos con los cuales las estaciones están conectadas. El switch aprende examinando el MAC address de la fuente de los bastidores enviados entre las estaciones en el LAN y observando en qué puerto llegó este marco. Después de una estación se han aprendido el MAC address y el puerto, el MAC address y el número de acceso se almacena en la tabla de la expedición.

Cuando los switches LAN primero comenzaron a aparecer en el mercado, la CPU principal en el switch realizó todas las tareas de conmutación. Cuando la CPU recibió un marco en

un puerto, miraría para arriba el MAC address de la destinación en la tabla de la expedición y después copiaría el marco al puerto de salida especificado. Para acelerar el proceso de las operaciones de búsqueda, la mayoría de éstos los switches tempranos almacenaron la tabla de la expedición en una cierta forma de memoria de contenido direccionable (CAM), que permite que el MAC address sea utilizado como el indicador a la entrada deseada. (esta tabla de la expedición se refiere generalmente como la tabla de la CAM.)

Pues la demanda para un funcionamiento mejor en estos switches creció, la lógica real de la conmutacion-decision era off-loaded de la CPU principal y fue construida en un motor especial de la conmutación que podría tener acceso a la tabla CAM y cambia los marcos de la entrada al puerto de salida a las velocidades wire-rate.

La Figura 5.1 muestra un diagrama de bloque de un switch típico del LAN que pueda realizar de alta velocidad, conmutación de la alambre-tarifa de los bastidores del MAC. Típicamente, una CPU por microprocesador pequeña en el switch realiza funciones de la dirección de la red y puebla la tabla CAM con las direcciones del MAC de las estaciones junto con sus números de acceso asociados. El motor que cambia de la capa 2 entonces utiliza la información en la tabla CAM para tomar decisiones de la expedición. Esta CPU generalmente también está conectada con un puerto en el motor de la conmutación apenas como cualquier otro puerto en el switch. Poblando la tabla con el MAC address del switch sí mismo del CAM y asociando esta entrada al puerto que conecta la CPU, los marcos entrantes tratados al switch (tal como Simple Network Management Protocol [SNMP] y telnet) se pueden cambiar a la CPU para procesar.

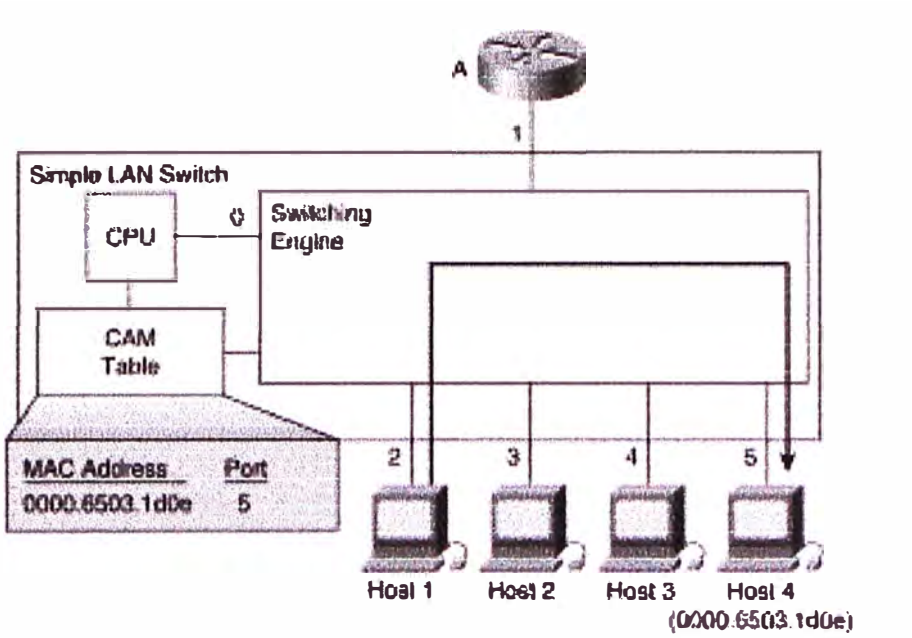


Fig. 5.1 Arquitectura de Simple LAN Switch

Para alcanzar velocidades de la conmutación de la alambre-tarifa, la mayoría de los switches LAN emplean un motor que cambia de la capa 2 basado en los circuitos integrados application-specific especiales, a la medida (ASICs). Este ASICs puede examinar la capa 2, MAC address de la destinación de un bastidor, mirar para arriba este MAC address en la tabla CAM, y cambiar el marco al puerto de salida indicado por la entrada de la tabla CAM. Porque la lógica en estos ASICs se pone en ejecucion en silicio, son capaces de realizar estas operaciones de búsqueda de tabla CAM y layer 2 que cambian a las velocidades que permiten la expedición de la alambre-tarifa de bastidores a través del switch del LAN.

En el ejemplo en la Figura 5.1, el host 1 está enviando un marco tratado al host 4. La CPU ha aprendido el MAC address y el número de acceso del host 4 y ha poblado previamente la tabla CAM con esta información. El motor de la conmutación entonces utiliza esta información para cambiar el marco fuera del puerto 5.

5.3 Inundacion Broadscast/Multicast.

Si un switch recibe un marco sin entrada que empareja en la tabla CAM, no tiene ninguna opción pero inundar el marco fuera de el resto de los puertos en el switch en esperanzas de conseguir el marco a la destinación. Esto sucede típicamente en las situaciones siguientes:

- El MAC address de la destinación todavía no se ha aprendido.
- El MAC address de la destinación es una dirección de el broadcast o del multicast.

La primera situación no es un problema porque el switch agregará eventual el MAC address de la destinación en la tabla CAM sobre la "audiencia" que la estación de destinación transmite un marco. De entonces encendido, todas las transmisiones a esta estación no serán inundadas. Es el segundo de estos casos con los cuales ser tratado.

En la segunda situación, los marcos de el broadcast se deben inundar siempre fuera de todos los puertos (con excepción del puerto entrante) que estén en estado de la expedición en el switch. De la misma manera, no hay generalmente manera para que un switch sepa en residen qué miembros del multicast de los puertos. Por lo tanto, los marcos del multicast se deben también inundar fuera de todos los puertos en la misma manera.

Es este metodo de entrega de tráfico multicast que entrega que los ingenieros de la red de la plano-tierra no han podido considerar en su acercamiento al diseño de red. Dado el renombre cada vez mayor de los usos multicast-basados de las multimedias, las redes basadas en la teoría plana de la tierra sufrirán como el tráfico indeseado del multicast se inunda a cada punto en la red.

5.4 Control de Inundación Multicast.

Mientras que la tecnología de la conmutación del LAN creció en renombre, las tentativas fueron hechas de poner algunos controles en el flooding de los bastidores de broadcast/multicast. El primer debía poner la limitación de la tarifa en ejecucion de broadcast/multicast. La idea era hacer cumplir un cierto límite configurable a la cantidad de anchura de banda que el tráfico de broadcast/multicast podría consumir antes de que los marcos fueran desechados. Pues resulta, la limitación de la tarifa es una idea realmente mala pues el caer arbitrario de ciertos tipos de bastidores de el broadcast puede dar lugar a la inestabilidad de la red que en algunos casos puede ser bastante mala derretir la red.

Por ejemplo, las unidades de datos de protocolo del puente (BPDUs) son multicast al especial todo el MAC address del multicast de los puentes. Si bastante de estos se desecha BPDUs, la red puede sufrir inestabilidades mientras que el algoritmo del árbol que atraviesa procura constantemente converger. Mientras que el algoritmo del árbol que atraviesa en los switches intenta converger, más BPDUs se puede perder, conduciendo a una fusión de la red. Abra los mensajes más cortos de la trayectoria primero (OSPF) hola son otro buen Ejemplo de un bastidor crítico que sea multicast a todo el MAC address del multicast de los routers del OSPF. Si bastantes de estos bastidores se desechan debido a la tarifa de broadcast/multicast que se limita, las adyacencias del OSPF pueden ser perdidas,

que pueden dar lugar a inestabilidad de la red de la capa 3. (mi lema personal es: "opinión justa no a la limitación de la tarifa de la capa broadcast/multicast del MAC.")

El segundo, un acercamiento más sano debe ampliar el formato de la tabla CAM para permitir que una lista de los números de acceso sea asociada a un MAC address. Este acercamiento permite que un administrador de la red incorpore manualmente una dirección del multicast de la capa del MAC en la tabla CAM del switch junto con una lista de puertos. Ahora, cuando el switch recibe los marcos del multicast que emparejan esta dirección, el flooding de estos bastidores se obliga solamente a esos puertos enumerados en la entrada de la tabla CAM. Este acercamiento trabajado inicialmente muy bien para los grupos algo estáticos del multicast, tales como todo el grupo de el router del OSPF, donde los miembros del grupo podrían ser configurados delante de tiempo y no eran probables cambiar. Desafortunadamente, el método manual de la configuración no se presta a los grupos dinámicos del multicast, al igual que el caso en el multicast del IP. Claramente, un cierto otro acercamiento era necesario obligar flooding del multicast en ambientes tradicionales del switch del LAN.

Hasta la fecha, dos métodos se han definido para tratar este problema:

- IGMP Snooping
- Cisco Group Management Protocol (CGMP)

De estos dos métodos, solamente el primeros dos han visto el despliegue wide-scale y se discuten detalladamente en las secciones siguientes. GARP de IEEE, por otra parte, es radicalmente un nuevo acercamiento que requerirá cambios al hardware y al software de la extremo-estacion al instrumento.

5.4.1 IGMP Snooping.

El método más obvio para obligar el flooding del tráfico del multicast en switches LAN es IGMP Snooping. Apenas mientras que su nombre implica, IGMP Snooping requiere el switch del LAN al snoop en la conversación de IGMP entre el host y la router . Cuando el switch oye un informe de IGMP de un host para un grupo particular del multicast, el switch agrega el número de acceso del host a la entrada asociada de la tabla CAM del multicast. Cuando el switch oye un mensaje del grupo de la licencia de IGMP de un host, quita el puerto del host de la entrada de la tabla CAM.

En la superficie, esto se parece como una solución simple poner en práctica. Sin embargo, dependiendo de la arquitectura del switch, poner IGMP en ejecucion Snooping puede ser difícil de lograr sin seriamente degradar el funcionamiento del switch.

Las secciones que siguen exploran a mecánicos implicados en IGMP eficiente que pone en ejecucion Snooping junto con el impacto potencial del funcionamiento que tiene en los switches de la capa 2 que carecen el hardware especial para asistir con el proceso de IGMP Snooping. Después, varios panoramas especiales por Ejemplo envi'an -solamente fuentes y la detección y la dirección automáticas de routers por el software de IGMP Snooping en el switch se exploran.

a. Uniendo un Grupo usando IGMP Snooping.

En el primer vistazo, usted puede ser que cuente con que los lugares adicionales de la carga IGMP Snooping en un switch del LAN sean mínimos. ¿Después de todo, IGMP fue diseñado reducir al mínimo su impacto en la CPU del host y de el router así como en la anchura de banda de la red, la derecha? Sin embargo, esta declaración verdadera no se aplica necesariamente a los dispositivos de la capa 2 tales como switches LAN. La razón que no aplica debe llegar a ser evidente pronto.

La Figura 5.2 muestra un ejemplo de un switch simple de la capa 2-only (es decir, un hardware especial de la capa que carece 3 a la ayuda con IGMP Snooping) que esté haciendo IGMP Snooping.

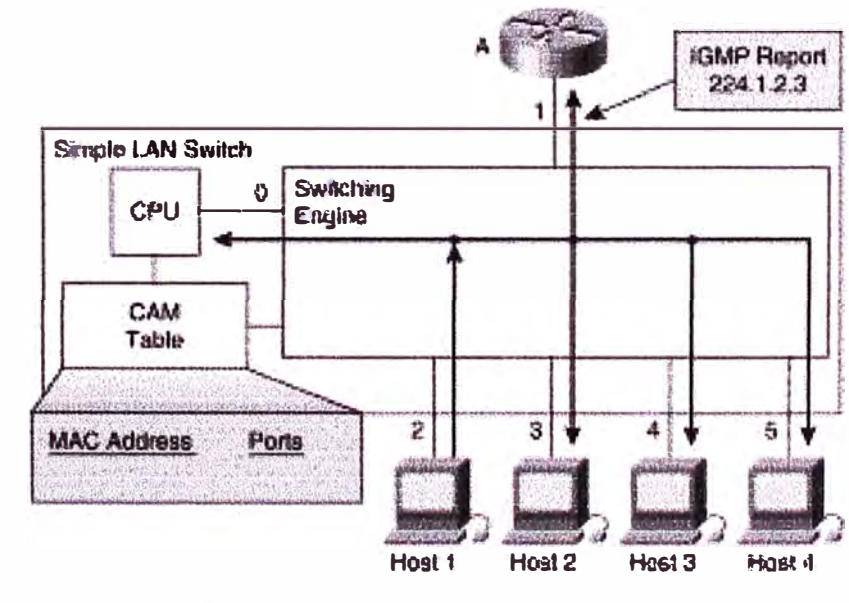


Fig. 5.2 Joining un Grupo con IGMP Snooping - Step 1

Hechemos una ojeada qué sucede típicamente en el switch cuando un par de hosts ensambla un grupo del multicast y el estado se instala en la tabla CAM del switch para obligar flooding del multicast.

1. Reciba los deseos 1 de ensamblar el grupo 224.1.2.3 del multicast y, por lo tanto, multicasts un informe no solicitado de la calidad de miembro de IGMP al grupo con una dirección de destinación del MAC de 0x0100.5E01.0203. Porque no hay inicialmente entradas en la tabla CAM para este MAC address del multicast (véase La Figura 5.2), el informe se inunda a todos los puertos en el switch (puerto interno incluyendo conectado con la CPU del switch).
2. Cuando la CPU recibe el multicast del informe de IGMP de Host 1, la CPU utiliza la información en el informe de IGMP para instalar una entrada de la tabla CAM según lo demostrado en la tabla 5.1 que incluye los números de acceso del host 1, del router , y del CPU interno del switch.

Tabla N° 5.1 CAM Tabla Entry After Host 1 Joins

Destination Address	Ports
01-00-5E-01-02-03	0, 1, 2

Como resultado de esta entrada de la tabla CAM, cualquier marco del multicast del futuro tratado al MAC address 0x0100.5E01.0203 del multicast será obligado a los puertos 0, 1, y 2 y no inundado a los otros puertos en el switch. (la CPU del switch debe continuar recibiendo estos marcos porque debe mirar para otros mensajes de IGMP tratados a este MAC address.)

Ahora asumamos que el host 4 desea ensamblar al grupo y envía un informe no solicitado de IGMP para el mismo grupo. La Figura 5.2 ahora muestra el host 4 que ensambla al grupo enviando un informe de la calidad de miembro de IGMP para el grupo 224.1.2.3. El switch transmite al informe de la calidad de miembro de IGMP los puertos externos 1 y 2 basados en la entrada de la tabla CAM demostrada previamente en la tabla 5.1. (esta misma entrada de la tabla CAM se puede ahora también considerar en La Figura 5.3).

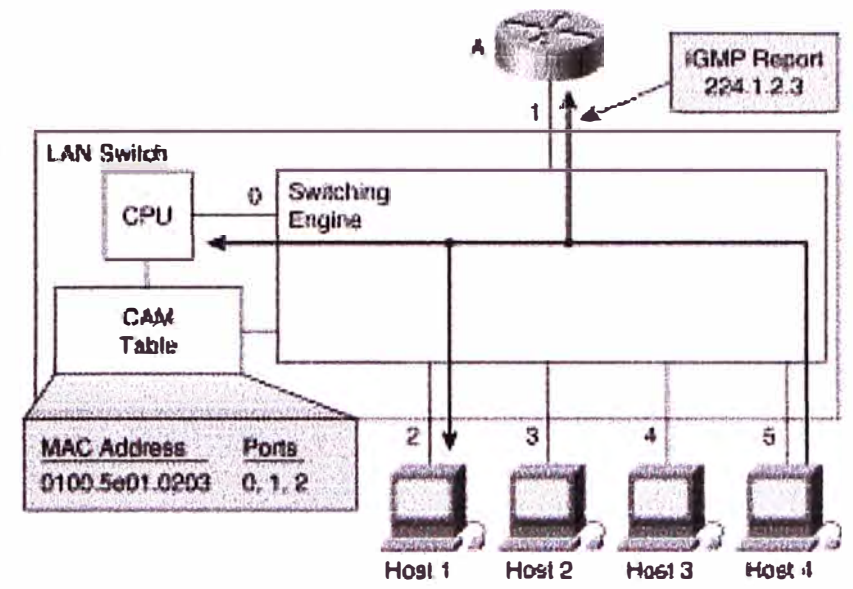


Fig. 5.3 Joining un Grupo con IGMP Snooping - Step 2

Porque la CPU del switch también recibió el informe de la calidad de miembro de IGMP, agrega el puerto en el cual el informe fue oído (en este caso, vire 5) hacia el lado de babor a la entrada de la tabla CAM para el MAC address 0x0100.5E01.0203. Esto da lugar a la tabla CAM demostrada en la tabla 5.2.

