PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

MAESTRÍA EN REDES DE COMUNICACIONES

"ESTUDIO DE REQUERIMIENTOS TÉCNICOS PARA LA IMPLEMENTACIÓN DE REDES IP MULTICAST EN AMBIENTES LAN"

TESIS DE GRADO

Previa la obtención del título de

MAGISTER EN REDES DE COMUNICACIONES

Presentado por:

ROBERTO ALEJANDRO LARREA LUZURIAGA

DIRECTOR DE TESIS

PhD. Gustavo Chafla

QUITO – ECUADOR

2012

A MI HIJO Y ESPOSA

Joaquín y Valeria, quienes son mi luz, mi corazón e inspiración para llevar a cabo esta investigación, les dedico este trabajo.

A MIS PADRES Y HERMANOS

Porque sin su apoyo y confianza no habría sido posible cumplir mis metas.

ÍNDICE

CAPÍTULO 2

ÍNDICE DE FIGURAS

Capítulo 2

Anexos

ÍNDICE DE TABLAS

Capítulo 2

Capítulo 3

Capítulo 4

CAPÍTULO 1

MARCO REFERENCIAL

1.1 Justificación

IP Multicast es un proceso de transmisión de canales de comunicación a un número de usuarios a través del uso de múltiples canales distribuidos. En principio utiliza grupos de direcciones las cuales permiten a los receptores recibir el mismo flujo de datos que ha sido transmitido sobre la red.

A diferencia de Unicast donde múltiple flujos de datos son enviados para cada receptor, Multicast provee un mayor uso eficiente de los recursos de la red, optimizando el uso del ancho de banda.

El desarrollo de nuevas aplicaciones que involucran sistemas de comunicación entre múltiples destinos requiere la implementación de este tipo de redes. El flujo de datos de estas comunicaciones puede corresponder a video o audio, que si se utilizara una comunicación tradicional unicast, podría ocasionar problemas de congestionamiento utilizando en un porcentaje mayor la capacidad del canal que si se utilizara una comunicación vía multicast.

Las comunicaciones generalmente se realizan entre puntos remotos, es decir que no se encuentren en la misma área local de red (LAN), siendo estrictamente necesario la utilización de IP Multicast para establecer una comunicación entre múltiples puntos, sin sufrir el deterioro de sus redes por el consumo de ancho de banda que estas aplicaciones requieren, además de la disminución de retardo entre punto y punto al tener un solo flujo que se dirija a todos los puntos receptores.

La creciente demanda de aplicaciones de comunicación entre múltiples puntos, ya no solo es utilizada para comunicarse entre cedes o entre diferentes redes que tienen acceso a Internet siendo este el medio por el cual se establece dicha conexión. Sino tiende a ser aplicada en la comunicación entre múltiples terminales que se encuentran en la misma red de área local (LAN), ya sea para transmitir un flujo de video o audio que solo un grupo de terminales tengan acceso, para establecer una video conferencia en la que participen múltiples usuarios para debatir sobre un tema, etc.

Dentro de la LAN donde el ancho de banda es significativamente mayor que el que se posee de conexión de salida al Internet, llevar a cabo una comunicación entre 'n' terminales de manera que se genere un flujo de datos por cada uno, esto multiplicado por el consumo de ancho de banda de la aplicación ya sea de transmisión de audio o video, ocasionaría un deterioro en el funcionamiento de la red y más aún en horas pico, por lo que implementar IP Multicast resulta beneficioso.

1.2 Planteamiento del Problema

En la actualidad las redes de área local (LAN), se han ido extendiendo cada vez más es decir ya no solo comprenden un edificio o pequeña zona de unos cuantos cientos de metros sino que pueden cubrir varios kilómetros, con la implementación de enlaces vía fibra óptica o radioenlaces, aumentando su tamaño y estableciendo puntos de conexión para más usuarios.

Todas las aplicaciones dentro de la LAN utilizan una comunicación punto a punto (Unicast), todos los dispositivos activos de red están configurados para soportar este tipo de tráfico filtrando el de otro tipo (tráfico broadcast y multicast).

El actual desarrollo de aplicaciones de comunicación con soporte multicast permite llevar a cabo la transmisión de flujos de audio o video, el establecimiento de videoconferencias, etc. servicios que hoy en día llegan a ser bastante atractivos a la hora de ofertarlos y ponerlos operativos para el uso de ciertos usuarios o grupos que lo demanden o requieran.

El uso de estas aplicaciones es diverso, sin embargo el soporte de IP Multicast dentro de la LAN requiere un análisis de la infraestructura de red, ancho de banda en los enlaces que se maneja tanto a nivel de núcleo (backbone), así como de capa de distribución y acceso, además del equipo activo de red que soporte protocolos Multicast para ser configurado, para determinar la viabilidad de un ambiente LAN que pueda albergar este tipo de tecnología, o que equipo es requerido para dicho propósito.

Otro de los retos para la implementación de redes IP Multicast dentro de la LAN, es el estudio del software adecuado, que puedan funcionen como servidores, y también como aplicaciones cliente para la distribución de audio y video con soporte multicast. Siendo de preferencia que este software sea desarrollado bajo el concepto de software libre de manera que no se tenga que invertir en licencias para el número de clientes y servicios que generalmente en software propietario se tiene que adquirir incursionando en gastos para la empresa.

1.3. Objetivos

1.3.1 Generales

- Estudio de requerimientos técnicos para la implementación de redes IP Multicast en ambientes LAN.

1.3.2 Específicos

- Analizar los requisitos a nivel de recursos de red que un ambiente de LAN debe disponer para soportar aplicaciones IP Multicast.
- Definir las configuraciones necesarias sobre el equipo de red activo a nivel de Switches y Routers para el soporte IP Multicast, dentro de la LAN.
- Investigar el software necesario para el desarrollo de servicios de video streaming y de video conferencias multipunto.

1.4 Marco Teórico y Conceptual

1.4.1 Antecedentes

Las redes IP Multicast tiene su origen en 1992 a través de un experimento llamado MBONE (Red Troncal Multimedia), que consistía en crear una red multicast a través de Internet utilizando túneles, cuyo objetivo era ahorrar un importante porcentaje de ancho de banda para las aplicaciones multimedia, quedando en experimento debido a la dificultad que tenían las empresas proveedoras de Internet (ISP), para ofertar redes con soporte multidifusión IP.

En la actualidad empresas de servicios de televisión por red, o instituciones que disponen de una red local de múltiples usuarios usan la multidifusión IP para ofrecer

streaming de video y audio a alta velocidad a un grupo de hosts receptores, también ocupándose en otros casos para llevar a cabo video conferencias.

No obstante la implementación de estas redes se lo ha relegado más a nivel investigativo, por la complejidad que conlleva manejar tráfico multicast.

En la actualidad existen muchas aplicaciones de comunicación con soporte multicast, siendo comerciales o bajo software libre.

1.4.2 Marco Teórico

El streaming es una tecnología que permite emitir audio y video por la red, tanto en directo como en diferido, dicha tecnología permite emitir contenidos, reduciendo los costos que suponen emitirlos a través de otros medios, siendo ideal para sectores educacionales, empresariales y corporativos.

La tecnología de multidifusión IP enfocada en ambientes LAN, permite hacer uso del streaming, basando su funcionamiento en IGMP (Internet Group Management Protocol), para gestionar la pertenencia de un receptor o grupo, ejecutándose en cada una de las subredes donde se encuentran los receptores. De la misma manera existen otros protocolos que pueden ser usados y configurados para administrar las sesiones multicast. Los procesos y capacidades de esos protocolos son los que determinan la cantidad de retardo, escalabilidad y sobrecarga.

Los grupos de multidifusión IP definen como los miembros encuentran, se unen y se desconectan de sesiones multicast. La transmisión multicast involucra al direccionamiento multicast. Dentro de las configuraciones requeridas es posible

proveer de una variedad de niveles de calidad de servicio para cada uno de los miembros multicast.

Calidad de Servicio (QoS) es uno de los parámetros prioritarios para un funcionamiento deseado u óptimo en los sistemas de comunicaciones. Calidad de servicio en ambientes multicast puede ser administrado o manejado a través de la asignación de ancho de banda, reservación de recursos y controles basados en clases.

Las sesiones multicast pueden usar mecanismos de seguridad para asegurar que los administradores puedan configurar árboles multicast, donde sólo los usuarios propietarios podrían tomar y decodificar el medio multicast.

1.4.3 Marco Conceptual

Los conceptos más importantes que se van a utilizar en la tesis son:

Broadcast:

Es un modo de transmisión de información, donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.

Equipo activo de red:

Son todos los dispositivos que permiten establecer conexiones de manera que se pueda transmitir información dentro de los puntos o terminales que se encuentren asociados a la red. Los dispositivos que forman parte del equipo activo de red son los switches y routers.

IGMP:

Protocolo de administración de grupos de Internet, es utilizado para intercambiar información acerca del estado de pertenencia entre enrutadores IP que soportan multidifusión y miembros de grupos de multidifusión. Los receptores individuales informan acerca de su pertenencia al grupo de multidifusión y los enrutadores de multidifusión monitorean periódicamente el estado de la pertenencia.

Multidifusión IP:

Es el envío de información en una red computadoras a múltiples destinos simultáneamente, usando la estrategia más eficiente para el envío de información sobre cada enlace de red sólo una vez, y creando copias cundo los enlaces en los destinos se dividen.

Multicast:

Denominado también como multidifusión, es el envío de información en una red a múltiples receptores, de forma simultánea, un emisor envía un mensaje y son varios los receptores que reciben el mismo.

LAN:

Red de área local, es la interconexión de varias computadoras dentro de un área limitada físicamente a un edificio, campus universitario etc.

QoS:

Calidad de Servicio, son las tecnologías que garantizan la transmisión de la información en un tiempo dado, de modo que se provea de un buen servicio.

Software libre:

Es la libertad de los usuarios sobre un producto adquirido y, por tanto, una vez obtenido puede ser usado, copiado, estudiado, cambiado y redistribuido libremente.

Unicast:

Se hace referencia al envío de paquetes desde un único emisor a un único receptor. Es la forma predominante de transmisión en Internet.

1.5 Hipótesis

La realización de estudios para la implementación de redes IP multicast en ambientes LAN, permitirá establecer servicios de video streaming y video conferencia, sin deteriorar el funcionamiento de la red.

La utilización de software libre para la implementación de servidores de streaming permitirá ahorrar costos, dando un servicio útil para los interese de la empresa.

1.6. Operacionalización de la Investigación

1.6.1 Variables

Independiente

- Conceptos de Multidifusión IP.

Dependientes

- Topología de redes LAN.
- Recursos de red.
- Equipo activo de red.
- Problemas de configuración multicast.

1.6.2 Dimensión

Tecnológica

- Utilización de equipo activo de red con soporte multicast.
- Implementación de servicios de video streaming y videoconferencia.
- Uso eficiente de los recursos de red.
- Utilización de software libre para la implementación de servidores de streaming y videoconferencia.

Económica

- Baja inversión para llevar a cabo su implementación.

1.6.3 Indicadores

- *Equipo activo de red*

  Versiones de sistemas operativos que soporten trafico multicast.

- *Red de área local*

  Recursos de red.

  Topología de red.

- *Servicios*

Video streaming.

Video conferencia.

- *Inversión*

  Baja a nivel software y reutilización de equipo activo de red ya existente.

1.6.4 Universo y/o muestra

El objeto de la tesis es el estudio de requerimientos técnicos de ambientes LAN para la implementación de servicios que utilicen multicast.

1.7. Procedimiento Marco Metodológico

1.7.1 Metodología.

El método a utilizar en el tema propuesto es el deductivo, partiendo de conocimientos y conceptos generales válidos, se llegará a formular una conclusión de tipo particular.

1.7.2 Técnicas

Se utilizarán las siguientes técnicas:

- Investigación Bibliográfica.
- Investigación en Internet.
- Análisis.
- Observación.
- Validación de lo investigado utilizando laboratorios virtuales

CAPÍTULO 2

FUNDAMENTOS TEÓRICOS

2.1 Introducción a IP Multicast

El espectro de comunicaciones IP, tiene por un lado la comunicación IP unicast, donde un host IP origen envía paquetes a un host específico, destino IP. En este caso la dirección destino en el paquete IP es una sola dirección de un único host en toda la red. Los paquetes IP son enviados a través de la red desde el host origen al host destino por routers. Los routers en cada punto a lo largo del enlace entre la fuente y el destino usa su Base de información de Ruteo (RIB, Routing Information Base) unicast, para realizar decisiones de reenvío basadas en la dirección IP destino en el paquete.

Por otro lado, al otro extremo de la comunicación IP unicast, está la de broadcast IP, donde un host fuente envía paquetes a todos los host IP sobre un segmento de red. La dirección destino de un paquete IP broadcast tiene los bits de la porción de host de la dirección destino puestos todos en uno, y los bits de la porción de red puestos la dirección de la subred, tal como se muestra en la Fig. 2.1.

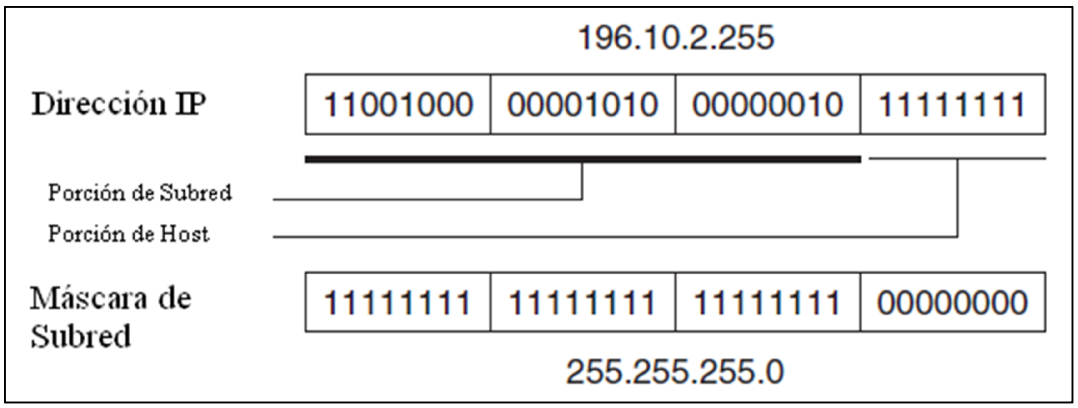


Fig. 2.1 [D]; Dirección Broadcast

Los hosts IP, incluidos los routers, entienden los paquetes que contienen como destino una dirección IP broadcast, estos son direccionados a todos los hosts IP sobre la subred. A menos que una configuración específica señale lo contrario, los routers no

reenvían paquetes IP broadcast, de manera que la comunicación IP broadcast es normalmente limitada a la subred local, tal como se muestra en la Fig. 2.2.

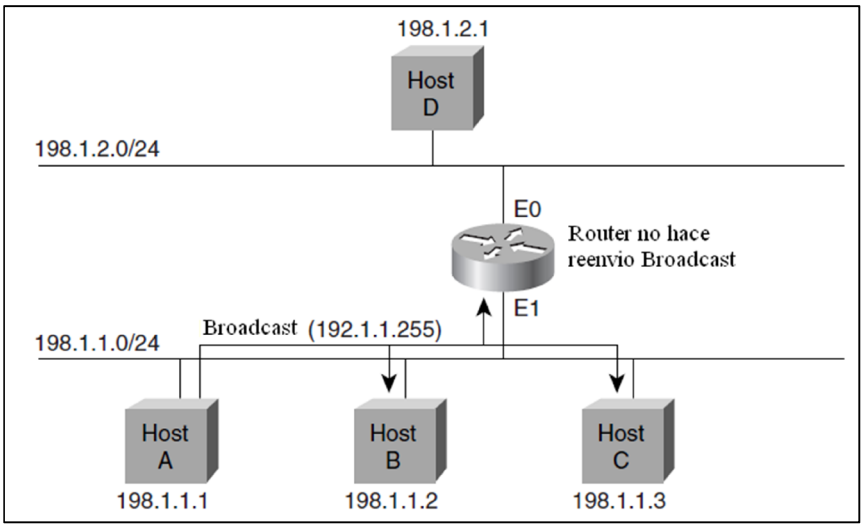


Fig. 2.2 [D]; Ejemplo de comunicación IP broadcast sobre una red

En el gráfico el host A envía un broadcast a la subred local 198.1.1.0/24, como el host B y el host C están sobre la misma subred, ellos reciben el broadcast, no así el host D que se encuentra sobre otra subred 198.1.2.0/24, porque el router no reenvía el broadcast. Si los routers reenviaran esos broadcast se produjeran bucles de rutas comúnmente llamados tormentas de broadcast.

Si el objetivo de una comunicación es permitir a un host enviar paquetes IP a otros host que no se encuentren sobre la misma subred local, entonces el IP broadcasting no es suficiente para llevar a cabo esta tarea.

IP multicasting cae entre la comunicación IP unicast e IP broadcast, y permite a un host enviar paquetes IP a un grupo de hosts en cualquier lugar que se encuentren dentro de la red IP. Para realizar esta tarea la dirección destino en un paquete IP

multicast, es una forma especial de dirección IP llamada grupo de direcciones multicast IP. Los routers IP multicast deben reenviar los paquetes entrantes IP multicast, afuera de todas las interfaces que conducen a los miembros del grupo IP multicast. El grupo de direcciones IP multicast está especificado en el campo de dirección destino del paquete.

2.1.1 Comunicaciones Multipunto

El envío de señales a múltiples usuarios requiere el uso de una combinación de servicios unicasting, broadcasting, anycasting o multicasting, que se denomina comunicaciones multipunto.

Unicasting.- transmite canales de comunicación a un número de usuarios a través del uso de un canal separado para cada usuario, cada canal puede ser configurado, administrado y desconectado separadamente bajo el control del host servidor. Si se usa para proveer servicios broadcast o multicast, una sesión de comunicación separada debe ser establecida y administrada entre cada usuario o cliente y el proveedor broadcast o servidor de comunicaciones.

En la Fig. 2.3 se muestra una distribución multipunto que puede ser desarrollada usando una comunicación unicast. Cada cliente debe crear una conexión unicast separada directamente al servidor de comunicaciones. Esto quiere decir que cada conexión (usuarios) es añadida. El servidor de comunicaciones y los routers cercanos a la fuente deben ser capaces de transportar simultáneamente todas las conexiones.

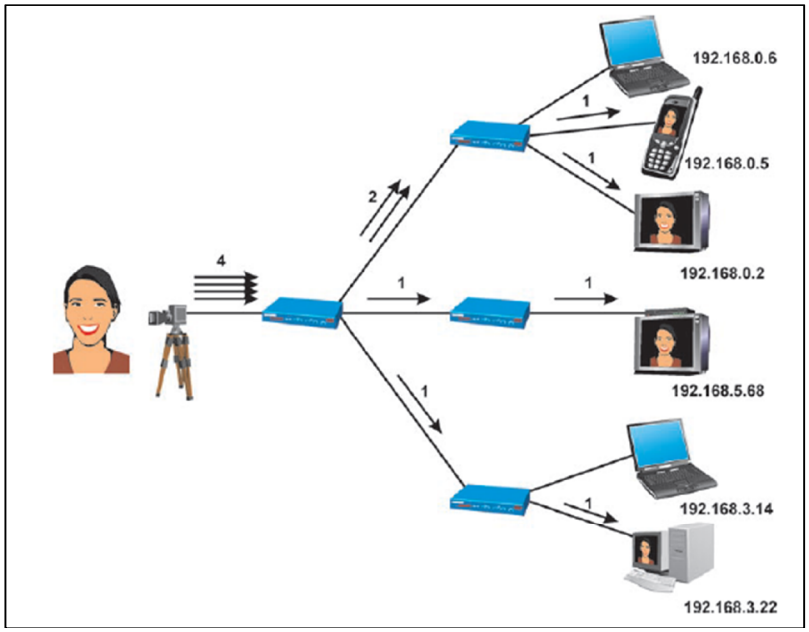


Fig. 2.3 [D]; Ejemplo de Comunicación Multipunto Unicast

Broadcasting.- es el proceso para enviar señales de voz, datos o video simultáneamente a un grupo de personas o compañías en un área geográfica específica o a quienes puedan conectar o recibir señales desde un sistema de red broadcast como el sistema satelital o el de televisión por cable. Broadcasting también es asociado con los sistemas de transmisión de radio y televisión que envían de igual manera señales de radio a muchos receptores en un área geográfica determinada.

El sistema de transmisión broadcast no sabe o no tiene cuidado sobre quien está interesado en recibir los paquetes, así cada paquete es distribuido a cada receptor sin importar si ellos desean recibir los datos o no.

En la Fig. 2.4 se muestra una distribución multipunto que puede ser desarrollada utilizando una transmisión broadcast. Cada router en la red de datos debe recibir paquetes desde una conexión de subida, copiar cada paquete y los paquetes en la

dirección de bajada. Cada router en la red de datos recibe paquetes, copia los paquetes y envía los paquetes hasta que estos alcancen todos los clientes en el sistema.

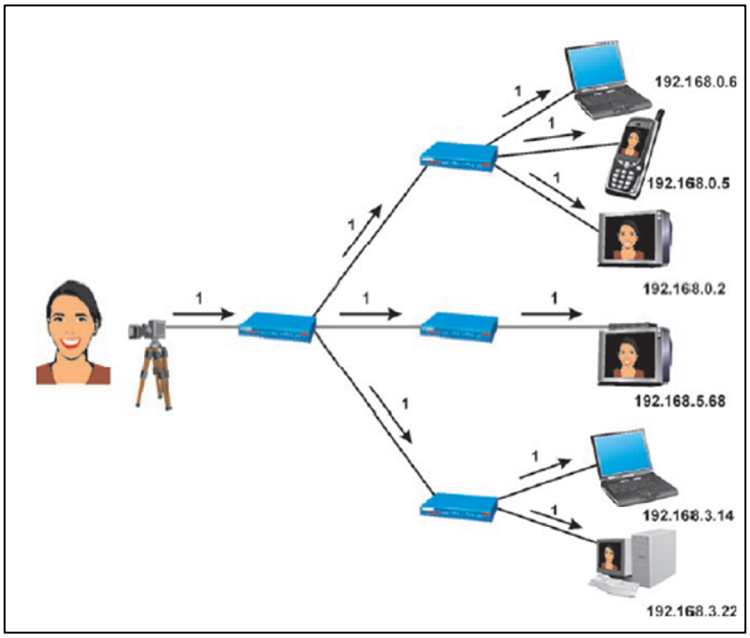


Fig. 2.4 [B]; Ejemplo de Comunicación Multipunto Broadcast

Anycasting.- es el proceso de creación de conexiones de flujo de comunicaciones a la mejor o más cercana fuente. Mientras la distribución podría permitir a todos los usuarios encontrar y conectar a la fuente de comunicaciones, la estructura de árbol para un sistema anycast podría no ser la estructura de distribución más eficiente.

Cada router en la red de datos anycast debe recibir paquetes desde cualquier flujo multicast, copiar cada paquete y enviar los paquetes en la dirección de bajada. Cada cliente puede encontrar y conectar a cualquier enlace en el árbol de distribución.

En la Fig. 2.5 muestra como la distribución multipunto puede ser desarrollada utilizando la transmisión anycast. Los clientes pueden encontrar y buscar una conexión

a un flujo multicast. En este caso la conexión no podría ser el enlace ideal o el más corto entre la fuente y el cliente.

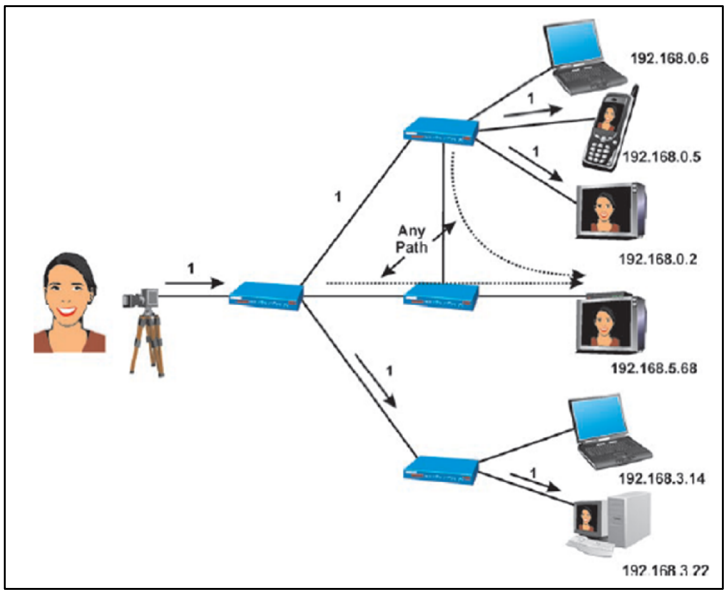


Fig. 2.5 [B]; Ejemplo de Comunicación Multipunto Anycast

Multicasting.- Es el proceso de transmisión de canales de comunicación a un número de usuarios a través del uso de canales distribuidos, según ellos vayan avanzando a través de la red. Usando un control de acceso al medio (MAC) o direccionamiento del protocolo de Internet (IP) multicast, múltiples usuarios finales podrían ajustar al mismo flujo de datos cuando este sea transmitido sobre la red.

Multicast provee un mayor uso eficiente de los recursos de la red, ya que los routers sólo reciben, copian y envían paquetes hacia sus destinatarios si hay clientes en los flujos de bajada del router.

La Fig. 2.6 muestra como una distribución multipunto puede ser desarrollada usando transmisiones multicast. Cada router en la red de datos que es parte del árbol de distribución multicast debe recibir paquetes desde las conexiones de subida y copiar

cada paquete en la dirección de bajada. Cada router en la red sólo recibe y envía paquetes si hay clientes multicast del flujo de bajada en el sistema.

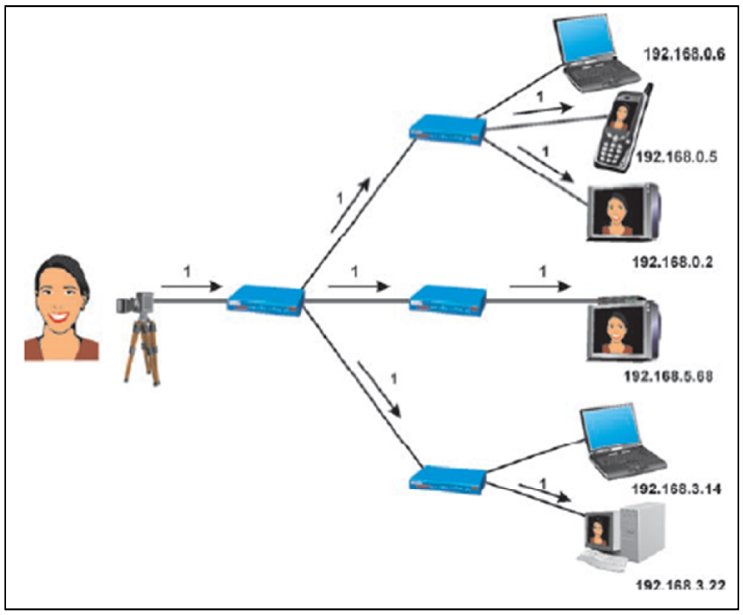


Fig. 2.6 [B]; Ejemplo de Comunicación Multipunto Multicast

2.1.2 Beneficios Multicast

El Internet y en muchos casos las intranets de muchas empresas han tenido un amplio crecimiento a nivel de usuarios conectados, de tal forma que un gran número de usuarios frecuentemente quieren acceder a la misma información en un mismo tiempo. Usando la técnica multicast IP para distribuir esta información puede a menudo reducir sustancialmente la demanda total de ancho de banda sobre la red. Un ejemplo de este enfoque es el rápido crecimiento en el área de audio y video en contenidos web.

A continuación se describen algunas de las ventajas del uso de IP multicast en aspectos como ancho de banda, carga en el servidor, carga sobre la red.

Ancho de Banda.- En una transmisión online de audio vía una técnica de compresión que requiere de 8kbps de flujo de datos para establecer la comunicación con el cliente, en la Fig. 2.7 la línea punteada muestra que cuando el número de clientes con conexiones unicast aumenta, la cantidad de ancho de banda de la red también aumenta linealmente. En la misma figura la línea sólida representa el uso de multicast en el mismo escenario de transmisión de audio, en donde un solo flujo de datos multicast de 8kbps puede entregar la transmisión a todos los clientes.