Tabla N° 5.2 Entrada de la Tabla CAM despues de Host 4 Joins

Destination Address	Ports
01-00-5E-01-02-03	0, 1, 2, 5

A este punto, se obligará a cualquier tráfico del multicast enviado con un MAC address de la destinación de 0x0100.5E01.0203 (que corresponda al grupo 224.1.2.3 del multicast) que reciba solamente 1, el host 4, la router , y la CPU interna. Se parecería ciertamente que éste toma el cuidado de los pasos necesarios para cubrir el proceso del unido en IGMP Snooping. Sin embargo, un problema potencialmente serio con los switches que utilizan esta clase de mecanismo de la capa 2 only se explica en la sección siguiente.

b. Impacto de Funcionamiento del IGMP Snooping.

Recuerde que la entrada de la tabla CAM demostrada en la tabla 5.2 incluyó el puerto 0 en su lista portuaria. Este puerto es incluido de modo que el motor de la conmutación continuara pasando los mensajes de IGMP tratados a este grupo a la CPU interna del switch. (recuerde que los informes de la calidad de miembro de IGMP son multicast al grupo del multicast de la blanco.) Si esto no fuera hecha, la CPU no habría oído el informe de IGMP del host 4 cuando intentó ensamblar al grupo. Por lo tanto, para continuar recibiendo cualquier informe del futuro IGMP, el motor de la conmutación fue mandado para enviar todos los marcos tratados al MAC address 0x0100.5E01.0203 al interno CPU. A este punto, usted comienza a funcionar en problemas de funcionamiento al intentar poner IGMP en ejecucion Snooping de este modo.

La Figura 5.4 ahora representa el mismo switch del LAN del Ejemplo anterior a menos que ese host 1 ahora sea multicasting a la corriente video del MPEG de 1.5 Mbps al grupo de blanco, 224.1.2.3. Esto significa que el MAC address del multicast de los bastidores video que son enviados por Host 1 es también 0x0100.5E01.0203. ¡Por lo tanto, la única manera para que la CPU intercepte cualquier mensaje de IGMP está para que intercepte todo el tráfico del multicast tratado al grupo!

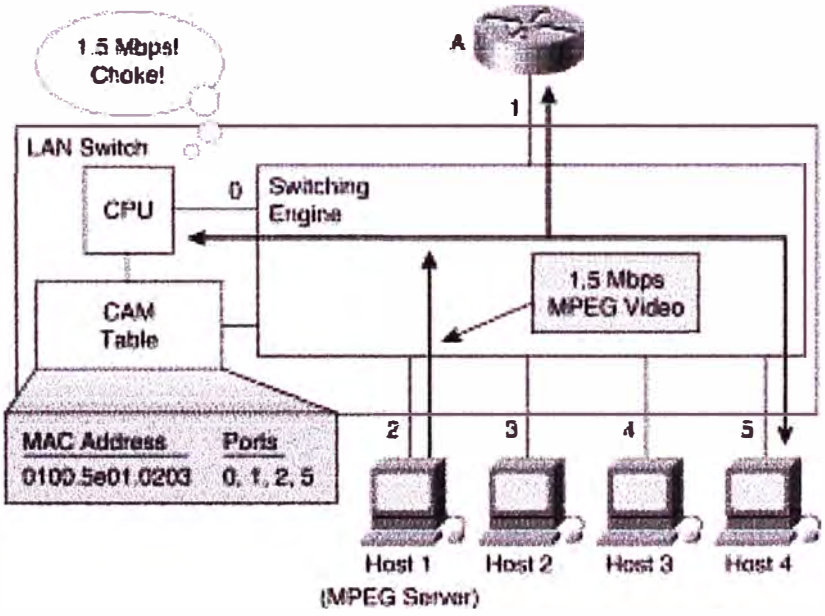


Fig. 5.4 Overloading del CPU de Switch con Trafico Multicast

Obviamente, la cantidad de trabajo del tener la CPU examina cada marco del multicast que pasa a través del switch apenas para encontrar un paquete ocasional de IGMP dará lugar generalmente a una reducción drástica en funcionamiento total del switch y, en algunos

casos, a una falta catastrófica del switch. Desafortunadamente, muchos de barato de hoy, los switches LAN de la capa 2-only que ponen IGMP en ejecucion Snooping sufren de este problema. El switch puede realizar la multa justa en un ambiente limitado de la versión parcial de programa pero puede comenzar a fallar cuando el comprador lo pone en un ambiente de la producción. En algunos casos, esta falta toma la forma de drops en el multicast y el tráfico del unicast atraviesa el switch. En otros casos, el motor de la conmutación continúa remitiendo el multicast y el tráfico del unicast sin ningunas drops, aunque la CPU interna comienza a caer los paquetes porque no puede continuar con la corriente del tráfico entrante. Estas drops en la entrada del resultado interno de la CPU en los paquetes faltados de IGMP, que pueden afectar seriamente ensamblan y dejan estados latentes.

Para evitar este problema, es necesario reajustar el motor de la conmutación en estos switches LAN para utilizar las tablas nuevas de ASICs y CAM que pueden parecer más profundas en el marco y examinar la información de la capa 3 antes de tomar una decisión de la conmutación. Dado un switch diseñó en esta manera, la tabla CAM puede ser programado para remitir solamente los marcos que contenían mensajes de IGMP a la CPU para procesar.

La Figura 5.5 muestra una versión simplificada del switch del LAN después de que su motor de switcheo se haya reajustado con el nuevo ASICs que es la capa 3 enterada.

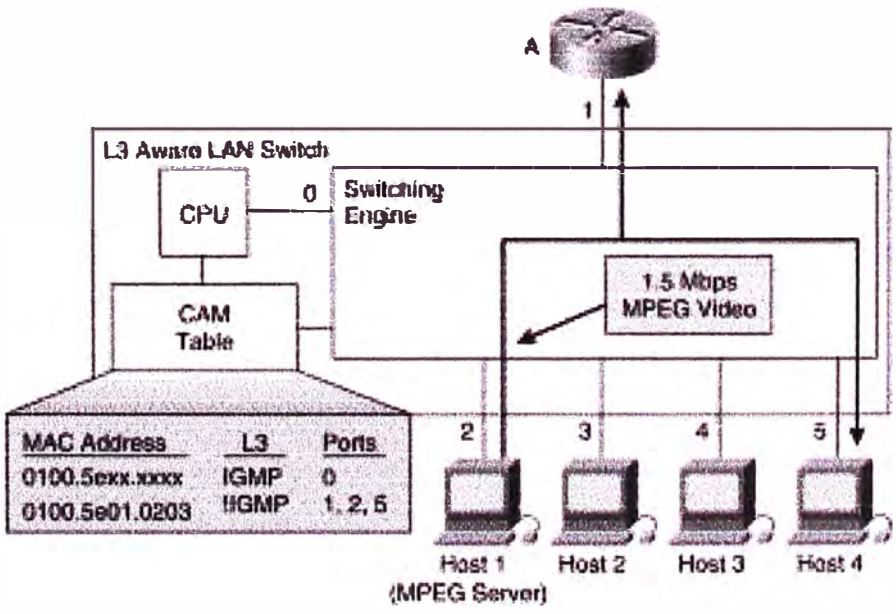


Fig. 5.5 Arquitectura Switching

Porque el switch ahora es la capa 3 enterada, cada entrada en la tabla CAM demostrada en la Figura 5.5 se puede cargar con la información adicional de la capa 3 que modifica más lejos el comportamiento del motor de la conmutación. Como usted puede ver, el vídeo del MPEG 1.5-Mbps es no más largo interrumpiendo la CPU pues atraviesa el switch. El índice del tráfico que es enviado a la CPU ahora se reduce solamente a algunos marcos del tráfico de IGMP por el segundo, que la CPU puede manejar absolutamente fácilmente.

Entendamos cómo este proceso trabaja, examinan las dos entradas que la CPU ha cargado en la tabla CAM demostrada en la Figura 5.5 más detalladamente:

- La primera entrada dice el motor de la conmutación enviar los paquetes de IGMP solamente a la CPU del switch.
- La segunda entrada dice el motor de la conmutación enviar los marcos tratados al MAC address del multicast 0x0100.5E01.0203 que no son paquetes de IGMP (!IGMP = "no IGMP") a el router y a los dos hosts que han ensamblado a grupo.

La primera entrada significa que la CPU está interceptando con eficacia todos los paquetes de IGMP y no está permitiendo que el motor del switch los remitiera a los otros puertos en el switch. Este acercamiento permite que la CPU realice el proceso especial de los paquetes de IGMP necesarios y esté en el control completo de los paquetes de IGMP que necesitan ser enviados a los otros dispositivos conectados con el switch. (la razón de esto se convertirá en más adelante claro.)

El proceso que ocurre en el nuevo switch del LAN de la capa 3-aware cuando los hosts ensamblan a grupo es básicamente igual que el proceso en el Ejemplo simple del switch del LAN. La diferencia dominante es que ahora la entrada de la tabla CAM se ha cargado con la información suplemental de la capa 3 así que el motor de la conmutación no transmite a datos del multicast la CPU. (realmente estamos en excedente -- la simplificaión del proceso aquí, pero de esta descripción debe permitirle entender los mecanismos básicos implicados.)

Continuemos la discusión de IGMP Snooping, si se asume otra vez que los hosts 1 y 4 son miembros del grupo según lo demostrado en La Figura 5.5. (el resto de esta sección en IGMP Snooping asume que el switch hace uso esta clase de arquitectura de la capa 3)

c. Salida de un Grupo con IGMPS Snooping.

Ahora, asuma que el host 1 sale del grupo. La salida del host 1 hace la secuencia de evento siguiente ocurrir:

1. Host 1 señala que está dejando a grupo por multicasting un mensaje del grupo de la licencia a todo el grupo del multicast de las router s, 224.0.0.2 (MAC address 0x0100.5E00.0002) según lo demostrado en La Figura 5.6.

   La primera entrada de la tabla CAM hace este mensaje ser interceptada por el CPU del switch y no ser remitida a cualquier otro puerto.

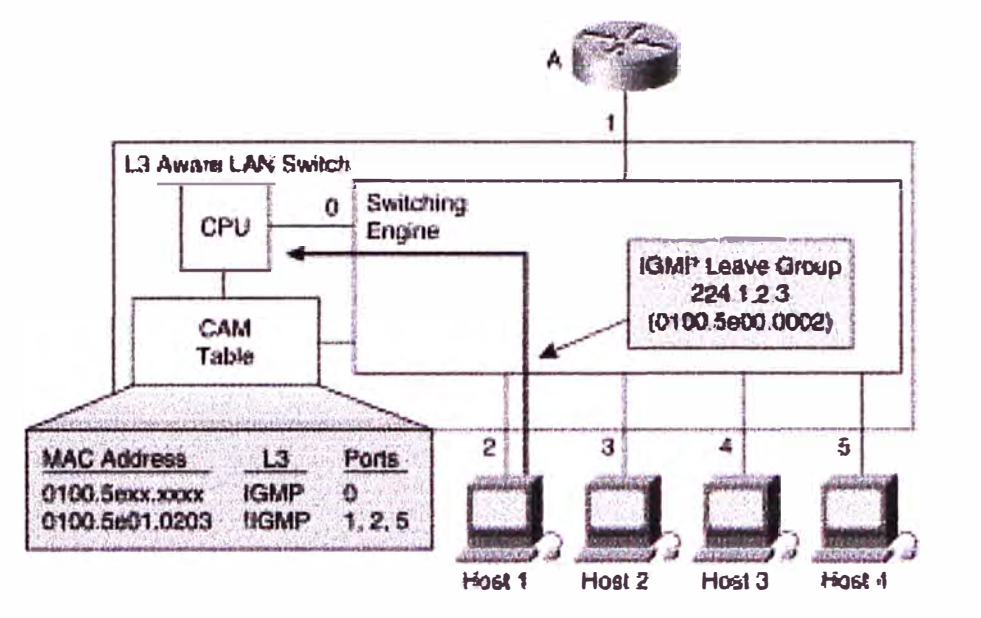


Fig. 5.6 IGMP Snooping: Leaving a Group - Step 1

2. El CPU en el switch responde al mensaje Leave Group Message una pregunta general de IGMP se retira el puerto 2 (véase La Figura 5.7) para ver si hay algunos otros hosts que sean miembros de este grupo en el puerto. (esto podría ocurrir cuando es múltiple los hosts está conectada con el puerto del switch vía un cubo.)

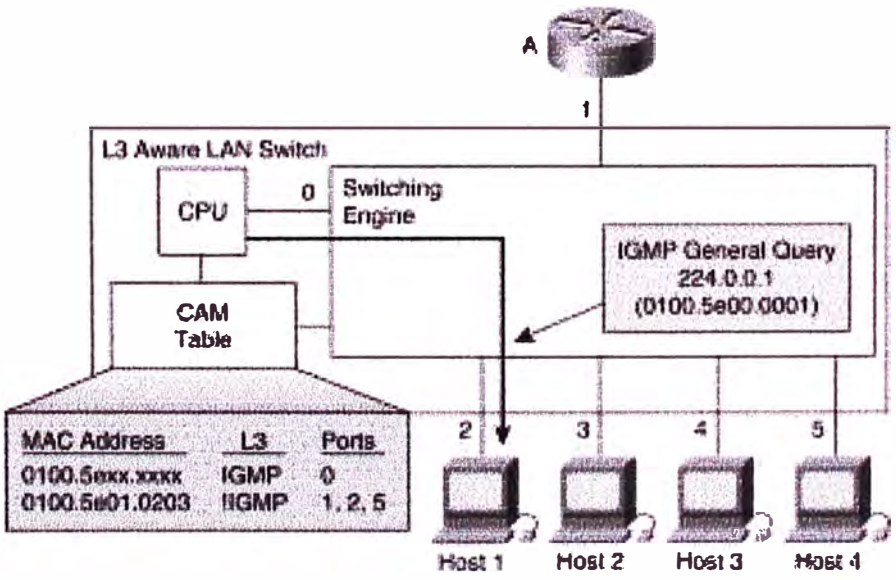


Fig. 5.7 IGMP Snooping: Leaving a Group - Step 2

3. Si otro informe de IGMP se recibe de un host conectado con el puerto 2, entonces el CPU desecha el mensaje original reservado del grupo de la licencia del host 1. Si, por otra parte, no se recibe ningún informe de IGMP en este puerto, (que es el caso), después las cancelaciones de la CPU el puerto de la entrada de la tabla CAM (véase la entrada de la tabla CAM que resulta en La Figura 5.8). Porque otros puertos del nonrouter todavía están en la entrada de la tabla CAM, no se envía ningún mensaje al router .

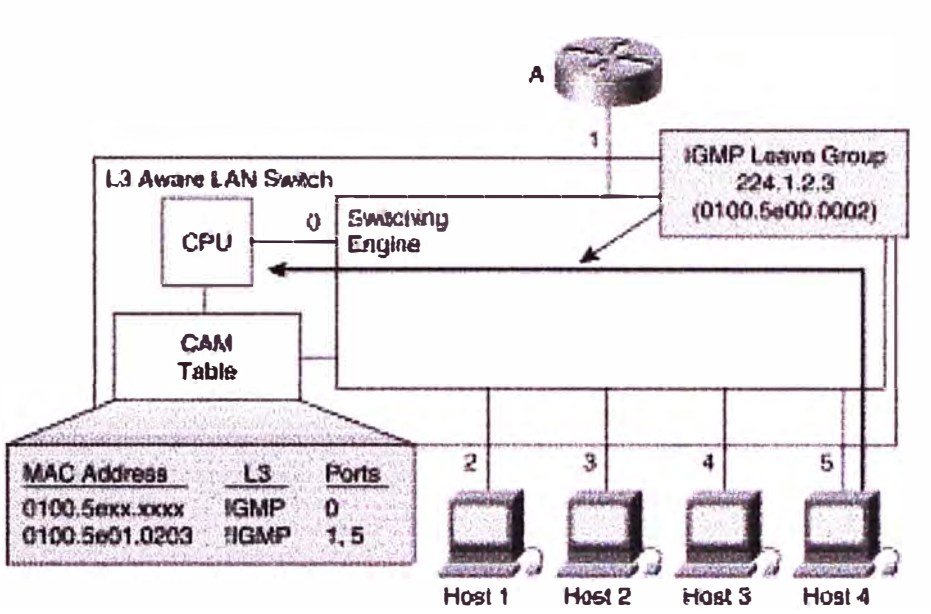


Fig. 5.8 IGMP Snooping: Leaving the Group - Step 3

4. Ahora, déjenos asumen que el host 4 sale del grupo y envía un mensaje del grupo de la licencia de IGMP. De nuevo, el mensaje del grupo de la licencia es interceptado por la CPU del switch, como demostrado en La Figura 5.8.

5. El CPU responde al leave Group Message enviando otra pregunta general el puerto 5 (véase la Figura 5.9) para considerar si hay algunos otros hosts que sean miembros de este grupo en el puerto.

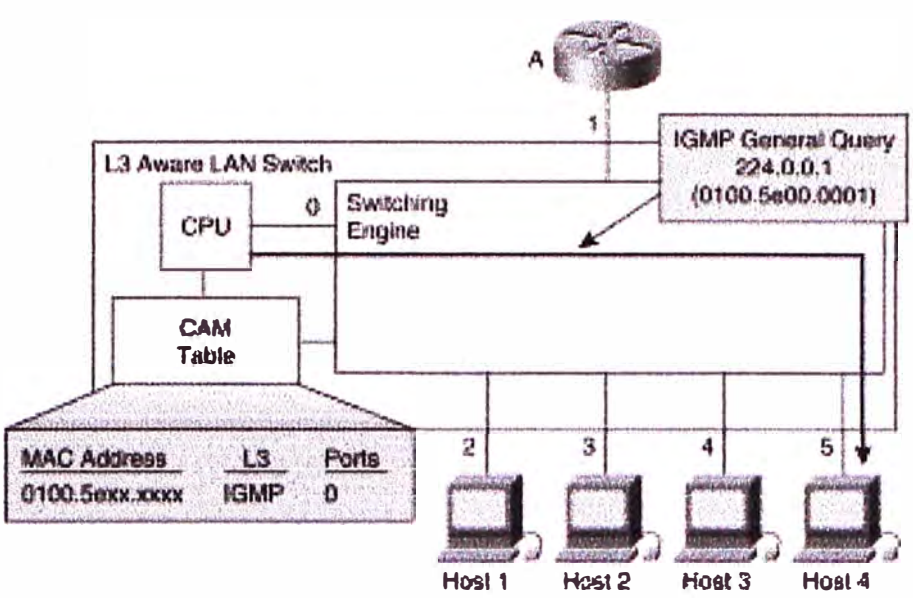


Fig. 5.9 IGMP Snooping: Leaving the Group - Step 4

6. Porque no hay otros hosts en este puerto en el Ejemplo , no se recibe ningún informe de IGMP para este grupo y las cancelaciones del switch este puerto de la entrada de la tabla CAM. Porque este puerto era el puerto pasado del nonrouter para la entrada de la tabla CAM para 0x0100.5E01.0203, la CPU del switch suprime Las entradas de la tabla CAM para este grupo y transmiten al mensaje del grupo de la licencia de IGMP el router para el proceso normal. (Véase la Figura 5.10.)

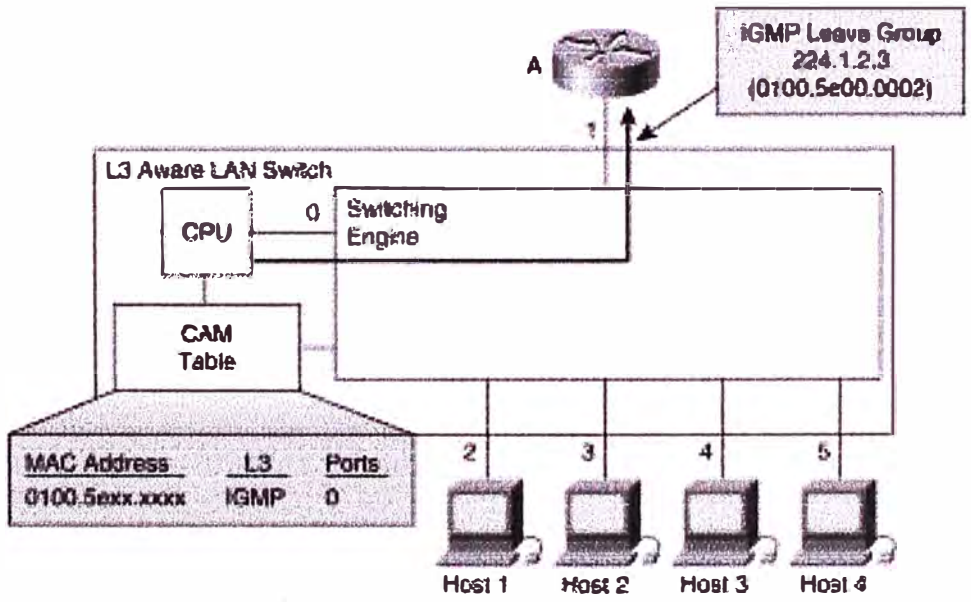


Fig. 5.10 IGMP Snooping: Leaving the Group - Step 5

d. Manteniendo Grupos con IGMP Snooping.

Obviamente, el proceso de la licencia descrito en la sección precedente asume que todos los hosts IGMPv2 envían siempre un mensaje del grupo de la licencia cuando salen del grupo. Desafortunadamente, sin embargo, el RFC 2236 dice que un host puede enviar siempre un mensaje de la licencia del grupo (no deba, como el RFC debe haber dicho quizá) cuando sale del grupo. Debido a este descuido de menor importancia, usted no puede contar siempre en la recepción de un mensaje del grupo de la licencia cuando un host se va. Además, el host puede funcionar IGMPv1 (que no utilice mensajes de la licencia del grupo) o el mensaje del grupo de la licencia se puede perder debido a la congestión en el switch. Así, en un panorama a lo peor, usted debe caerse de nuevo al procedimiento de mantenimiento del estado de group/port, usando el mecanismo general de Query/Report para detectar cuando un host ha salido del grupo (o debido a un mensaje perdido del grupo de la licencia o porque un host IGMPv1 apenas sale del grupo reservado).

Asuma que los hosts 1 y 4 han ensamblado otra vez previamente el grupo 224.1.2.3 del multicast, que da lugar a las entradas de la tabla CAM demostradas en la Figura 5.11 que representa el procedimiento de mantenimiento del estado de la calidad de miembro de group/port en la acción.

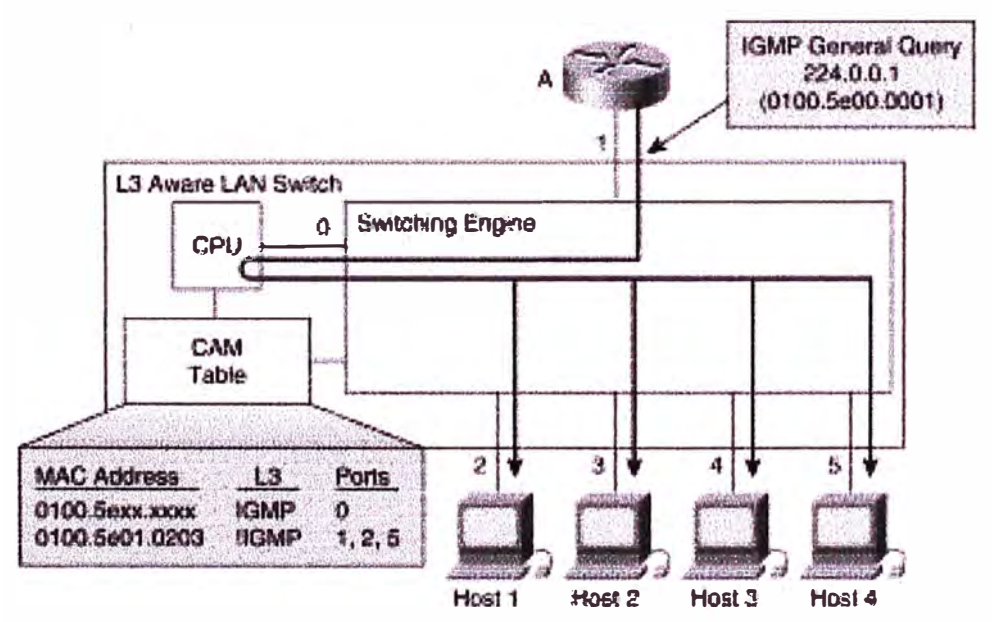


Fig. 5.11 Maintaining a Group with IGMP Snooping - Step 1

1. El router multicasts A periódicamente una pregunta general a todo el grupo de los hosts, 224.0.0.1 (MAC address 0x0100.5E00.0001). La CPU del switch intercepta la pregunta general y la retransmite fuera de todos los puertos en el switch. (Véase La Figura 5.11.)
2. Cada host que sea un miembro del grupo (en este caso, hosts 1 y 4) envía un informe de IGMP en respuesta a la pregunta general. (Véase La Figura 5.12.) Note que porque la CPU del switch está interceptando todos los mensajes de IGMP, los hosts no se oyen informe de IGMP. Esto elimina con eficacia el mecanismo de la supresión del informe del host, forzando cada uno para enviar un informe de IGMP. Esto es necesario de modo que la CPU del switch reciba un informe de IGMP sobre cada puerto donde hay un miembro del grupo así que mantendrá esos puertos en la lista.

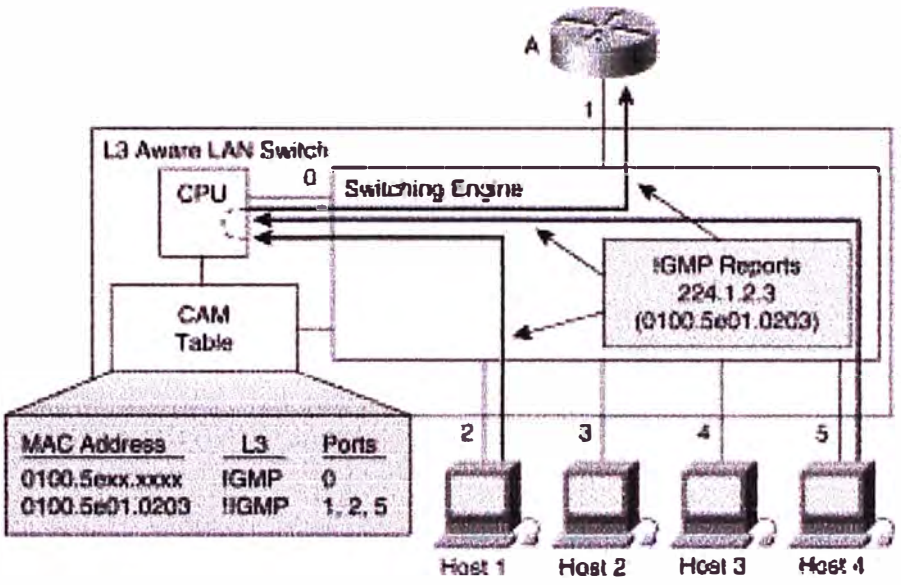


Fig. 5.12 Maintaining a Group with IGMP Snooping - Step 2

3. Para mantener el estado de la calidad de miembro de grupo de IGMP activo el router, el switch LAN debe remitir a cualquiera uno o más (preferiblemente solamente uno) de los informes de IGMP hasta el router A.

5.4.2 Protocolo de Administración de Grupos Cisco.

A principios de 1996, Dino Farinacci y Alex Tweedly del Cisco Systems reconocieron la necesidad de una solución alternativa al problema del flooding del multicast (con excepción de IGMP Snooping). El trabajo era en curso en el diseño de la nueva capa 3-aware ASICs para el catalizador del Cisco los switches de 5000 series que permitirían que

IGMP eficiente Snooping fuera puesto en ejecucion. Sin embargo, este ASICs no sería pronto para usar en el switch del catalizador 5000 por una cierta hora. Además, el uso de estos ASICs en los switches catalizador del bajo-extremo no sería económico, y por lo tanto una cierta otra solución era necesaria obligar flooding del multicast en estos switches baratos.

Junto, Dino y Alex diseñaron un nuevo, ligero protocolo que funcionaría en el router y la serie del catalizador de switches y permitiría que la información de la calidad de miembro de grupo de la capa 2 fuera comunicada de el router al switch. Esta información se podía entonces utilizar al estado de la calidad de miembro del multicast del instantiate en las entradas de la tabla CAM para obligar tráfico del multicast a los puertos con los miembros del grupo. Este nuevo protocolo fue llamado el protocolo de administracion de grupo Cisco (CGMP) y ahora se apoya en todas los router Cisco y la mayoría de los switches LAN.

a. Mensajes CGMP.

Los mensajes de CGMP se componen de un tipo campo del código seguido por una lista de los tuples de la dirección de la dirección de destinación del grupo (GDA) y de la fuente de Unicast (los E.E.U.U.) que cada uno identifica a un host y a grupo a que el host acaba de ensamblar o a la izquierda.

Todos los mensajes de CGMP son multicast de la capa del MAC al bien conocido de CGMP del multicast todos los CGMP-enabled switches MAC address 0x0100.0cdd.dddd. escuchan este MAC address bien conocido del multicast para recibir mensajes de CGMP. Usar un MAC address del multicast para comunicar mensajes de CGMP tiene la ventaja agregada que son inundados fuera de todos los puertos del switch por el defecto, si el switch es un switch de CGMP-enabled o no. Esto permite que los mensajes de CGMP viajen a través de todos los acoplamientos del interswitch a través del dominio que cambia de la capa 2 enteros y alcancen todos los switches de CGMP-enabled, incluso si hay switches de non-CGMP en el centro la red.

Porque los switches LAN funcionan en la capa 2 y por lo tanto entienden solamente direcciones del MAC, los GDA y los campos ambos de los E.E.U.U. contienen direcciones del MAC de 48-bit IEEE. El campo de GDA contiene la dirección del grupo del IP multicast traducida a su equivalente del MAC address (por Ejemplo , el grupo 239.255.1.2 del IP multicast aparecería como 0x0100.5e7f.0102), y el campo de los

E.E.U.U. contiene la dirección del unicast del nivel del MAC del host que envió el mensaje original del informe de IGMP.

La información del MAC address del host en el campo de los E.E.U.U. de un mensaje de CGMP es utilizada por el switch de CGMP para mirar para arriba el número de acceso asociado al host. Usando esta información portuaria, el switch de CGMP agrega o quita este puerto to/from que la entrada de la tabla CAM se asoció al MAC address del multicast en el campo de GDA.

La tabla 5.3 enumera los varios mensajes de CGMP. Los primeros dos mensajes permiten que el router informe a los switches de CGMP cuando un host ensambla o sale a grupo.

Además de poder informar los CGMP cambian cuando un host ensambla o sale de un grupo del multicast, el router utilizan mensajes de CGMP para decir el switch realizar otras funciones especiales de CGMP. Los valores especiales en los campos de GDA y de los E.E.U.U., demostrados en la tabla 5.3, comunican estas funciones especiales.

Tabla N° 5.3 Mensajes CGMP

GDA	USA	Join/ Leave	Meaning
Mcst MAC	Client MAC	Join	Add port to group
Mcst MAC	Client MAC	Leave	Delete port from group
00000000	Router MAC	Join	Assign router port
00000000	Router MAC	Leave	Deassign router port
Mcst MAC	00000000	Leave	Delete group
00000000	00000000	Leave	Delete all groups

Los terceros y cuartos mensajes en la tabla 5.3, el puerto del router de Assign/Deassign, (significado por un campo cero de GDA y un campo distinto a cero de los E.E.U.U.) son

particularmente importantes. Estos mensajes de CGMP permiten que el router informe a los switches de CGMP que la estación que MAC address aparece en el campo de los E.E.U.U. es una router y o al sistema (vía un mensaje del unido) o claro (vía un mensaje de la licencia) el puerto asociado como puerto de la router . El switch del LAN necesita saber qué puertos tienen routers conectadas. Debe incluir estos puertos en cada entrada de la tabla CAM del multicast se cree que de modo que los routers reciban todo el tráfico multicast.

Los dos pasados dejan mensajes en la tabla 5.3, suprimen a grupo y suprimen a todos los grupos, son utilizados para las funciones especiales del mantenimiento por la router . Por Ejemplo , el comando del interfaz del router Cisco.

clear ip cgmp <interface>

Este comando hace que el router envia la cancelación a todos los grupos mensaje al switch, que quita todas las entradas de la tabla CAM del multicast del switch. El mecanismo normal de la pregunta de IGMP hace el switch volver a aprender el estado de la calidad de miembro de grupo del multicast y al repopulate su tabla CAM del multicast con la operación normal de CGMP.

b. Union de un Grupo con CGMP.

El concepto básico de CGMP se muestra en La Figura 5.13. Cuando un host ensambla un grupo del multicast (según lo mostrado en la parte A de la Figura 5.13), él los multicasts un mensaje no solicitado del informe de la calidad de miembro de IGMP al grupo de blanco (224.1.2.3, en este Ejemplo). El informe de IGMP se pasa a través del switch a el router para el proceso normal de IGMP. El router (que debe tener CGMP permitido en este interfaz) recibe este informe de IGMP y, además de setting-up su estado interno de IGMP para el grupo, traduce el informe de IGMP (referido a veces libremente mientras que un IGMP ensambla) un mensaje CGMP Join.