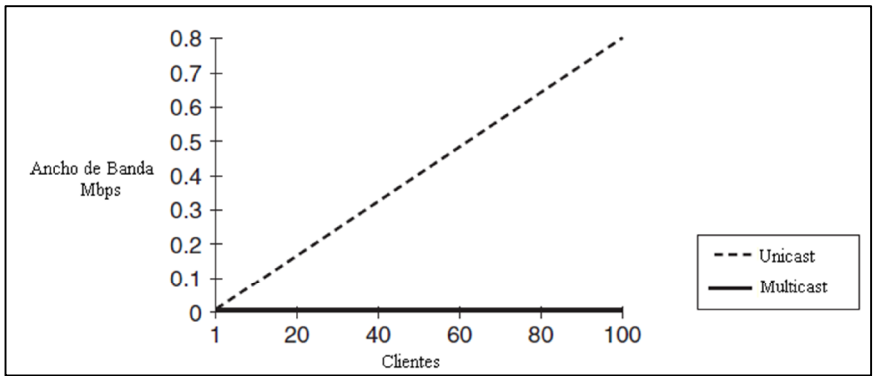


Fig. 2.7 [D]; Utilización Ancho de Banda para una transmisión de audio vía Unicast y Multicast

Si ahora se quisiera transmitir video, y se asume que se transmitirá con alta compresión y a una baja tasa de flujo de datos de video de 120kbps, más los 18kbps del flujo de datos de audio, la Fig. 2.8 muestra nuevamente que la utilización del método de conexión unicast para la entrega de los datos a los clientes, los requerimientos de ancho de banda continúan siendo elevados en comparación si se utilizara multicast.

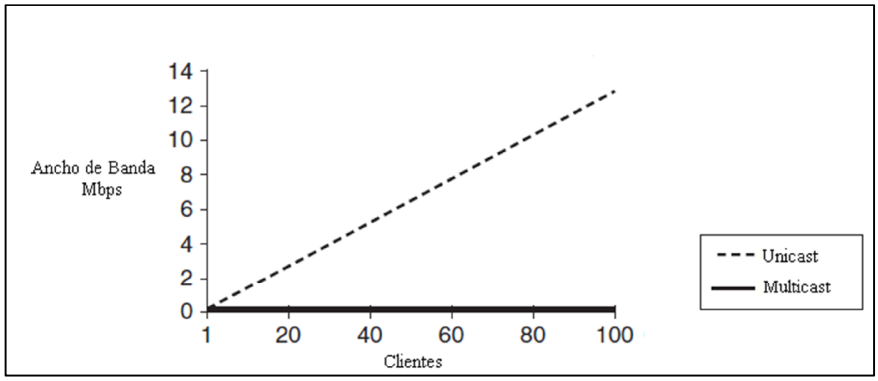


Fig. 2.8 [D]; Utilización Ancho de Banda para una transmisión de audio y video vía Unicast y Multicast

Carga en el Servidor.- En la transmisión online de audio descrita anteriormente, si se mantiene el uso de unicast como mecanismo para establecer la comunicación con el cliente, esto implicaría que para continuar con el servicio se necesitará incrementar la capacidad y el número de servidores de audio en tiempo real, para soportar el incremento de número de clientes conectados.

Si el número de clientes conectados se incrementa, la carga sobre el servidor también se incrementara, hasta que en algún punto, el servidor sea incapaz de establecer desde la fuente el flujo de 8kbps de velocidad de datos necesarios para entregar una comunicación de audio sin cortes. Esta es una situación clásica de éxito o falla, en la cual el servicio ofertado es satisfactorio hasta que este excede la capacidad de la tecnología o infraestructura de red para mantener la demanda.

Si se utiliza IP multicast como mecanismo de comunicación en este caso la transmisión online de audio, un solo flujo de datos en tiempo real será necesaria para establecer la entrega de datos a todos los clientes conectados, de esta manera no se tendrá que incurrir en gastos en el incremento de recursos y número de servidores cuando el número de clientes crezca.

Carga sobre la red.- Como IP multicast puede significativamente reducir los requerimientos de ancho de banda, cuando se entrega el mismo contenido a múltiples clientes, la reducción en el consumo de ancho de banda debería igualar a una reducción en la carga ocupada sobre los routers en la red. Esto resulta ser cierto, pero es importante notar que, en algunos casos, la sobrecarga de trabajo en el router puede incrementarse en ciertos puntos en la red.

En la Fig. 2.9 se muestra que el primer salto del router (el router conectado directamente al servidor), está recibiendo un solo flujo de datos desde el servidor. Nótese también que el primer salto del router está replicando el flujo de datos en dos flujos de datos de salida así para entregar los datos a los clientes en el flujo de bajada. El proceso de replicación ocupa una carga de trabajo adicional sobre el router, el cual debe ser considerado en el diseño de toda la red. Si un router no tiene un eficiente mecanismo de replicación, la carga en el router puede incrementarse significativamente cuando el número de interfaces de salida es alto.

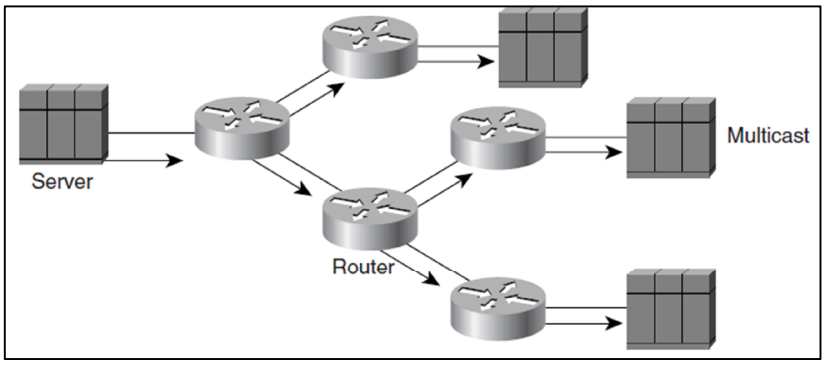


Fig. 2.9 [D].- Flujo de datos multicast

Nuevas versiones de código de envío multicast evita el proceso de duplicación por encolamiento y punteros a los datos en el paquete original a cada interfaz de salida, así

permite a cada interfaz compartir el mismo buffer de datos. Esto elimina virtualmente la necesidad de replicar los datos para cada interfaz de salida y significativamente reduce los recursos de CPU y memoria necesarios para enviar el paquete multicast.

2.1.3 Debilidades Multicast

Aunque hay un número de buenas razones para mantener el uso de IP multicast en las redes, se tiene que tener en mente que hay limitaciones y desventajas para esta tecnología. Limitaciones que deben ser claramente entendidas, particularmente si se está desarrollando nuevas aplicaciones que contemplen el uso de IP multicast.

Algunos de los principales inconvenientes asociados con la implementación de un sistema IP multicast incluye la entrega de paquetes no fiable, duplicación de paquetes y congestión de red.

Entrega de paquetes no fiable.- IP multicast como IP unicast son inherentemente no fiables. Los flujos de datos IP unicast sólo a través del uso de TCP en capa 4 (o algunos protocolos más altos) puede ser hecho fiable. Como IP multicast asume un modo de comunicación de uno a muchos, no fue diseñado para usar mecanismos de extremo a extremo inherentes en TCP. Los paquetes IP multicast usan típicamente el Protocolo de Datagrama de Usuario (UDP), el cual es por naturaleza el de mejor esfuerzo. De esta manera una aplicación que utiliza IP multicast debe esperar ocasionalmente una pérdida de paquetes y estar preparado, ya sea para aceptar la pérdida o de alguna manera mantener esta en la capa de aplicación o vía un protocolo multicast fiable de capa superior a UDP.

Según estudios realizados se ha determinado que en los periodos cuando los enlaces están siendo cambiados inmediatamente seguido de un cambio de topología, los paquetes multicast que resultan estar en tránsito tienen una probabilidad menor de alcanzar sus destinos que los paquetes unicast. Incluso si el reenvío de información errónea unicast existe en algunos routers en la red durante el cambio de topología, la red podría eventualmente entregar satisfactoriamente el paquete al destino. La razón de que esto suceda es que el mecanismo de reenvío unicast continúa intentando enviar el paquete a través de la dirección destino mientras la topología de red está en transición, aunque el enlace actual resulte ser algo complicado. El mecanismo de reenvío de IP multicast, de manera opuesta, está basado sobre la dirección IP origen, y previene lazos, de esta manera el paquete es descartado si no llega sobre la interfaz que podría conducirlo de regreso a la fuente.

Duplicación de Paquetes.- Los paquetes duplicados, al igual que en el mundo de IP unicast, son un factor de vida. Sin embargo la diferencia entre el ruteo unicast y multicast es que los routers intencionalmente envían copias de un paquete multicast sobre múltiples interfaces de salida. Esto incrementa la probabilidad que múltiples copias del paquete multicast puedan arribar a un receptor.

Congestión de Red.- En el caso de TCP unicast, el estándar backoff y los mecanismos de ventana de comienzo despacio, ajustan automáticamente la velocidad de la transferencia de datos y por lo tanto provee un grado de evasión de congestión dentro de la red. Como IP multicast no puede utilizar TCP, debido a que no es orientado a la conexión y su naturaleza de uno a muchos, no puede incorporar un mecanismo para

evitar la congestión, para prevenir que un flujo multicast agote el ancho de banda del enlace u otros recursos críticos del router. Se debe tener en cuenta que los flujos de datos UDP unicast sufren los mismos problemas para evitar la congestión, además el crecimiento en popularidad de aplicaciones multimedia de audio y video, ambas sobre la Internet y dentro de las intranets privadas está incrementando la cantidad de tráfico UDP unicast.

2.1.4 Aplicaciones Multicast

No es poco común para la gente pensar en IP multicast y video conferencias como casi la misma cosa, aunque la primera aplicación a ser usada sobre una red IP multicast habilitada es a menudo la videoconferencia, el video solo es una de muchas aplicaciones IP multicast que pueden añadir valor al modelo de negocios de una compañía.

Aplicaciones como la misma conferencia multimedia, replicación de datos, datos multicast en tiempo real, juegos y simulación de aplicaciones, tienen el potencial para mejorar la productividad.

Conferencia Multimedia.- Las conferencias de audio y video es una forma interesante de comunicarse a través de la red. Pero esto suele resultar desalentador cuando el ancho de banda y la potencia de las estaciones de trabajo son consumidas por la conferencia de video, sobre todo si todos se abastecen del video al mismo tiempo, dado este resultado no es poco común ver sólo audio conferencias que lleguen a ser el modo normal. Adicionalmente si una conferencia de audio se combina con un direccionamiento IP multicast basado en el intercambio de datos de

aplicaciones, como la aplicación de una pizarra, que permite a los miembros compartir información gráfica, el resultado es una forma muy potente de las conferencias multimedia que no consume mucho ancho de banda.

Distribución de Datos.- La replicación de datos es otra área de las aplicaciones IP multicast que ha llegado a ser rápidamente muy populares. Los departamentos están adoptando un modelo de inserción de archivos y actualizaciones de bases de datos, utilizando un producto denominado MFTP que permite la entrega segura de archivos y datos a grupos de nodos de la red. Como su nombre lo indica, este producto es como una forma de FTP multicast, donde uno o más archivos pueden ser enviados simultáneamente con FTP a un grupo de nodos en la red pero usando IP multicast.

Datos en tiempo real Multicast.- La entrega de datos en tiempo real a grandes grupos de hosts es otra área de IP multicast, un ejemplo de esta necesidad es la entrega de información de acciones a las estaciones en salas de comercio, de establecimientos financieros y de inversión donde el tiempo de entrega de información resulta ser crucial para la toma de decisiones.

Juegos y Simulaciones.- IP multicast se adapta muy bien para su uso en juegos en red o aplicaciones de simulación. Muchos juegos de PC y simulaciones permiten a los grupos de jugadores en red luchar entre sí, en combates aéreos simulados u otros ambientes de fantasía, virtualmente todas esas aplicaciones hacen uso de unicast y conexiones punto a punto.

2.2 Funcionamiento Multicast

2.2.1 Direccionamiento Multicast

A diferencia del direccionamiento IP unicast que únicamente identifica a un solo host IP, el direccionamiento IP multicast determina a un grupo arbitrario de hosts IP, que se han unido al grupo y que desean recibir el tráfico enviado a este grupo.

Direcciones IP Clase D.- Las direcciones IP multicast han sido asignadas al viejo espacio de direcciones clase D, por el Número de Autoridad de Asignación (IANA). Las direcciones en este espacio son denotadas con un prefijo binario 1110 en los cuatro primeros bits del primer octeto, como se muestra en la Fig. 2.10. De esta manera el rango de direcciones IP multicast va desde 224.0.0.0 hasta 239.255.255.255.

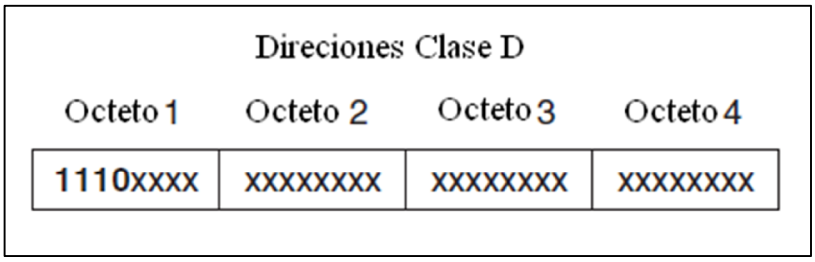


Fig. 2.10 [D]; Formato de Direcciones Multicast

Direcciones Multicast Asignadas.- IANA controla la asignación de direcciones multicast, por lo que antes de buscar un bloque de direcciones IP multicast para usar, es necesario entender que este espacio de direcciones es un recurso limitado. Por tal razón, IANA es muy renuente a asignar las direcciones IP multicast a menos que exista una justificación para hacerlo. Esto no quiere decir que IANA asigna bloques de direcciones para uso personal, sino que generalmente no asigna individualmente direcciones IP multicast a nuevos programas de aplicaciones sin una justificación

técnica realmente buena, en lugar de aquello, tiende asignar individualmente direcciones IP multicast para el uso específico de protocolos de red. Esto significa que toda la Internet debe compartir el rango de direcciones restantes IP multicast no asignadas con algún método dinámico de cooperación. Esta situación permite a las direcciones multicast ser asignadas o arrendadas cuando sea necesario y luego liberada para su uso por otras personas cuando la dirección ya no sea utilizada.

La tabla 2.1 muestra los rangos de direcciones IP multicast dedicadas para propósitos especiales:

Rango	Propósito
224.0.0.0 a 224.0.0.255	Reservada para direcciones de Enlace Local
224.0.1.0 a 238.255.255.255	Direcciones de Ámbito Global
232.0.0.0 a232.255.255.255	Direcciones Multicast de Fuente Específica
233.0.0.0 a 233.255.255.255	Direcciones GLOP
239.0.0.0 a 239.255.255.255	Direcciones de Ámbito Administrativo

Tabla 2.1 [A]; Rangos de direcciones IP multicast con propósito especial

Direcciones Multicast de Enlace Local.- IANA ha reservado el rango de direcciones de 224.0.0.0 hasta 224.0.0.255, para el uso de protocolos de red sobre un segmento de red local. Los paquetes con una dirección en este rango son de alcance local, no son enviadas por los routers IP (sin tener en cuenta el valor de su tiempo de vida TTL), y de esta manera no vaya más lejos de la red local.

La tabla 2.2 muestra una lista parcial de direcciones multicast reservadas, con la función de protocolo de red por la cual haya sido asignada y la persona que solicito la dirección o el RFC asociado con el protocolo.

Direción	Uso	Referencia
224.0.0.1	All Hosts	[RFC 1112, JBP]
224.0.0.2	All Multicast Routers	[JBP]
224.0.0.3	Unassigned	[JBP]
224.0.0.4	DVMRP Routers	[RFC 1075, JBP]
224.0.0.5	OSPF Routers	[RFC 1583, JXM1]
224.0.0.6	OSPF Designated Routers	[RFC 1583, JXM1]
224.0.0.7	ST Routers	[RFC 1190, KS14]
224.0.0.8	ST Hosts	[RFC 1190, KS14]
224.0.0.9	RIP2 Routers	[RFC 1723, SM11]
224.0.0.10	IGRP Routers	[Farinacci]
224.0.0.11	Mobile-Agents	[Bill Simpson]
224.0.0.12	DHCP Server/Relay Agent	[RFC 1884]
224.0.0.13	All PIM Routers	[Farinacci]
224.0.0.14	RSVP-Encapsulation	[Braden]
224.0.0.15	All CBT Routers	[Ballardie]
224.0.0.16	Designated-SBM	[Baker]
224.0.0.17	All SBMS	[Baker]
224.0.0.18	VRRP	[Hinden]
224.0.0.19 to 224.0.0.255	Unassigned	[JBP]

Tabla 2.2 [D]; Direcciones Multicast de Enlace Local

Direcciones de Ámbito Global.- IANA asigna típicamente solo solicitudes de direcciones IP multicast para protocolos de red o aplicaciones de red fuera del rango de direcciones 224.0.1.xxx. Los routers multicast si realizan el envío de este rango de direcciones multicast.

La tabla 2.3 muestra una lista parcial de direcciones multicast asignadas a protocolos de red o aplicaciones de red, con la función de protocolo de red por la cual haya sido asignada y la persona que solicito la dirección o el RFC asociado con el protocolo.

Dirección	Uso	Referencia
224.0.1.0	VMTP Managers Group	[RFC 1045, DRC3]
224.0.1.1	NTP-Network Time Protocol	[RFC 1119, DLM1]
224.0.1.2	SGI-Dogfight	[AXC]
224.0.1.3	Rwhod	[SXD]
224.0.1.6	NSS-Name Service Server	[BXS2]
224.0.1.8	SUN NIS+ Information Service	[CXM3]
224.0.1.20	Any Private Experiment	[JBP]
224.0.1.21	DVMRP on MOSPF	[John Moy]
224.0.1.32	Mtrace	[Casner]
224.0.1.33	RSVP-encap-1	[Braden]
224.0.1.34	RSVP-encap-2	[Braden]
224.0.1.39	Cisco-RP-Announce	[Farinacci]
224.0.1.40	Cisco-RP-Discovery	[Farinacci]
224.0.1.52	Mbone-VCR-Directory	[Holfelder]
224.0.1.78	Tibco Multicast1	[Shum]
224.0.1.79	Tibco Multicast2	[Shum]

Tabla 2.3 [D]; Direcciones Multicast de Ámbito Global

Direcciones Multicast de Fuente Específica (SSM).- Se utiliza con IGMPv3 para permitir una solicitud de un receptor multicast, no sólo para pertenecer a un grupo, sino también para solicitar fuentes específicas para recibir tráfico de ellas. Por lo tanto, en un entorno de SSM, múltiples fuentes con diferentes contenidos pueden todas ser enviadas a la misma dirección destino multicast.

Direcciones GLOP.- Proporciona un rango de direcciones multicast único a nivel mundial basado sobre el número de sistema autónomo (AS). Por ejemplo, si el sistema autónomo de una empresa es AS 65000, su rango mundial único de direcciones IP multicast podría ser 233.253.232.0 a 233.253.232.255. El número AS

calcula el segundo y tercer octeto en este rango de direcciones. Primero se convierte el número de AS en hexadecimal, del ejemplo la empresa con AS 65000 en decimal equivale a FD-E8 en hexadecimal, FD equivale a 253 en decimal y E8 equivale a 232 en decimal. El primer octeto de una dirección GLOP es siempre 233.

Direcciones de Ámbito Administrativo.- IANA ha reservado el rango de 239.0.0.0 al 239.255.255.255 como ámbitos administrativos para uso en dominios multicast privados. El uso de este rango de direcciones IP multicast es de libre uso dentro de un dominio sin temor a entrar en conflicto con otros en otras partes sobre la Internet. El uso de este rango de direcciones también ayuda a conservar el limitado espacio de direcciones IP multicast, porque estas pueden ser rehusadas en diferentes regiones de la red. Cuando se use este rango de direcciones se debe configurar los routers multicast para asegurar que el tráfico multicast en este rango de direcciones no se cruce dentro o fuera de su dominio multicast.

2.2.2 Direccionamiento MAC Multicast

La especificación original Ethernet (estandarizada por la IEEE) tomó medidas para la transmisión de paquetes broadcast y/o multicast. Como se muestra en la Fig. 2.11, el bit 0 del octeto 0 en una dirección MAC IEEE indica si la dirección de destino es una dirección broadcast/multicast o una dirección unicast.

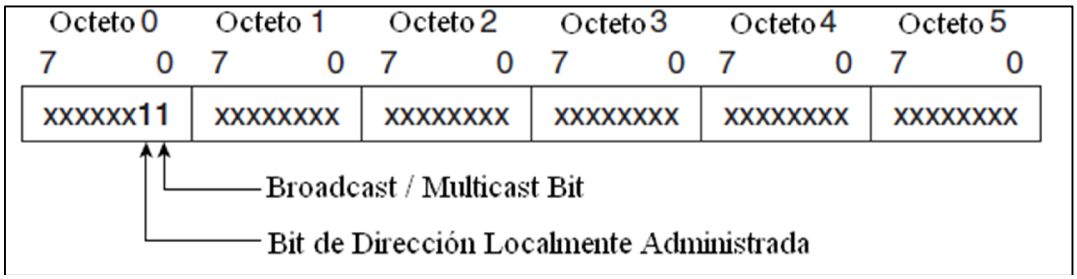


Fig. 2.11 [A]; Formato de dirección MAC IEEE 802.3

Si este bit es puesto en uno, entonces la trama MAC es destinada ya sea para un grupo arbitrario de hosts o todos los hosts sobre la red (Si la dirección MAC de destino es la dirección broadcast se vería así 0xFFFF.FFFF.FFFF.FFFF). IP multicast en capa 2 hace uso de esta capacidad para transmitir paquetes IP multicast a un grupo de hosts sobre un segmento LAN.

A continuación se determina como las direcciones IP multicast capa 3 son mapeadas dentro de las direcciones MAC IEEE para Ethernet.

Mapeo de direcciones MAC Multicast Ethernet.- Todas las tramas IP multicast usan direcciones de la capa MAC, comenzando con el prefijo de 24 bits 0x0100.5Exx.xxxx. Desafortunadamente, sola la mitad de esas direcciones MAC están disponibles para el uso de IP multicast. Esto deja 23 bits de espacio de direccionamiento MAC para el mapeo de capa 3 IP multicast dentro del direccionamiento MAC de capa 2. Como todas las direcciones IP multicast de capa 3 tienen los primeros 4 bits de los 32, puestos a 0x1110, esto deja 28 bits de información significativa de direcciones IP multicast. Estos 28 bits deben mapearse dentro de sólo 23 bits disponibles del direccionamiento MAC. La Fig. 2.12 muestra el proceso de mapeo.

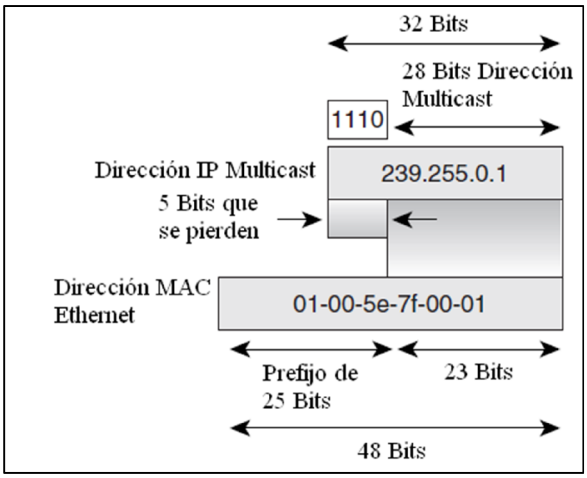


Fig. 2.12 [D]; Mapeo de direcciones MAC Multicast Ethernet

Impacto del rendimiento del Mapeo de direcciones MAC.- Como todos los 28 bits de información de direcciones de capa 3 IP multicast no pueden ser mapeados dentro de los 23 bits disponibles del espacio de direcciones MAC, 5 bits de información de la dirección se pierden en el proceso de mapeo. Esto resulta en 2^5 ó 32:1 direcciones ambiguas cuando una dirección IP multicast de capa 3 es mapeada a una dirección de capa 2 MAC IEEE. Lo que significa que cada dirección MAC IEEE multicast puede representar 32 direcciones IP multicast, como se muestra en la Fig. 2.13.

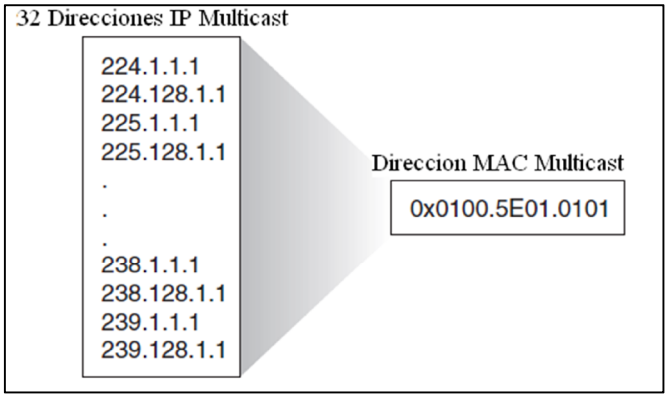


Fig. 2.13 [D]; Ambigüedad de la dirección MAC Multicast

Esta ambigüedad de 32 direcciones IP multicast a 1 dirección MAC multicast puede causar algunos problemas. Por ejemplo si un host que quiere recibir información del grupo multicast 224.1.1.1 programará los registros de hardware en la tarjeta de interfaz de red (NIC) para interrumpir el CPU cuando una trama con una dirección destino MAC multicast 0x0100.5E01.0101 sea recibida. Desafortunadamente, esta dirección MAC multicast es también utilizada para otros 31 grupos IP multicast. Si cualquiera de esos otros 31 grupos está también activos sobre la red local LAN, los CPU de los hosts recibirán interrupciones en cualquier momento que una trama sea recibida para cualquiera de esos grupos, provocando que el CPU tenga que examinar la

porción IP de cada trama recibida para determinar si este es su grupo configurado, el cual en el ejemplo es 224.1.1.1. Teniendo un impacto en la disponibilidad del CPU de los hosts si la cantidad de tráfico de los grupos es lo suficientemente alta.

Esta ambigüedad también puede tener un impacto negativo sobre la disponibilidad de los CPU de los hosts, cuando se trata de limitar las inundaciones multicast en los switch LAN de capa 2 basados únicamente sobre esa dirección MAC multicast.

2.2.3 Árboles de distribución Multicast

Para entender el modelo IP multicast, se debe tener un buen conocimiento sobre los árboles de distribución multicast. En el modelo unicast, el tráfico es ruteado a través de la red a lo largo de un único enlace desde la fuente al host destino. En el modelo multicast, sin embargo, la fuente está enviando tráfico a un grupo arbitrario de hosts que están representados por una dirección de grupo multicast.

Para la entrega de tráfico a todos los receptores multicast, los árboles de distribución multicast son usados para describir el enlace que el tráfico IP multicast toma a través de la red. Hay dos tipos básicos de árboles de distribución multicast que son árboles fuente y árboles compartidos.

Árboles Fuente.- La forma más simple de un árbol de distribución multicast es un árbol fuente cuya raíz es el origen del tráfico multicast y cuyas ramas forman un árbol de expansión a través de la red a los receptores. Como este árbol utiliza el camino más corto a través de la red, es también conocido como árbol de camino más corto (SPT).

En la Fig. 2.14 se puede apreciar un ejemplo de SPT para el grupo 224.1.1.1 arraigado a la fuente, host A, y conectado a dos receptores, host B y C.

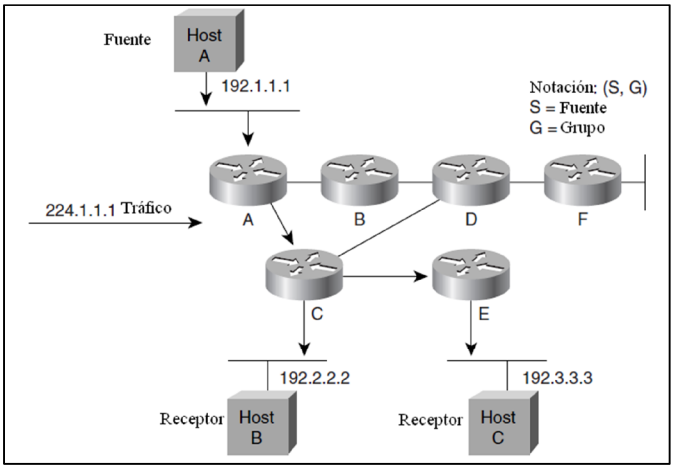


Fig. 2.14 [D]; Árbol de camino más corto Host A

Árboles Compartidos.- A diferencia de los árboles fuente que tienen sus raíces en la fuente, los árboles compartidos usan un único lugar raíz en algún punto en la red. Dependiendo de los protocolos de ruteo multicast, esta raíz es a menudo llamada 'rendezvous point' (RP) o núcleo. Este tipo de árbol se los llama también: árboles RP (RPT) o árboles basados en el núcleo (CBT).

Cuando se usa árboles compartidos, las fuentes deben enviar su tráfico a la raíz para que el tráfico llegue a todos los receptores.

La Fig. 2.15 muestra un árbol compartido para el grupo 224.2.2.2 con la raíz localizada en el router D.