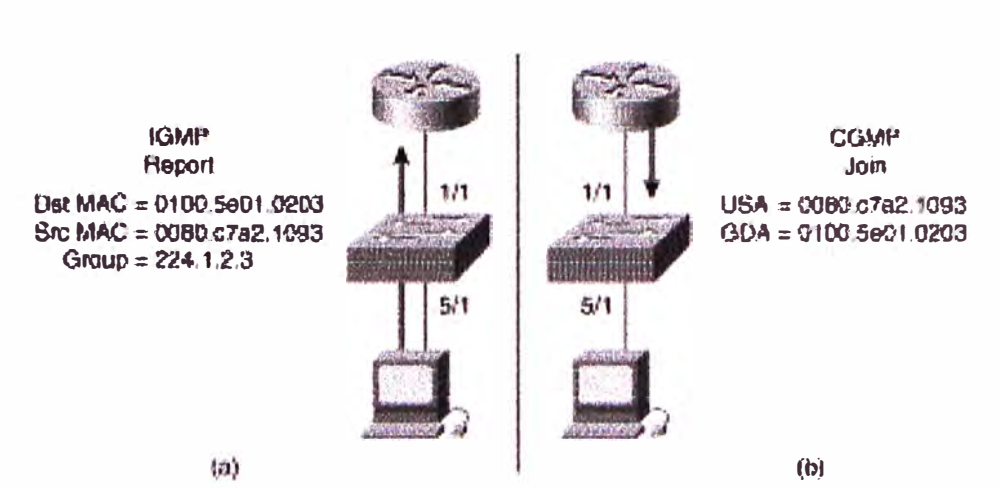


Fig. 5.13 Operacion Basica del CGMP

El router logra la traducción del informe de IGMP a CGMP ensambla en los pasos del siguiente:

1. Copy el MAC address de la destinación, 0x0100.5e01.0203, (que corresponde al grupo 224.1.2.3 del multicast del IP) del mensaje del informe de IGMP en el campo de GDA del mensaje CGMP Join.
2. La copy 2 el MAC address de la fuente, 0x0080.c7a2.1093, (que es el MAC address del unicast del host que está ensamblando a grupo) del informe de IGMP en el campo de los E.E.U.U. del CGMP ensambla. Ahora que los CGMP ensamblan se ha construido el mensaje, el router envía el mensaje al switch de CGMP-enabled (parte B de la Figura 5.13) vía el MAC address bien conocido del multicast de 0x0100.0cdd.dddd CGMP.

c. Manteniendo Grupos con CGMP.

El estado de la calidad de miembro de grupo que mantiene en el switch es mucho más fácil con CGMP que con IGMP Snooping. Los puertos individuales se quitan de la entrada de la tabla CAM solamente como resultado de recibir un mensaje del puerto de la cancelación de la router . Se reajusta el contador de tiempo de la expiración de la entrada de la tabla CAM cada vez que un CGMP ensambla el mensaje se recibe para el grupo, que ocurre el router envió cada vez la pregunta general. Sin embargo, hay otras veces en que el switch suprime la entrada de la tabla CAM y el estado de la calidad de miembro de grupo debe ser vuelto a aprender. Las entradas de la tabla CAM del multicast se suprimen en las circunstancias siguientes:

- Siempre que el VLAN que atraviesa topología del árbol cambie. (este cambio puede ocurrir cuando un puerto en las transiciones de VLAN del estado que aprende al estado de la expedición.)
- Cuando el router envía a grupo de la cancelación o suprima todo el mensaje del grupo.
- Cuando una línea tarjeta en el switch es removed/inserted.

Siempre que se supriman las entradas de la tabla CAM del multicast, el switch vuelve a aprender automáticamente el group/port estado de la calidad de miembro a través del mecanismo general normal de la pregunta de IGMP. Durante este período que vuelve a aprender, los hosts envían informes de IGMP en respuesta a preguntas generales de IGMP de la router . Estos informes, alternadamente, se traducen a CGMP ensamblan por la router , que causa a switch al repopulate las entradas en su tabla CAM. (las tomas de proceso que vuelven a aprender enteras a partir de 1 a 1.5 intervalos de la pregunta de IGMP a completar.)

d. Salida de un Grupo con CGMP.

Cuando un host IGMPv2 sale de un grupo, él normalmente los multicasts un mensaje Leave Group Message a todo el 224.0.0.2) grupos del multicast de el router (. Cuando CGMP se permite en el router y el switch del LAN, el router puede traducir simplemente este mensaje del grupo de la licencia a un mensaje de la licencia de CGMP usando el método de la traducción. Como IGMP Snooping, este mecanismo de la licencia de CGMP depende del host que envía siempre un mensaje del grupo de la licencia IGMPv2 para accionar este proceso. Desafortunadamente, los hosts IGMPv2 no se requieren enviar siempre un mensaje del grupo de la licencia de IGMP cuando salen del grupo. Además, hay muchos inmóviles de hosts (Windows 95 incluyendo) ese solamente funcionamiento IGMPv1 y por lo tanto no envía mensajes Leave Group Message.

e. Procesando Salida Local con CGMP.

Versiones más últimas de las puestas en práctica de CGMP en los switches catalizador del Cisco tienen la capacidad para hacer la licencia IGMPv2 que procesa localmente en el switch sin conseguir el router implicada.

Sabemos que el IGMPv2 requiere todos los mensajes (del grupo de la licencia ser multicast a todo el 224.0.0.2) grupos del multicast de los routers (y no al grupo del multicast se está dejando que. Esto abre la puerta en tener el switch de CGMP-enabled hace a algo del

grupo de la licencia que se procesa. Templando adentro a los 224.0.0.2 grupos del multicast en el nivel del MAC (MAC address 0x0100.5e00.0002 del multicast), la CPU en el switch del LAN puede recibir y procesar estos mensajes del Leave Group Message sin tener que interceptar todos los datos multicast trafican.

Sigue habiendo preocupaciones de proceso Local Leave en sí mismo para cerciorarse que ningunos otros oyentes en el segment/port después de que se haya recibido un mensaje de la licencia del grupo. Si sigue habiendo un miembro, la canceladura del puerto está cancelada porque el flujo a ese puerto debe continuar. Si ningunos miembros responden en ese puerto, los cheques del switch entonces si algunos miembros están en otros puertos del switch. Si encuentran a un miembro, nada sucede. Si existen ningunos otros miembros, sin embargo, el switch envía a grupo de la licencia de IGMP que el mensaje a el routers ourced del switch. El router entonces pasa con su proceso a cerciorarse de ningunos otros miembros existir en el LAN.

La Figura 5.14 muestra a CGMP la licencia local que procesa en un switch cuando los hosts múltiples están conectados con el puerto del switch vía cubos compartidos de los medios.

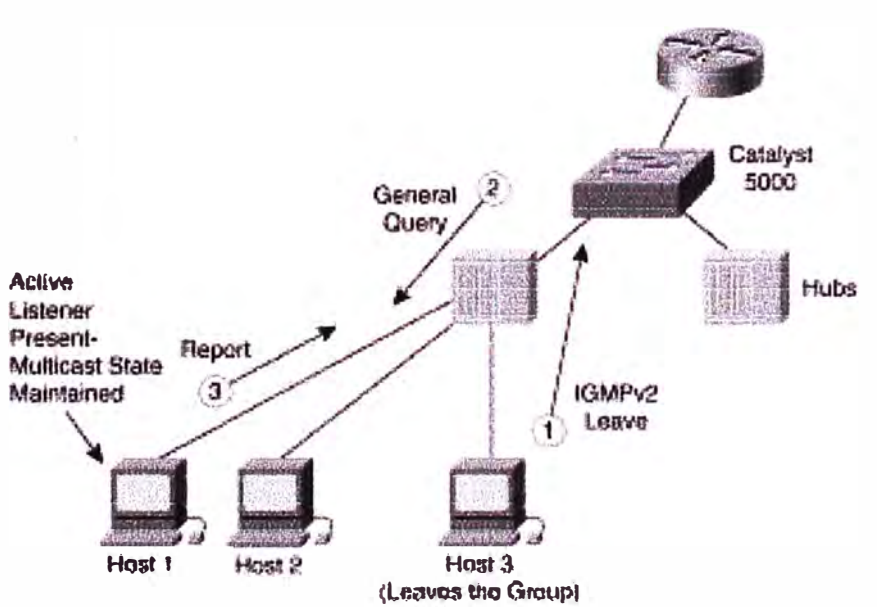


Fig. 5.14 CGMP Local Leaving Processing

f. Impacto de Funcionamiento con CGMP.

El impacto del funcionamiento de CGMP que pone en ejecucion en un switch es muy bajo comparado al impacto de IGMP Snooping. La razón es que el switch tiene que recibir y procesar solamente marcos low-rate de CGMP de la router , en comparación con la recepción y el proceso de todos los marcos del multicast para IGMP Snooping. Por lo tanto, CGMP se puede poner en ejecucion en incluso los switches baratos del LAN, tales como los switches de la serie del Cisco 1900 y 2800, sin la necesidad de ASICs especial que conduciría encima del coste del switch.

El impacto del funcionamiento de CGMP en los routers es también absolutamente bajo. En la mayoría de los casos, los gastos indirectos adicionales de la CPU de CGMP en el routers on demasiado pequeños medir y no necesitan ser una preocupación a los ingenieros de red.

g. CGMP y solo envia Fuentes.

Diferente de IGMP Snooping, los switches de CGMP no necesitan hacer el proceso especial para manejar eficientemente el caso donde una fuente del enviar-solamente existe sin ningunos otros miembros para el grupo en el LAN. En este caso, es deseable que el switch de CGMP obligue el tráfico de la fuente para no inundarla a el resto de hosts en el switch que no son miembros del grupo. El único puerto en el switch que debe recibir el tráfico de la fuente es el router

Teniendo un router que detecte cuando ocurre esto en un proceso relativamente simple. Por ejemplo , si una router está recibiendo tráfico del grupo del multicast de una fuente directamente conectada en un interfaz y no hay estado del grupo de la calidad de miembro de IGMP en este interfaz, entonces el routers abe que hay una fuente del enviar-solamente en el interfaz. En este caso, el router responde enviando un CGMP ensambla el mensaje para sí mismo de modo que el switch cree una nueva entrada de la tabla CAM del multicast que contenga solamente el puerto de el router en su lista portuaria. Si la fuente para el enviar de tráfico al grupo, el estado del multicast en el router mide el tiempo eventual hacia fuera. Esto hace el router enviar un mensaje del grupo de la cancelación al switch para quitar la entrada de la tabla CAM del multicast para el grupo.

h. Detección de Routers con CGMP.

Aunque los switches catalizador del Cisco tienen un comando de señalar manualmente un puerto como puerto de la router , este paso no es necesariò cuando una router Cisco está

conectada con el switch. CGMP asignan el router que los mensajes portuarios son enviados automáticamente al switch por cualquier router Cisco que tenga CGMP permitido en su interfaz. Este mensaje informa al switch que el puerto tiene una router unida y se debe incluir en todas las entradas nuevamente creadas de la tabla CAM multicast.

Los routers Cisco pueden también realizar esta función en el favor de otros routers del multicast de DVMRP que sean conectadas con el mismo interfaz usando el siguiente comando de interfase: **ip cgmp proxy**

Este comando manda al router Cisco para enviar un poder de CGMP asigna a router el mensaje portuario cada vez que recibe un paquete de la punta de prueba de DVMRP en este interfaz. El poder asigna el router que el mensaje portuario se envía con el MAC address de el router de DVMRP (tomada del paquete de la punta de prueba de DVMRP) en el campo de los E.E.U.U. del mensaje. (nota que este comando trabaja solamente para los routers del multicast que están funcionando el protocolo de DVMRP.) Sobre oír este mensaje del poder, el switch asigna el puerto en el cual el router de DVMRP está conectada como puerto de la router . Del router de información tiempos que automáticamente en el switch no son restaurado periódicamente. Por lo tanto, si va el router de DVMRP abajo, las puntas de prueba de DVMRP pararán el ser recibido por el router del Cisco, que causa la información de el router del poder al tiempo hacia fuera en el switch.

5.5 Resumen del capitulo.

Con la creciente popularidad del IP multicast, el viejo debate de frente a la conmutación de enrutamiento (que es la misma cosa como puente) se vuelve a plantear. Como IP multicast se convierte en una parte importante de las empresas la infraestructura de la red, la necesidad de limitar el tráfico multicast en grandes redes de conmutación LAN se convierte en importante. Porque con el control de la corriente de tráfico multicast exige hoy en día el Nivel 3 tecnologías, la necesidad de una mayor ruta en la red de campus se encuentra una vez más en aumento. Las grandes redes de campus plana, diseñado por miembros de la Sociedad de la Tierra Plana, están condenados a sufrir el aumento de los desechos de ancho de banda en los enlaces entre conmutadores. Cuando es una cuestión de ancho de banda, red de ingenieros y diseñadores que se encuentra su vivienda, red de campus diseños del pasado son insuficientes para satisfacer la demanda futura de más aplicaciones multimedia.

CAPITULO VI
CONFIGURACIÓN Y VERIFICACIÓN MULTICAST

6.1 Introducción.

El presente capitulo tiene como finalidad detallar los trabajos y pautas a tener en cuenta en la configuración del multicast sobre los equipos de redes, desde su habilitación inicial del multicast hasta los protocolos de enrutamiento que definen el manejo de la tabla de rutas en multicast. Dependiendo de la modalidad de trabajo del multicast debe ser habilitado los protocolos modo denso o esparcido. Ademas se hace un análisis detallado de interpretación del resultado delcomando "show". Un detalle muy importante es que en unicast es usual el IP de la fuente, sin embargo en multicast es todo lo contrario, en este caso lo que interesa es la IP destino que esté asociado a un grupo multicast, esto hace posible que los paquetes de envio tengan un destino comun en multicast. Finalmente se incluye un set de comando que permiten la verificación de funcionamiento en una red multicast, de ser posible este procedimiento sirve de ayuda para diagnosticar alguna falla de configuración que debe ser corregido oportunamente. En suma, debemos prestar vital importancia a los comandos que se describen en el desarrollo de este capítulo.

6.2 Habilitando PIM Sparse Mode y Sparse-Dense Mode

Los comandos necesarios para el despliegue de los modos PIM-SM y PIM-sparse-dense son los siguientes:

- El comando global **ip multicast-routing** habilita el soporte del IP multicast en un router.
- El commando de interface **ip pim sparse-mode** permite la habilitación de la operación PIM-SM en la interface seleccionada. El comando **ip pim sparse-dense-mode** permite a la interface del router para funcionar con el PIM-SM para grupos sparse-mode (conocido con los RPs) y en el dense mode para otros grupos.
- El comando global **ip pim send-rp-announce** {interface type} **scope** {ttl} group-**list** {acl} es editado en el router que desea ser un RP. Este router envía un mensaje auto-RP

a 224.0.1.39, que anuncia el router como candidato RP para los grupos en el rango descrito en la lista de acceso (access-list).

- El comando global **ip pim send-rp-discovery** {interface type} **scope** {ttl} (configura el router como un agente RP. Este recibe a la direccion 224.0.1.39 y envía un mensaje RP-to-grupo a 224.0.1.40. Otros routers PIM reciben la direccion 224.0.1.40 para descubrir automáticamente a la RP.
- El commando **ip pim spt-threshold** {rate | **infinity**} controla el paso de la shared distribution tree (distribución compartida de árboles) a la SPT en sparse mode. La palabra clave infinity significa que el cambio de modalidad jamás ocurrirá.

Nota:

El método recomendado para configurar una interface para la operación del PIM-SM es usar en comando de interface **ip pim sparse-dense-mode**. Este método permite auto RP, de arranque del router (BSR), o estaticamente definir los RPs que se utilizará con el menor esfuerzo de configuración.

Veamos los comandos mancionados en la Figura 6.1:

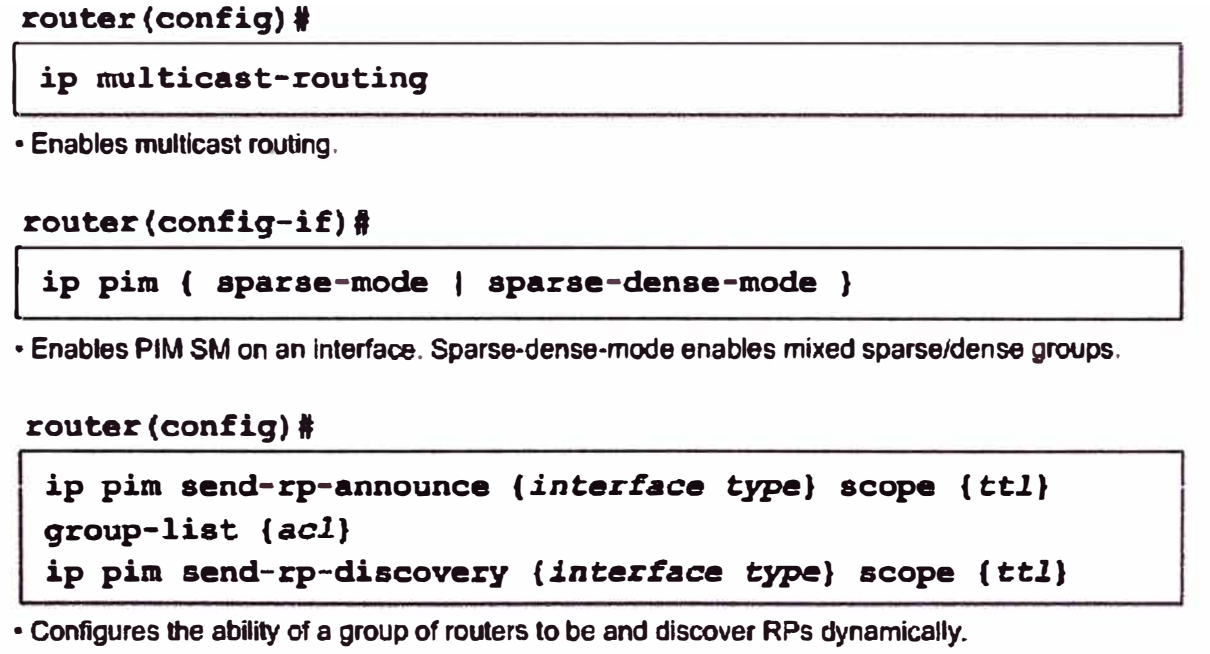


Fig. 6.1 Comando de Configuración PIM-SM

6.3 Analisis de la Tabla de Enrutamiento Multicast.

El comando **show ip mroute** es el comando más útil para determinar el estado de las fuentes y grupos multicast desde la perspectiva del router seleccionado.

La salida del comando generalmente representa una parte del árbol de distribución multicast, con una interface de entrada y una lista de interfaces salientes. Están disponibles las siguientes opciones:

- **summary**: Muestra a una línea, el resumen abreviado de cada entrada en la tabla de enrutamiento IP multicast.
- **count:** Muestra las estadísticas sobre el grupo y la fuente, incluido el número de paquetes, los paquetes por segundo, el tamaño promedio de paquetes, y los bits por segundo.
- **active:** Muestra la velocidad a la que las fuentes se activan enviando a los grupos multicast. La activación de las fuentes son de los que en un porcentaje especificado en kbps. El valor por defecto es de 4 kbps.

El resultado del comando **show ip mroute** in Figure 2 muestra la tabla de enrutamiento multicast en un entorno PIM-SM:

- **(*, G) entry:** Se enumeran los timers (temporizadotes), la dirección RP para el grupo, y los flags (banderas) para el grupo (S es sparse).
    - La entrada de la interface es la interface hacia el RP—si es nulo, el router es el RP. El Reverse Path Forwarding (RPF) vecino es la próxima dirección (next-hop address) hacia el RP. Si se trata de 0.0.0.0, el router es el RP para el grupo.
    - La lista de Interfaces de salida (OIL - The outgoing interface list) enumera las interfaces salientes, junto con modos and timers.
- **(S, G) entry:** Enumeran las entradas de timers y flags (T indica que se encuentra en el SPT; A indica que sera anunciado por el Multicast Source Discovery Protocolo [MSDP]).
    - La interface de entrada es la interface hacia la fuente S. El RPF vecino es la direccion hacia la fuente. Si se trata de 0.0.0.0, la fuente se asigna directamente.
    - The OIL enumera las interfaces salientes, ademas de modos and timers.

```
router#
show ip mroute [group-address] [summary] [count] [active
kbps]
```

Fig. 6.2 Inspeccion de la Tabla de Enrutamiento Multicast

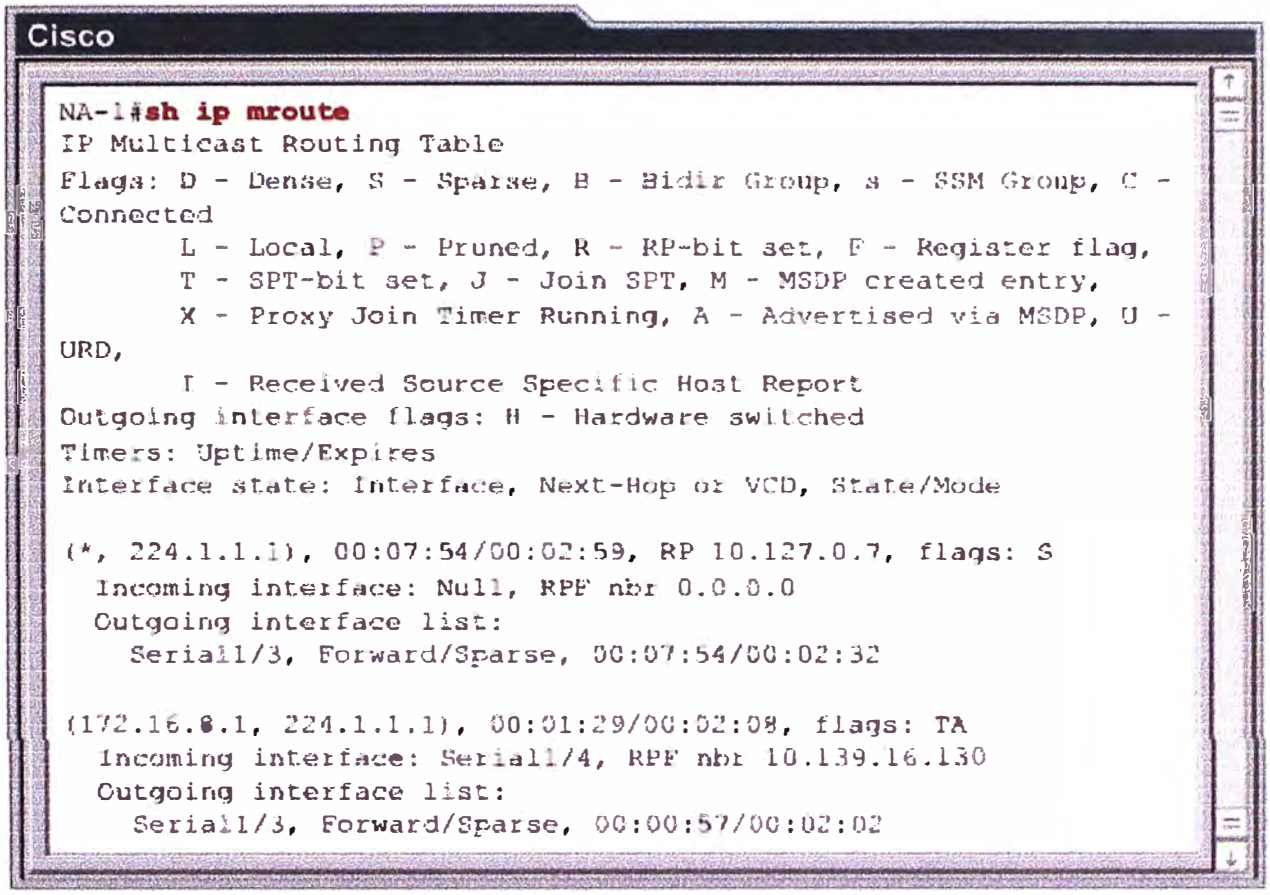


Fig. 6.3 Comando show ip mroute

6.4 Descubriendo Vecinos PIM.

Cuando el PIM-SM está configurado, el primer paso en la verificación del buen funcionamiento es comprobar si las interfaces PIM estan habilitados para determinar si los PIM vecinos son correctos.

Se puede usar los siguientes comandos para lograr esto:

show ip pim interface: Muestra información de las interfaces configurados con PIM.

show ip pim neighbor: Muestra a los vecinos PIM descubiertos.

mrinfo: Muestra informacion de routers multicast que hacen peering (fija su atención) con el router local o con routers destinados.

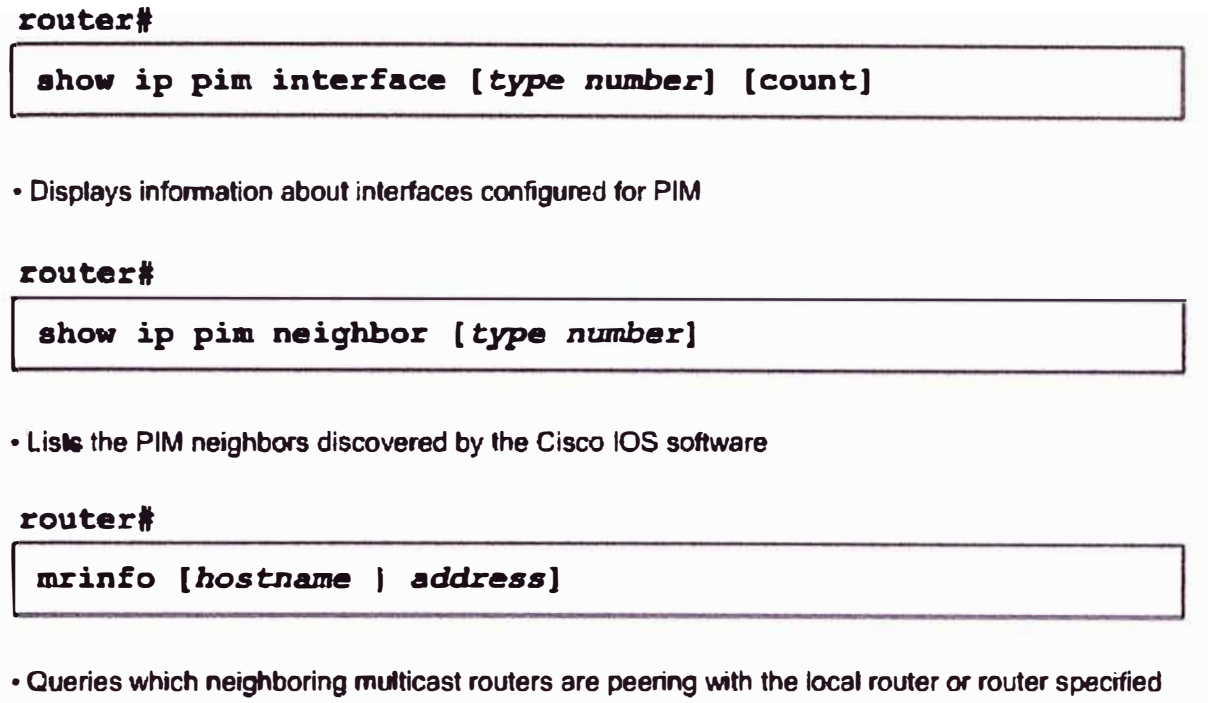


Fig. 6.4 Descubriendo vecinos PIM

El comando **show ip pim interface** muestra la siguiente informacion:

- **Address:** Es la direccion IP de la interface
- **Interface:** Tipo y numero de interface configurado con PIM.
- **Ver/Mode:** Indica la version del PIM (1 or 2) que esta corriendo en la interface y el tipo de modo (dense mode, sparse mode, or sparse-dense mode).
- **Nbr Count:** Indica el numero de vecinos en este enlace.
- **Query Intvl:** Indica la frecuencia con que los hellos PIM y queries (solicitudes) son enviados (Por defecto es 30 segundos).
- **DR Prior:** Usa la prioridad para la eleccion del DR (Designated Router). Si todos los routers en u enlace multiaccess tiene la misma prioridad (por defecto es 1), la mas alta direccion IP es el desempate.
- **DR:** Es la direccion IP del DR. (En enlaces point-to-point, no existen DRs, asi que la salida muestra 0.0.0.0)

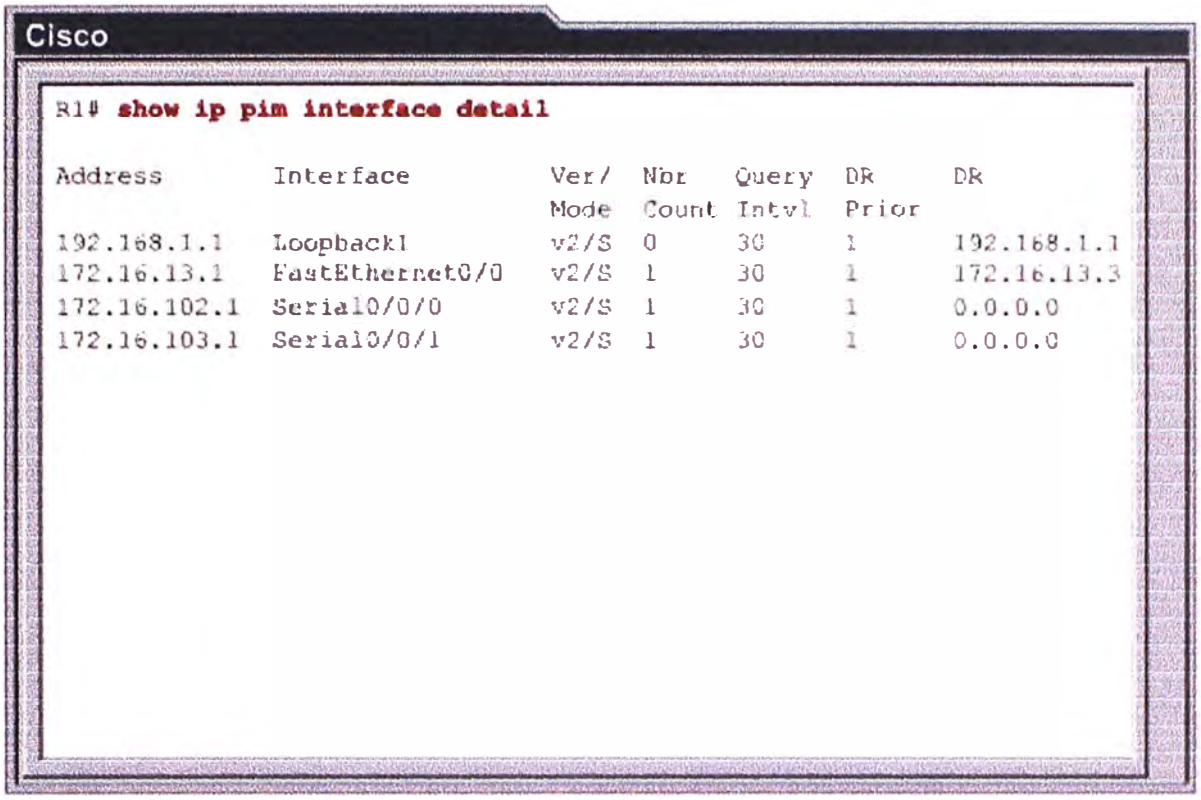


Fig. 6.5 Comando show ip pim interface

El comando **show ip pim neighbor** muestra la siguiente informacion:

- **Neighbor Address:** Es la direccion IP del PIM vecino.
- **Interface:** Es la interface donde el Hello PIM (PIM query in PIMv1) del vecino fue recibido.
- **Uptime:** Es el periodo de tiempo en que el PIM del vecino ha sido activado.
- **Expires:** Es el periodo de tiempo (hold time) despues de que este PIM vencino ya no se considera activo. La recepción de otro Hello PIM o Query reestablece o resetea el timer.
- **Ver:** Es la version PIM (1 o 2) que esta usando el vecino.
- **DR Priority:** Si el vecino soporta esta opcion, el valor numerico es mostrado. Si un numero no es mostrado, el vecino no soporta esta opcion.

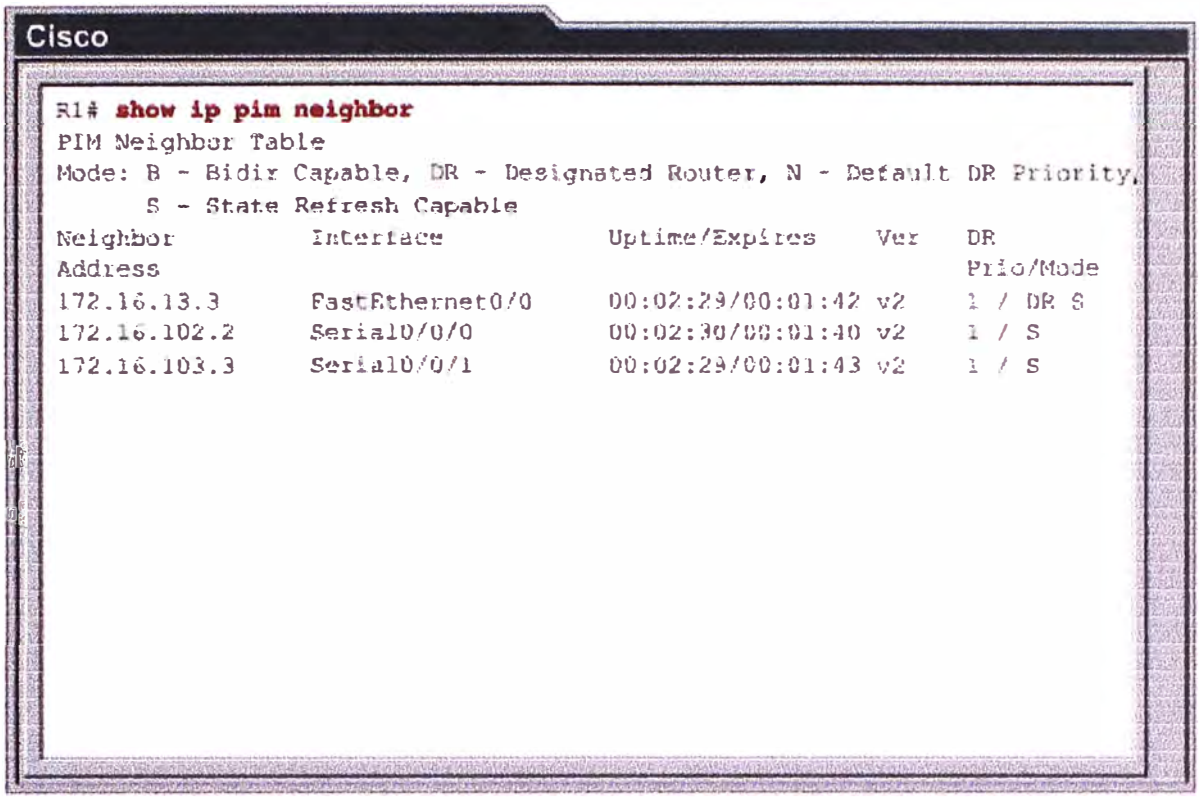


Fig. 6.6 Comando show ip pim neighbor

El ejemplo de salida del commando **mrinfo** de la Figure 6.7 muestra informacion de los routers multicast conectados al router R1.