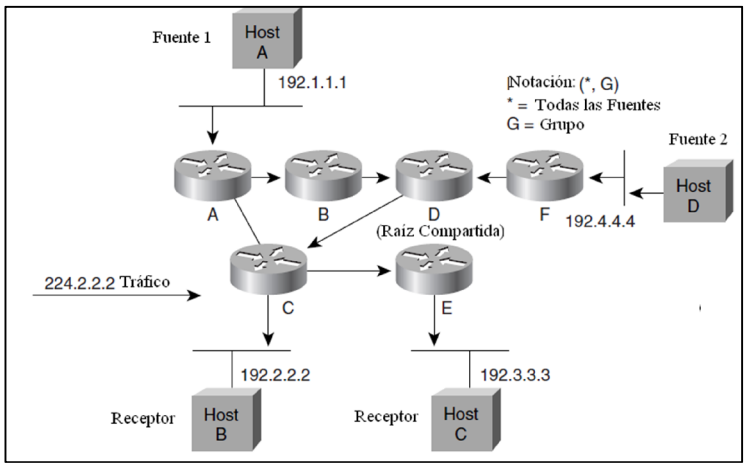


Fig. 2.15 [D]; Árbol de distribución Compartido

2.2.4 Reenvío Multicast

En el modelo unicast, los routers envían tráfico a través de la red a lo largo de un único enlace, el origen al host destino cuya dirección IP aparece en el campo de dirección destinatario del paquete IP. Cada router en el camino hace una decisión de reenvío unicast, usando la dirección IP destino en el paquete, buscando la dirección de destino en la tabla de rutas unicast y luego enviar el paquete al siguiente salto a través de la interfaz indicada hacia el destino.

En el modelo multicast, la fuente está enviando tráfico a un grupo arbitrario de hosts representado por una dirección multicast grupo en el campo de dirección destinatario del paquete IP. En contraste al modelo unicast, el router multicast no puede basar su decisión de reenvío sobre la dirección destino en el paquete. Los routers típicamente tienen que enviar los paquetes multicast por múltiples interfaces para que llegue a todos los receptores. Estos requerimientos hacen al proceso de reenvío multicast más complejo que el usado para el reenvío unicast.

Para entender el proceso de reenvío multicast es necesario revisar los conceptos de Reenvío de enlace inverso (RPF), y otros como cache de reenvío multicast, umbrales TTL y límites de ámbito administrativo.

Reenvío de enlace inverso.- Virtualmente todos los protocolos de ruteo IP multicast hacen uso de alguna forma de RPF, o chequeo de la interfaz entrante, como el mecanismo primario para determinar si envía o descarta un paquete multicast entrante. Cuando un paquete multicast arriba en un router, el router desarrolla una revisión RPF sobre el paquete. Si la revisión RPF es satisfactoria, el paquete es enviado caso contrario es descartado.

Para el tráfico que fluye a un árbol fuente, el mecanismo de revisión RPF trabaja de la siguiente manera:

1- El router examina la dirección origen del paquete multicast que arribó para determinar si llegó a través de una interfaz que está en el camino de retorno a la fuente.

2- Si el paquete arribó sobre la interfaz que conduce de regreso al origen, el mecanismo RPF revisa exitosamente esta condición y el paquete es enviado.

3- Si la condición del mecanismo RPF falla, el paquete es descartado.

Para que un router multicast determine cuál es la interfaz que conduce al enlace de regreso a la fuente, dependerá del protocolo de ruteo que se esté utilizando. En algunos casos, el protocolo de ruteo multicast mantiene una tabla de ruteo multicast separada y usa esta para el mecanismo de revisión RPF.

La Fig. 2.16 muestra el mecanismo de revisión RPF, en este ejemplo se utiliza una tabla de ruteo multicast separada, aunque el concepto es el mismo si la tabla de ruteo unicast o alguna otra tabla de accesibilidad son utilizadas, aquí la comprobación RPF falla, ya que la interfaz S0 no se encuentra sobre el camino de retorno a la fuente, por lo que el paquete es descartado.

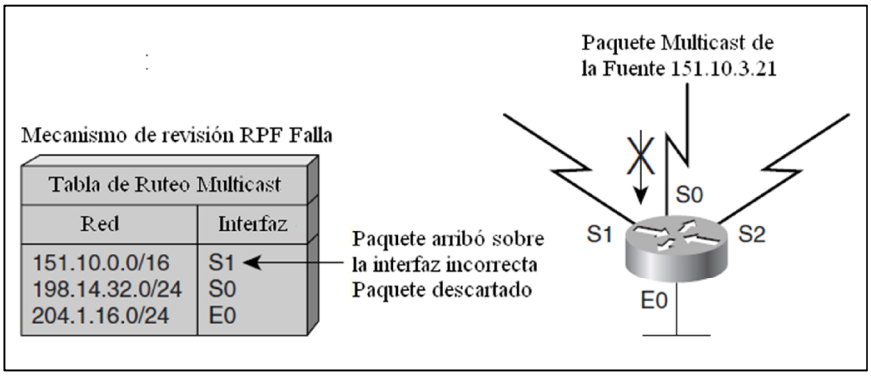


Fig. 2.16 [D]; Mecanismo de revisión RPF Falla

La Fig. 2.17 muestra otro ejemplo de mecanismo de revisión RPF, en este caso, la comprobación del RPF es satisfactoria ya que la interfaz S1 se encuentra en el camino de retorno a la fuente, y por lo tanto el paquete es enviado a todas las interfaces en la lista de ces de salida. Nótese también que las interfaces de salida no tienen que incluir necesariamente todas las interfaces del router.

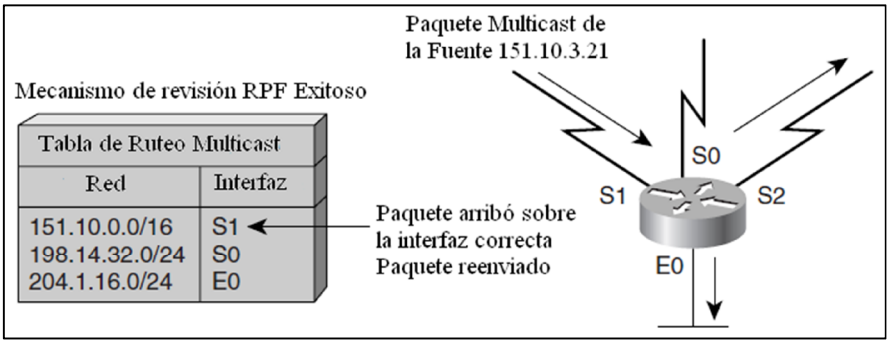


Fig. 2.17 [D]; Mecanismo de revisión RPF Exitoso

Cache de Reenvío Multicast.- Como se mencionó anteriormente en la sección de árboles de distribución multicast, el concepto de construcción de árboles de distribución multicast que son usados para enviar tráfico multicast a través de la red a todos los receptores. Desde el punto de vista del router, cada árbol fuente o árbol compartido puede ser representado en una entrada de cache de reenvío multicast (referida algunas veces como una entrada en la tabla de rutas multicast) como una interfaz entrante asociada con cero o más interfaces salientes.

Realizando la revisión RPF sobre cada paquete multicast entrante, resulta en un substancial deterioro del rendimiento sobre el router. Por lo tanto, es común para un router multicast determinar la interfaz RPF cuando la cache de reenvío multicast es creada. La interfaz RPF entonces llega a ser la interfaz entrante de la entrada de cache de reenvío multicast. Si un cambio ocurre en la tabla de ruteo utilizada por el

mecanismo de revisión RPF, la interfaz RPF debe ser recalculada y la entrada de la cache de reenvío multicast actualizada para reflejar esta información. Debe tenerse en cuenta que la interfaces salientes son determinadas de varias maneras dependiendo del protocolo de ruteo multicast en uso.

La Fig. 2.18 muestra una entrada de la tabla de ruteo multicast, obtenida del router de las Fig. 2.17 que describe (S,G) como (151.10.3.21/32, 224.2.127.254) SPT. Con esta información se puede ver que el router detecta una interfaz entrante Serial 1 y dos interfaces salientes Serial 2 y Ethernet 0.

```
(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
```

Fig. 2.18 [D]; Entrada de la tabla de ruteo multicast

Umbrales TTL.- Como se sabe que, cada vez que un paquete IP multicast es enviado por un router, el valor TTL en la cabecera IP es sustraído en uno. Si el valor TTL del paquete se disminuye a cero, el router descarta el paquete.

Los umbrales TTL pueden ser aplicados q interfaces individuales de un router multicast para prevenir paquetes multicast con un TTL menor que el umbral TTL para ser enviado a la interfaz. La Fig. 2.19 muestra un router multicast con varios umbrales TTL aplicados a sus interfaces.

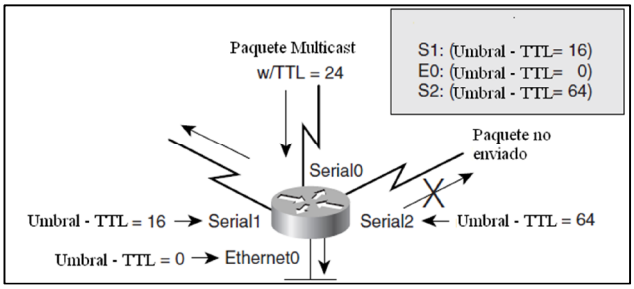


Fig. 2.19 [D]; Umbrales TTL

En el gráfico se puede observar el ingreso de un paquete multicast vía interfaz Serial0 con un valor TTL en 24. Asumiendo que el mecanismo de revisión RPF es satisfactorio, y que las interfaces Serial1, Serial2 y Ethernet0 son todas las interfaces de salida listadas, el paquete por lo tanto normalmente podría ser enviado por esas interfaces. Como algunos umbrales TTL han sido aplicados a esas interfaces, el router debe cerciorarse que el valor TTL del paquete, que se ha reducido a 23, sea mayor o igual al umbral TTL de la interfaz antes de enviar el paquete a la interfaz. De este modo el paquete es enviado por las interfaces Serial1 y Ethernet0, téngase en cuenta que el umbral TTL de cero significa que no hay umbral TTL sobre esta interfaz. El valor TTL del paquete de 23 es menor que el valor del umbral TTL de la interfaz Serial2, por lo cual el paquete no puede ser enviado por esta interfaz.

El umbral TTL provee un método simple para prevenir el reenvío de tráfico multicast más allá del límite de un sitio o región basado sobre el campo TTL en un paquete multicast. Esta técnica es referida como alcance TTL (TTL scoping). Las aplicaciones multicast que deben mantener su tráfico dentro de un sitio o región, transmiten su tráfico multicast con un valor inicial TTL para no cruzar los límites del umbral TTL.

La tabla 2.4 muestra valores típicos iniciales TTL y umbrales TTL sobre interfaces del router para varios límites TTL.

Alcance TTL	Valor Inicial TTL	Umbral TTL
Red Local	1	N/A
Sitio	15	16
Región	63	64
Mundo	127	128

Tabla 2.4 [A]; Valores típicos TTL

Límites de Ámbito Administrativo.- Como los umbrales TTL, los límites de ámbito administrativo podrían ser utilizados para limitar el reenvío de tráfico multicast fuera de un dominio o subdominio. Este enfoque utiliza un rango especial de direcciones multicast llamadas, direcciones de ámbito administrativo, como mecanismo limitante. Si se configura un límite de ámbito administrativo sobre la interfaz de un router, el tráfico multicast cuyas direcciones de grupo multicast caen sobre este rango, no serán permitidas entrar o salir por esta interfaz, proporcionando así un firewall para el tráfico multicast en este rango de direcciones.

La Fig. 2.20 muestra el mecanismo de límites de ámbito administrativo en funcionamiento, donde se configura un rango de direcciones multicast 239.0.0.0 hasta 239.255.255.255 sobre la interfaz Serial0. Este mecanismo efectivamente configurado levanta un firewall que los paquetes multicast en este rango no pueden cruzar.

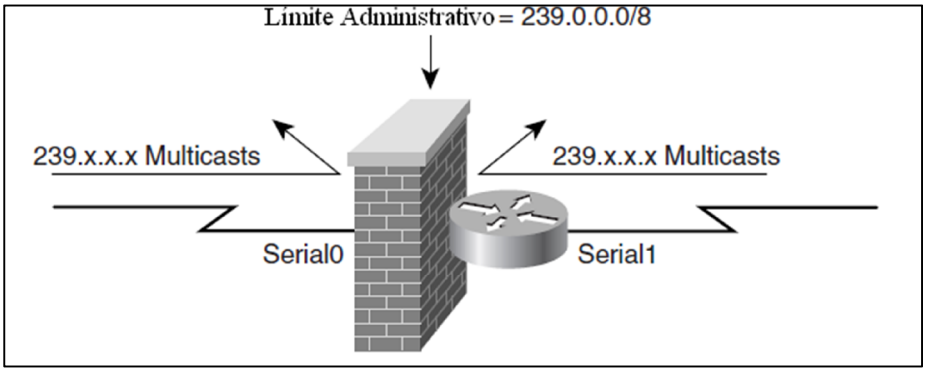


Fig. 2.20 [D]; Mecanismo de Límite Administrativo

2.3 Protocolos de Ruteo Multicast

Existen dos categorías o modos para los protocolos de ruteo multicast: Protocolos de modo denso y Protocolos de modo disperso.

El protocolo de ruteo utilizado en multicast se llama Protocolo Independiente Multicast (PIM), tiene la capacidad de operar en ambos modos, denso o disperso, dependiendo de cómo el router haya sido configurado. Es posible también configurar CISCO PIM, como protocolo propietario, que permite al router tomar una decisión dinámica del modo de operación denso o disperso basado sobre un grupo multicast.

2.3.1Protocolos de Modo Denso

Los protocolos en este modo solo emplean árboles fuente o SPT para entregar el tráfico multicast (S,G), utilizando el principio del empuje. El principio del empuje asume que cada subred en la red tiene al menos un receptor de tráfico multicast (S,G), y por lo tanto el tráfico es empujado o inundado a todos los puntos en la red. Este proceso es análogo al broadcast de radio o televisión que es transmitido sobre el aire a todos los hogares dentro del área de cobertura, para lo cual los receptores solo necesitan sintonizar la transmisión para recibir el programa.

Comportamiento de Inundación y Podado.- A diferencia del broadcast de ondas de radio sobre el aire, la inundación de tráfico multicast a cada punto en la red viene con un costo asociado (ancho de banda, CPU del router, etc.). Por lo que para evitar el innecesario consumo de los valiosos recursos de red, los router envían mensajes de podado al árbol de distribución fuente para cortar el tráfico multicast no deseado. El resultado es que las ramas sin receptores son podadas del árbol de distribución, dejando sólo las ramas que contengan receptores.

En la Fig. 2.21 muestra al router B respondiendo con un mensaje de podado a un tráfico multicast no deseado

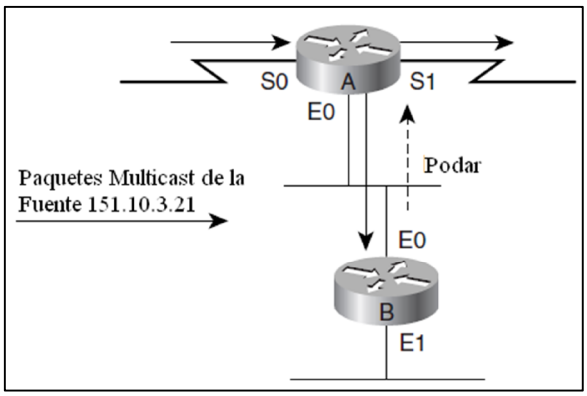


Fig. 2.21 [D]; Podando un Flujo de Modo Denso

Cuando el router A recibe el mensaje de podar para el flujo del tráfico multicast (S,G) sobe una interfaz de salida, del gráfico la interfaz Ethernet0, el router coloca la interfaz en el estado de podado y para de reenviar el tráfico (S,G) fuera de la interfaz. La interfaz de este ejemplo está conectada a una red multi-acceso, y se está asumiendo que otros routers abajo de esta interfaz no quieren recibir el tráfico todavía. El método utilizado para determinar si otros routers en una interfaz de acceso múltiple desean continuar recibiendo el tráfico multicast depende del protocolo en uso.

El podado tiene un valor de tiempo de espera asociado con el de tal manera que cuando el tiempo de espera termina, causa que el router ponga la interfaz de regreso al estado de envío y comience a inundar enviando tráfico multicast por la interfaz.

La Fig. 2.22 muestra una entrada de la tabla de ruteo para el router A de la figura anterior, donde se puede observar que la interfaz Ethernet0 está en estado podado, puesto con el indicador “Prune/Dense”, y que ningún tráfico del grupo 224.2.127.254 de la fuente 151.10.3.21 está siendo reenviado por esta interfaz.

```
(151.10.3.21/32, 224.2.127.254), 00:04:15/00:01:10, flags: T
 Incoming interface: Serial0, RPF nbr 171.68.0.91
 Outgoing interface list:
   Serial1, Forward/Dense, 00:04:15/00:00:00
   Ethernet0, Prune/Dense, 00:00:25/00:02:35
```

Fig. 2.22 [D]; Tabla de Ruteo Multicast

Se puede observar también que el tiempo de espera para el estado de podado será de 2 minutos y 30 segundos, indicado en el último valor de tiempo sobre la línea. Cuando el valor de tiempo de espera de podado se agote, el estado de la interfaz regresa a envío o con el indicador "Fordward/Dense", y el tráfico otra vez comenzara a fluir por la interfaz. Asumiendo que el flujo de bajada al Router B en este caso, todavía no necesite recibir el tráfico multicast, este enviará de nuevo un mensaje de podado para cortar el tráfico no deseado.

El valor de tiempo de espera utilizado para el podado, depende del protocolo de ruteo multicast que se utilice, típicamente ese valor oscila de 2 a 3 minutos. Este comportamiento periódico de inundación y podado es característico de los protocolos de modo denso, como PIM-DM (Protocolo Independiente Multicast Modo Denso).

Injerto.- La mayoría de los protocolos en modo denso pueden rápidamente injertar de regreso una rama podada al árbol de distribución. Esta capacidad se demuestra cuando un nuevo receptor sobre una rama previamente podada del árbol se une al grupo multicast, en tal caso el router detecta al nuevo receptor he inmediatamente envía un mensaje de injerto (graft) en el árbol de distribución hacia la fuente. Cuando el flujo de subida del router recibe el mensaje de injerto, el router pone inmediatamente sobre la interfaz por la cual recibió el mensaje de injerto el estado de envío, de manera que el tráfico multicast comienza a fluir hacia el receptor.

La Fig. 2.23 muestra el proceso de injerto, se observa la fuente, host E, transmitiendo tráfico multicast por el SPT, a los receptores host A, B y C.

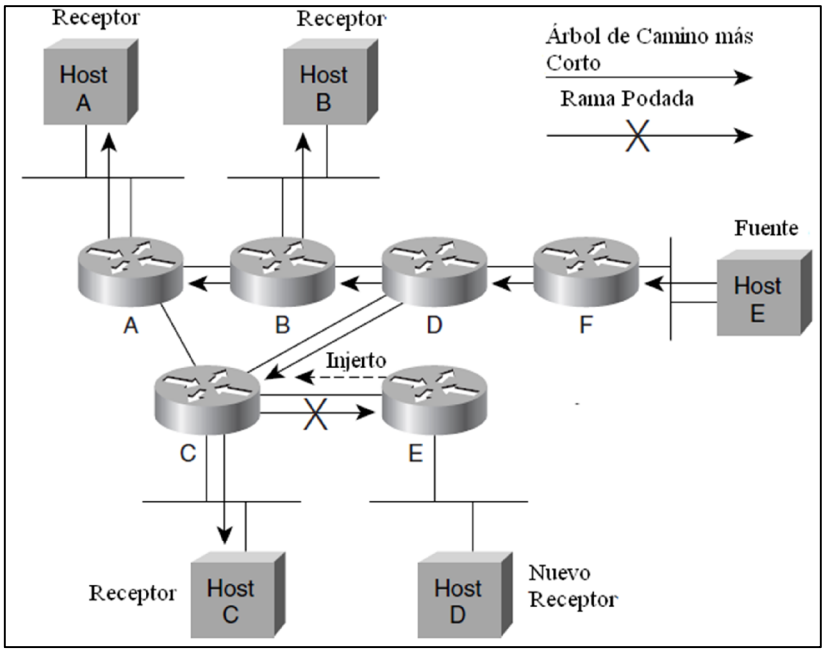


Fig. 2.23 [D]; Injerto de Modo Denso

El router E previamente ha podado su enlace al router C, ya que inicialmente no tenía receptores directamente conectados. Del gráfico el host D se une al grupo multicast como nuevo receptor, esta acción indica al router E que envíe un mensaje de injerto en el SPT al router C, e inmediatamente reiniciar el flujo de tráfico multicast. Usando el proceso de injerto el router E puede evitar tener que esperar que el tiempo de espera de podado termine, así se reduce la latencia de unión vista por el host D.

2.3.2Protocolos de Modo Disperso

Los protocolos de este modo hacen uso de árboles de distribución compartidos y ocasionalmente, como en el caso de PIM-SM (Protocolo Independiente Multicast Modo Disperso), utiliza árboles de camino más corto SPT para distribuir tráfico multicast a receptores multicast en la red. En lugar de usar el modelo de empuje, los

protocolos de modo disperso hacen uso del modelo de halar en el que el tráfico multicast es halado a los receptores en la red. Este modelo de halar por lo tanto asume que el tráfico multicast no es deseado a menos que este sea solicitado usando un mecanismo explícito de unión.

Mensajes de Unión de Árbol Compartido.- Para halar el tráfico multicast al receptor en una red en modo disperso, una rama del árbol compartido debe ser creada desde el nodo raíz (denominado RP cuando se utiliza PIM-SM) al receptor. Para construir esta rama del árbol compartido, un router envía un mensaje de unión de árbol compartido hacia la raíz del árbol compartido. Este mensaje viaja router por router hacia la raíz, construyendo una rama del árbol a medida que avanza.

La Fig. 2.24 muestra mensajes de unión siendo enviados al árbol compartido a la raíz. En el gráfico el árbol compartido tiene un receptor localmente conectado y por lo tanto envía un mensaje de unión hacia la raíz vía el router C. El mensaje viaja salto a salto hasta que este alcance la raíz y construya una rama del árbol compartido.

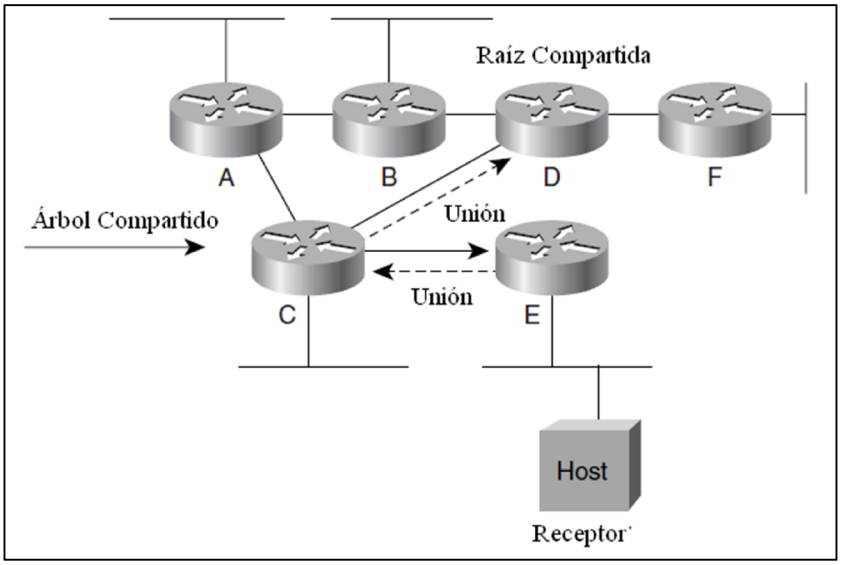


Fig. 2.24 [D]; Mensajes de Unión en un Árbol Compartido

Cuando se utiliza PIM-SM, los mensajes de unión del SPT podrían también ser enviados en dirección de la fuente para construir un SPT desde una fuente individual multicast a los receptores en la red. Los árboles de camino más corto SPT, permiten a los routers que tienen directamente receptores conectados cortar a través de la red y evitar el nodo raíz de manera que el tráfico multicast de una fuente pueda ser recibido vía un enlace más directo.

La Fig. 2.25 muestra un SPT siendo construido usando mensajes de unión enviados hacia una fuente multicast específica. En el gráfico, el router E envía un mensaje de unión, denotado por la flecha punteada, hacia la fuente vía el router C. La unión al SPT viaja salto a salto hasta alcanzar el router A, construyendo de este modo el SPT, denotado por las flechas sólidas, a medida que avanza.

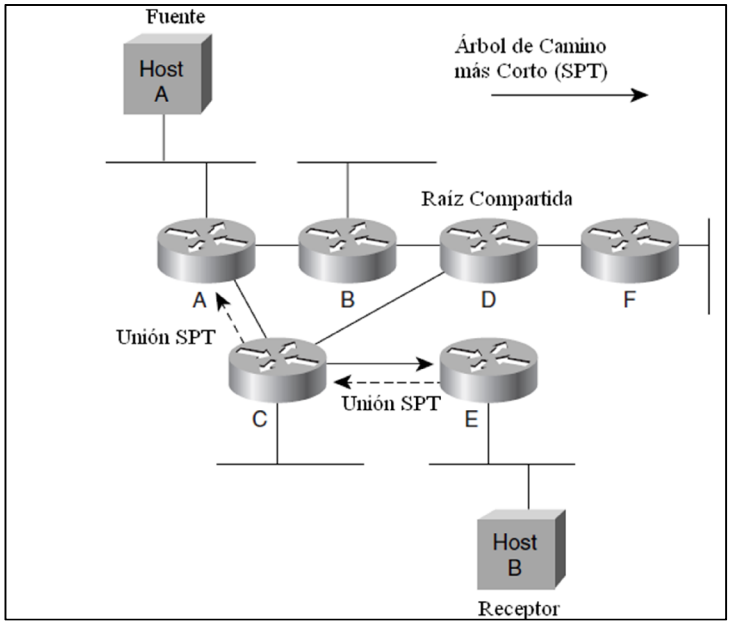


Fig. 2.25 [D]; Mensajes de Unión SPT

Se debe tener en cuenta que si las ramas de los árboles de distribución en una red de modo disperso (siendo árboles compartidos o SPT) no son actualizados, el tiempo de

espera expiraría y serían borrados, por lo que pararía el tráfico que fluye a la rama del árbol compartido. Para evitar este problema, las ramas de los árboles de distribución en modo disperso son mantenidas por algunos mecanismos periódicos de actualización de unión, que los routers envían a lo largo de las ramas. El protocolo PIM-SM mantiene la actualización por el reenvío de mensajes de unión al árbol para actualizar las ramas periódicamente.

Mensajes de Podado.- En modo disperso, los mensajes de podado son enviados al árbol de distribución cuando el tráfico del grupo multicast no es deseado en mucho tiempo. Esta acción permite a las ramas del árbol compartido o del árbol de camino más corto, que fueron creados vía mensajes de unión explícitos, ser derribados cuando ellos no han sido necesitados en mucho tiempo. Se puede dar como ejemplo, si un router hoja ya no tiene conectado directamente ningún host (flujos de bajada de routers multicast) para un grupo particular multicast, el router envía un mensaje de podado al árbol de distribución para cortar el flujo del tráfico del grupo multicast no deseado. Enviar mensajes de podado en lugar del tiempo de espera para las ramas del árbol de distribución en modo disperso, mejora en gran medida la latencia de la red.

La Fig. 2.26 muestra el proceso de podado en funcionamiento, el host A acaba de dejar el grupo multicast, por lo tanto, el router A no necesita más el tráfico que fluye del árbol compartido, y envía mensajes de podado al árbol compartido hacia el RP. Este mensaje poda el enlace entre el router A y el router B del árbol compartido, y para el flujo del tráfico multicast ahora innecesario al router A.

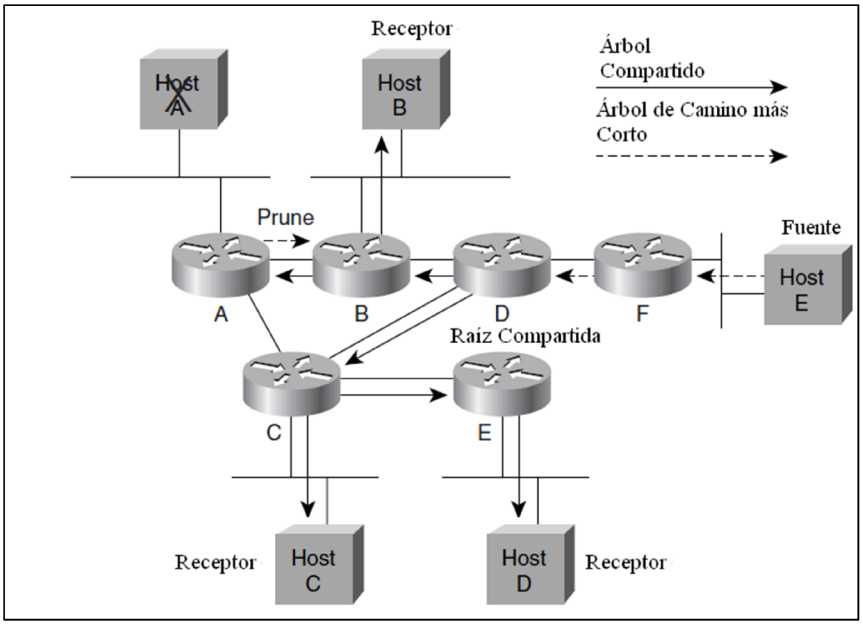


Fig. 2.26 [D]; Podado de Modo Disperso

2.3.3 PIM-DM (Protocolo Independiente Multicast – Modo Denso)

PIM modo denso es el método más simple de distribución multicast. Este es usado cuando la mayoría de los hosts sobre una red están interesados en recibir el flujo multicast. El modo denso opera inundando los datos en la red, asumiendo que todos los nodos están interesados. Si un segmento de la red no desea recibir el flujo, el tráfico es podado. Como resultado las operaciones multicast en modo denso son algunas veces referidas como inundar y podar.