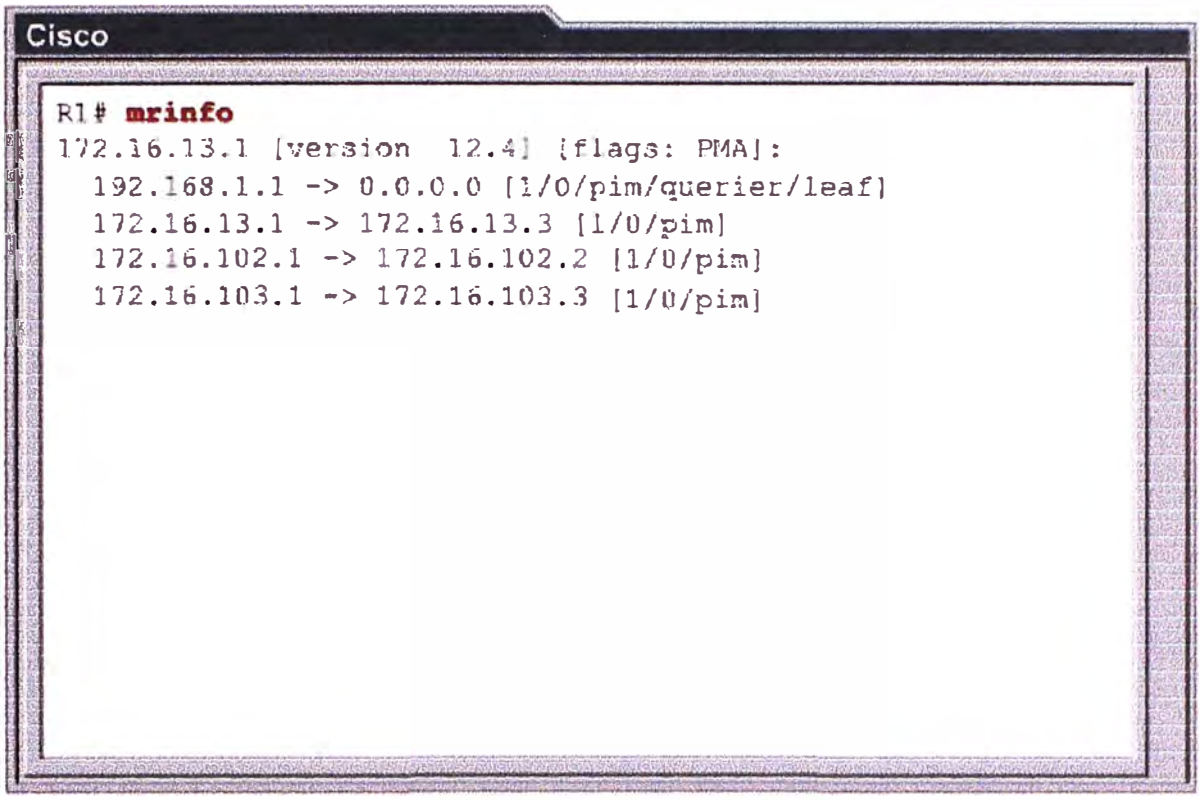


Fig. 6.7 Comando mrinfo

6.5 Checking RP Information.

El RP para un determinado grupo multicast en funcionamiento con el PIM-SM ha de ser accesible y conocido por el router. Además de usar un **ping** unicast, se puede usar los siguientes comandos en la solución de problemas accesibles al RP:

- **show ip pim rp:** Muestra, sin argumentos, informacion del RP sobre grupos activos. Si el grupo de direcciones o nombres es seleccionado, solo se mostrara la información del RP para el grupo seleccionado (suponiendo que se trata de un grupo activo).
- **show ip pim rp mapping:** Muestra el contenido del importante mapeo de group-to-RP en la memoria caché, que contiene la información acerca del RP que se activa para el rango de grupo. Esta caché es poblada por el mecanismo auto-RP o BSR y por la asignación del RP estático. Es muy importante comprobar esta información para verificar que el router tiene la información del mapeo RP en consonancia con el debido funcionamiento de la red.
- **show ip rpf:** Muestra informacion del RPF para el RP o para la fuente (source).

```
router(config)#
show ip pim rp [group-name | group-address | mapping]
```

- Display active rendezvous points (RPs) that are cached with associated multicast routing entries
  - **Mapping**—displays all group-to-RP mappings that the router is aware of

```
router(config)#
show ip rpf {address | name }
```

- Displays how IP multicast routing does Reverse Path Forwarding (RPF)
  - *Address*—IP address of a source of an RP

Fig. 6.8 Chequeo de Informacion RP

El comando **show ip pim rp** sólo enumera todos los grupos activos y de sus asociados RPs. Lo mostrado en la Figura 6.9 el comando se está convirtiendo en obsoleto, ya que ofrece información limitada. En la mayoría de los casos, debe utilizar el **show ip pim rp mapping** en lugar de la Fig. 6.10, ya que proporciona detalles sobre el contenido actual del group-to-RP de la memoria caché, como las siguientes:

- La dirección IP de un router que distribuye la información—cuando la fuente de la información es un router local que tiene configuración manual del RP o es una fuente de la información distribuida automáticamente.
- Mecanismos por el cual esta informacion fue determinada—auto RP, BSR, o statica.
- Si este router funciona como un candidato-RP, mapping agent (agente de mapeo) o BSR.

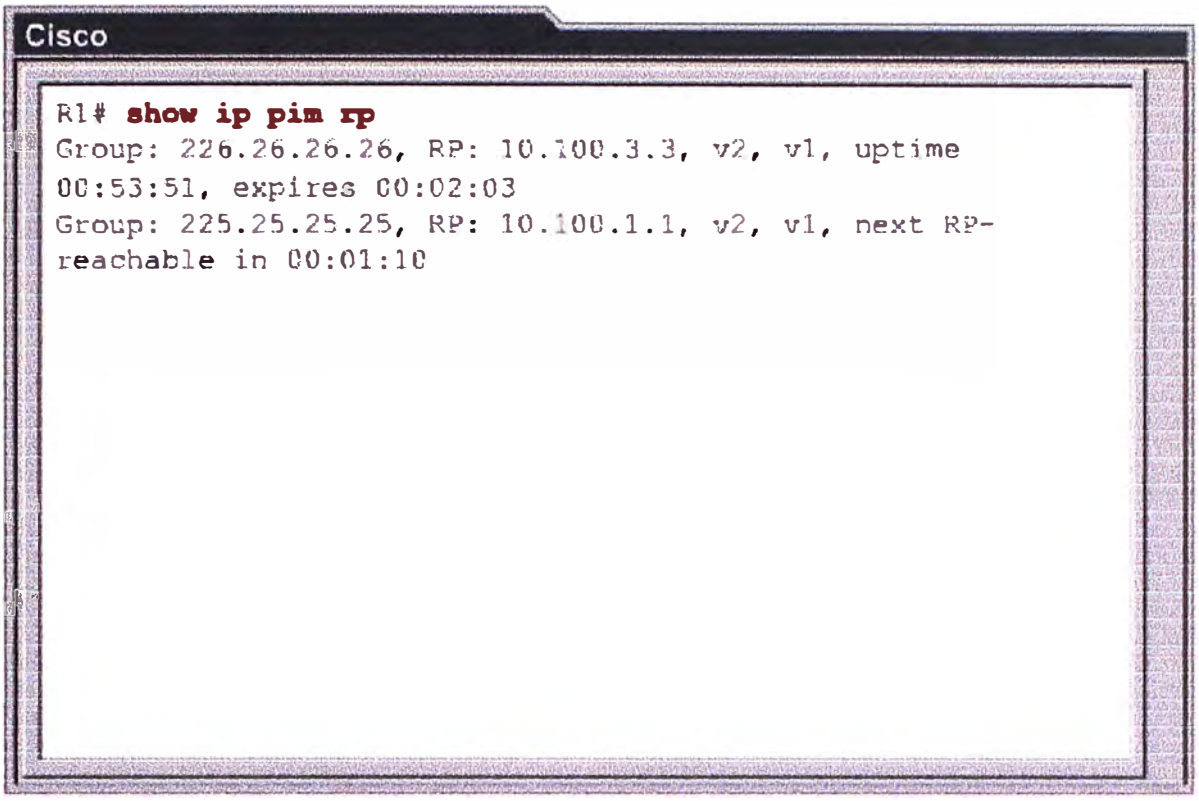


Fig. 6.9 Comando show ip pim rp

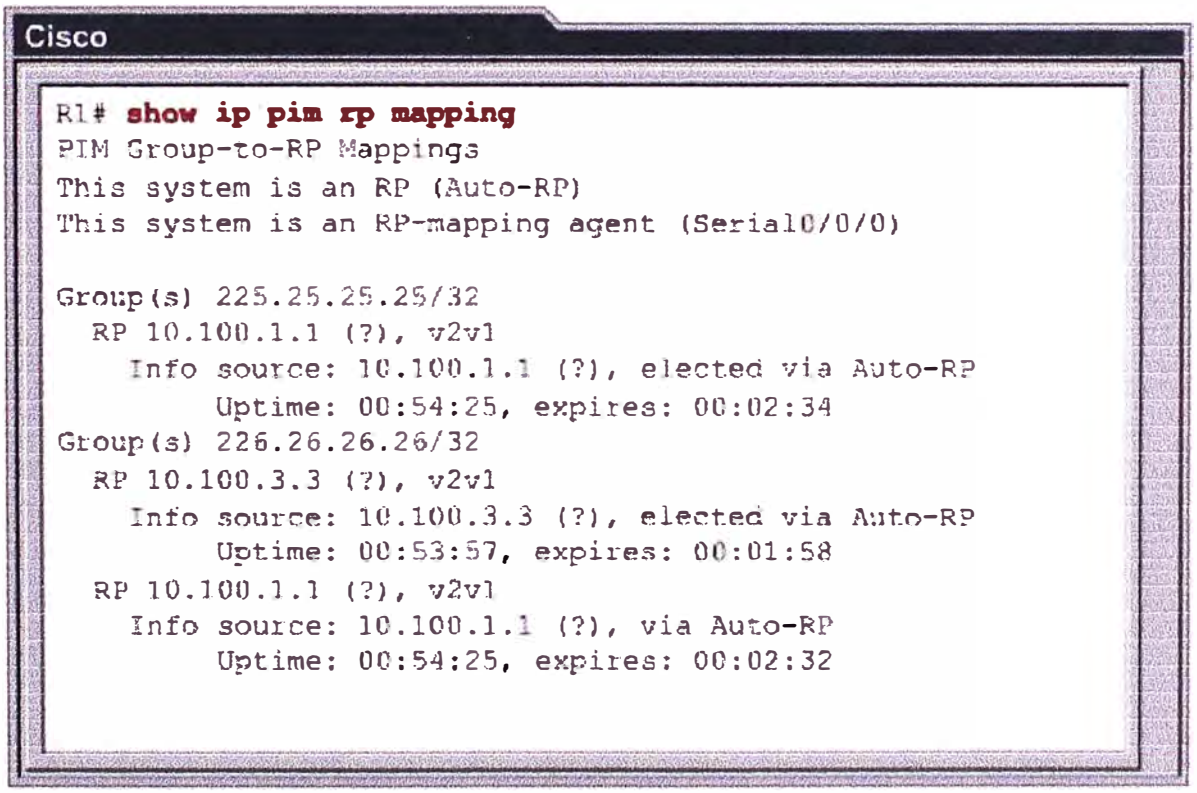


Fig. 6.10 Comando show ip pim rp mapping

El comando **show ip rpf** muestra la información asociada a la dirección fuente especificada. La Figura 6.11 muestra que la dirección especificada no necesariamente tiene que ser una fuente activa actualmente. De hecho, puede ser una dirección IP, incluida la dirección del RP. Especificando la dirección del RP es muy útil en la determinación de información RPF para el arbol compartido.

"RPF interface" es la interface en la dirección de la fuente (o RP), mientras que "el RPF vecino" es la proxima dirección del router en la dirección de la fuente (o RP).

"RPF type", indica la fuente de información del RPF. En el ejemplo, unicast indica que la información se deriva de la tabla de enrutamiento unicast (en este caso, la ruta más corta desde Open Shortest Path First Protocol [OSPF]). Otros tipos incluyen RPF incluyen Distancia Vector Multicast Routing Protocol (DVMRP), Multiprotocol Border Gateway Protocol (BGP) para extensiones IP multicast, o estática.

La información RPF es esencial en el enrutamiento multicast, y el especial cuidado que se ha tomado al inspeccionar la información del PIM-SM es debido a la posible coexistencia de árboles compartidos y SPTs.

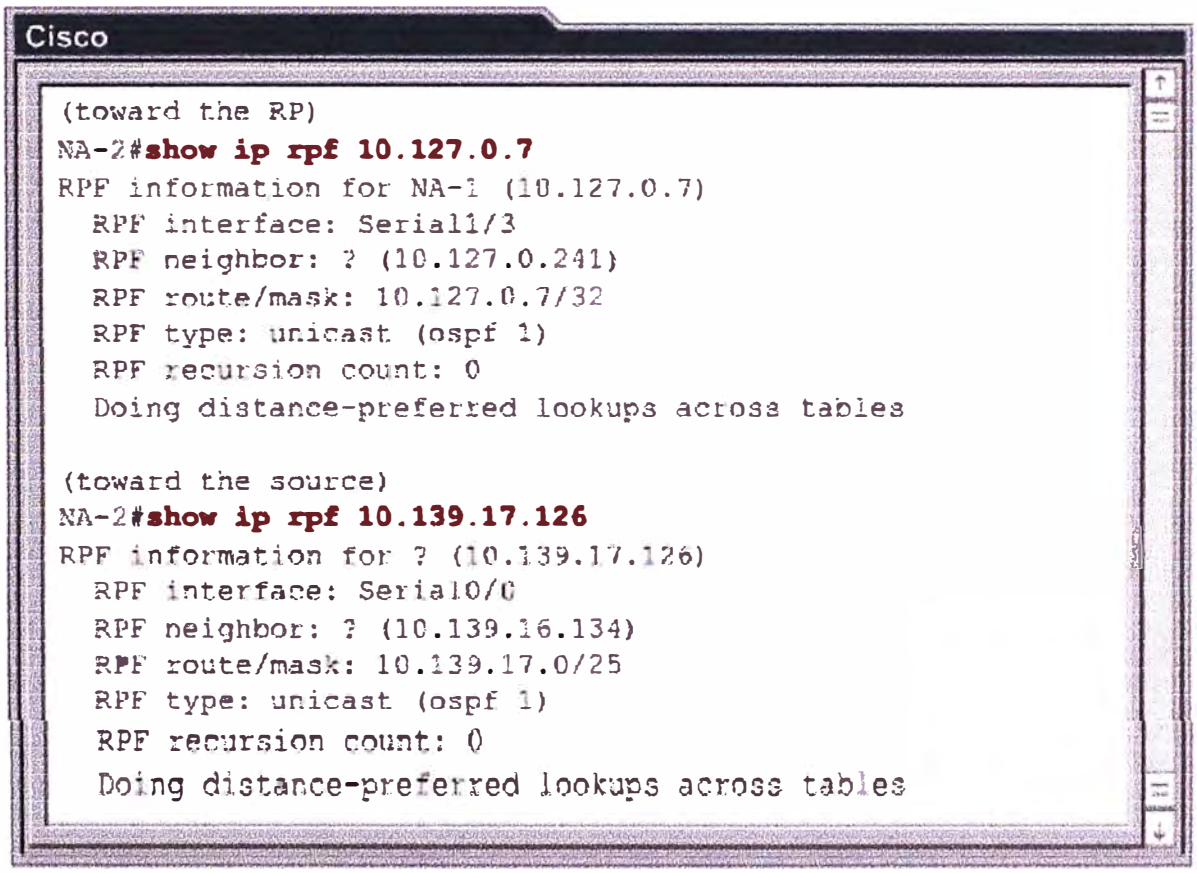


Fig. 6.11 Comando show ip rpf

6.6 Chequeo del Estado de Grupo.

Si el tráfico de multicast no está fluyendo a los receptores, el grupo de miembros del IGMP que se ha comprobado en la hoja de routers. El comando **show ip igmp interface** muestra información sobre las interfaces seleccionados, y el comando **show ip igmp groups** enumera los grupos locales conocido por el router. Fig. 1

Al habilitar el PIM en una interface tambien permite la operación del IGMP en esa interface. Una interface puede ser configurado como dense, sparse, or sparse-dense mode. El modo determina la forma en que el router rellena su tabla de enrutamiento multicast y la forma en que el router envía paquetes multicast que recibe de sus redes de área local conectadas directamente. Se debe habilitar el PIM en uno de estos modos de una interface para realizar el enrutamiento IP multicast.

En las figuras 6.13 y 6.14 se muestra la salida para cada comando.