PIM-DM opera usando el concepto de árboles de distribución fuente, ya que los datos son inundados desde la fuente hacia el exterior, el árbol multicast es enraizado en el flujo fuente.

Un router CISCO está globalmente habilitado para ruteo multicast con el siguiente comando en modo de configuración global:

```
Router(config)#ip multicast-routing
```

Después de habilitar globalmente IP multicast, las interfaces individualmente necesitan ser configuradas para soportar PIM.

Para configurar la interfaz de un router CISCO que utilice PIM-DM:

```
Router(config-int)# ip pim dense-mode
```

Mecanismo de Funcionamiento PIM-DM.-

1- Una fuente multicast se levanta y comienza a inundar con tráfico multicast toda la red.

2- Si más de un router está reenviando tráfico multicast sobre un medio común broadcast, como un enlace Ethernet. Los mensajes determinan el PIM promotor. El router con la mejor métrica o por defecto la dirección IP más alta gana la elección.

3- Algunos routers podrían no tener receptores multicast para el grupo cuyo tráfico actualmente está siendo inundado. Esos routers envían mensajes de podado a los routers en el flujo de subida, pidiendo que la rama del árbol de distribución sea podada. Sin embargo si otro router está sobre el mismo medio broadcast como el router que envía el podado, y si ese otro router tiene receptores IP multicast conectados, el mensaje de podado es ignorado porque el router conectado a los receptores IP multicast envían un mensaje de anulación de unión.

4- Si un receptor se levanta sobre un router previamente podado del árbol, el router puede volver a unirse al árbol enviando un paquete de injerto.

Otra consideración del comportamiento es que el proceso de inundar y podar se repite cada 3 minutos, por lo que PIM-DM no es escalable. Una mejor alternativa es PIM-SM.

2.3.4 PIM-SM (Protocolo Independiente Multicast – Modo Disperso)

Multicast modo disperso es usado cuando un número pequeño de hosts receptores están sobre una subred y especialmente si se extiende sobre una serie de redes. Si el flujo multicast es inundado dentro de una red y solo un número pequeño de hosts está relativamente interesado, esto resulta en un gasto de ancho de banda. Cuando el modo disperso es utilizado, los hosts específicamente deben solicitar los datos del flujo multicast en lugar de recibirlos automáticamente.

PIM-SM opera usando el principio de árboles de distribución compartidos. Como los hosts deben solicitar una afiliación al flujo multicast, los routers deben saber dónde enviar los reportes de afiliación, así la necesidad del punto RP. El RP provee un punto donde la fuente puede enviar los datos para distribuirlos a los hosts solicitantes. Un router puede enviar solicitudes de afiliación.

Para configurar la interfaz de un router CISCO que utilice PIM-SM:

```
Router(config-int)# ip pim sparse-mode
```

Mecanismo de Funcionamiento PIM-SM.-

Considerar la formación de un árbol de distribución PIM-SM

1- Un receptor envía un mensaje de reporte IGMP a su router indicando que el quiere participar en un particular grupo multicast. El router receptor (router del último salto) envía mensajes de unión al RP, creando el estado (*,G) a lo largo del árbol compartido entre el RP y el router del último salto.

2- Una fuente se levanta y crea un árbol fuente entre su router (router del primer salto) y el RP, el estado (S,G) es creado en los routers a lo largo de este enlace. Sin embargo después de que el árbol fuente está completamente establecido,

la fuente envía sus paquetes multicast al encapsulado RP, dentro de mensajes de registro unicast.

3- Después el RP recibe el primer paquete multicast sobre el árbol fuente, este envía un mensaje de registro de parada a la fuente, diciéndole a la fuente que pare de enviar el tráfico multicast dentro de mensajes de registro. Dos árboles existen ahora: un árbol fuente del router del primer salto al RP, y un árbol compartido del RP al router del último salto. Sin embargo este no podría ser un enlace óptimo.

4- El router del último salto observa de donde el tráfico multicast está arribando, y el router del último salto envía un mensaje de unión directamente al router del primer salto, para formar un enlace óptimo (árbol de enlace fuente) entre la fuente y el receptor.

5- Si el router del último salto no necesita el tráfico multicast del RP, porque este está recibiendo el tráfico multicast directamente desde el router del primer salto, este envía un mensaje de podado (S,G) RP-bit al RP, pidiendo al RP que pare de enviar tráfico multicast.

6- Con el árbol compartido al router del último salto es podado, el RP no necesita más tráfico multicast desde el router del primer salto. Así el RP envía un mensaje de podado (S,G) al router del primer salto. En este punto el tráfico fluye en un enlace óptimo desde el router del primer salto al router del último salto. El proceso de corte del enlace vía el RP al enlace directo es llamado conmutación de árbol de camino más corto (SPT).

2.4 Protocolo de Administración de Grupo de Internet (IGMP)

El protocolo de Administración de Grupo de Internet surgió del protocolo de membresía de host de la tesis doctoral del Dr. Esteve Deering, siendo la primera versión IGMPV1 definida en el RFC 1112. Después se ratificó la segunda versión IGMPV2 en Noviembre de 1997 como estándar por el Grupo de Trabajo de Ingenieros de Internet IETF, definida en el RFC 2236. La última versión corresponde a IGMPV3 ratificada por IETF en Octubre del 2002, definida en el RFC 3376.

Los mensajes IGMP son utilizados principalmente por los hosts multicast para comunicarse con el router multicast local, cuando desean unirse a un grupo específico IP multicast y comenzar a recibir tráfico de grupo. Los hosts podrían también comunicarse con el router multicast local, para indicarle que se desea salir del grupo IP multicast, y entonces no estar más interesado en recibir el tráfico del grupo multicast.

Usando la información obtenida vía IGMP los routers mantienen una lista de membresías de grupos multicast basada sobre una interfaz. Un membresía multicast se activa sobre una interfaz, si al menos un host comunica su deseo de recibir el tráfico multicast del grupo.

2.4.1 IGMP V1

Los mensajes IGMP son transmitidos dentro de datagramas IP denotados por un número de protocolo IP de 2. Los mensajes IGMP son transmitidos con el campo de tiempo de vida (TTL) IP puesto en 1, por lo que es de ámbito local y no es reenviado por los routers, la Fig. 2.27 muestra el formato de un mensaje IGMPV1.

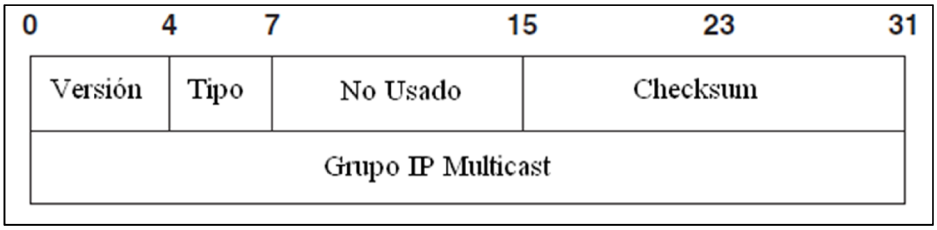


Fig. 2.27 [A]; Formato Mensaje IGMPV1

Campos del mensaje IGMPV1:

- Campo versión.- Contiene la identificación de versión IGMP, en este caso está puesto en 1. En la versión 2 de IGMP este campo es eliminado.
- Campo Tipo.- En la versión 1 se manejan dos tipos de mensajes por los routers y los hosts: Membership Query y Membership Report.
- Campo Checksum.- Es un campo de 16-bits, con el complemento de la suma de los complementos a uno del mensaje IGMP.
- Campo Dirección Grupo.- Este campo contiene la dirección del grupo multicast cuando un reporte de membresía (Membership Report) este siendo enviado. Este campo está puesto a cero, cuando se utiliza una consulta de membresía (Membership Query) y debería ser ignorado por los hosts.

Los reportes de membresía (Membership Reports), son emitidos por los hosts que desean recibir el tráfico de un grupo específico multicast.

Las consultas de membresía (Membership Query), son emitidas por los routers en intervalos regulares (60 segundos) para comprobar si aún hay algún host interesado en el tráfico del grupo IP multicast en ese segmento.

Los reportes de membresía de los hosts son emitidos, primero cuando se desea recibir el tráfico de un grupo IP multicast, y en contestación a las consultas de membresía.

Los reportes de membresía contienen los siguientes campos:

Información de Capa 2:

MAC fuente: Dirección MAC del host.
MAC destino: Dirección MAC de destino para el grupo multicast.

Información de Capa 3:

IP fuente: Dirección IP del host.
IP destino: Dirección IP grupo multicast.

Paquete IGMP:

Contiene datos IGMP además del grupo IP multicast y algunos otros campos.

Las consultas de membresía a los hosts son enviadas por el router a todos con la dirección IP multicast 224.0.0.1. Estas consultas utilizan la dirección IP 0.0.0.0 en el campo del grupo multicast. Un host de cada grupo debe responder a esa consulta, o el router detiene el reenvío de tráfico para ese grupo IP multicast en ese segmento (después de tres intentos). El router mantiene una entrada de ruteo multicast para cada fuente, y la enlaza a una lista de interfaces de salida (interfaces desde donde llega el reporte IGMP). Después de tres intentos de consultas IGMP sin respuesta, esta interfaz es borrada de la lista de interfaces de salida para todas las entradas enlazadas a ese grupo IP multicast.

IGMPV1 no tiene un mecanismo de salida si un host no desea continuar recibiendo el tráfico del grupo IP multicast, este simplemente corta la comunicación, y si el router no recibe contestación a la consulta de membresía por ningún host dentro de la subred, este elimina el grupo IP multicast para esa subred.

2.4.2 IGMP V2

IGMPV2 fue desarrollado principalmente para resolver algunas de las deficiencias de IGMPV1 que fueron descubiertas con el paso del tiempo y a través de la experiencia práctica.

Los mensajes de reporte de consulta y membresía de IGMPV2 son los mismos que los mensajes de IGMPV1 con dos excepciones:

1- Los mensajes de consulta (Membership Queries) de IGMPV2 están divididos en dos categorías:

   Consultas Generales (General Queries).- las cuales funcionan de la misma manera que las consultas de IGMPV1.

   Consultas de grupo específico (Group Specific Queries).- son consultas dirigidas a un solo grupo.

2- Los reportes de membresía de IGMPV1 e IGMPV2 tienen diferentes tipos de código IGMP.

El proceso de respuesta a consulta es el mismo en ambas versiones.

IGMPV2 está diseñado para soportar cualquier fuente multicast (ASM) de red. En una red ASM, el host especifica el grupo IP multicast al que desea unirse, y escucha todo el tráfico de ese grupo, sin tener en cuenta quién está enviando el tráfico.

IGMPV2 incluye nuevas funciones:

- Proceso de elección de consulta (Querier Election Process).- provee la capacidad para los routers IGMPV2, elijan el router consulta (router query), sin tener que confiar sobre un protocolo de ruteo multicast para desarrollar este proceso.

- Campo de tiempo de respuesta máximo.- Un nuevo campo en los mensajes de consulta permite al router de consulta especificar el máximo tiempo de respuesta de consulta. Este campo permite ajustar el proceso de consulta y respuesta, para controlar explosividad de respuesta y ajustar la latencia de salida.
- Mensajes de consulta de grupo específico.- permite al router consulta desarrollar operaciones de consulta, sobre un grupo específico en lugar de todos los grupos.
- Mensajes de salida de grupo.- provee a los hosts con un método de notificación de routers sobre la red que ellos desean dejar el grupo.

Las dos últimas funciones habilitan a los hosts y a los routers reducir la latencia de salida, lo cual fue un problema en IGMPV1, de minutos caídos a pocos segundos.

El formato de mensaje de IGMPV2 se muestra en la Fig. 2.28, donde el campo tipo ha sido fusionado con el campo versión de IGMPV1 y ahora ocupa un octeto completo. El valor asignado a los varios tipos de mensajes han sido escogidos cuidadosamente para proveer un compatibilidad hacia atrás con IGMPV1.

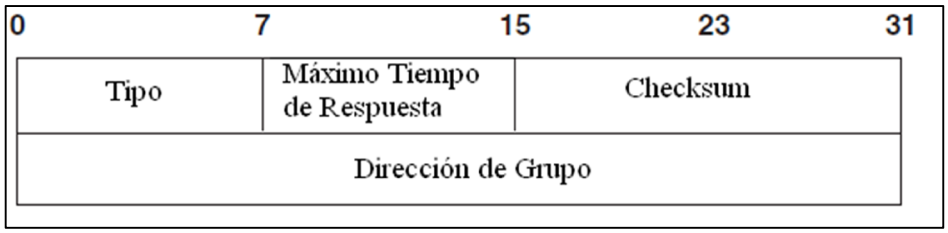


Fig. 2.28 [A]; Formato Mensaje IGMPV2

Campos del mensaje IGMPV2:

- Campo Tipo.- existen cuatro tipos de mensajes usados entre hosts y routers.

1. Consulta de Membresía (Membership Query), se divide en dos sub tipos de mensajes de consulta de membresía.
   1.1 Consulta General (General Query).- permite determinar qué grupo multicast está activo del mismo modo que IGMPV1 lo hace. Esta consulta es denotada por una dirección de ceros en el campo de grupo IP multicast.
   1.2 Consulta de Grupo Específico (Group Specific Query).- determina si un grupo específico multicast tiene algunos miembros restantes. Esta consulta es denotada por la dirección de grupo que está siendo consultada en el campo de grupo IP multicast.
2. Reporte de Membresía Versión 1 (Membership Report Version 1), este tipo de mensaje es proveído solamente para compatibilidad hacia atrás con IGMPV1.
3. Reporte de Membresía Versión 2 (Membership Report Version 2)
4. Dejar Grupo (Leave Group).

- Campo de Tiempo Máximo de Respuesta (MRT).- este campo es usado sólo en los mensajes de consulta de membresía y especifica el tiempo máximo en unidades de 1 a 10 segundos que un host podría esperar a responder un mensaje de consulta. El valor por defecto de este campo es 100 (10 segundos).

Los hosts utilizan el valor en este campo como el límite superior para la configuración aleatoria de su reporte de tiempos de grupo, que son utilizados por el mecanismo de supresión de reporte.

El valor en este campo puede ser ajustado para controlar tanto la explosividad de respuesta de los miembros o la latencia de salida.

- Campo Checksum.- Es un campo de 16-bits, con el complemento de la suma de los complementos a uno del mensaje IGMP.
- Campo Dirección Grupo.- Este campo contiene la dirección en cero cuando una consulta general es enviada, cuando se envía una consulta de grupo específico este campo contiene la dirección de grupo multicast que está siendo consultada.

  Si se envía un mensaje de reporte de membresía o de dejar grupo este campo contiene la dirección IP multicast de grupo objetivo.

Una de las más importantes nuevas funciones incluidas en IGMPV2 es el mensaje de dejar grupo (Leave Group), que cuando un host ya no desea continuar recibiendo el tráfico del grupo IP multicast, este debe enviar un mensaje de dejar grupo a la dirección 224.0.0.2 que corresponde a la dirección de todos los routers multicast.

En la Fig. 2.29 se muestra las operaciones básicas de IGMPV2, para cada una de sus tres funciones básicas descritas a continuación:

Unir (Join).- Cuando un host que utiliza IGMPV2 necesite unirse a un grupo, este envía un reporte de membresía no solicitado, destinado al grupo IP multicast al que se desea unirse. Al recibir el reporte de membresía el router multicast comenzará a reenviar el

tráfico del grupo por una apropiada interfaz de salida, si el tráfico aún no ha sido enviado por ahí.

Salir (Leave).- Cuando un host que utiliza IGMPV2 deja un grupo, este envía un mensaje de dejar grupo a la dirección multicast de routers 224.0.0.2, indicando el grupo a dejar en el campo de dirección de grupo multicast. El router después de recibir este mensaje inmediatamente responde sobre la interfaz lógica una consulta de grupo específico a la dirección de grupo multicas especificada, para determinar si algún host está todavía deseando recibir el tráfico multicast de este grupo específico. El valor MRT determina el periodo de tiempo a esperar para una respuesta del host a la consulta. Si no hay respuestas recibidas dentro del intervalo de tiempo MRT, el router no enviará más tráfico del grupo multicast en cuestión por la interfaz de salida específica.

Consulta (Query).- La consulta general de membresía es emitida periódicamente a todos los hosts con la dirección multicast 224.0.0.1, para determinar que grupos están actualmente siendo utilizados por los hosts que utilicen IGMPV2. El MRT es usado para especificar el periodo de tiempo que el router debe esperar a las respuestas de consulta de los hosts. Si no hay respuesta durante el intervalo de tiempo MRT, el tráfico reenviado es parado para cualquiera de los grupos no requeridos sobre la interfaz de salida. Esto es utilizado para recobrarse de condiciones de error como el apagado de equipo activo de red, que no permita el envío de mensajes de dejar grupo, o que los mensajes de dejar grupo hayan sido descartados por elementos de acceso. Esto provee un mecanismo de auto recuperación IGMP para sincronizar el estado multicast dentro de la red.

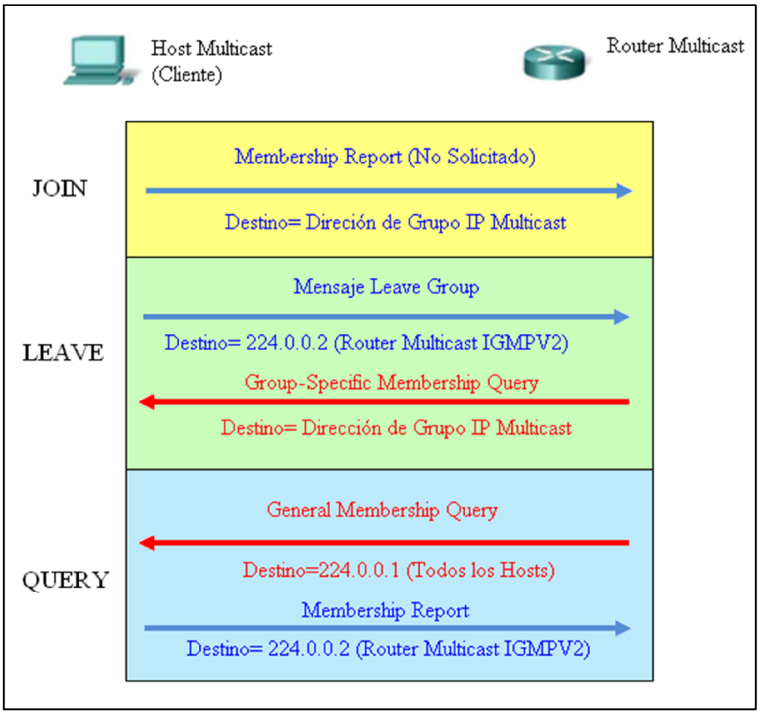


Fig. 2.29 [I]; Operaciones básicas IGMPV2

2.4.3 IGMP V3

La mejor funcionalidad en IGMPV3 es el soporte para una sola fuente multicast (SSM). Cuando se utiliza SSM, el host especifica la dirección fuente que desea escuchar. En otras palabras, si un grupo multicast con la dirección 239.0.0.1, la cual está recibiendo tráfico de un dispositivo origen con la dirección 172.30.60.10, es un grupo multicast asociado a una sola dirección IP fuente, que recibir tráfico del mismo grupo con una dirección IP origen diferente. Esta es una importante función de seguridad que previene al cliente la recepción de tráfico generado de una fuente no deseada.

La solicitud de cambio de grupo, puede ser hecha utilizando una sola solicitud IGMPV3 en lugar de solicitudes separadas de dejar grupo y de unirse a un grupo. La velocidad de este proceso de cambio de grupo representa una capacidad crítica que mejora el rendimiento y latencia sobre la red.

IGMPV3 usa dos tipos de mensajes IGMP:

1. Reporte de Membresía (Membership Report), usa un formato diferente que en IGMPV2. Para distinguir esto, los reportes de membresía IGMPV3 ajustan el campo tipo a 0x22. Estos reportes en IGMPV3 son utilizados para unirse o dejar un grupo multicast. El mensaje de dejar grupo no es utilizado en IGMPV3.
2. Consulta de Membresía (Membership Query), consiste de una consulta general (General Query), consulta de grupo específico (Group-Specific Query) o consulta de grupo y fuente específica (Group and Source Specific Query), lo último es nuevo de IGMPV3. Las consultas de membresía utilizan el mismo valor tipo 0x11 que las versiones anteriores, aunque el formato del paquete haya cambiado.

IGMPV3 hace uso de 2 direcciones reservadas multicast:

- 224.0.0.1 es la dirección IP utilizada para enviar mensaje a todos los hosts, esta es la misma dirección utilizada en IGMPV2.
- 224.0.0.22 es la dirección IP utilizada para enviar mensajes a los routers multicast. Esta dirección difiere de la utilizada en IGMPV2.

La Fig. 2.30 muestra el formato de mensaje de consulta IGMPV3.

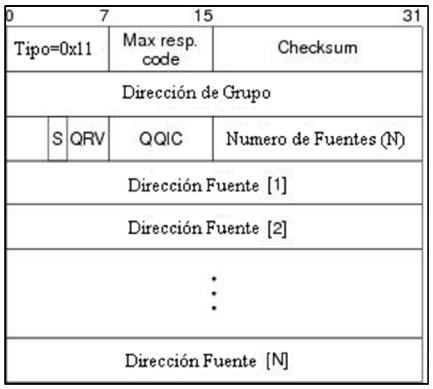


Fig. 2.30 [D]; Formato de mensaje de consulta IGMPV3

Campos del mensaje de consulta IGMPV3:

- Tipo.- Con el valor 0x11 indica una consulta IGMP.
- Max. Resp. Code (MRC).- Al igual que en IGMPV2 (MRT), este campo especifica el tiempo máximo, en segundos, permitido antes de enviar un informe de respuesta.
- Dirección de Grupo.- Dirección de grupo multicast. Esta dirección es 0.0.0.0 para consultas generales.
- S.- Bandera S, indica que el procesamiento por los routers está siendo suprimido.
- QRV.- Valor de Consulta Robusto (Querier Robustness Value), este valor afecta a los temporizadores y al número de reintentos.
- QQIC.- Consultor de Consulta de Intervalo de Código, en segundos, este campo especifica el intervalo de consulta usado por el consultor.
- Número de Fuentes (N).- Número de fuentes presentes en la consulta, este valor es diferente de cero para consultas de grupo y fuente.
- Dirección Fuente (1..N).- Direcciones de las Fuentes.

L a Fig. 2.31 muestra el formato del mensaje de reporte IGMPV3.

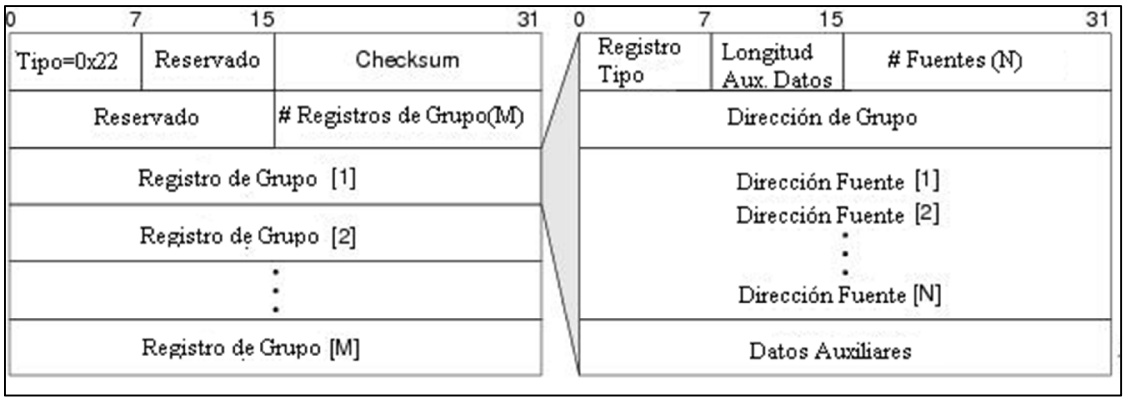


Fig. 2.31 [D]; Formato de mensaje de reporte IGMPV3

Campos del mensaje de reporte IGMPV3:

- # de Registros de Grupo (M).- Número de registros de grupo presentes en el reporte.
- Registro de Grupo (1..M).- Bloque de campos que contienen información con respecto a la membresía del remitente con un solo grupo multicast sobre la interface desde la cual el reporte fue enviado.
- Tipo de registro.- Tipo de registro de grupo, que puede ser de modo de inclusión o de exclusión.
- # de Fuentes (N).- Número de fuentes presentes en el registro.
- Dirección Fuente (1..N).- Dirección de la fuente o fuentes.

En la Fig. 2.32 se muestra las operaciones básicas de IGMPV3, para cada una de sus tres funciones básicas descritas a continuación:

Unir (Join).- Como sus predecesores, IGMPV3 envía un reporte de membresía (Membership Report) no solicitado para unirse a un grupo multicast. Después de recibir el reporte de membresía, el router coloca la dirección IP del host en la lista de interfaz de salida para el grupo multicast, y comenzar a reenviar el tráfico del grupo a los hosts por la respectiva interfaz.

Dejar (Leave).- Cuando un host que utiliza IGMPV3 desea dejar un grupo, este envía un reporte de membresía (Membership Report) incluyendo un mensaje de cambio de estado de registro (State Change Record) , a la dirección multicast de IGMPV3 224.0.0.22, que excluye la dirección fuente de los grupos que ya no se espera ser recibir. Excluyendo la actual fuente para un grupo multicast, resulta en que ya no se unirá al grupo multicast. Similar a un mensaje de dejar grupo en IGMPV2.

El router responde inmediatamente sobre la interfaz lógica con una consulta de grupo específico (Group Specific Query) o una consulta de grupo y fuente específica (Group and Source Specific Query), a todos los hosts con la dirección multicast 224.0.0.1 con un MRC definido para determinar si algún host todavía desea recibir este grupo multicast específico. Si no se recibe una respuesta dentro del periodo MRC, el router ya no enviará el tráfico del grupo multicast por la interfaz de salida específica.

Consulta (Query).- Como IGMPV2, IGMPV3 emite periódicamente consultas generales de membresía (General Membership Query), para determinar que grupos están actualmente siendo usados por hosts que utilizan IGMPV3 por un segmento lógico de red. Esto también se utiliza para recobrarse de condiciones de error, como el apagado de equipo activo, que no haya permitido el envío de mensajes de salida.

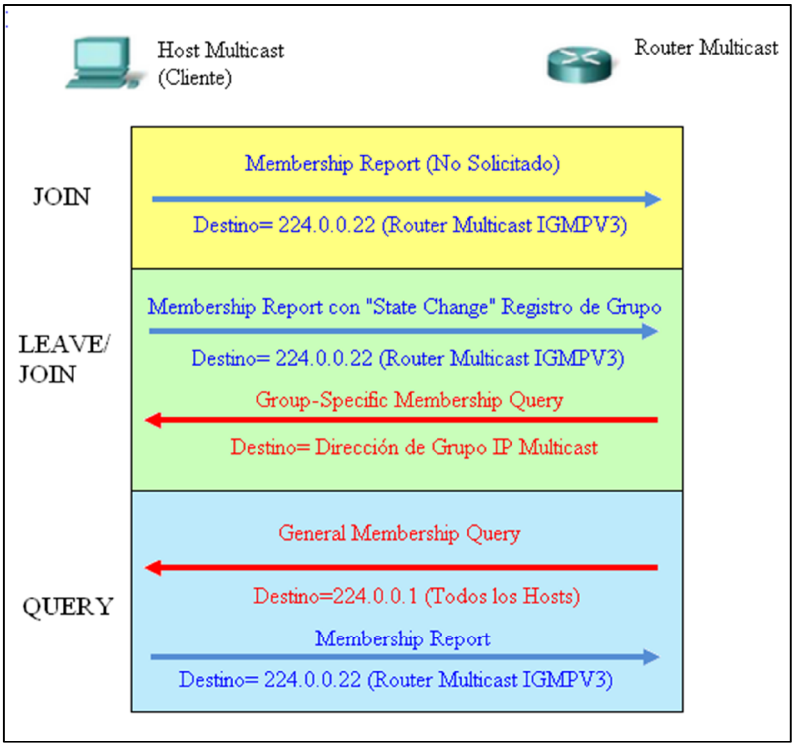


Fig. 2.32 [I]; Operaciones básicas IGMPV3

2.4.4 Interoperabilidad entre versiones de IGMP

Interoperabilidad entre IGMPV1 e IGMPV2.- Con IGMPV1 e IGMPV2 solo un router por subred IP envía consultas, denominado router consulta. En IGMPV1 el router consulta es seleccionado con ayuda de un protocolo de ruteo multicast, mientras que en IGMPV2, este es seleccionado por la dirección IP más baja entre los routers. A continuación se presentan varias posibilidades:

1- *Router con IGMPV1 y Hosts que utilizan unos IGMPV1 y otros IGMPV2*

   El router no entiende el reporte de IGMPV2, por lo tanto sola usa el reporte de IGMPV1.