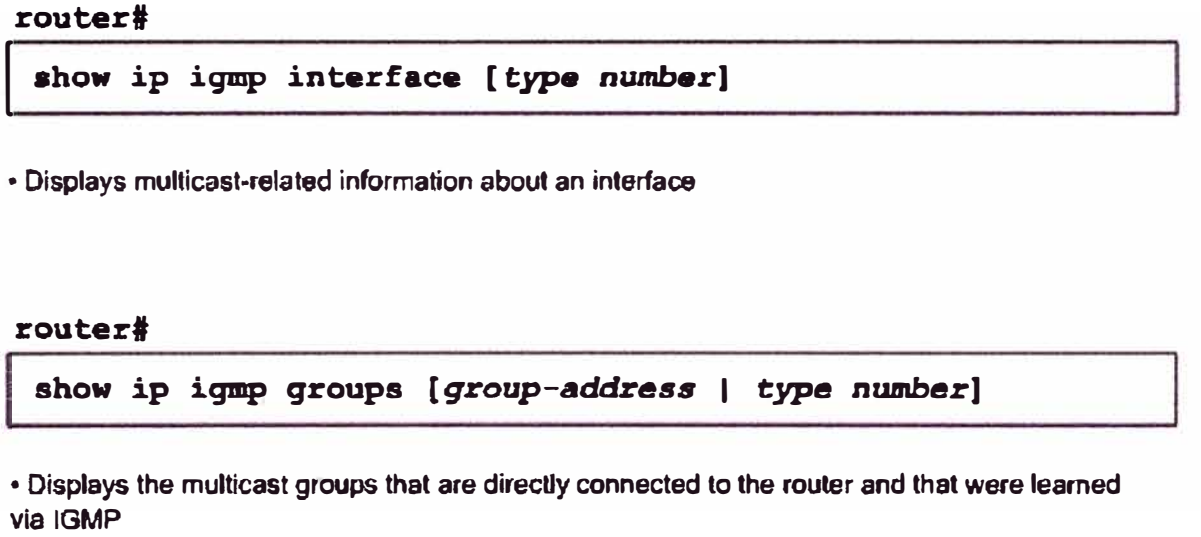


Fig. 6.12 Chequeo del Estado de Grupo

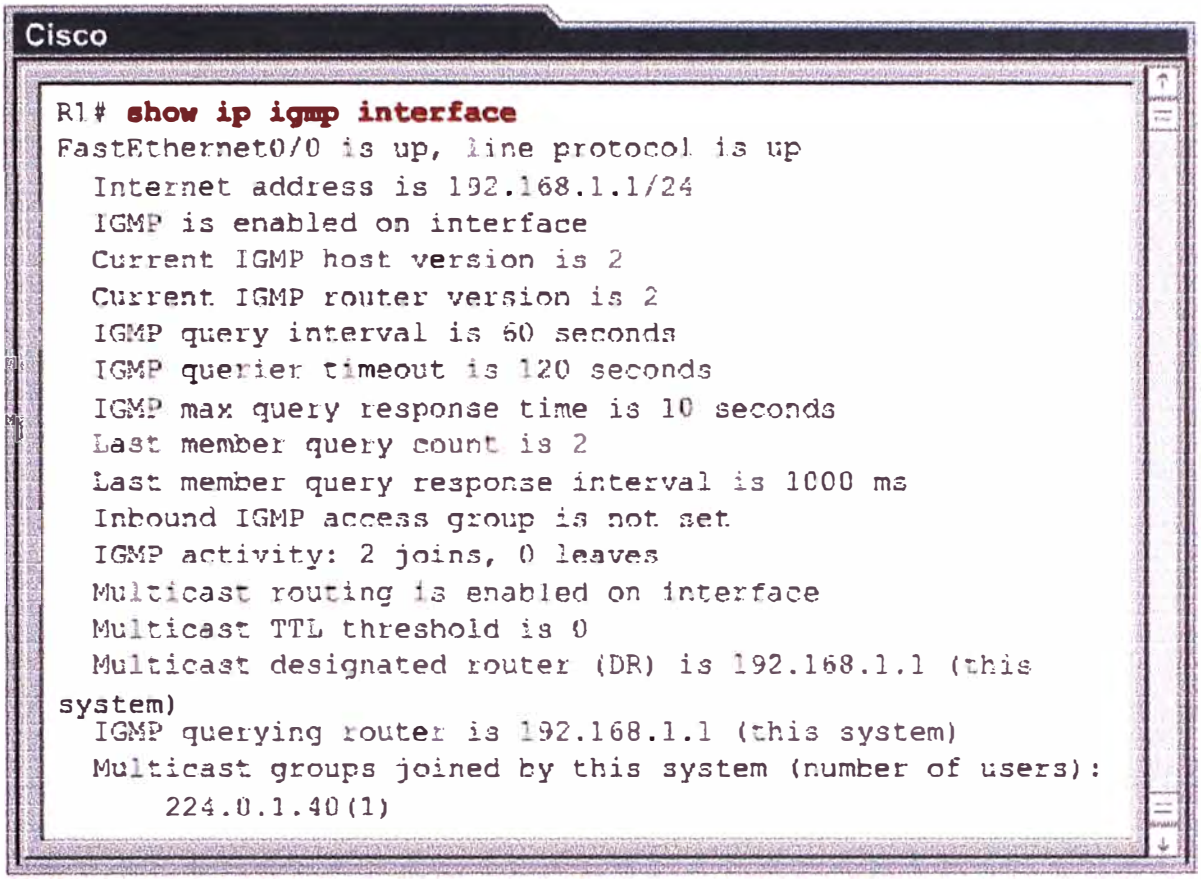


Fig. 6.13 Comando show ip igmp interface

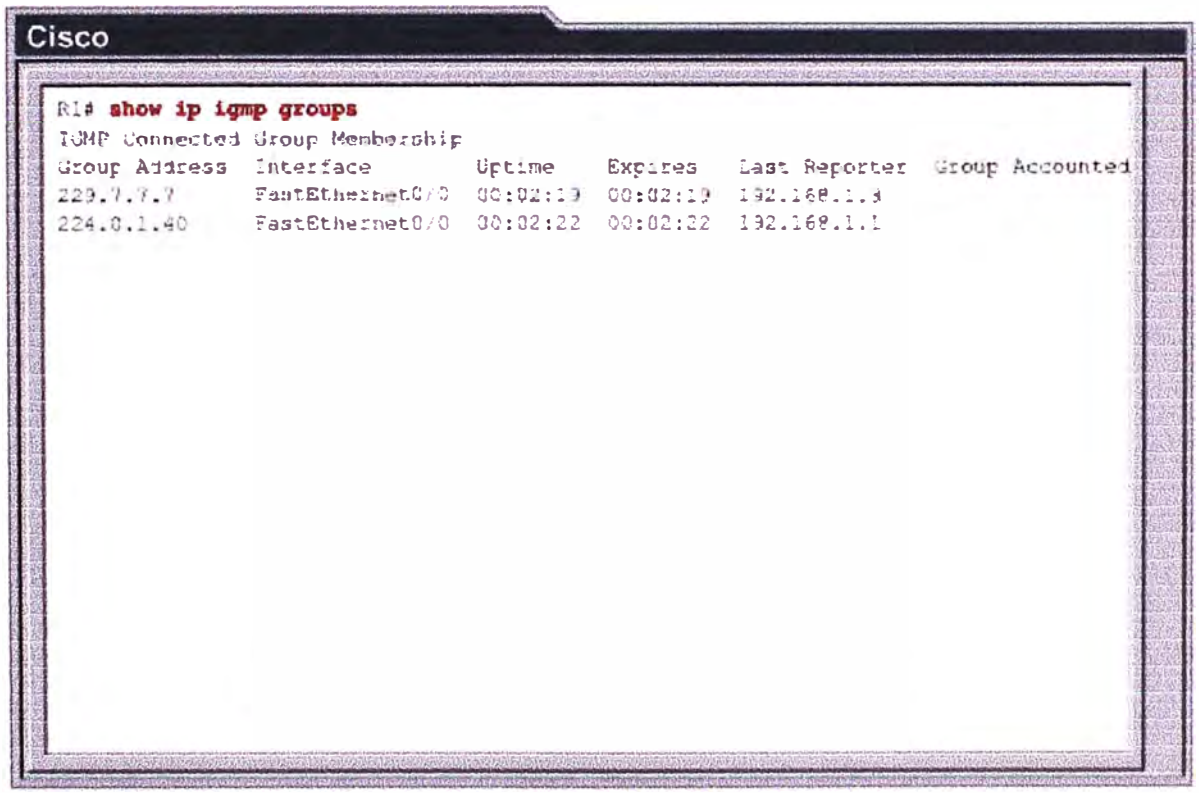


Fig. 6.14 Comando show ip igmp groups

6.7 Configuracion de Router para ser Miembro de Grupo.

En algunos casos, es necesario configurar el tráfico multicast para ir a un segmento donde no hay miembro de grupo o cuando un host en ese segmento no puede informar como miembro de grupo utilizando IGMP.

Se puede configurar los routers Cisco para llegar a ser miembros de un grupo multicast, que es útil para determinar la accesibilidad multicast en una red. Si un dispositivo se configura para ser un miembro de grupo y soporta el protocolo que se transmite al grupo, que puede responder (por ejemplo, el comando **ping**). El dispositivo responde al IGMP de los paquetes de solicitud dirigida a un grupo del cual es miembro.

Los siguientes son dos formas de tirar hacia abajo el tráfico multicast a un segmento de la red. Estos comandos se utilizan a menudo en entornos de laboratorio donde los servidores y receptores no están configurados con multicast.

ip igmp join-group: El router acepta los paquetes multicast, además de transmitirlas. La aceptación de los paquetes multicast impide al router del fast switching (rápido cambio). (ver Tabla 6.1)

ip igmp static-group: El router no acepta los paquetes, pero reenvia hacia delante. Por lo tanto, este método permite cambiar rápidamente (fast switching). La interface saliente aparece en el cache del IGMP, pero el router en sí no es miembro, como pone de manifiesto la falta de una L (local) flag en la ruta de entrada multicast.

La Figura 6.15 muestra un ejemplo de configuración de un router uniendose a un grupo multicast y permitiendo el IGMP usando el comando **ip igmp join-group** en el modo de configuración de interface.

Tabla N° 6.1 Comando ip igmp join-group

Command	Purpose
ip igmp join-group *group-address*	Joins a multicast group.

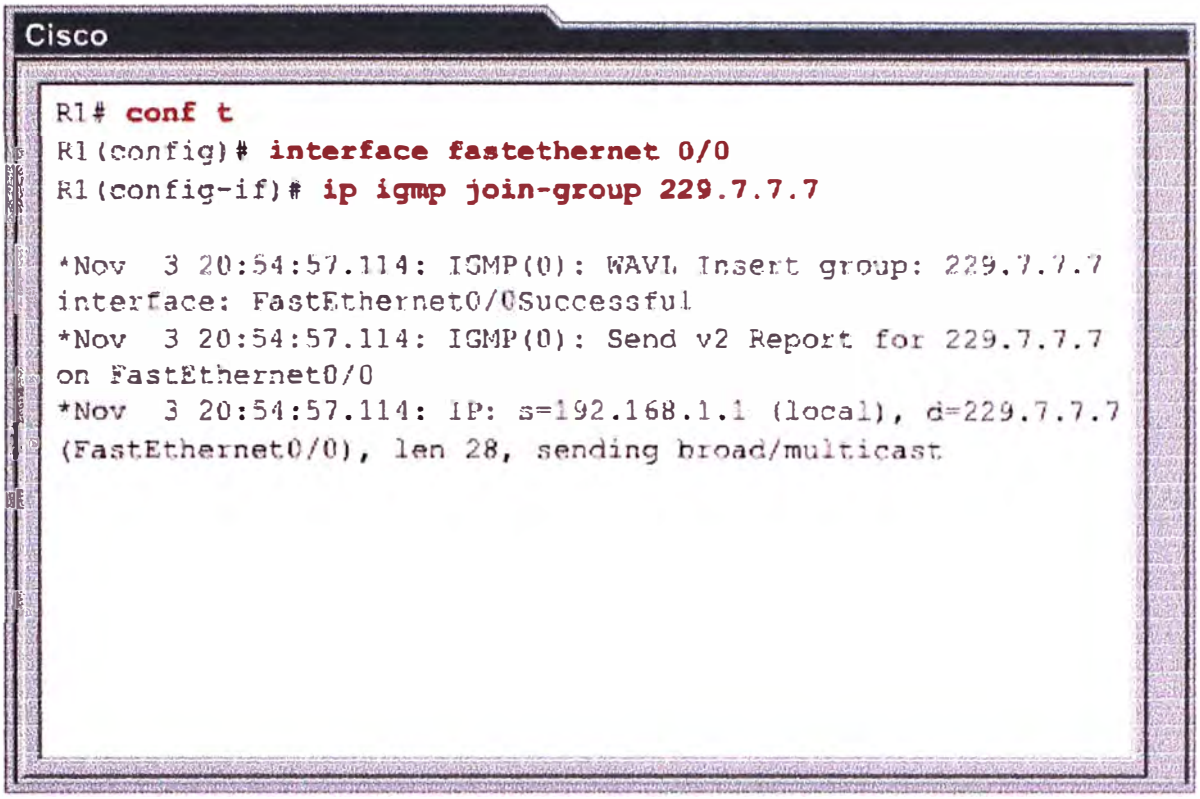


Fig. 6.15 Comando ip igmp join-group

6.8 Configuracion de un Router como Miembro Conectado Estaticamente.

Para configurar el router para ser miembro de grupo estáticamente conectado (y permitir el fast switching), el uso del comando **ip igmp static-group** se muestra en la tabla 6.2 en el modo de configuración de interface.

Utilice el comando **show ip igmp interface** para mostrar los grupos multicast que están directamente conectados al router, y que fueron aprendidos a través del IGMP. Este comando se utiliza para determinar la siguiente información:

- Interface configuration for multicast and IGMP
- Version for which the IGMP interface is configured
- IGMPv2 querier on the multiaccess network
- Multicast designated router
- Joined multicast groups on the current router

En la Figura 6.16, el router por si mismo se une (join) a esos dos grupos:

- **224.0.1.40 group:** Auto RP, donde es unido (joined) automaticamente.
- **224.2.127.254 group:** SDR, el cual fue unido (joined) al configurar el comando **ip sdr listen** en la interface.

El uso del comando **show ip igmp groups** muestra que grupo multicast estan directamente conectados hacia el router y de que manera fueron aprendidas via IGMP.

En la Figura 6.17, el router reconoce dos grupos multicast:

- **Grupo 224.1.1.1** está activo en Ethernet0 y ha estado activado en esta interfaz por 6 días y 17 horas. Este grupo expira (y se eliminarán) en 1 minuto y 47 segundos si un IGMP Host Membership Report de este grupo no es escuchado en ese momento. El último host informa a los miembros que fue 1.1.1.12.
- **Grupo 224.0.1.40 (auto RP)** esta automáticamente unido por todos los routers Cisco. Así, muestra su expiracion "never".