2- *Router con IGMPV2 y Hosts que utilizan unos IGMPV1 y otros IGMPV2*

   Los hosts que utilizan IGMPV1 no entienden la consulta IGMPV2 o la consulta de membresía de grupo IGMPV2. El router debe solo utilizar IGMPV1 y suspende la operación de salida (Leave).

3- *Un Router con IGMPV1 y otro Router con IGMPV2 localizados en el mismo segmento de red*

   El router con IGMPV1 no tiene manera de detectar al router con IGMPV2. Por lo que el router con IGMPV2 debe ser configurado como router con IGMPV1. En cualquier caso es posible que ellos no concuerden sobre el router consulta.

Interoperabilidad entre IGMPV1, IGMPV2 e IGMPV3.- Con todas las versiones de IGMP, solo un router por subred IP envía consultas, denominado router consulta. En IGMPV1 el router consulta es seleccionado con ayuda de un protocolo de ruteo multicast, mientras que en IGMPV2 e IGMPV3, este es seleccionado por la dirección IP más baja entre los routers. A continuación se presentan varias posibilidades:

1- *Un Router con IGMPV1 o IGMPV2 y Hosts que utilizan unos IGMPV1 o IGMPV2 y otros IGMPV3*

   El router no entiende el reporte de IGMPV3, todos los hosts utilizan reportes IGMPV1 o IGMPV2.

2- *Un Router con IGMPV3 y Hosts que utilizan unos IGMPV1 o IGMPV2 y otros IGMPV3*

   Los hosts que utilizan IGMPV1 o IGMPV2 no entienden la consulta IGMPV3 o la consulta de membresía IGMPV3. EL router debe solo utilizar la versión IGMP que corresponda a la versión IGMP más baja de un cliente presente. Si hay clientes IGMPV2 e IGMPV3, el router utilizará IGMPV2. Si hay clientes IGMPV1, IGMPV2 e IGMPV3, el router utilizará IGMPV1.

3- *Diferentes versiones de IGMP sobre Routers en un mismo segmento de red*

   Cuando se presentan varios routers con diferentes versiones de IGMP sobre el mismo segmento de red, los routers con la versión más baja, no tienen manera de detectar a los routers con las versiones más altas. Por lo que los diferentes routers deben ser configurados con la misma versión. Esta versión tiene que ajustarse a la versión más baja de cualquier router consulta presente.

2.5 Aplicaciones Multimedia Multicast

Cuando se escucha el término multicast es muy probable que se lo asocie con video conferencias, por lo que es muy común que el primer acercamiento a aplicaciones multicast sea el de aplicaciones multimedia para conferencias de audio y video.

Los protocolos utilizados para aplicaciones multimedia asociados a conferencias son: El Protocolo de Tiempo Real RTP (Real Time Protocol) y su compañero Protocolo de Control de Tiempo Real RTCP (Real Time Control Protocol), que son utilizados para encapsular los flujos de dados de conferencias de audio y video y monitorear la entrega de los datos a los clientes finales en la conferencia. También se examina el Protocolo de Anuncio de Sesión SAP (Session Announcement Protocol) y el Protocolo de Descripción de Sesión SDP (Session Description Protocol), que aplicaciones de conferencias utilizan estos protocolos para anunciar y aprender acerca de la existencia de sesiones de conferencias multimedia en la red.

2.5.1 Protocolo de Tiempo Real (RTP)

RTP es un protocolo de capa de red, documentado en el RFC 1889, que permite a las aplicaciones transmitir varios tipos de cargas en tiempo real, tales como audio, video u otros datos con características de tiempo real. RTP se encuentra en la parte superior del Protocolo de Datagrama de Usuario UDP, y puede ser usado sobre flujos de datos unicast o multicast. El protocolo también provee la identificación del tipo de carga, numeración de secuencia y tiempo, como un buen mecanismo para monitorear la entrega de los datos.

RTP por sí mismo no provee ninguna garantía de mecanismos de entrega y normalmente se basa sobre el protocolo de capa más bajo para desarrollar esta

función, ya que es frecuente que se encuentre en la parte superior de IP y UDP (Como es el caso para la mayoría de las aplicaciones multimedia, sin embargo RTP depende sobre la aplicación para hacer frente con los problemas de muchos datagramas y entregas fuera de orden. Estas condiciones pueden ser detectadas por el uso del campo número de secuencia en la cabecera RTP.

RTP consiste de dos componentes:

- El componente RTP, el cual lleva los datos en tiempo real.
- El componente RTCP o protocolo de control, el cual provee información acerca de los participantes de una sesión y monitorea la entrega de datos por el uso de varias medidas simples de calidad de servicio, tales como perdida de paquetes y jitter.

2.5.2 Protocolo de Control de Tiempo Real (RTCP)

Todas las aplicaciones basadas en RTP utilizan periódicamente RTCP para información de control de sesión a todos los participantes de la conferencia para lograr las siguientes funciones:

1. Proveer una retroalimentación sobre la calidad de recepción de los datos, y en muchos casos modificar esquemas de codificación para mejorar la calidad de recepción en general. Aplicaciones de terceras partes pueden también usar esta información para diagnosticar problemas de entrega y determinar áreas de la red que están sufriendo un pobre calidad de recepción.
2. Únicamente identifica cada fuente de la capa de transporte en la conferencia por el uso de un nombre canónico. Este nombre puede ser utilizado para asociar varios flujos de datos desde un participante dado como parte de una

sola sesión multimedia. Esto es importante si se está tratando de sincronizar flujos de datos de audio y video.

3. Transmitir paquetes RTCP, así al número total de participantes puede ser determinado. Esto es necesario de todos los participantes con el fin de cumplir con las funciones 1 y 2. La información es necesaria así la velocidad con lo que los datos de control RTCP son transmitidos, pueden ser ajustados a un pequeño porcentaje del ancho de banda total de la sesión.
4. Distribuir información (nombre de usuario, localización, etc.) que identifica a los participantes en la sesión de una manera fácil de usar. Esta información es normalmente desplegada en la interfaz de usuario de la aplicación.

Si se utiliza RTP sobre IP multicast, las funciones 1, 2 y 3 son obligatorias para permitir a la aplicación escalar a un número mayor de participantes. El factor que muchas de las aplicaciones populares multimedia multicast utilice el modelo RTP tiene la siguiente implicación muy importante en el diseño de la red multicast: Cada estación final en una sesión multimedia multicast basada en RTP, es una fuente de tráfico multicast.

2.5.3 Protocolo de Anuncio de Sesión (SAP)

SAP es el protocolo de anunciamiento para sesiones de conferencia multicast. Los clientes SAP anuncian sus sesiones de conferencia periódicamente por paquetes multicast SAP que contienen información de la sesión para un apropiado de la dirección multicast y puerto.

La información de sesión dentro del paquete utiliza el protocolo de descripción de sesión SDP. Cuando se requiera privacidad, la información SDP podría ser encriptado opcionalmente para evitar su lectura por personas no autorizadas.

Anuncios SAP.- La dirección multicast y puerto utilizado para difundir un anuncio SAP depende sobre el mecanismo en ámbito multicast en efecto en el cliente SAP. El ámbito de una sesión multicast está basada sobre el valor de tiempo de vida de la sesión TTL, o sobre un rango de direcciones administrativas que caen dentro del rango de direcciones multicast 239.0.0.0 hasta 239.255.255.255.

Si el ámbito TTL de anuncio está en uso, la dirección multicast utilizada es 224.2.127.254 y el puerto UDP es el 9875. El anuncio de sesión de ámbito TTL siempre es difundido con el mismo valor TTL con el que se encuentra la sesión multicast.

Si el ámbito administrativo de anuncio está en uso, entonces una dirección reservada dentro de la zona de ámbito administrativo (generalmente la dirección más alta) es utilizada con un puerto. Por lo que los clientes SAP, podrían necesitar escuchar a varios grupos multicast para recibir todos los anuncios cuando los anuncios de ámbito administrativo están en uso.

2.6 Multicast en Capa 2

Los equipos de conmutación LAN de capa 2 han pasado de ser una tecnología cara a una de vanguardia, que se ha implementado sólo en el backbone de la red, siendo una tecnología rentable que ahora se ve a menudo. Esto ha llevado a algunos cambios bastante grandes de topologías LAN, siendo construidas donde un número de conmutadores LAN están interconectados a través de enlaces trunk de alta velocidad para formar una sola subred conmutada de gran tamaño.

2.6.1 IGMP Snooping

IGMP snooping es el método por el cual se contrarresta la inundación de tráfico multicast en los switches LAN. Como su nombre lo indica IGMP snooping requiere que los switches fisgoneen la conversación IGMP entre los hosts y el router. Cuando los switches escuchan un reporte IGMP desde un host a un grupo particular multicast, los switches añaden el número del puerto del host a la entrada de la tabla de memoria de contenido direccionable CAM (Content Addressable Memory) multicast asociada. Cuando el switch un mensaje de dejar grupo desde un host, este remueve la entrada del puerto del host de la tabla CAM.

Superficialmente, parecería una simple solución puesta en práctica, sin embargo depende la arquitectura del switch, la implementación de IGMP snooping podría ser difícil de lograr sin degradar gravemente el rendimiento del switch.

Funcionamiento IGMP Snooping.- El software de IGMP snooping examina los mensajes del protocolo IGMP dentro de una VLAN para descubrir cuales interfaces están conectadas a los hosts o a otros dispositivos interesados en recibir este tráfico. Utilizando la información de interfaz, IGMP snooping puede reducir el consumo de

ancho de banda en ambientes multiacceso LAN, para evitar una inundación en toda la VLAN. Dentro de sus funciones se encuentra el seguimiento de cuales puertos están conectados a routers multicast capaces de ayudar a administrar el reenvío de reportes de membresía IGMP. El software IGMP snooping responde a notificaciones de cambio de topología en la red.

La Fig. 2.33 muestra a un switch IGMP snooping que se localiza entre el host y el router IGMP, quien intercepta los reportes de membresía y mensajes de salida, y los reenvía solo cuando es necesario a los routers IGMP conectados.

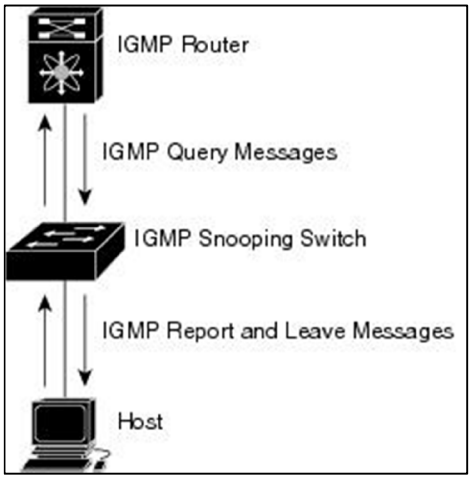


Fig. 2.33 [D]; Funcionamiento IGMP Snooping

CAPÍTULO 3

REQUERIMIENTOS TÉCNICOS PARA LA IMPLEMENTACIÓN DE REDES MULTICAST EN AMBIENTES LAN

3.1 Aspectos a Considerar

Implementar una red multicast en ambientes LAN requiere tener en cuenta varios aspectos, que van desde el host del cliente, equipo activo de red, ancho de banda, políticas de seguridad y calidad de servicio, aplicaciones y servidores multicast.

El host cliente debe cumplir los requerimientos mínimos necesarios a nivel de hardware que asegure un funcionamiento óptimo, así como también a nivel de software, la versión del sistema operativo y soporte de versión IGMP.

A nivel de equipo activo de red se debe verificar la versión de sistema operativo de Internetwork (IOS), y soporte multicast, versión IGMP.

El ancho de banda es un recurso de red, los enlaces por lo general dentro de la LAN son de 100/1000 Mbps, de los cuales comúnmente se distribuye conexiones a 100 Mbps al nivel de acceso y de 1000 Mbps a nivel de troncales, capa de núcleo y distribución de la red. Con estos niveles de ancho de banda es poco probable saturar el enlace haciendo uso de multicast, no obstante las políticas de calidad de servicio juegan un papel predomínate para las transmisiones en tiempo de real de audio y video, asegurando una transmisión con retardos mínimos permisibles.

La seguridad es un aspecto muy importante, no se puede permitir que otras fuentes no confiables inyecten tráfico multicast sobre la red, y peor aún si se utilizan direcciones de grupos ya establecidos. Para esto se debe registrar las direcciones IP multicast que se admiten dentro de la red y las fuentes asociadas a esas direcciones de grupo de manera que se asegure que el tráfico que se desea recibir es confiable.

Las aplicaciones son quienes permitirán a los hosts clientes asociarse y a los servidores inyectar el tráfico multicast sobre la red, estas aplicaciones cliente-servidor deben

soportar las diferentes versiones de IGMP, así como las diferentes plataformas de sistemas operativos sobre las cuales se van a ejecutar.

Los servidores multicast deben ser computadores de igual o mejores prestaciones que los hosts clientes, no influye el número de clientes asociados al grupo ya que el servidor multicast inyecta el tráfico del grupo a la red, y el procesamiento, creación de árboles de distribución y rutas es ejecutado por el equipo activo de red.

3.2 Análisis de requerimientos LAN

3.2.1 Análisis de Recursos de red

Como recursos de red se puede especificar al ancho de banda suficiente para efectuar un streaming de video o realizar una videoconferencia con 'N' participantes, sin saturar los enlaces y degradar los demás servicios de red.

Cuando se habla de multicast se debe tener en mente que se va hacer uso de un solo flujo de datos por grupo multicast, el cual puede contener 1 a 'N' clientes, es decir que la utilización de ancho de banda se mantiene constante indistintamente del número de clientes que deseen acceder al flujo de datos del grupo en cuestión.

La utilización del ancho de banda en sí, queda relegada a la calidad del video o videoconferencia que se desea transmitir, lo cual es configurable en la aplicación de los servidores multicast.

Estas aplicaciones permiten utilizar codecs de audio y de video para realizar una transmisión de alta calidad y bajo consumo de ancho de banda, para nuestro estudio se ha utilizado el códec de video H.264 y de audio MPEG 4 (AAC).

El ancho de banda requerido bajo estas condiciones no supera los 2 Mbps de consumo, por lo que, el uso de multicast en ambientes LAN, permite hacer un uso eficiente de este recurso.

3.2.2 Análisis de Hardware

Para implementar IP multicast se debe considerar los requisitos a nivel de hardware tanto a nivel de host como de equipo activo de red.

A nivel de Computadores.- Tanto para los hosts clientes como para los hosts que funcionen como servidores multicast, se debe cumplir con ciertos requerimientos que las aplicaciones requieren para funcionar de una manera eficiente y sin problemas.

Al hacer varias pruebas de streaming se comprobó que los hosts con mejores recursos a nivel de Procesador y Memoria RAM, no tenían problemas al ejecutar o cargar los archivos de video.

Para que un host cliente o servidor funcione de una manera correcta, sin problemas debe cumplir como requisito mínimo:

Procesador:	Pentium 4 o superior.
Velocidad Procesador:	1.6 GHz o superior.
Memoria RAM:	2 GB o superior.

Si no se cumple con los requisitos mínimos se puede experimentar una cierta anomalía con la velocidad de reproducción del video, y continuos cortes, además que limita el número de aplicaciones ejecutándose simultáneamente dando como resultado lentitud en el procesamiento.

A nivel de Equipo Activo de Red.- El equipamiento necesario para implementar IP multicast sobre una red LAN consta de:

- Router multicast
- Switches

El equipamiento utilizado para las pruebas se basa en equipo CISCO, de las siguientes series, que no representan un limitante, sino una referencia ya que el soporte multicast radica en la versión del IOS que los equipos tengan instalados, y que se verá más adelante.

A nivel de router se ha utilizado el CISCO 3800.

A nivel de switches se ha utilizado los CISCO Catalyst 2950.

3.2.3 Análisis de Software

El software utilizado es una parte fundamental en la implementación, ya que este requiere soportar la tecnología IP multicast. Tanto a nivel de computadores, los hosts clientes y servidores como a nivel de equipo activo de red es necesario comprobar el soporte multicast y la versión IGMP que el sistema soporta.

A nivel de Computadores.- Se utilizó sistemas operativos a nivel de software libre y comercial, con los cuales se realizó pruebas de compatibilidad y funcionalidad para operar con multicast.

Los sistemas operativos comerciales utilizados son Windows XP/Vista/Seven, que soportan multicast, y se describen a continuación:

Para verificar que el host tiene soporte multicast, en los sistemas operativos Windows, se puede verificar la existencia de una ruta definida para las direcciones clase D. En el Shell de comandos de Windows se teclea el comando:

```
route print o netstat –nr
```

Al introducir el comando, se puede notar que aparecerá una tabla de rutas, en la cual una ruta estará definida para que cuando el host quiera enviar un paquete multicast lo haga directamente a través de dicha interfaz, tal como se muestra en la Fig. 3.1.

```
C:\Documents and Settings\robert>route print
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x30002 ...00 13 02 40 bf f1 ...... Intel(R) PRO/Wireless 3945ABG Network Connec
tion - Packet Scheduler Miniport
0x40003 ...00 13 a9 08 c6 cc ...... Intel(R) PRO/100 VE Network Connection - Pac
ket Scheduler Miniport
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      172.30.60.1    172.30.60.243       20
        127.0.0.0        255.0.0.0        127.0.0.1        127.0.0.1        1
     172.30.60.0    255.255.255.0    172.30.60.243    172.30.60.243       20
    172.30.60.243  255.255.255.255        127.0.0.1        127.0.0.1       20
   172.30.255.255  255.255.255.255    172.30.60.243    172.30.60.243       20
        224.0.0.0        240.0.0.0    172.30.60.243    172.30.60.243       20
  255.255.255.255  255.255.255.255    172.30.60.243          30002        1
  255.255.255.255  255.255.255.255    172.30.60.243    172.30.60.243        1
Default Gateway:       172.30.60.1
===========================================================================
Persistent Routes:
  None
```

Fig. 3.1 [A]; Ruta Multicast de un host Windows

Del gráfico se puede observar que la ruta 224.0.0.0 con máscara 240.0.0.0 corresponde a todas las direcciones multicast clase D, de lo cual se concluye que el host tiene soporte multicast.

Después de verificar si tiene soporte multicast, es importante saber que versión de IGMP se está utilizando para comunicarse con el router multicast.

En la investigación se determinó que los sistemas operativos Windows XP/Vista/Seven utilizan IGMPV3 por defecto para comunicarse, lo cual indica que no hace falta configurar nada a nivel de host puesto que los sistemas operativos señalados pueden comunicarse vía IP multicast haciendo uso de IGMPV3 en su última versión actualizada.

El sistema operativo de versión libre utilizado es Ubuntu, en su última versión 11.04, que soporta multicast, y que también hace uso de IGMPV3 por defecto para

comunicarse, sin embargo la versión es configurable cambiando ciertos valores de registro, '0' para utilizar la versión más alta de IGMP y '2' para utilizar IGMPV2. El registro que se debe ajustar es el siguiente:

```
/proc/sys/net/ipv4/conf/eth0/force_igmp_version
```

Esta modificación no solo sirve bajo Ubuntu, sino también se la puede hacer para todos los sistemas operativos LINUX.

A nivel de Equipo Activo de Red.- Tanto el router como los switches utilizados en la implementación deben tener instalados IOS que soporten IP multicast.

La plataforma utilizada para la implementación está basada en equipamiento CISCO, sobre el cual se realiza el presente análisis.

A nivel de router.- IP multicast ha sido soportado en los IOS con el protocolo PIM desde la versión 10.2. Multicast interdominio es soportado eficientemente en las versiones 11.1CC y 12.0. Pero es aconsejable utilizar versiones de IOS 12.0 en adelante para aplicaciones multicast.

La versión de IOS utilizada en la implementación de IP multicast a nivel de capa 3 para el modelo de router CISCO 3800 es la versión 12.4 (17a).

Multicast se encuentra disponible en todos los IOS CISCO basados en plataformas de ruteo, incluyendo los modelos de routers de la tabla 3.1.

Cisco 1003
Cisco 1004
Cisco 1005
Cisco 1600 series
Cisco 2500 series
Cisco 2600 series
Cisco 2800 series
Cisco 2900 series
Cisco 3600 series
Cisco 3800 series
Cisco 4000 series (Cisco 4000, 4000-M, 4500, 4500-M, 4700, 4700-M)
Cisco 7200 series
Cisco 7500 series
Cisco 12000

Tabla 3.1 [J]; Routers CISCO con soporte Multicast

A nivel de switch.- A nivel de capa 2, los switches deben soportar IGMP Snooping, y una versión de software mínima de IGMPV3 para interpretar los mensajes de reporte y de consulta, si se está utilizando esta versión en el proceso de comunicación host – router.

La versión de IOS utilizada en la implementación de IP multicast a nivel de capa 2 para el modelo de switch CISCO Catalyst 2950 es la versión 12.1(22)EA1.

IGMP Snooping tiene varias funciones, las cuales no todas necesariamente deben ser soportadas por versiones de IOS que soporten IGMP Snooping, es decir cada versión de IOS para cada modelo de plataforma CISCO Catalyst incorpora una o varias características de IGMP Snooping, además que los comandos necesarios para aplicarlos también varía de acuerdo al modelo del equipo utilizado.

La tabla 3.2 muestra las plataformas de los switch CISCO Catalyst que soportan el protocolo IGMP Snooping, la versión de IOS mínima necesaria, y si este está habilitado por defecto. Además también indica la versión de IOS mínima necesaria para soportar IGMPV3.

Plataformas Catalyst	IGMP Snooping (Versión de software Mínimo)	Por Defecto	IGMP V3 (Versión de software Mínimo)
Catalyst 6000 - Catalyst OS (CatOS) Software	Si (todas las versiones)	Habilitado	Si (Versión 7.5)
Catalyst 6000- Cisco IOS® Software	Si (todas las versiones)	Habilitado (Desde la versión 5.5.9 y 6.3.1)	Si (Cisco IOS versión 12.1(8a)E)
Catalyst 5000	Si (Versión 4.1)	Deshabilitado	No soportado
Catalyst 4000 - CatOS (Supervisor Engine 1/2) / (2948G/4912G/2980G)	No soportado		No soportado
Catalyst 4000 - Cisco IOS (Supervisor Engine 2+/3/4/5)	Si (todas las versiones)	Habilitado	Si (Cisco IOS versión 12.1(19)EW)
Catalyst 3550	Si (todas las versiones)	Habilitado	Si (Cisco IOS versión 12.1(19)EA1)
Catalyst 3560	Si (Cisco IOS versión 12.1(19)EA1)	Habilitado	Si (Cisco IOS versión 12.1(19)EA1)
Catalyst 3750	Si (todas las versiones)	Habilitado	Si (Cisco IOS versión 12.1(19)EA1)
Catalyst 2940	Si (todas las versiones)	Habilitado	Si (Cisco IOS versión 12.1(19)EA1)
Catalyst 2950/2955	Si (todas las versiones)	Habilitado	Si (Cisco IOS versión 12.1(19)EA1)
Catalyst 2960	Si (todas las versiones)	Habilitado	Si (todas las versiones)
Catalyst 2970	Si (todas las versiones)	Habilitado	Si (Cisco IOS versión 12.1(19)EA1)
Catalyst 2900XL/3500XL	No soportado		No soportado
Catalyst 2948G-L3 / 4908G-L3	No soportado		No soportado
Catalyst 1900/2820	No soportado		No soportado
Catalyst 8500	No soportado		No soportado

Tabla 3.2 [3]; Switches CISCO que soportan IGMP Snooping

3.3 Configuración IGMP en equipo activo de red

Para implementar IP multicast se debe configurar el equipo activo de red, tanto a nivel de capa 3 Routers, quienes permitirán establecer las rutas para el tráfico multicast de los grupos definidos entre las diferentes VLANS o subredes configuradas, además de la versión de IGMP a utilizar para establecer una comunicación con los hosts, y a nivel de capa 2 Switches, quienes permitirán dirigir el tráfico multicast hacia los hosts cliente asociados a los grupos por los puerto adecuados, a través de la interpretación de los mensajes interceptados de la comunicación IGMP entre los hosts y el router multicast.

3.3.1 Configuración multicast Router

Para configurar IP multicast sobre el router se debe introducir los siguientes comandos en la interfaz de configuración del router:

1- Habilitar globalmente multicast

```
Router(config)#ip multicast-routing
```

2- Habilitar el protocolo de ruteo PIM sobre la interfaz o interfaces conectadas hacia los segmentos de red sobre los cuales se establecerá la comunicación multicast, en nuestro caso se utilizara el protocolo de ruteo PIM en modo denso, ya que las características de la topología de red implementada se adapta a la utilización de este modo.

```
Router(config-int)#ip pim dense-mode
```

3- Establecer la versión de IGMP a utilizar sobre la interfaz o interfaces conectadas hacia los segmentos de red sobre los cuales se establecerá la comunicación multicast. Se configurará IGMPV3 para comunicarse con los hosts.

```
Router(config-int)#ip igmp version 3
```

Esta es la configuración básica necesaria para habilitar IP multicast sobre un router CISCO, sin embargo se puede cambiar ciertos parámetros con respecto al funcionamiento del protocolo de ruteo PIM e IGMP.

3.3.2 Configuración multicast Switch

Para configurar IP multicast a nivel de capa 2, el IOS del switch debe soportar IGMP snooping, para interpretar los mensajes interceptados entre los hosts clientes y el router multicast, de manera que se pueda registrar los puertos asociados al grupo multicast y permitir el flujo del tráfico a través de dichos puertos.

Se debe configurar el switch introduciendo los siguientes comandos en la interfaz de configuración del switch:

1- Habilitar IGMP Snooping globalmente, para la versión de IOS utilizada por defecto ya se encuentra activo.

```
Switch(config)#ip igmp-snooping
```

2- Habilitar IGMP Snooping sobre cada VLAN, donde se quiera habilitar la comunicación multicast, para la versión de IOS utilizada por defecto ya se encuentra activo sobre todas las VLANS creadas.

```
Switch(config)#ip igmp-snooping <número de vlan>
```

La configuración por defecto de IGMP Snooping para la versión de IOS utilizada activa el soporte de IGMPV3 de manera mínima, de la misma manera activa la supresión de reportes entre otras opciones.

Sobre cada VLAN se puede realizar ciertos cambios con respecto al comportamiento de IGMP Snooping, sin embargo se mantendrá la configuración por defecto, ya que no se requiere realizar cambios para la implementación multicast propuesta.

3.4 Implementación de un ambiente de Prueba Multicast

Para la realización de las pruebas pertinentes con respecto a la funcionalidad de IP multicast bajo la LAN, se ha implementado un escenario con la finalidad de ejecutar aplicaciones que soporten multicast para emitir streaming de video y realizar video conferencias, de manera que se pueda observar detalladamente el comportamiento y funcionalidad de aplicar IP multicast sobre la LAN.

La Fig. 3.2 muestra el escenario de pruebas, de una topología de red en estrella de una LAN típica.

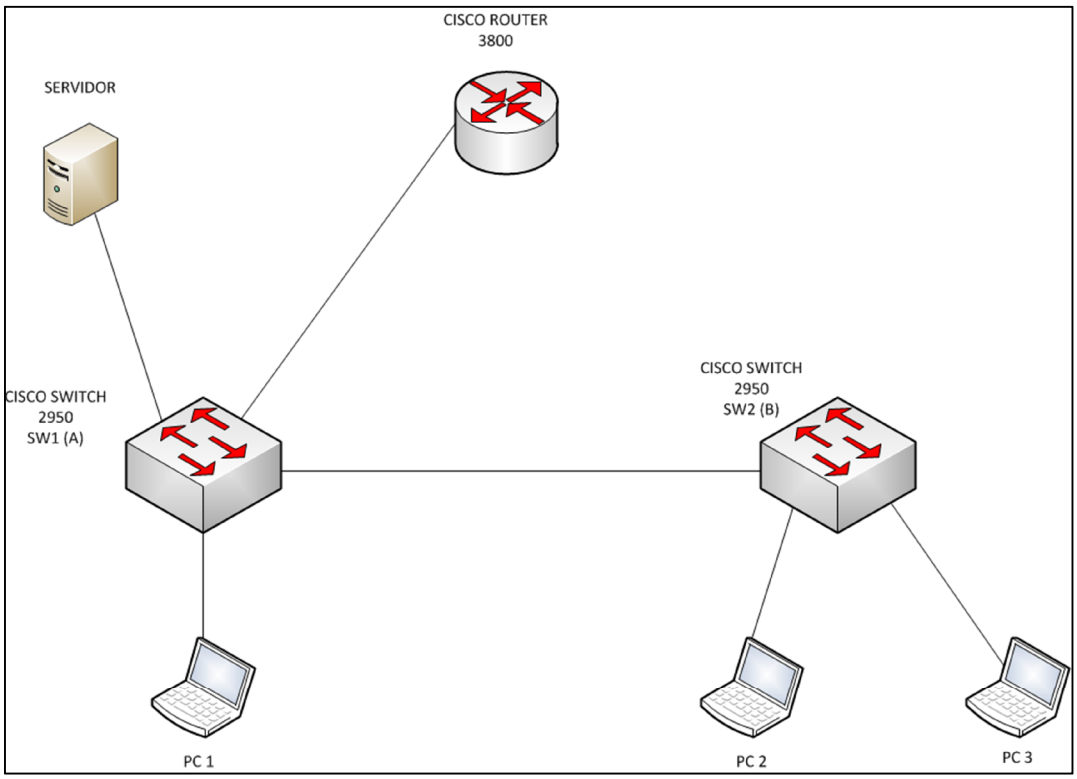


Fig. 3.2 [A]; Ambiente de pruebas multicast

En el ambiente de pruebas se ha configurado varias subredes, se ha establecido el direccionamiento IP, y se ha hecho la asignación de los puertos en los switches tal como se detalla en la tabla 3.3.

# VLAN	Nombre VLAN	Dirección de Subred / Máscara	Gateway	Switch 1 (A) Puertos	Switch 2 (B) Puertos
1	Administración	172.30.0.0/24	172.30.0.1	1	1
2	Facultad de Informática y Electrónica	172.30.10.0/24	172.30.10.1	2 -3	2 -3
3	Facultad de Salud Pública	172.30.20.0/24	172.30.20.1	4 - 5	4 - 5
4	Facultad de Mecánica	172.30.30.0/24	172.30.30.1	6 - 7	6 - 7
5	Facultad de Ciencias	172.30.40.0/24	172.30.40.1	8 - 9	8 - 9
6	Facultad de Recursos Naturales	172.30.50.0/24	172.30.50.1	10 - 11	10 - 11
7	Facultad de Ciencias Pecuarias	172.30.60.0/24	172.30.60.1	12 -13	12 -13
8	Facultad de Administración de Empresas	172.30.70.0/24	172.30.70.1	14 -15	14 -15
9	Administrativos	172.30.80.0/24	172.30.80.1	16 -17	16 -17
10	Servidores	172.30.90.0/24	172.30.90.1	18 - 22	18 - 22

Tabla 3.3 [A]; Detalle configuración escenario de pruebas

La asignación de puertos a los hosts clientes y servidor, además de las conexiones entre equipo activo de red se detalla en la tabla 3.4.

Equipo de Red	Interfaz	Conexión a	Interfaz	Tipo Conexión	Conexión` VLAN	VLANS Permitidas
Router Cisco 3800	GEth0/0	Switch 1 (A)	FEth0/24	Trunk	-	Todas
	GEth0/0.1			-	1	-
	GEth0/0.2			-	2	-
	GEth0/0.3			-	3	-
	GEth0/0.4			-	4	-
	GEth0/0.5			-	5	-
	GEth0/0.6			-	6	-
	GEth0/0.7			-	7	-
	GEth0/0.8			-	8	-
	GEth0/0.9			-	9	-
	GEth0/0.10			-	10	-
Switch 1 (A) Cisco 2950	FEth0/23	Switch 2 (B)	FEth0/24	Trunk	-	Todas
	FEth0/22	Servidor	Eth0	Acceso	10	-
	FEth0/6	PC 1	Eth0	Acceso	4	-
Switch 2 (B) Cisco 2950	FEth0/17	PC2	Eth0	Acceso	9	-
	FEth0/15	PC3	Eth0	Acceso	8	-

Tabla 3.4 [A]; Detalle de conexiones ambiente de pruebas

La Fig. 3.3 detalla el diagrama de conexiones lógico, del ambiente de pruebas para realizar un streaming de video, vía multicast para la dirección IP multicast de grupo 239.0.0.10.

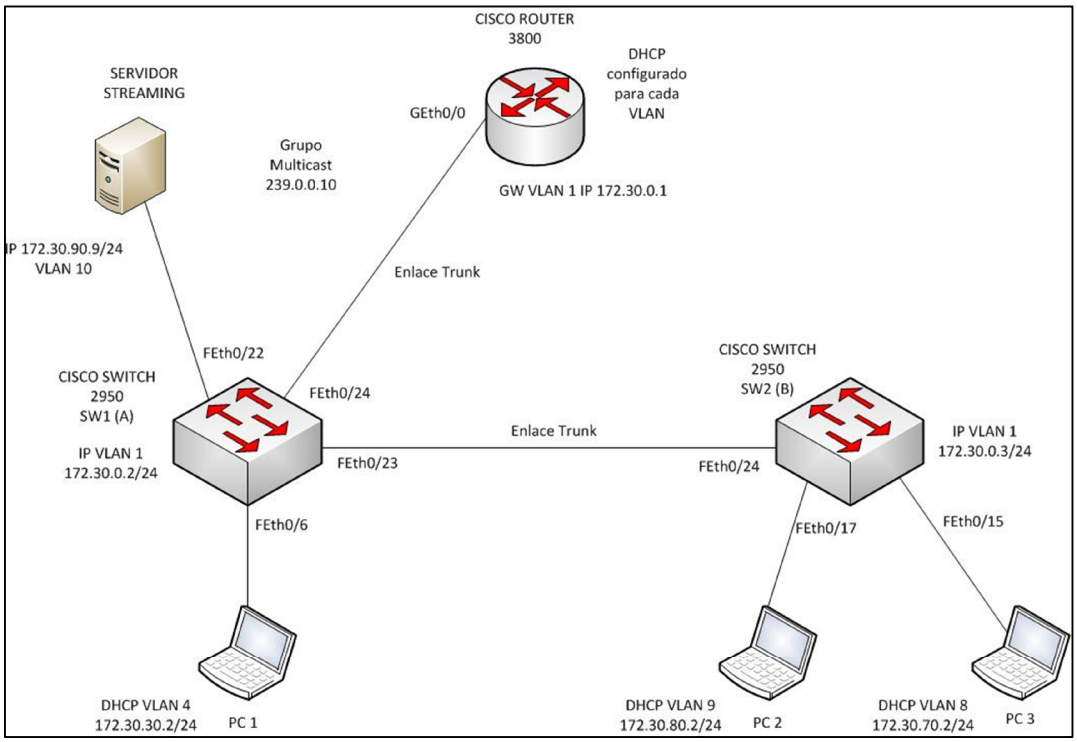


Fig. 3.3 [A]; Diagrama lógico de conexiones para escenario de streaming de video

Después de aplicar la configuración para habilitar IP multicast a nivel de capa 3 en el Router, estableciendo el protocolo de ruteo multicast PIM en modo denso, y la versión de IGMPV3 a utilizar, además de las configuraciones pertinentes a nivel de capa 2 de los Switches, para habilitar IGMP Snooping, se puede analizar el comportamiento de IP multicast en un escenario donde se realizó un streaming de video para el grupo 239.0.0.10, donde todos los hosts clientes de las VLANS excepto la VLAN 1 pueden asociarse al grupo multicast para acceder al flujo de datos del servidor de streaming fuente.

3.4.1 Pruebas a nivel de host

Para realizar las pruebas a nivel de host sobre el comportamiento de IGMP, se ha utilizado un sniffer para capturar todo el tráfico que pase por la subred, la aplicación utilizada para este propósito es Wireshark.

Con esta herramienta se pudo analizar los paquetes tanto de los hosts clientes como del servidor de streaming e interpretar y corroborar la comunicación vía IGMP con el router.

Pruebas sobre el servidor de streaming.- El servidor de streaming configurado con IP estática 172.30.90.9/24, ejecuta una aplicación para realizar un streaming de video al grupo multicast 239.0.0.10.

Al iniciar el proceso de streaming se puede ver el tráfico inyectado vía UDP hacia la subred con destino la dirección IP multicast del grupo, esto se puede evidenciar en la Fig. 3.4.

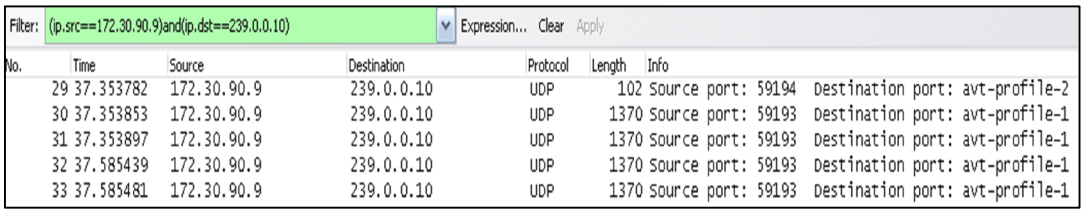


Fig. 3.4 [A]; Flujo de tráfico multicast inyectado por el servidor fuente

Al analizar un paquete UDP del flujo de datos del servidor fuente se puede comprobar cierta información, como la dirección MAC del grupo multicast, la cual siguiendo el proceso mencionado en el capítulo anterior, de la sección correspondiente, y haciendo uso de los 23 bits menos significativos de la dirección IP fuente, se obtiene la dirección MAC 01:00:5E:00:00:0A que representa a la dirección IP multicast, tal como se muestra en la Fig. 3.5.

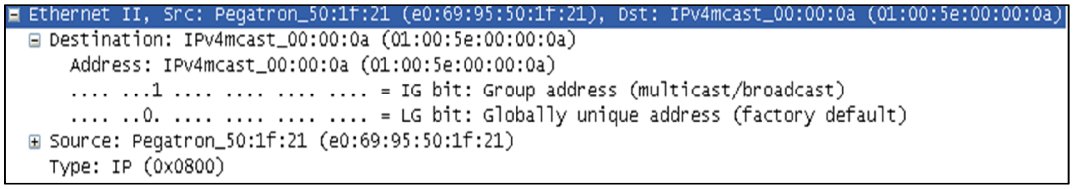


Fig. 3.5 [A]; Dirección MAC grupo multicast streaming de video

El servidor al inyectar el tráfico multicast sobre la subred en la cual se encuentra, producirá que el router multicast detecte este tráfico cuyos paquetes tienen como destino dicho grupo multicast y añada una ruta multicast para alcanzar el servidor fuente.

Pruebas sobre los hosts clientes.- En el escenario multicast, se ha instalado varios hosts indistintamente en diferentes VLANS y Switches para comprobar la comunicación multicast entre VLANS. Los hosts ejecutan una aplicación cliente para formar parte del grupo multicast a quien se le asociado el streaming de video del servidor fuente, en este proceso también se ha capturado paquetes para evidenciar el proceso de asociación al grupo y comunicación con el router multicast.

El host 1 que se encuentra en el Switch1 (A), que pertenece a la VLAN 4, inicia el proceso de asociación al grupo multicast para lo cual hace uso de IGMPV3 para comunicarse con el router multicast y realizar la petición, tal como se evidencia en la Fig. 3.6.

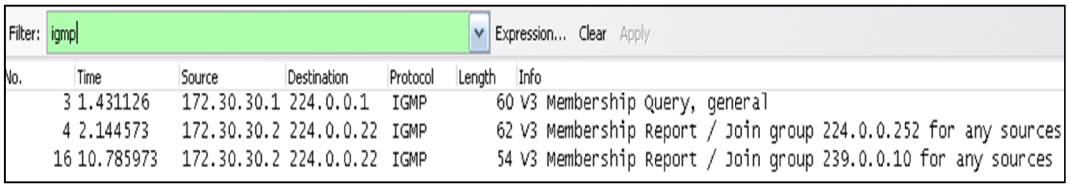


Fig. 3.6 [A]; Comunicación IGMP entre PC1 y el router multicast

Los paquetes capturados indican que el PC1 cuya dirección IP es la 172.30.30.2, primero recibe una consulta de membresía (Membership Query) IGMPV3, emitida por

el router multicast para consultar al host su deseo de pertenecer o de seguir perteneciendo algún grupo multicast, a través de la dirección multicast destino 224.0.0.1 la cual indica todos los hosts dentro de la subred. El host responde a esta consulta con un reporte de membresía (Membership Report) IGMPV3, y a su vez con una petición de unión al grupo (Join Group) 224.0.0.252 que corresponde a un protocolo multicast basado en el sistema de nombre de dominio DNS (Domain Name System) incluido en Windows en sus versiones Vista/Seven y que representa a un grupo de resolución de nombre de enlace local LLMNR (Link Local Multicast Name Resolution). Después envía nuevamente otro reporte de membresía IGMPV3, para unirse al grupo multicast del servidor de streaming 239.0.0.10 para cualquier fuente, lo que indica que el PC1 podrá recibir tráfico multicast del grupo 239.0.0.10 pero no necesariamente del servidor de streaming deseado, lo que representa un problema a nivel de seguridad, para lo cual se puede especificar la dirección IP de la fuente tanto a nivel de aplicación en el cliente o por medio de un control de asociación a grupo sólo para una fuente específica hecho en el router multicast lo cual se indicará más adelante. También se observa que la dirección destino a la cual la PC1 envía los paquetes IGMP corresponden a la dirección multicast 224.0.0.22, utilizada específicamente para comunicarse con el router haciendo uso de IGMPV3

Si el host no deseara seguir recibiendo el tráfico multicast, al cerrar la aplicación, se envía un mensaje de dejar grupo a través de un reporte de membresía con cambio de estado IGMPV3 al router, para que este inicie el proceso de comprobación de la existencia de usuarios que continúan deseando el tráfico multicast, caso contrario el tráfico multicast para ese grupo es cesado en la interfaz correspondiente.

Al asociarse el PC1 al grupo multicast 239.0.0.10, este comenzará a recibir todo el tráfico UDP de dirección origen 172.30.90.9 y de dirección destino el grupo multicast 239.0.0.10.

Para el PC2 en contraste al modo de asociación especificada en la aplicación cliente del PC1, si se especifica la dirección IP de la fuente de la cual se desea recibir el tráfico multicast del grupo al cual se asocia, tal como se muestra en la Fig. 3.7 del proceso de comunicación IGMP del PC2.

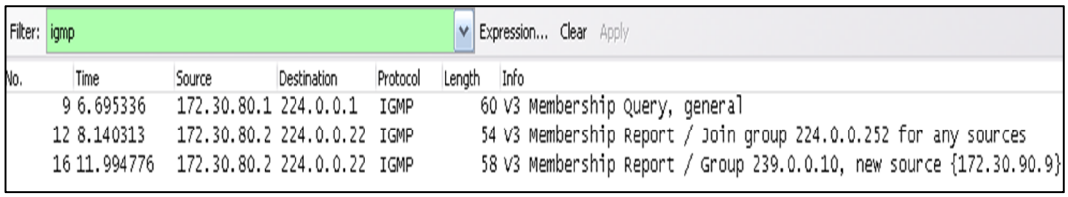


Fig. 3.7 [A]; Comunicación IGMP entre PC2 y el router multicast

Para el PC3 el proceso de asociación es el mismo que el utilizado en el PC2.

3.4.2 Pruebas a nivel de switches

A nivel de capa 2, hay varios comandos proporcionados por CISCO que permiten mostrar la configuración de IP multicast en los switches, y el funcionamiento de IGMP Snooping

Los comandos de verificación de configuración y debug pueden variar dependiendo de la versión de IOS instalada.

Información configuración IGMP.- En el switch1 (A) se puede verificar la configuración de IGMP Snooping ingresando el comando ***show igmp snooping,*** que muestra información sobre los parámetros de configuración global, y también de los parámetros de configuración de cada VLAN tal como se indica en la Fig. 3.8.

```
SwitchA#show ip igmp snooping
Global IGMP Snooping configuration:
-----------------------------------
IGMP snooping              : Enabled
IGMPv3 snooping (minimal)  : Enabled
Report suppression         : Enabled
TCN solicit query          : Disabled
TCN flood query count      : 2
Last member query interval : 1000

Vlan 1:
--------
IGMP snooping                        : Enabled
Immediate leave                      : Disabled
Multicast router learning mode       : pim-dvmrp
Source only learning age timer       : 10
Last member query interval           : 1000
CGMP interoperability mode           : IGMP_ONLY

Vlan 2:
--------
IGMP snooping                        : Enabled
Immediate leave                      : Disabled
Multicast router learning mode       : pim-dvmrp
Source only learning age timer       : 10
Last member query interval           : 1000
CGMP interoperability mode           : IGMP_ONLY

Vlan 3:
--------
IGMP snooping                        : Enabled
Immediate leave                      : Disabled
Multicast router learning mode       : pim-dvmrp
Source only learning age timer       : 10
Last member query interval           : 1000
CGMP interoperability mode           : IGMP_ONLY
```

Fig. 3.8 [A]; Configuración IGMP Snooping Switch1 (A)

De la información de salida del comando se puede verificar que IGMP Snooping, se encuentra habilitado tanto globalmente como en cada una de las VLANS, así también se puede obtener información sobre cómo va a funcionar el protocolo, de esta información, los parámetro más importantes configurados globalmente se describen a continuación:

- IGMPV3 Snooping (minimal).- Corresponde al soporte de IGMPV3 en una versión limitada, para la interpretación de los reportes y consultas de membresía de IGMP en su tercera versión.
- Report suppression.- Limita el tráfico de los reportes de membresía enviados a los routers multicast, por defecto se encuentra habilitado.

- Last member query interval.- Corresponde al intervalo de tiempo (milisegundos) de espera, después de enviar una consulta IGMP para verificar que ningún host que quiera recibir un grupo particular multicast, se encuentre sobre un segmento de red. Si ningún host responde antes que el intervalo de consulta del último miembro expire, se remueve el grupo del puerto de la VLAN asociada.

De la información específica de cada VLAN, los parámetros más importantes se describen a continuación:

- Immediate leave.- Cuando se habilita esta función el switch remueve inmediatamente un puerto del grupo IP multicast cuando este detecta un mensaje de dejar grupo (leave group) IGMP en su versión 2, sobre ese puerto, por defecto se encuentra deshabilitado.
- Multicast router learning mode.- Especifica el modo de aprendizaje del router multicast, y como el switch va a aprender a través de esos puertos utilizando IGMP Snooping, por defecto se encuentra en modo de aprendizaje PIM-DVMRP.
- Source only learning age timer.- Corresponde al tiempo (segundos) de envejecimiento de las entradas de la tabla de reenvío, que el switch aprende usando el método de aprendizaje de fuente única.
- CGMP interoperability mode.- Corresponde a cómo va a funcionar modo CGMP, protocolo propietario de CISCO. Por defecto solo se opera IGMP.

El switch2 (B), utiliza la misma configuración IGMP Snooping que el switch1 (A).

Información de grupos multicast.- Para desplegar información acerca de los grupos IGMP multicast, su modo de compatibilidad y los puertos que se encuentran asociados a cada grupo, se utiliza el comando ***show ip igmp snooping group,*** tal como se muestra en la Fig. 3.9, que corresponde a los host asociados en el switch1 (A).

```
SwitchA#show ip igmp snooping group
Vlan      Group           Version     Port List
------------------------------------------------------
4         239.0.0.10      v3          Fa0/6
8         239.0.0.10                  Fa0/23
9         239.0.0.10                  Fa0/23
```

Fig. 3.9 [A]; Grupos multicast asociados a los puertos en el Switch1 (A)

De la información de salida del comando se puede decir que el grupo 239.0.0.10, que corresponde al streaming de video posee 3 clientes en diferentes VLANS, que el host cliente que se encuentra conectado al puerto 6, utiliza IGMPV3, y que hay dos clientes más que se encuentran conectados en el switch2 (B), ya que el puerto listado para estos clientes corresponde al enlace trunk (puerto 23) que existe entre los dos dispositivos, no muestra la versión que utilizan estos hosts, por cuanto solo se indica que se está enviando tráfico multicast por las VLANS donde se encuentran, más no a los puertos donde se encuentran conectados. La información de los puertos y versión utilizada de estos dos clientes se muestra en el switch2 (B), tal como se indica en la Fig. 3.10.

```
SwitchB#show ip igmp snooping group
Vlan      Group           Version     Port List
------------------------------------------------------
8         239.0.0.10      v3          Fa0/15
9         239.0.0.10      v3          Fa0/17
```

Fig. 3.10 [A]; Grupos multicast asociados a los puertos en el Switch2 (B)

Información de rutas multicast.- Para obtener información sobre las interfaces de las rutas multicast que han sido aprendidas dinámicamente o que se han configurado

manualmente se utiliza el comando ***show ip igmp mrouter,*** tal como se indica en la Fig. 3.11 y Fig. 3.12.

```
SwitchA#show ip igmp snooping mrouter
Vlan     ports
----     -----
   2     Fa0/24(dynamic)
   3     Fa0/24(dynamic)
   4     Fa0/24(dynamic)
   5     Fa0/24(dynamic)
   6     Fa0/24(dynamic)
   7     Fa0/24(dynamic)
   8     Fa0/24(dynamic)
   9     Fa0/24(dynamic)
  10     Fa0/24(dynamic)
```

Fig. 3.11 [A]; Interfaces rutas multicast aprendidas dinámicamente sobre el Switch1 (A)

```
SwitchB#show ip igmp snooping mrouter
Vlan     ports
----     -----
   2     Fa0/24(dynamic)
   3     Fa0/24(dynamic)
   4     Fa0/24(dynamic)
   5     Fa0/24(dynamic)
   6     Fa0/24(dynamic)
   7     Fa0/24(dynamic)
   8     Fa0/24(dynamic)
   9     Fa0/24(dynamic)
  10     Fa0/24(dynamic)
```

Fig. 3.12 [A]; Interfaces rutas multicast aprendidas dinámicamente sobre el Switch2 (B)

De la información de salida se puede notar que las interfaces multicast aprendidas para el switch1 (A) corresponde a las interfaz que se encuentra conectada directamente en modo trunk al router multicast, y en el switch2 (B), corresponde a la interfaz que se encuentra conectada en modo trunk al switch1(A). Como en el router se configuró sub-interfaces para habilitar el ruteo entre VLANS y además se habilitó también el protocolo independiente multicast PIM en cada sub-interfaz, se obtiene una interfaz de ruta multicast por VLAN.

Información versión IGMP interfaces router.- Para obtener información con respecto a la versión IGMP que las interfaces del router multicast soportan se utiliza el comando ***show ip igmp querier,*** la información de salida tanto para el switch1 (A) como para el switch2 (B) es la misma, diferenciándose en la interfaz con la que cada

switch se conecta o a través de la cual se comunica con el router multicast, tal como se indica en la Fig. 3.13 para el switch1 (A).

```
SwitchA#show ip igmp snooping querier
Vlan      IP Address      IGMP Version        Port
-----------------------------------------------------
2         172.30.10.1     v3                  Fa0/24
3         172.30.20.1     v3                  Fa0/24
4         172.30.30.1     v3                  Fa0/24
5         172.30.40.1     v3                  Fa0/24
6         172.30.50.1     v3                  Fa0/24
7         172.30.60.1     v3                  Fa0/24
8         172.30.70.1     v3                  Fa0/24
9         172.30.80.1     v3                  Fa0/24
10        172.30.90.1     v3                  Fa0/24
```

Fig. 3.13 [A]; Versión IGMP que soportan interfaces del router multicast

Información capa 2 direcciones MAC.- De la información obtenida se puede decir que el router multicast en cada sub-interfaz ha sido configurado para que utilice IGMPV3.

Para obtener información de capa 2 con respecto a la tabla de direcciones MAC multicast aprendidas a través de IGMP Snooping, se utiliza el comando ***show mac address-table multicast igmp-snooping***, tal como se indica en la Fig. 3.14 y 3.15.

```
SwitchA#show mac address-table multicast igmp-snooping
Vlan    Mac Address       Type        Ports
----    -----------       ----        -----
   4    0100.5e00.000a    IGMP        Fa0/6, Fa0/24
   8    0100.5e00.000a    IGMP        Fa0/23, Fa0/24
   9    0100.5e00.000a    IGMP        Fa0/23, Fa0/24
```

Fig. 3.14 [A]; Información Capa 2 Switch1 (A)

```
SwitchB#show mac address-table multicast igmp-snooping
Vlan    Mac Address       Type        Ports
----    -----------       ----        -----
   8    0100.5e00.000a    IGMP        Fa0/15, Fa0/24
   9    0100.5e00.000a    IGMP        Fa0/17, Fa0/24
```

Fig. 3.15 [A]; Información Capa 2 Switch2 (B)

La información obtenida permite corroborar la dirección MAC asociada al grupo multicast de streaming de video, además de la VLAN sobre la cual se aprendió, y las interfaces del switch que se encuentran asociadas al grupo multicast.

3.4.3 Pruebas a nivel de router

A nivel de capa 3, hay varios comandos proporcionados por CISCO que permiten mostrar la configuración de IP multicast en los routers, el protocolo de ruteo multicast y el funcionamiento de IGMP.

Información protocolo de ruteo PIM multicast.- Para obtener información acerca del protocolo de ruteo multicast configurado PIM, se utiliza el comando ***show ip pim interface*** o en su defecto para una información más detallada ***show ip pim interface detail.*** Esta información permite saber sobre que interfaces se encuentra configurado, la dirección IP de la interfaz, la versión del protocolo, parámetros sobre su funcionamiento y la dirección IP de la interfaz del router designado (que por lo general es la dirección IP más alta de las interfaces de los routers interconectados) quien se encargará de enviar los mensajes de unión (join), tal como se indica en la Fig. 3.16 y Fig. 3.17.

```
Router#show ip pim interface

Address          Interface                Ver/   Nbr    Query  DR     DR
                                          Mode   Count  Intvl  Prior
172.30.10.1      GigabitEthernet0/0.2     v2/D   0      30     1      172.30.10.1
172.30.20.1      GigabitEthernet0/0.3     v2/D   0      30     1      172.30.20.1
172.30.30.1      GigabitEthernet0/0.4     v2/D   0      30     1      172.30.30.1
172.30.40.1      GigabitEthernet0/0.5     v2/D   0      30     1      172.30.40.1
172.30.50.1      GigabitEthernet0/0.6     v2/D   0      30     1      172.30.50.1
172.30.60.1      GigabitEthernet0/0.7     v2/D   0      30     1      172.30.60.1
172.30.70.1      GigabitEthernet0/0.8     v2/D   0      30     1      172.30.70.1
172.30.80.1      GigabitEthernet0/0.9     v2/D   0      30     1      172.30.80.1
172.30.90.1      GigabitEthernet0/0.10    v2/D   0      30     1      172.30.90.1
```

Fig. 3.16 [A]; Información PIM

De la información obtenida se puede observar que el protocolo de ruteo multicast PIM está configurado sobre todas las sub-interfaces creadas en el router, excepto la interfaz GEth0/0.1, que la versión de PIM utilizada es la segunda, que se encuentra configurado en modo denso, y que el router designado es la misma interfaz, ya que el ambiente multicast configurado sobre la LAN comprende un solo dispositivo router.

```
Router#show ip pim interface detail
GigabitEthernet0/0.2 is up, line protocol is up
  Internet address is 172.30.10.1/24
  Multicast switching: fast
  Multicast packets in/out: 2/0
  Multicast TTL threshold: 0
  PIM: enabled
    PIM version: 2, mode: dense
    PIM DR: 172.30.10.1 (this system)
    PIM neighbor count: 0
    PIM Hello/Query interval: 30 seconds
    PIM Hello packets in/out: 0/246
    PIM State-Refresh processing: enabled
    PIM State-Refresh origination: disabled
    PIM NBMA mode: disabled
    PIM ATM multipoint signalling: disabled
    PIM domain border: disabled
  Multicast Tagswitching: disabled
```

Fig. 3.17 [A]; Información PIM detallada

La información obtenida con este comando detalla la configuración PIM de cada interfaz, indica claramente los intervalos de tiempo en los cuales PIM emite sus mensajes de control, además de otros parámetros de funcionamiento del protocolo.