Tabla Nº 6.2 Comando ip igmp static-group

Command	Purpose
ip igmp static-group *group-address*	Configures the router as a statically connected member of a group

Cisco

```
rtr-a>show ip igmp interface e0
Ethernet0 is up, line protocol is up
  Internet address is 1.1.1.1, subnet mask is 255.255.255.0
  IGMP is enabled on interface
  Current IGMP version is 2
  CGMP is disabled on interface
  IGMP query interval is 60 seconds
  IGMP querier timeout is 120 seconds
  IGMP max query response time is 10 seconds
  Inbound IGMP access group is not set
  Multicast routing is enabled on interface
  Multicast TTL threshold is 0
  Multicast designated router (DR) is 1.1.1.1 (this system)
  IGMP querying router is 1.1.1.1 (this system)
  Multicast groups joined: 224.0.1.40 224.2.127.254
```

Fig. 6.16 Comando show ip igmp interface

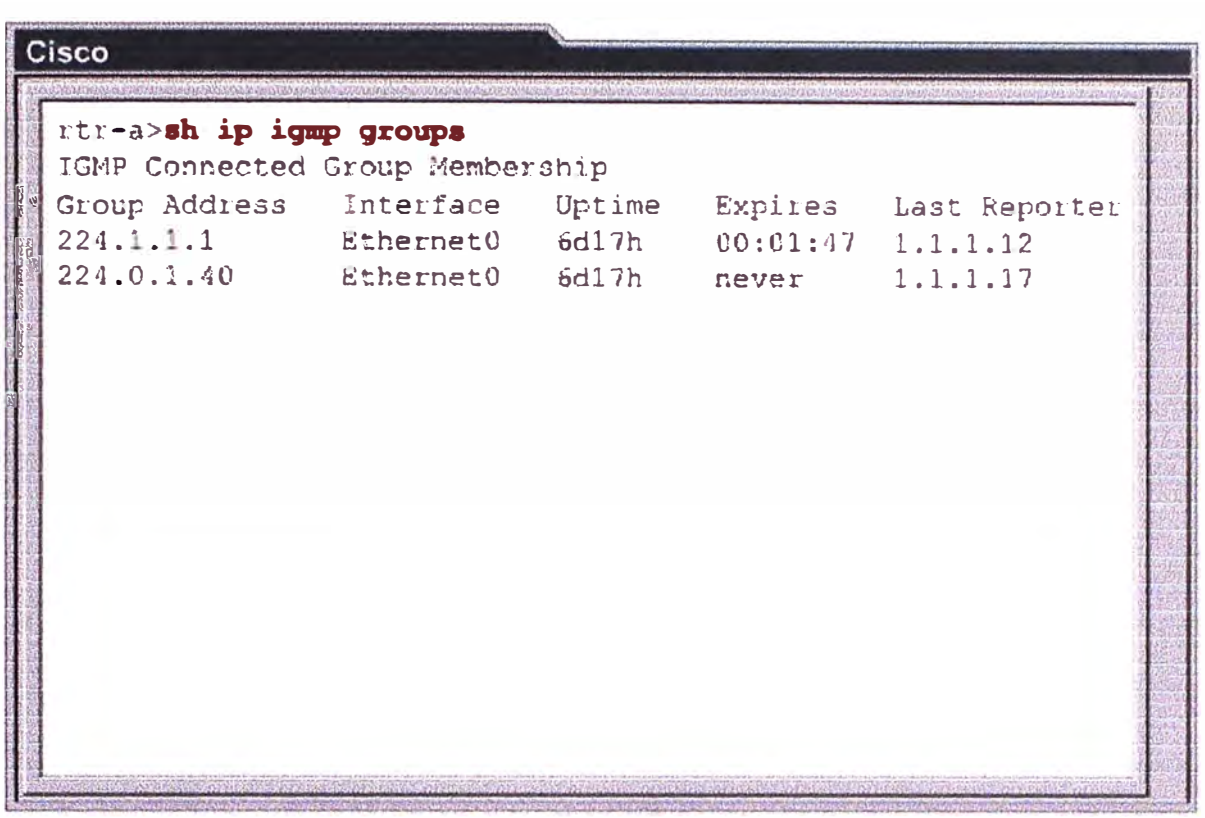


Fig. 6.17 Comando show ip igmp groups

6.9 Verificando IGMP Snooping.

Cuando verificamos el IGMP snooping en un switch, usamos el comando **show ip igmp snooping** para mostrar la información de configuración para todas las VLANs en el switch o para una determinada VLAN. (ver Figura 6.18)

Notemos que el IGMP snooping está activado por defecto en la configuración global y sobre una base per-VLAN en el SW1. En este caso, IGMP snooping identifica un switchport como un puerto de router multicast sólo si recibe mensajes enviados (PIM o DVMRP) hacia el puerto del switch.

En la Figura 6.19 nos proporciona un ejemplo de los resultados generados por el comando **show ip igmp snooping** en un switch Catalyst 4000. Por lo tanto, el formato de salida será diferente según el modelo del switch Catalyst.

Tambien se puede utilizar el comando **show mac-address-table multicast** para mostrar las entradas en la tabla de direcciones MAC de una VLAN que ha permitido IGMP snooping. (ver Figura 6.20)

Cisco

```
SW1# show ip igmp snooping
vlan 1
----------
 IGMP snooping is globally enabled
 IGMP snooping is enabled on this Vlan
 IGMP snooping immediate-leave is disabled on this Vlan
 IGMP snooping mrouter learn mode is pim-dvmrp on this Vlan
 IGMP snooping is running in IGMP_ONLY mode on this Vlan
```

Fig. 6.18 Comando show ip igmp snooping

Cisco

```
Switch# show ip igmp snooping
Global IGMP Snooping configuration:
-----------------------------------
IGMP snooping              : Enabled
IGMPv3 snooping            : Enabled
Report suppression         : Enabled
TCN solicit query          : Disabled
TCN flood query count      : 2

Vlan 1:
--------
IGMP snooping                    : Enabled
IGMPv2 immediate leave           : Disabled
Explicit host tracking           : Enabled
Multicast router learning mode   : pim-dvmrp
CGMP interoperability mode       : IGMP_ONLY
```

Fig. 6.19 Comando show ip igmp snooping (Catalyst 4000)

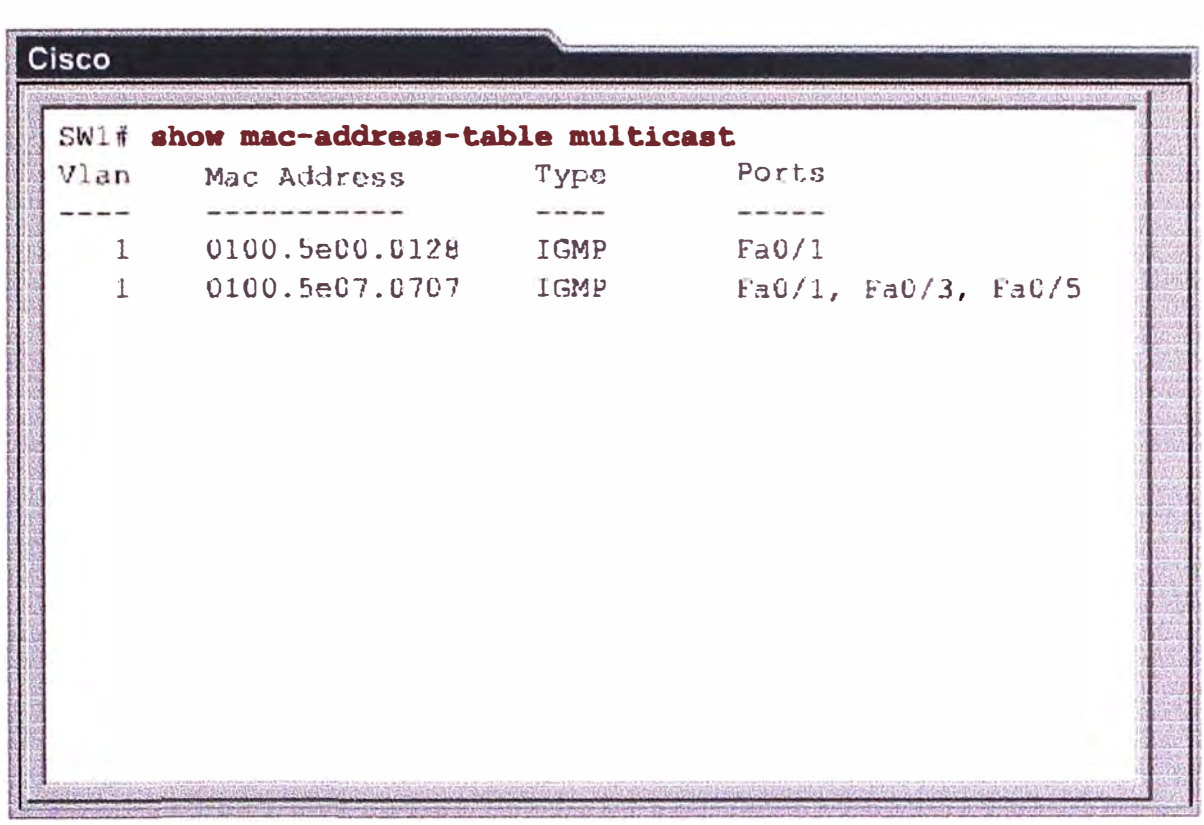


Fig. 6.20 Comando show mac-address-table multicast

6.10 Resumen del capitulo.

Es este capitulo hemos realizado la descripción de los principales comandos que son usados en los routers como parte de implementacion de una red multicast. Es de suma importancia conocer el uso de estos comandos que nos permitiran adecuar nuestra red de acuerdo a las necesidades requeridas con redes multicast.

CONCLUSIONES

1. La primera conclusión que se obtiene del presente estudio es que las redes multicast son una solución que se ajustan a las necesidades las nuevas aplicaciones multimedia, las cuales pueden ser implementadas teniendo en cuenta los criterios de diseño, en apoyo al despliegue del IP multicast. La incursión del multicast pretende proporcionar información necesaria para tomar buenas decisiones de diseño a medida que se modifican las redes de hoy en multicast habilitado para las redes del mañana.
2. Sobre la base de que un buen entendimiento de cómo se construye una red IP multicast, se ha comprendido los conceptos más básicos de IP multicast, en el ambito de direcciones IP clase D se ha presentado la clasificacion de direcciones de acuerdo al uso particular que sera tratado, ademas incluye el mapeo de direccionamiento MAC Ethernet en Multicast y como se aborda la relación en Multicast tanto en Capa 2 y Capa 3..
3. Las implementaciones de redes multicast requieren comprender cómo IGMP se utiliza como base el mecanismo de señalización para informar a los routers en una subred donde algun miembro tiene el deseo unirse al grupo multicast. El IGMPv2 amplia este mecanismo de señalización para permitir que alberga a la señal cuando ya no quería pertenecer a un grupo multicast. Esta extensión del protocolo ha reducido significativamente la latencia de la licencia que, a su vez, permite que los routers y conmutadores para responder rápidamente y cierre el flujo de tráfico multicast innecesarios a las partes de las redes en las que ya no es necesario.
4. La implementación de una red multicast requiere contar con equipos de redes routers y switches, donde el hardware y software deben soportar las características del IP Multicast. Actualmente esta solucion se puede dar en redes LAN, tambien puede extenderse hacia otras LANs pasando por una red privada de transporte.

5. Es necesario realizar un control de la situación con la creciente popularidad del IP multicast, como IP multicast se convierte en una parte importante de las empresas la infraestructura de la red, la necesidad de limitar el tráfico multicast en grandes redes de conmutación LAN se convierte en un tema de suma importancia. Porque con el control de la corriente de tráfico multicast exige hoy en día las tecnologías de Capa 3, y la necesidad de una mayor ruta alterna en la red de campus se encuentra una vez más en aumento.
6. La descripción de los principales comandos que son usados en los routers como parte de implementacion de una red multicast nos permiten hacer el uso adecuado de comandos los mismos que se ajustan a las necesidades requeridas con redes multicast.

ANEXOS

ANEXO A

Hojas de Datos de los Equipos

Se presentan a continuación las hojas técnicas de los equipos que para la implementacion de una red multicast.

Estas hojas técnicas son proveídas por los fabricantes de los equipos.

Cisco 2851 Integrated Services Router

Product Series Information
Cisco 2851 Product Details

Cisco 2851 Integrated Services Router

- Up to 5 times the routing performance offered by comparable Cisco 2600 series routers
- Ability to run concurrent integrated services
- Support for next generation of High-speed WAN Interface Cards (HWICs), Extension Voice Modules (EVMs) and Network Modules (NMEs)
- Support for up to 44 ports of integrated managed 10/100 Switching with inline power
- Enhanced security with onboard hardware encryption, Network Admission Control (NAC) and a wide range of security software feature sets
- Additional flexibility with two internal AIM slots, three internal DSP Slots, 2 USB ports, 1 NME-XD slot, 1 EVM slot, and 4 HWIC slots
- Complete voice solution with support for localized call-processing and voicemail using Cisco Call Manager Express (CME) and Cisco Unity Express (CUE)

The Cisco 2851 Integrated Services Router is part of the Cisco 2800 Integrated Services Router Series which complements the Integrated Services Router Portfolio. The Cisco 2800 Series features the ability to deliver multiple high-quality simultaneous services at wire speed up to multiple T1/E1/xDSL connections. The routers offer embedded encryption acceleration and on the motherboard voice digital-signal-processor (DSP) slots; intrusion prevention system (IPS) and firewall functions; optional integrated call processing and voice mail support; high-density interfaces for a wide range of connectivity requirements; and sufficient performance and slot density for future network expansion requirements and advanced applications.

The Cisco 2851 Integrated Services Router provides the following support:
•Wire-speed performance for concurrent services such as security and voice , and advanced services to multiple T1/E1/xDSL WAN rates
•Enhanced investment protection through increased performance and modularity
•Enhanced investment protection through increased modularity
•Increased density through High-Speed WAN Interface Card Slots (four)
•Enhanced Network Module Slot
•Support for over 90 existing and new modules
•Support for majority of existing AIMs, NMs, WICs, VWICs, and VICs
•Two Integrated 10/100/1000 ports
•Optional Layer 2 switching support with Power over Ethernet (PoE) (purchased separately), supports the 36-port Cisco EtherSwitch module (NMD-36ESW)

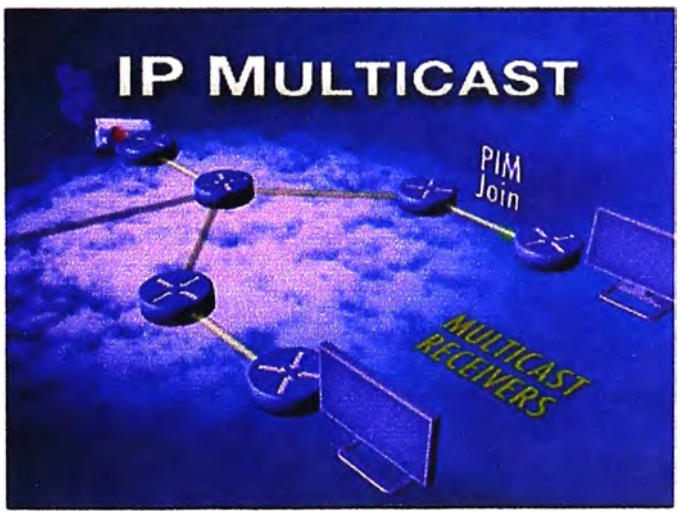
Architecture:
•A wide variety of LAN and WAN options are available. Network interfaces can be upgraded in the field to accommodate future technologies
•Each of the Cisco 2800 Series routers comes standard with embedded hardware cryptography accelerators, which when combined with an optional Cisco IOS Software upgrade help enable WAN link security and VPN services.
•The Cisco 2800 Series provide two 10/100 on the Cisco 2801 and Cisco 2811 and two 10/100/1000 on the Cisco 2821 and Cisco 2851

Modularity:
•Dual AIM slots support concurrent services such as hardware-accelerated security, ATM segmentation and reassembly (SAR), compression, and voice mail.
•Four integrated HWIC slots on Cisco 2851 allow for more flexible and dense configurations.
•Enhanced network-module (NME) slots

Specifications:
•DRAM:Default: 256 MB;Maximum: 1 GB
•Compact Flash:Default: 64 MB;Maximum: 256 MB
•Fixed USB 1.1 ports:2
•Onboard LAN ports: 2 10/100/1000
•Onboard AIM (internal) slot: 2
•Interface card slots:4 slots, each slot can support HWIC, WIC, VIC, or VWIC type modules
•Network-module slot:1 slot, supports NM, NME, NME-X, NMD and NME-XD type modules
•Extension Voice Module Slot:1
•PVDM (DSP) slots on motherboard:3
•Integrated hardware-based encryption:Yes
•VPN hardware acceleration (on motherboard):DES, 3DES, AES 128, AES 192, and AES 256
•Optional integrated in-line power (PoE): Yes, requires AC-IP power supply
•Console port (up to 115.2 kbps): 1
•Auxiliary port (up to 115.2 kbps): 1
•Minimum Cisco IOS Software release: 12.3(8)T
•Rack mounting:Yes, 19- and 23-in. options
•AC input voltage: 100 to 240 VAC, autoranging
•RPS:External only, connector for RPS provided by default
•Rack height:2RU

Cisco Catalyst 2960 Series Switches

Product Name (Part Number)	Description
Cisco Catalyst 2960-24LT-L Switch (WS-C2960-24LT-L)	• 24 Ethernet 10/100 ports with 8 PoE ports and two 10/100/1000TX uplinks • 1 RU fixed-configuration • LAN Base Image Installed
Cisco Catalyst 2960-24PC-L Switch (WS-C2960-24PC-L)	• 24 Ethernet 10/100 PoE ports and two dual-purpose uplinks • 1 RU fixed-configuration • LAN Base Image installed
Cisco Catalyst 2960PD-8TT-L Switch (WS-C2960PD-8TT-L)	• 8 Ethernet 10/100 ports and one 10/100/1000 PoE input port • Power adaptor (PWR-A=) and power cord sold separately • Compact size with no fan; magnet included • LAN Base Image installed



BIBLIOGRAFÍA

1. Ralph Wittman – Martina Zitterbart, "Multicast Communication: Protocols and Applications", Volumen 1, Hardcover – USA, 2000.
2. Kenneth Miller, "Multicast Networking and Applications", – 1ª Edición", Volumen 1, Hardcover – USA, 1998.
3. Van Jacobson series – , "El PIM architecture for wide-area multicast routing", Volumen 4, Berkeley CA, USA, 1996.
4. Documentos del IETF: RFC 1112 (Host extensions for IP Multicast), RFC 1918 (Address Allocation for Address Internet), RFC2236 (Internet Group Management Protocol, Version 2), RFC 2362 (Protocol Independent Multicast Sparse-Mode), RFC2365 (Administratively Scoped IP Multicast)
5. Cisco IOS Software Multicast Services web page
   http://www.cisco.com/go/ipmulticast
6. Cisco IOS Software IP Multicast Groups External Homepage
   ftp://ftpeng.cisco.com/ipmulticast.html
7. IP Multicast Technology
   http://www.cisco.com/en/US/products/ps6552/products_ios_technology_home.html
8. Internet Protocol IP Multicast Technology
   http://cisco.com/en/US/tech/tk828/tech_brief09186a00800a4415.html