Información IGMP grupos.- Para obtener información acerca de los grupos multicast que han sido asociados a host clientes haciendo uso de IGMP, se utiliza el siguiente comando ***show ip igmp groups,*** o en su defecto para una información más detallada el comando ***show ip igmp groups detail.*** Esta información permite saber que grupos se encuentran activos en el sistema, sobre que interfaz del router se ha establecido una membresía de grupo, la dirección IP de la interfaz que ha emitido el último reporte entre otros datos de interés, tal como se indica en la Fig. 3.18 y Fig. 3.19.

```
Router#show ip igmp groups
IGMP Connected Group Membership
Group Address    Interface                Uptime    Expires   Last Reporter
oup Accounted
239.255.255.255  GigabitEthernet0/0.10    02:28:20  stopped   172.30.90.1
239.255.255.255  GigabitEthernet0/0.9     02:28:20  stopped   172.30.80.1
239.255.255.255  GigabitEthernet0/0.8     02:28:20  stopped   172.30.70.1
239.255.255.255  GigabitEthernet0/0.7     02:28:20  stopped   172.30.60.1
239.255.255.255  GigabitEthernet0/0.6     02:28:20  stopped   172.30.50.1
239.255.255.255  GigabitEthernet0/0.5     02:28:20  stopped   172.30.40.1
239.255.255.255  GigabitEthernet0/0.4     02:28:20  stopped   172.30.30.1
239.255.255.255  GigabitEthernet0/0.3     02:28:20  stopped   172.30.20.1
239.255.255.255  GigabitEthernet0/0.2     02:28:20  stopped   172.30.10.1
239.0.0.10       GigabitEthernet0/0.9     00:00:28  stopped   172.30.80.2
239.0.0.10       GigabitEthernet0/0.4     00:00:28  00:02:31  172.30.30.2
239.0.0.10       GigabitEthernet0/0.8     00:01:28  stopped   172.30.70.2
```

Fig. 3.18 [A]; Información IGMP grupos

De la información obtenida se puede observar dos grupos multicast, uno por defecto el 239.255.255.255 al cual están asociadas todas las interfaces y es propia del sistema, y el grupo de streaming 239.0.0.10, que se encuentra asociado a las sub-interfaces del router conectadas a cada VLAN donde se encuentran los hosts clientes, que para el escenario de prueba corresponde las VLANS 4, 8 y 9, además también se puede verificar que la dirección IP de la última interfaz que ha emitido un reporte corresponde a la de los hosts clientes, ya que sólo se tiene un cliente por VLAN. El tiempo que se encuentra enviando el tráfico por la interfaz y el tiempo de expiración también se puede observar en dicha información.

```
Router#show ip igmp groups 239.0.0.10 detail

Flags: L - Local, U - User, SG - Static Group, VG - Virtual Group,
       SS - Static Source, VS - Virtual Source,
       Ac - Group accounted towards access control limit

Interface:      GigabitEthernet0/0.8
Group:          239.0.0.10
Flags:
Uptime:         00:00:52
Group mode:     INCLUDE
Last reporter:  172.30.70.2
Group source list: (C - Cisco Src Report, U - URD, R - Remote, S - Static,
                    V - Virtual, M - SSM Mapping, L - Local,
                    Ac - Channel accounted towards access control limit)
  Source Address   Uptime    v3 Exp   CSR Exp   Fwd  Flags
  172.30.90.9      00:00:52  00:02:07  stopped   Yes  R

Interface:      GigabitEthernet0/0.9
Group:          239.0.0.10
Flags:
Uptime:         00:01:19
Group mode:     INCLUDE
Last reporter:  172.30.80.2
Group source list: (C - Cisco Src Report, U - URD, R - Remote, S - Static,
                    V - Virtual, M - SSM Mapping, L - Local,
                    Ac - Channel accounted towards access control limit)
  Source Address   Uptime    v3 Exp   CSR Exp   Fwd  Flags
  172.30.90.9      00:01:19  00:01:40  stopped   Yes  R

Interface:      GigabitEthernet0/0.4
Group:          239.0.0.10
Flags:
Uptime:         00:02:17
Group mode:     EXCLUDE (Expires: 00:01:43)
Last reporter:  172.30.30.2
Source list is empty
```

Fig. 3.19 [A]; Información IGMP grupos detallada

La información obtenida con este comando detalla la asociación con el grupo multicast de streaming 239.0.0.10, donde se puede observar información descrita anteriormente, y nueva información como una lista de direcciones IP de servidores fuente que estén emitiendo tráfico bajo el grupo multicast antes mencionado, y al cual se haya asociado explícitamente, para el escenario el host2 y el host3 si especifican la fuente del grupo multicast (172.30.90.9) del cual desean obtener el streaming, el host1 no lo hace, esto se especificó vía la aplicación cliente para la recepción del streaming.

Información IGMP miembros.- Para obtener información acerca de los miembros o clientes asociados a los grupos, se hace uso del siguiente comando ***show ip igmp membership,*** o en su defecto la información detallada de miembros del grupo que se requiere analizar ***show ip igmp membership <grupo> all.*** Esta información permite saber la dirección IP del cliente asociado, la versión IGMP que utiliza, tiempos e interfaz del router sobre la cual se está enviando el tráfico multicast, tal como se indica en la Fig. 3.20 y Fig. 3.21.

```
Router#show ip igmp membership
Flags: A  - aggregate, T - tracked
       L  - Local, S - static, V - virtual, R - Reported through v3
       I - v3lite, U - Urd, M - SSM (S,G) channel
       1,2,3 - The version of IGMP the group is in
Channel/Group-Flags:
       / - Filtering entry (Exclude mode (S,G), Include mode (*,G))
Reporter:
       <mac-or-ip-address> - last reporter if group is not explicitly tracked
       <n>/<m>      - <n> reporter in include mode, <m> reporter in exclude

 Channel/Group                 Reporter        Uptime   Exp.  Flags  Interface
 *,239.255.255.255             172.30.90.1     02:35:46 stop  3LA    Gi0/0.10
 *,239.255.255.255             172.30.80.1     02:35:46 stop  3LA    Gi0/0.9
 *,239.255.255.255             172.30.70.1     02:35:46 stop  3LA    Gi0/0.8
 *,239.255.255.255             172.30.60.1     02:35:46 stop  3LA    Gi0/0.7
 *,239.255.255.255             172.30.50.1     02:35:46 stop  3LA    Gi0/0.6
 *,239.255.255.255             172.30.40.1     02:35:46 stop  3LA    Gi0/0.5
 *,239.255.255.255             172.30.30.1     02:35:46 stop  3LA    Gi0/0.4
 *,239.255.255.255             172.30.20.1     02:35:46 stop  3LA    Gi0/0.3
 *,239.255.255.255             172.30.10.1     02:35:46 stop  3LA    Gi0/0.2
 *,239.0.0.10                  172.30.70.2     00:02:23 stop  3A     Gi0/0.8
 *,239.0.0.10                  172.30.80.2     00:02:50 stop  3A     Gi0/0.9
 *,239.0.0.10                  172.30.30.2     00:03:47 00:13 3A     Gi0/0.4
```

Fig. 3.20 [A]; Información de IGMP miembros

De la información se puede observar que para el grupo local del sistema 239.255.255.255 los miembros son las interfaces del router sobre las cuales está configurado IGMP. Para el grupo de streaming 239.0.0.10 se puede verificar que los miembros son los hosts clientes, que la versión de IGMP es la tercera, y que el cliente ha sido agregado (A).

```
Router#show ip igmp membership 239.0.0.10 all
Flags: A  - aggregate, T - tracked
       L  - Local, S - static, V - virtual, R - Reported through v3
       I - v3lite, U - Urd, M - SSM (S,G) channel
       1,2,3 - The version of IGMP the group is in
Channel/Group-Flags:
       / - Filtering entry (Exclude mode (S,G), Include mode (*,G))
Reporter:
       <mac-or-ip-address> - last reporter if group is not explicitly tracked
       <n>/<m>      - <n> reporter in include mode, <m> reporter in exclude

 Channel/Group                 Reporter        Uptime   Exp.  Flags  Interface
 *,239.0.0.10                  172.30.30.2     00:00:57 02:57 3A     Gi0/0.4
 *,239.0.0.10                  172.30.70.3     00:02:38 stop  3A     Gi0/0.8
 172.30.90.9,239.0.0.10                        00:02:38 02:52 RA     Gi0/0.8
 *,239.0.0.10                  172.30.80.2     00:03:35 stop  3A     Gi0/0.9
 172.30.90.9,239.0.0.10                        00:03:35 01:52 RA     Gi0/0.9
```

Fig. 3.21 [A]; Información de IGMP miembros grupo 239.0.0.10

La información obtenida con este comando detalla los miembros del grupo multicast en cuestión, desplegando además de la información antes mencionada, también la fuente de la cual se está obteniendo el tráfico multicast para el grupo de streaming, en el caso del escenario tanto para el host2 y host3 corresponde a la fuente 172.30.90.9 con el grupo multicast 239.0.0.10.

Información IGMP interfaces.- Para obtener información acerca de cómo está configurado IGMP en las interfaces del router, se utiliza el comando ***show ip igmp interface,*** esta información permite saber los parámetros de funcionamiento de IGMP sobre la interfaz, además de mostrar estadística con respecto al uso de multicast e IGMP, tal como se indica en la salida parcial del comando de una interfaz de la Fig.3.22.

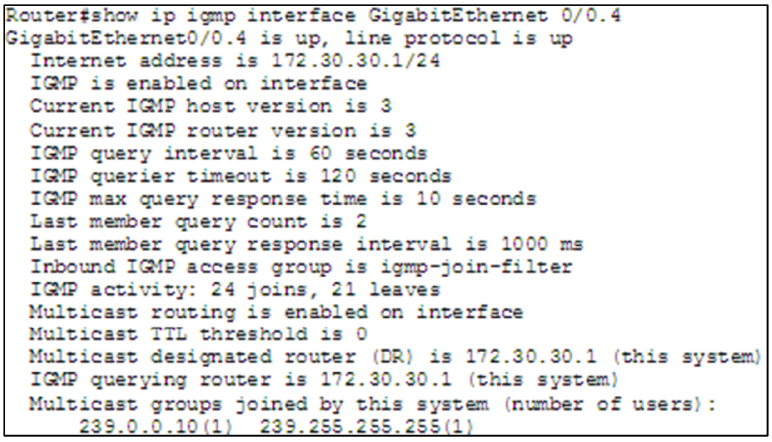


Fig. 3.22 [A]; Información IGMP sobre interfaces

De la información obtenida se puede verificar que para la interfaz Gateway de la VLAN 4, se encuentra habilitado IGMP en su tercera versión, a nivel de host también se detecta que se está utilizando IGMPV3, se obtiene también los valores de tiempo con los cuales IGMP está operando, como:

- IGMP query interval.- Se refiere al intervalo de tiempo de consulta IGMP de 60 segundos, tiempo que el router almacena un estado IGMP si no escucha ningún reporte sobre el grupo.
- IGMP query timeout,- Se refiere al tiempo utilizado por los routers que no ganaron el proceso de router consultor IGMP, y si no escuchan ninguna consulta en el tiempo de 2 veces el tiempo de timeout, ellos inician el proceso de elección nuevamente, el valor por defecto es 120 segundos.
- IGMP max query response time.- Se refiere al tiempo máximo que un router espera para recibir un contestación o mensaje de reporte a una consulta, si este no recibe ninguna contestación se iniciará el proceso de verificación si existe algún cliente que desee el tráfico de algún grupo, sino se recibe respuesta se cesa el envío de tráfico por esa interfaz. El valor por defecto es de 10 segundos.

Indica también si está aplicando algún filtro a nivel de IGMP como seguridad, para la asociación de grupos, información multicast, la IP del router designado, la IP del router consultor IGMP, y los grupos a los cuales se han unido por esa interfaz.

Información rutas multicast.- Para obtener información con respecto a las rutas multicast necesarias para saber a dónde reenviar el tráfico multicast se utiliza el comando ***show ip mroute,*** esta información permite saber la ruta para alcanzar un grupo multicast, en qué modo se está ruteando el tráfico entre otros datos, tal como se indica en la Fig. 3.23.

```
Router#show ip mroute
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 239.255.255.255), 04:12:20/stopped, RP 0.0.0.0, flags: DCL
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    GigabitEthernet0/0.10, Forward/Dense, 04:12:20/00:00:00
    GigabitEthernet0/0.9, Forward/Dense, 04:12:20/00:00:00
    GigabitEthernet0/0.8, Forward/Dense, 04:12:20/00:00:00
    GigabitEthernet0/0.7, Forward/Dense, 04:12:20/00:00:00
    GigabitEthernet0/0.6, Forward/Dense, 04:12:20/00:00:00
    GigabitEthernet0/0.5, Forward/Dense, 04:12:20/00:00:00
    GigabitEthernet0/0.4, Forward/Dense, 04:12:20/00:00:00
    GigabitEthernet0/0.3, Forward/Dense, 04:12:20/00:00:00
    GigabitEthernet0/0.2, Forward/Dense, 04:12:20/00:00:00

(*, 239.0.0.10), 03:47:29/stopped, RP 0.0.0.0, flags: DC
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    GigabitEthernet0/0.4, Forward/Dense, 00:00:20/00:00:00
    GigabitEthernet0/0.9, Forward/Dense, 00:02:42/00:00:00
    GigabitEthernet0/0.8, Forward/Dense, 00:04:49/00:00:00

(172.30.90.9, 239.0.0.10), 01:06:24/00:02:55, flags: T
  Incoming interface: GigabitEthernet0/0.10, RPF nbr 0.0.0.0
  Outgoing interface list:
    GigabitEthernet0/0.4, Forward/Dense, 00:00:20/00:00:00
    GigabitEthernet0/0.9, Forward/Dense, 00:02:42/00:00:00
    GigabitEthernet0/0.8, Forward/Dense, 00:04:49/00:00:00
```

Fig. 3.23 [A]; Rutas Multicast

De la información obtenida se puede verificar las rutas para alcanzar los grupos multicast detectados, el modo de propagación del envío del tráfico, en modo denso, y

las interfaces por las cuales se está enviando el tráfico. Para el grupo de streaming se observa también que se tiene dos rutas para alcanzar los hosts clientes, una ruta hacia el grupo sin especificar la fuente y otra especificando la fuente.

Información sobre las rutas multicast activas.- Para obtener información con respecto a las rutas multicast activas hacia los grupos multicast, y el promedio de ancho de banda utilizado se utiliza el comando ***show ip mroute active,*** tal como se indica en la Fig. 3.24.

```
Router#show ip mroute active
Active IP Multicast Sources - sending >= 4 kbps
 a negative (-) Rate counts pps being fast-dropped

Group: 239.0.0.10, (?)
   Source: 172.30.90.9 (?)
     Rate: 60 pps/654 kbps(1sec), 715 kbps(last 20 secs), 455 kbps(life avg)
```

Fig. 3.24 [A]; Información rutas multicast activas

De la información obtenida, se puede verificar que la única ruta multicast activa corresponde a la del grupo de streaming 239.0.0.10, cuya fuente es la 172.30.90.9, y en donde estadísticamente se obtiene un consumo promedio de ancho de banda de 445kbps para este grupo multicast.

3.5 QoS en ambientes Multicast

Calidad de servicio multicast es una o varias mediciones de prioridades y funcionamiento deseado de un sistema de comunicaciones. QoS a nivel de multicast puede ser administrado o controlado a través del uso de asignación de ancho de banda, prioridad de enlaces, reserva de recursos y controles basados en clases.

Aplicación QoS sobre equipo activo de red.- Para que QoS funcione de manera óptima esta tiene que ser aplicada de extremo a extremo, es decir desde el cliente, dispositivos en la capa de acceso de la red, siguiendo por la capa de distribución y núcleo.

A nivel de equipo activo de red estos deben soportar QoS, para que se pueda aplicar cualquiera de los mecanismos antes mencionados. Para los equipos CISCO dependerá del IOS que se utilice para el soporte de mecanismos de QoS.

Para establecer los valores QoS se ha utilizado un mapeo de marcas tanto a nivel de capa 2 y capa 3, para los diferentes tipos de aplicaciones, tal como se indica en la tabla 3.5.

Application	Layer 3 Classification			Layer 2 CoS
	IPP	PHB	DSCP	
Reserved	7	—	56–62	7
Reserved	6	—	48	6
Voice bearer	5	EF	46	5
Video-data traffic	4	AF41	34	4
Mission-critical data	3	AF31	26	3
Transactional data	2	AF2x	18, 20, 22	2
Scavenger	1	—	8	1
Bulk data	1	AF1x	10, 12, 14	1
Best-effort data	0	BE	0	0
Less-than-best-effort data	0	—	2, 4, 6	0

Tabla 3.5 [6]; Correspondencia de Marcas a Nivel de Capa 2 y 3 para la aplicar QoS

Configuración QoS a nivel de switches.- Para establecer QoS a nivel de capa 2, se ha establecido el mecanismo de clasificación y marcaje de paquetes, a nivel de servidores de streaming y video conferencia utilizando los valores clase de servicio COS (Class of Service).

El marcaje de paquetes se lo realiza a nivel de capa de acceso en los switch, que para el ambiente de pruebas corresponde a cualquiera de los puertos que se encuentren en la VLAN 10 (Servidores) del Switch1 (A), para lo cual se utiliza el siguiente comando:

```
SwitchA(config)#interface range fastEthernet 0/18 – 22
SwitchA(config-if-range)#mls qos cos 4
SwitchA(config-if-range)#mls qos cos override
```

Al aplicar esta configuración, se ha establecido el marcaje de paquetes para el rango de interfaces cuyo valor COS es de 4, además que se indica que se sobrescriba este valor aún si los paquetes que ingresen por la interfaz ya hayan sido marcados.

Para las interfaces de los enlaces trunk, de conexiones al router y entre switches se establece la siguiente configuración: para ambos switches:

```
SwitchA(config)#interface range fastEthernet 0/23 – 24
SwitchA(config-if-range)#mls qos trust cos pass-through dscp
SwitchB(config)#interface fastEthernet 0/24
SwitchB(config-if)#mls qos trust cos pass-through dscp
```

Al aplicar esta configuración en los enlaces trunk de ambos switches, se aplicará COS sin modificar los valores de diferenciación de servicios de código de punto DSCP (Diferent Service Code Point), dejando pasar las tramas a través del switch sin modificar los valores COS y DSCP, para todo el tráfico entrante en esas interfaces.

Después de aplicar la configuración sobre las interfaces, se debe establecer que planificador de colas se va a utilizar, para priorizar el tráfico, para el escenario de pruebas se utiliza el planificador WRR-PQ(Weighted Round-robin), que es un planificador basado en turnos con mezcla del planificador de prioridad de cola. Para establecer los valores del planificador se ha establecido porcentajes de utilización para los diferentes colas que representan a diferente tipo de tráfico, tal como se indica en la siguiente configuración:

```
SwitchA(config)#wrr-queue bandwidth 20 20 80 0
SwitchA(config)# wrr-queue cos-map 1 0 1 2
SwitchA(config)# wrr-queue cos-map 2 4
SwitchA(config)# wrr-queue cos-map 3 3 6 7
SwitchA(config)# wrr-queue cos-map 4 5
```

De la configuración indicada se nota la existencia de 4 colas, en la que la cola 4, al tener el valor asignado de 0 en la asignación de pesos para cada cola en el ajuste de ancho de banda, está será la cola de prioridad asociada con el valor COS de 5 que representa a la aplicación de VOZ sobre IP, para la videoconferencia y streaming de video se ha establecido un peso de 20 para la asignación de ancho de banda en la cola 2, asociada con el valor COS de 4 que representa a las aplicaciones de video, del mismo modo se ha establecido valores para la cola 1 y 3, de acuerdo a la figura de correspondencia de marcas antes indicada. Esta configuración también se aplica en el Switch2 (B).

Configuración QoS a nivel de router.- Para establecer la configuración QoS a nivel de capa 3, se ha utilizado la tabla 3.6, que indica la relación de la aplicación a correr,

con los valores IPP, PHB y DSCP a utilizar, además del mecanismo de encolamiento a aplicar para cada aplicación en cuestión.

APLICACIÓN O CLASE	DSCP		IP PRECEDENCE	MECANISMO ENCOLAMIETO
	PHB	Dec.		
VOICE BEARER	EF	46	5	LLQ
VIDEO CONFERENCING	AF41	34	4	LLQ
CALL SIGNALING	AF31	26	3	CBWFQ
HIGH PRIORITY DATA	AF21	18	2	CBWFQ
BEST EFFORT DATA	BE	0	0	FWQ

Tabla 3.6 [A]; Valores para configurar QoS de acuerdo a la clase de aplicación

Para configurar QoS en el router primero se debe crear las clases de tráfico sobre las cuales se va aplicar la configuración y los valores con respecto al ancho de banda a asignar de acuerdo al mecanismo de encolamiento asignado, tal como se indica en la tabla 3.7.

APLICACIÓN O CLASE	MECANISMO ENCOLAMIETO	ANCHO DE BANDA
VOICE BEARER	LLQ	10%
VIDEO CONFERENCING	LLQ	20%
CALL SIGNALING	CBWFQ	10%
HIGH PRIORITY DATA	CBWFQ	20%
BEST EFFORT DATA	FWQ	15%

Tabla 3.7 [A]; Clases de tráfico y asignación de ancho de banda

Para crear las clases y filtrar los diferentes tipos de tráfico de acuerdo a los valores DSCP en los paquetes que llegan al router se aplica la siguiente configuración:

```
Router(config)# class-map match-all voice
Router(config-cmap)#match dscp EF
Router(config)# class-map match-all video_conferencing
Router(config-cmap)#match cos 4
```

```
Router(config)# class-map match-all call_signaling
Router(config-cmap)#match dscp AF31
Router(config)# class-map match-all high_priority_data
Router(config-cmap)#match dscp AF21
```

Después de crear las clases se crea las políticas sobre cada una de las clases aplicando los mecanismos de encolamiento pertinentes al tipo de tráfico:

```
Router(config)#policy-map qos_clases
Router(config-pmap)#class voice
Router(config-pmap-c)priority percent 10
Router(config-pmap)#class video_conferencing
Router(config-pmap-c) priority percent 20
Router(config-pmap)#class call_signaling
Router(config-pmap-c)bandwidth percent 10
Router(config-pmap)#class  high_priority_data
Router(config-pmap-c)bandwidth percent 20
Router(config-pmap)#class class-default
Router(config-pmap-c)fair-queue 16
```

Después de crear la política, esta debe ser asignada sobre la interfaz en sentido de salida de tráfico, en este caso para el escenario de prueba planteado, tal como indica la siguiente configuración:

```
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#service-policy output qos_clases
```

La Fig. 3.25 muestra la información obtenida al aplicar un comando de monitoreo ***show policy-map interface*** de la política de QoS aplicada sobre la interfaz que conecta al router a la LAN.

```
Router#show policy-map interface gigabitEthernet 0/0
 GigabitEthernet0/0

  Service-policy output: qos_clases

    Class-map: video_conferencing (match-all)
      64565 packets, 88400102 bytes
      5 minute offered rate 509000 bps, drop rate 0 bps
      Match:  dscp cs4 (32)
      Queueing
        Strict Priority
        Output Queue: Conversation 24
        Bandwidth 20 (%)
        Bandwidth 20000 (kbps) Burst 500000 (Bytes)
        (pkts matched/bytes matched) 2/2748
        (total drops/bytes drops) 0/0
```

Fig. 3.25 [A]; Información de política de QoS aplicada

De la información obtenida se puede observar la clase creada video_conferencing, con cierta estadística de los paquetes que han sido tratados como tráfico prioritario de videoconferencia, además se puede observar que todos los paquetes cumplen con el marcaje realizado a nivel de capa 2, con un valor COS igual a 4, equivalente a DSCP igual a 32. Para esta clase de tráfico se señala también el mecanismo de encolamiento aplicado para aplicaciones que transmiten datos en tiempo real, como lo es LLQ, y el parámetro aplicado de reserva de ancho de banda del 20% para este tipo de tráfico.

3.6 Seguridad en ambientes Multicast

Para aplicar seguridad en ambientes multicast se requiere limitar la proliferación de grupos multicast no autorizados sobre la red, es necesario también establecer filtros para que el tráfico multicast se quede dentro de la LAN y no salga hacia el Internet, además de establecer políticas para que los clientes puedan asociarse a los grupos publicados, pero siempre de una fuente confiable.

Filtros sobre clientes multicast.- Para limitar el acceso de una red o a uno o varios clientes, para que no puedan acceder a ningún grupo multicast se aplica listas de acceso sobre las interfaces en dirección de entrada de manera que se niegue todo el tráfico IGMP, impidiendo la comunicación con el router multicast, a continuación se muestra la configuración para el ambiente de pruebas multicast, negando el tráfico multicast para la VLAN 2.

```
Router(config)#ip access-list extended bloqueo_IGMP_VLAN2
Router(config-ext-nacl)#deny igmp 172.30.10.0 0.0.0.255 any log
Router(config-ext-nacl)#permit ip host 0.0.0.0 host
255.255.255.255 log
Router(config-ext-nacl)#permit ip 172.30.10.0 0.0.0.255 any log
Router(config-ext-nacl)#deny ip any any
Router(config)#inter gigabitEthernet 0/0.2
Router(config-subif)#ip access-group bloqueo_IGMP_VLAN2 in
```

Políticas de Seguridad sobre el tráfico entrante y saliente.- Para no permitir suplantación de IP (IP Spoofing) y tráfico no deseado sobre cada subred se aplica listas de acceso en cada subred tanto en dirección de entrada como de salida, como se muestra a continuación para el ambiente de pruebas.

Creación de las listas de acceso de seguridad para cada VLAN en sentido de entrada y salida de tráfico:

```
Router(config)#ip access-list extended seguridad_vlan2_out
Router(config-ext-nacl)#permit ip any 172.30.10.0 0.0.0.255 log
Router(config-ext-nacl)#permit  ip  any  239.0.0.0  0.255.255.255
log
Router(config-ext-nacl)#deny ip any any
Router(config)#ip access-list extended seguridad_vlan3_out
Router(config-ext-nacl)#permit ip any 172.30.20.0 0.0.0.255 log
Router(config-ext-nacl)#permit  ip  any  239.0.0.0  0.255.255.255
log
Router(config-ext-nacl)#deny ip any any
Router(config)#ip access-list extended seguridad_vlan3_in
Router(config-ext-nacl)#permit    ip    host    0.0.0.0    host
255.255.255.255 log
Router(config-ext-nacl)#permit ip 172.30.20.0 0.0.0.255 any log
Router(config-ext-nacl)#deny ip any any
```

Esta configuración se debe realizar para cada VLAN.

Aplicación de las listas de acceso de seguridad sobre las sub-interfaces creadas para cada VLAN en sentido de entrada y salida de tráfico:

```
Router(config)#interface gigabitEthernet 0/0.2
Router(config-subif)#ip access-group seguridad_vlan3_out out
Router(config)#interface gigabitEthernet 0/0.3
Router(config-subif)#ip access-group seguridad_vlan3_in in
Router(config-subif)#ip access-group seguridad_vlan3_out out
```

Esta configuración se la debe realizar sobre cada sub-interfaz.

Para evitar que los paquetes del tráfico multicast se filtren hacia la Internet, es necesario aplicar dos políticas:

1- Limitar el valor TTL de los paquetes multicast para la red LAN, para un sitio el valor adecuado TTL es de 15, como en el ambiente de pruebas multicast se utiliza un solo router que rutea varias VLANS el valor TTL adecuado será de 2, que indica un solo salto, después de ello el paquete si vuelve a llegar a la interfaz de un router este será eliminado.

2- Aplicar una lista de acceso en la interfaz de salida hacia el Internet, negando todo el tráfico multicast, o en su defecto el rango de direcciones multicast de uso interno.

Filtros sobre grupos multicast.- Para limitar la asociación de los clientes, sólo a grupos multicast permitidos y de una fuente confiable, se crea una lista de acceso indicando los grupos a los cuales se permite asociarse y se la aplica en cada interfaz donde se encuentre habilitado multicast. Tal como se muestra en la configuración siguiente:

```
Router(config)#ip access-list standard igmp-join-filter
Router(config-ext-nacl)#permit 239.0.0.10
Router(config-ext-nacl)#permit 239.255.6.1
Router(config-ext-nacl)#deny igmp any any
Router(config)#inter gigabitEthernet 0/0.2
Router(config-subif)#ip igmp access-group igmp-join-filter
```

CAPÍTULO 4

SOFTWARE PARA VIDEO STREAMING Y VIDEOCONFERENCIA CON SOPORTE MULTICAST

4.1 Introducción

Para que un ambiente multicast sea productivo, requiere de aplicaciones que soporten esta tecnología y estándares IGMP. En el mercado no se encuentra muy difundida la tecnología IP multicast, con respecto a su implementación y uso. A nivel WAN por los costos elevados de utilización de ancho de banda, se utiliza ciertas aplicaciones propietarias para transmitir streaming de video y realizar conferencias a lugares remotos, a nivel universitario es utilizado frecuentemente. A nivel LAN su uso no es muy popular ya que por la diferencia de anchos de banda a utilizar superiores en gran medida a los utilizados en la WAN, se prefiere establecer conexiones unicast, no obstante estas aplicaciones con un incremento de usuarios a gran escala, cientos, ya no son escalables y el deterioro de los recursos de red a nivel LAN son notables.

En el mercado se puede encontrar numerosas aplicaciones para streaming y videoconferencia con soporte multicast para utilización tanto a nivel LAN como WAN, siendo estas aplicaciones costosas ya que requieren el pago por licencias de utilización por número de usuarios soportados.

El incremento de aplicaciones con categoría de software libre ha permitido desarrollar potentes aplicaciones con los fines de streaming y videoconferencia, que soportan multicast, es así como haciendo uso de dos aplicaciones ampliamente difundidas en la red ha sido posible realizar streaming de video y establecer conferencias multipunto.

En el ambiente de pruebas multicast, las aplicaciones fueron probadas, con resultados positivos, dando una perspectiva para su implementación y utilización en ambiente de producción LAN. En este capítulo se describe las aplicaciones utilizadas para estos fines y se detalla su instalación, configuración y modo de operación.

4.2 Aplicaciones disponibles de software libre

4.2.1 Aplicación para realizar streaming de video

Para realizar un streaming de video se ha utilizado la aplicación Video LAN VLC, en su versión más reciente 1.1.11 bajo Windows a nivel de servidor y clientes.

VLC es un poderoso reproductor multimedia libre y de código abierto con soporte multiplataforma, con una amplia librería de codecs para reproducir la mayoría de formatos multimedia incluyendo varios protocolos de streaming.

VLC puede ser instalado bajo las siguientes plataformas, tal como se indica en la tabla 4.1.

Windows	MAC OS X	GNU/LINUX	Otros Sistemas Operativos
Windows 2000 (SP4+UR1)	MAC OS C	Debian GNU/Linux	FreeBSD
XP	iOS	Ubuntu	NetBSD
Vista		Mint	OpenBSD
Seven		OpenSUSE	Solaris
		Gentoo Linux	Android
		Fedora	QNX
		Arch Linux	Syllable
		Slackware Linux	OS/2
		Mandriva Linux	
		ALT Linux	
		Red Hat Enterprise Linux	

Tabla 4.1 [A]; Plataformas Soportadas VLC

El soporte de streaming depende de la plataforma sobre la cual se ha instalado la aplicación, además de los protocolos utilizados para establecer el streaming, su encapsulación y el soporte de formatos de video y audio por protocolo de streaming, tal como se indica en las tablas 4.2, 4.3.

Streaming	Protocolo	Windows	MAC OS	GNU/LINUX
Entrada	RTP/UDP	Si	Si	Si
	RTSP	Si	Si	Si
	RTP/DCCP	No	No	Si
	RAW UDP	Si	Si	Si
Salida	(RTP or raw) Multicast	Si	Si	Si
	FILE	Si	Si	Si
	HTTP	Si	Si	Si
	MMSH	Si	Si	Si
Otros	Transcodificador	Si	Si	Si
	Enviar subtítulos DVD	Parcial	Parcial	Parcial
	Enviar anuncios SAP	Si	Si	Si

Tabla 4.2 [7]; Protocolos de streaming soportados según plataforma

		PS	TS	Ogg	ASF	MP4	MOV	MPMJPEG	RTP	RAW
Formatos de Video	MPEG-1 video	Si	Si	Si	No	No	No	No	No	Si
	MPEG-2 video	Si	Si	Si	No	No	No	No	Si	Si
	MPEG-4 video	Si	Si	Si	Si	Si	Si	No	Si	Si
	DivX 1/2/3 video	No	Si	Si	Si	No	No	No	No	No
	WMV 1/2	No	Si	Si	Si	No	No	No	No	No
	H/I 263	No	Si	No	No	No	No	No	Si	No
	MJPEG	No	Si	No	Si	No	No	Parcial	No	No
	Theora	No	No	No	No	No	No	No	No	No
	H.264/MPEG-4 AVC	No	Si	No	No	Si	Si	No	Si	No
Formatos de Audio	MPEG Layer 1/2/3 audio	Si	Si	Si	Si	No	No	No	Si	Si
	AC3 (i.e. A52)	Si	Si	Si	Si	No		No	Si	Si
	MPEG-4 audio (i.e. AAC)	No	Si	No	No	Si	Si	No	Si	No
	Vorbis	No	No	Si	No	No	No	No	No	No
	Speex	No	No	Si	No	No	No	No	Si	No
	FLAC	No	No	Si	No	No	No	No	No	Si
	PCM (Wave)	No	No	No	No	No	No	No	Si	No
	µ-law/A-law	No	No	No	No	No	No	No	Si	No

Tabla 4.3 [7]; Formatos multimedia soportados según protocolo de streaming

De la información de las tablas se observa los parámetros señalados utilizados para realizar el streaming de video a nivel de protocolo, y los formatos de video y audio empleados.

VLC a nivel de multicast soporta el estándar del protocolo IGMP en su tercera versión.

4.2.2 Aplicación para realizar video conferencias

Para realizar video conferencias se ha utilizado la aplicación Isabel en su versión 4.12.beta15-24 bajo Ubuntu 10.10, a nivel de clientes y servidor.

Isabel se distribuye bajo la licencia de software libre, y la aplicación permite ser descargada ya sea para realizar una instalación sobre un host, o en live-cd, para correr la aplicación desde un Cd. Para las pruebas realizadas se hizo uso de los live-cd para realizar la video conferencia multipunto.

Isabel es una herramienta de colaboración en tiempo real para Internet, que soporta avanzadas colaborativas videoconferencias con uso compartido de aplicaciones web, e integración de medios de comunicación como la televisión. Isabel ha sido diseñado para soportar reuniones de empresa o proyectos, mejorar el aprendizaje, así como congresos o conferencias distribuidas. Las sesiones de Isabel se puede acceder desde los navegadores Web, así como de los clientes nativos de Linux que se utilizan para conectar salas y auditorios.

Isabel utiliza el estándar de protocolos de Internet TCP-UDP/IP, y permite procedimientos de trabajo eficientes sobre anchos de banda públicos de Internet, Intranets, VPNs corporativas, redes satelitales, etc.

Entre las funciones de Isabel se puede enumerar varias:

Servicios de apoyo para la realización de:

- Reuniones de proyectos o corporativas.
- Aulas distribuidas.
- Talleres, Conferencias y Congresos distribuidos.
- Servicios a medida según requerimientos específicos.

Amplio conjunto de componentes:

- Utilización de la aplicación bloc de notas.
- Utilización de la aplicación pizarra.
- Uso compartido de aplicaciones Windows, Linux, MacOS.

Videoconferencia que conecta con:

- Navegador WEB estándar.
- Cliente SIP.
- Aplicaciones cliente ejecutadas bajo LINUX para auditorios o salas.

Transmisión en vivo y grabación de las sesiones:

- En combinación con un servidor Flash (como Red5, Adobe Server)

La Fig. 4.1 indica el modo de operación de Isabela, y el alcance de las funciones que esta aplicación posee.

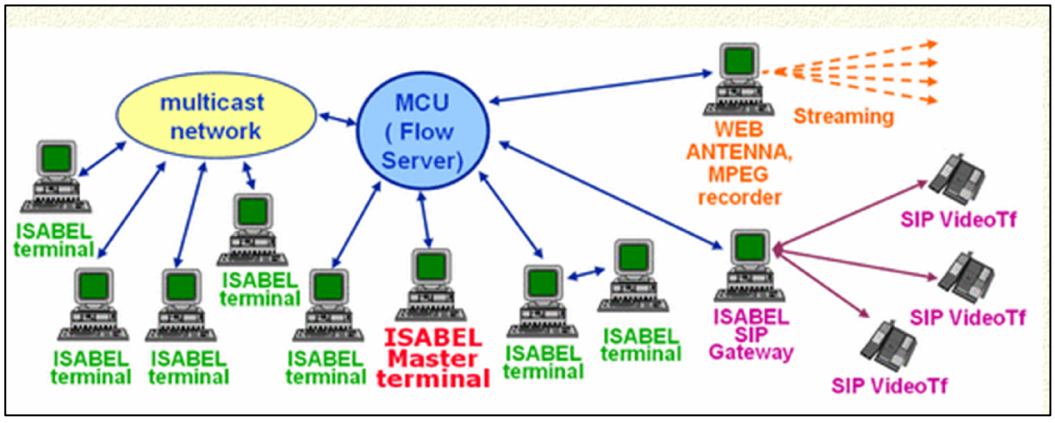


Fig. 4.1 [8]; Modo de operación Isabel

4.3Instalación y Configuración del software seleccionado

4.3.1 Instalación y configuración VLC

Instalación.- Para instalar la aplicación VLC, se necesita descargar el software del sitio oficial, para el sistema operativo sobre el cual se desea trabajar, se debe ejecutar el instalador y seguir las instrucciones como cualquier otro software.

Configuración Servidor.- Para configurar la aplicación servidor VLC, se ejecuta la aplicación ya instalada y se efectúa las siguientes configuraciones:

1- Se Despliega el menú Medio, como en la Fig. 4.2.

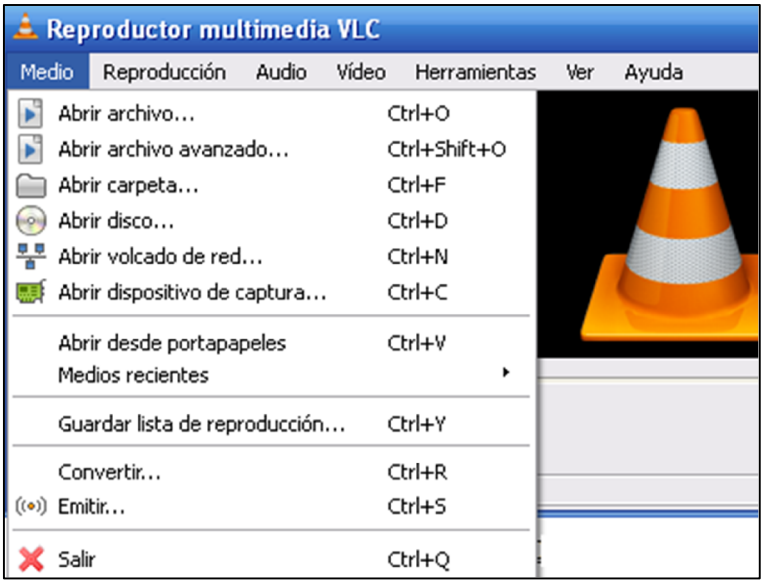


Fig. 4.2 [A]; Menú Medio VLC

2- Acceder a la opción Emitir (Streaming) y desplegar la ventana: Abrir Medio, en esta ventana se tiene la opción de escoger la fuente u origen de los datos, los cuales se van a emitir. Para nuestro streaming se escogerá la pestaña Archivo, y se añade el archivo de video, como se muestra en la Fig. 4.3, luego se da clic sobre el botón Emitir, para obtener la ventana: Salida de Emisión (Output Stream).

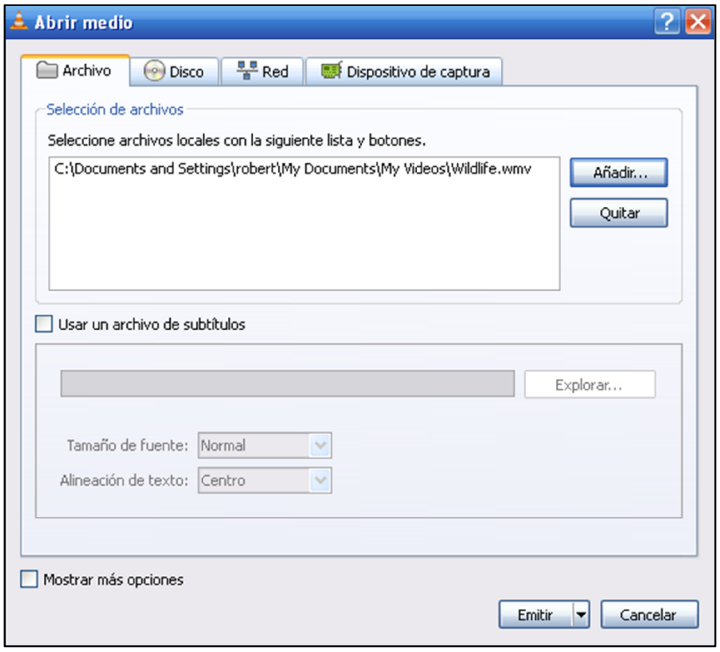


Fig. 4.3 [A]; Menú VLC Abrir Medio

3- En la ventana Salida de Emisión, se vé la fuente, que señala al archivo de video seleccionado, se presiona siguiente para continuar con la configuración parámetros de destino, como se muestra en la Fig. 4.4.

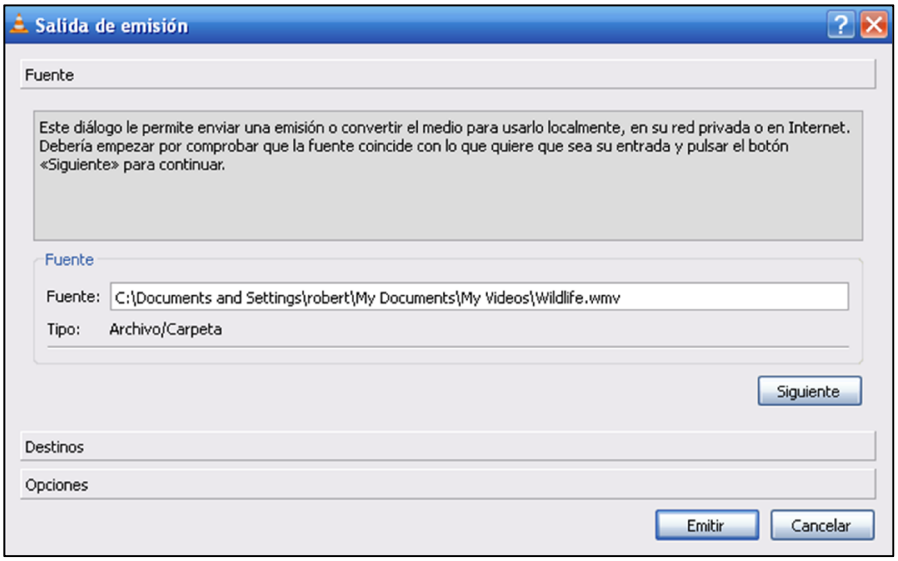


Fig. 4.4 [A]; Menú VLC Salida de Emisión

4- Al acceder a los parámetros de destino, se añade el destino escogiendo la opción RTP / MPEG Transport Stream, se escribe la dirección multicast de grupo a utilizar,

para el streaming de video la dirección 239.0.0.10, para el puerto base se conserva el que se encuentra por defecto 5004. Debe estar habilitada la opción de transcodificar, y se escoge el perfil de Video H.264 + AAC (MP4), como se muestra en la Fig. 4.5, se presiona siguiente para continuar con los parámetros de opciones.

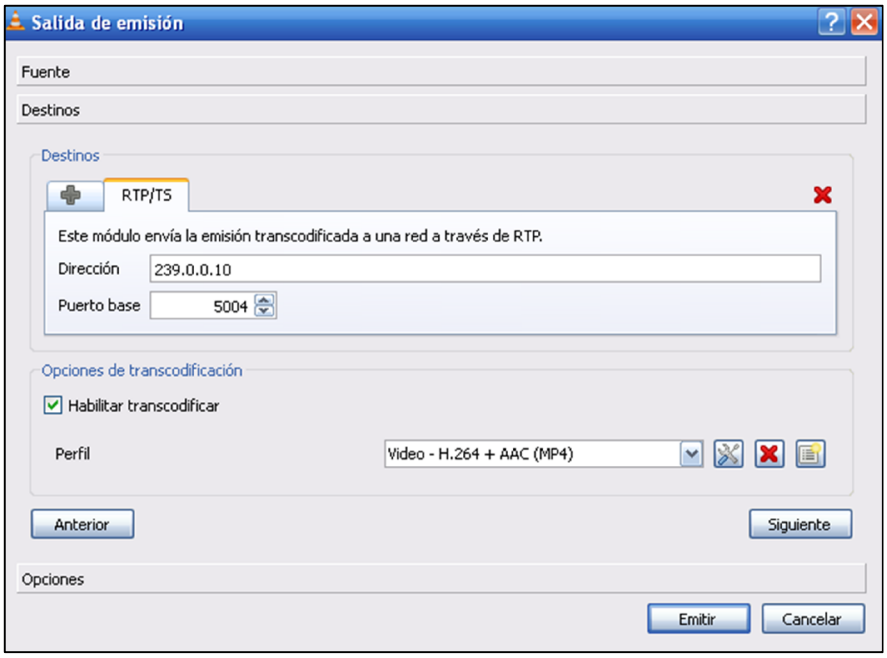


Fig. 4.5 [A]; Configuración parámetros de destino VLC

5- Al acceder a los parámetros de opciones, se ajusta el tiempo de vida para los paquetes en un valor de 2, como se muestra en la Fig. 4.6. Luego se presiona emitir. De esta manera ya se estará realizando el streaming de video para el grupo multicast 239.0.0.10, y el servidor de streaming multicast estará configurado.

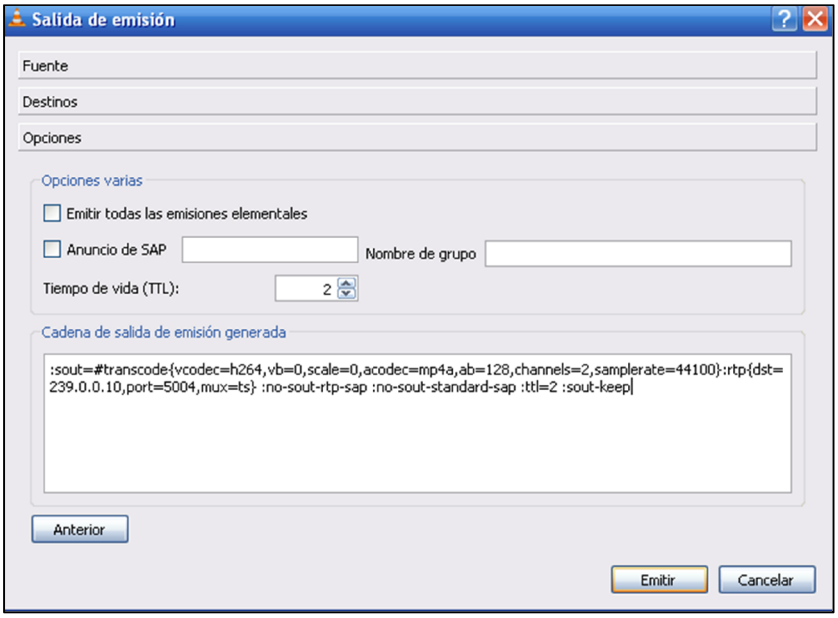


Fig. 4.6 [A]; Configuración opciones VLC

Configuración Cliente.- Para configurar la aplicación VLC en el cliente y obtener el streaming de video, se ejecuta la aplicación ya instalada y se efectúa las siguientes configuraciones:

1- Se Despliega el menú Medio, como en la anterior Fig. 4.2.

2- Se Accede a la opción Abrir volcado de red (Open Network Stream) y desplegar la ventana Abrir Medio, en la opción Red (Network), aquí se debe escribir la dirección del grupo al cual se desea asociar y el protocolo a utilizar. También se puede especificar la fuente de origen del flujo de tráfico multicast ingresando la dirección IP del servidor como se indica a continuación:

`rtp://<Dir IP fuente-opcional>@<Dir. Grupo Multicast>`

Para acceder al grupo multicast de streaming del ambiente de pruebas:

`rtp://@239.0.0.10`

`rtp://172.30.90.9@239.0.0.10`

La Fig. 4.7 muestra la configuración realizada

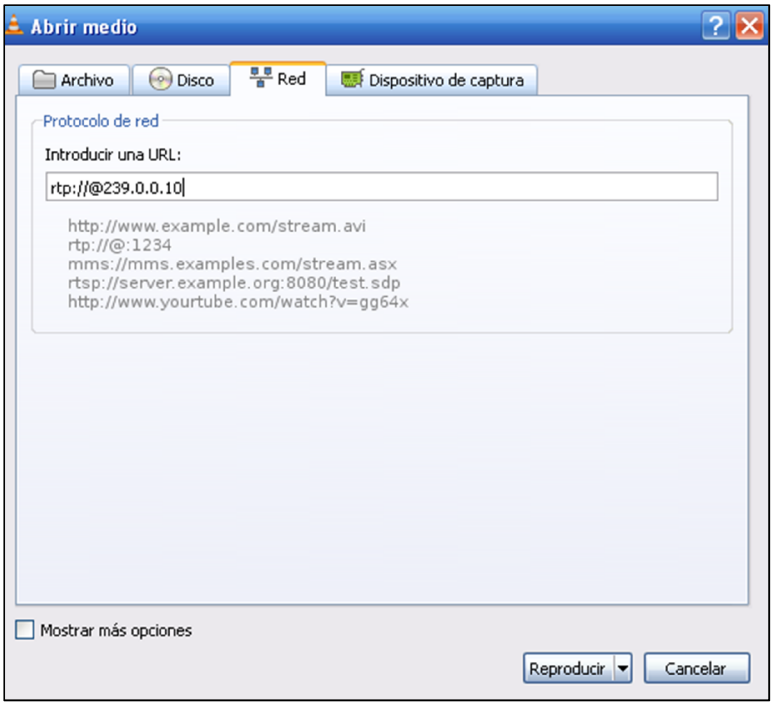


Fig. 4.7 [A]; Configuración cliente VLC

3- Luego de ingresar el grupo al cual se desea asociar para obtener el streaming de video, se presiona reproducir, de esta manera se enviará vía IGMP al router el deseo de asociarse al grupo multicast, en donde si el grupo se encuentra activo el host cliente obtendrá el streaming de video.

4.3.2 Instalación y configuración Isabela

Instalación.- Para establecer videoconferencias se hace uso de la aplicación Isabela en su versión de live-cd, por lo que es suficiente con arrancar el host desde el CD, lo que ejecuta el sistema operativo Ubuntu sobre el cual se encuentra instalada la aplicación.

Configuración Servidor.- Para configurar la aplicación servidor Isabela, se ejecuta la aplicación ya instalada y se efectúa las siguientes configuraciones:

1- Después de arrancar Ubuntu como live-cd, primero se debe configurar el perfil de configuración de Isabel, que corresponde a los parámetros necesarios para ejecutar la aplicación en modo servidor, en modo multicast etc. Para acceder al menú de configuración local, se accede al menú Aplicaciones de la barra superior de Ubuntu, y se escoge la opción Isabel. Aparecerá un sub-menú donde se escoge la opción Editar Configuración Local (Edit Local Configuration), tal como se muestra en la Fig. 4.8.

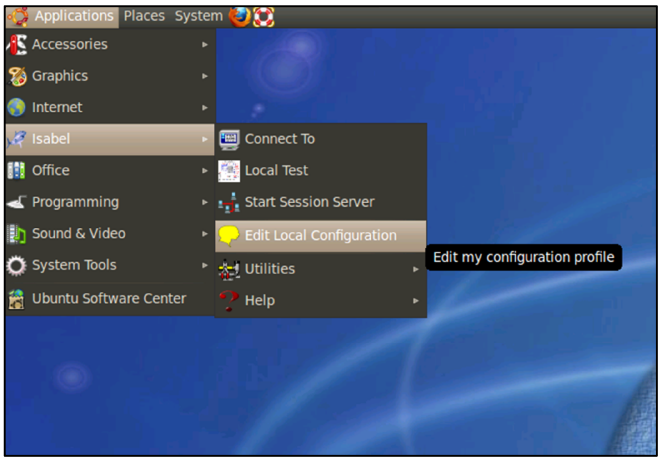


Fig. 4.8 [A]; Menú de operaciones aplicación Isabela

2- En el menú de opciones de Isabela, se debe crear un nuevo perfil, al cual se le denomina Servidor_Conf, en la opción Profile (Perfil). La primera opción a editar es Site ID, o identificación de sitio, ahí se escribe el nombre y ubicación, tal como se muestra en la Fig. 4.9.

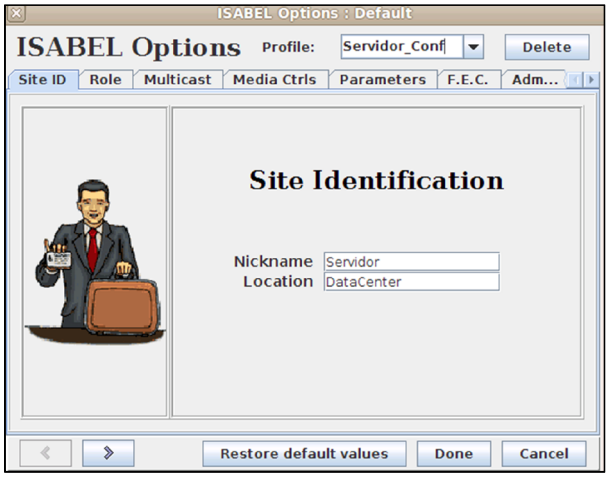


Fig. 4.9 [A]; Menú de opciones configuración identificación de sitio

3- En la opción Role, modo de operación Isabel, se configura la aplicación en modo de servidor de flujo, unidad de control multicast MCU (Multicast Control Unit), tal como se muestra en la Fig. 4.10.

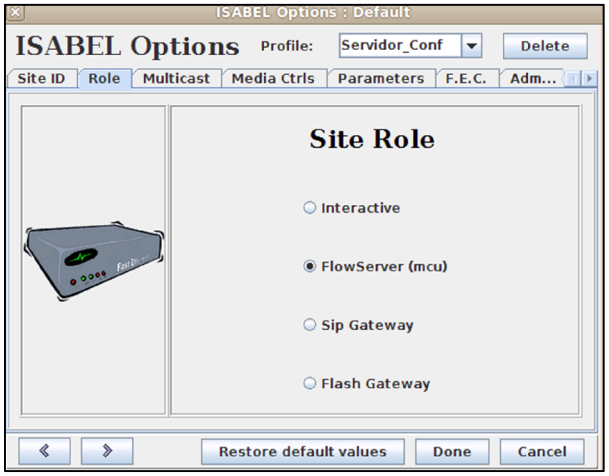


Fig. 4.10 [A]; Menú de opciones configuración modo de operación

4- En la opción Multicast, se habilita Radiate Multicast, irradiar multicast, se accede sobre configurar, para visualizar el menú de opciones de grupo multicast y se establece el valor TTL = 2, la dirección IP del grupo multicast para la transmisión de todo, que será 239.255.6.1. Por último se activa la opción Act as multicast

Gateway, actuar como puerta de enlace multicast, tal como se muestra en la Fig. 4.11.

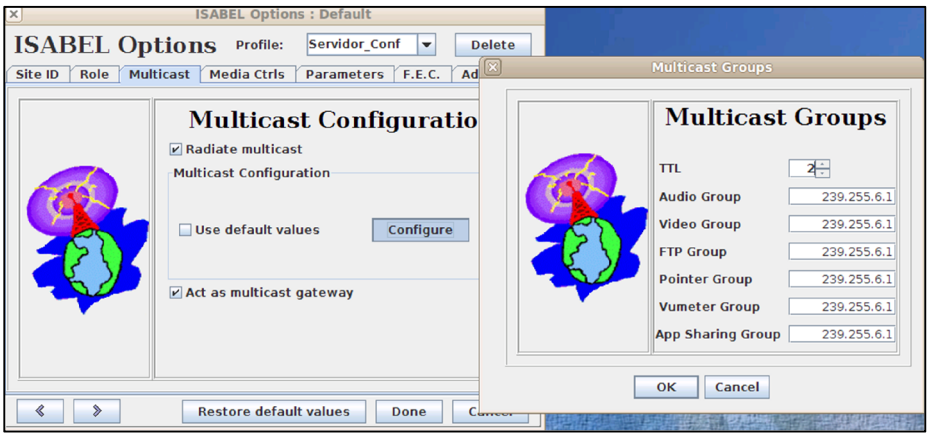


Fig. 4.11 [A]; Menú de opciones configuración multicast

5- La demás opciones se mantiene con los valores por defecto, se presiona sobre Done (Hecho) y se crea el perfil de configuración local con la cual va a funcionar el servidor.

6- Ya creado el perfil de configuraciones locales, se accede a la opción Start Session Server en el menú de operaciones de la aplicación Isabela, tal como se muestra en la Fig. 4.12.

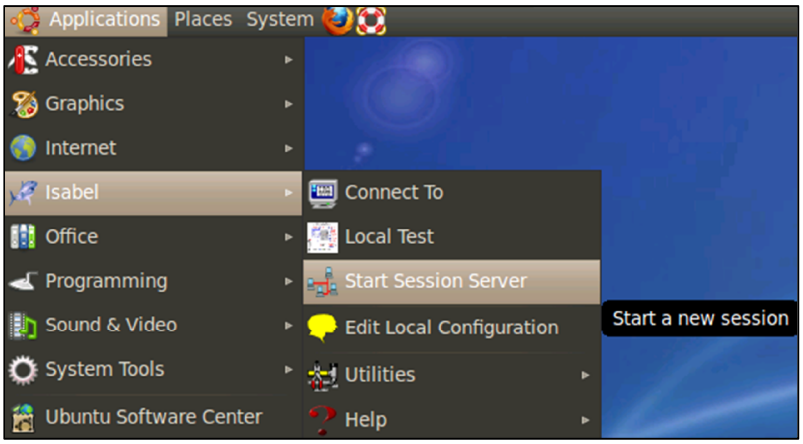


Fig. 4.12 [A]; Iniciar servidor Isabela

7- Desplegada la ventana de inicio de servidor, se configura ciertos parámetros como el nombre de la sesión que es videoconferencia, el tipo de servicio Tele-Conference, la calidad 1M (1 megabit), el nombre, ubicación y seleccionar el perfil antes creado Servidor_Conf, tal como se muestra en la Fig. 4.13.

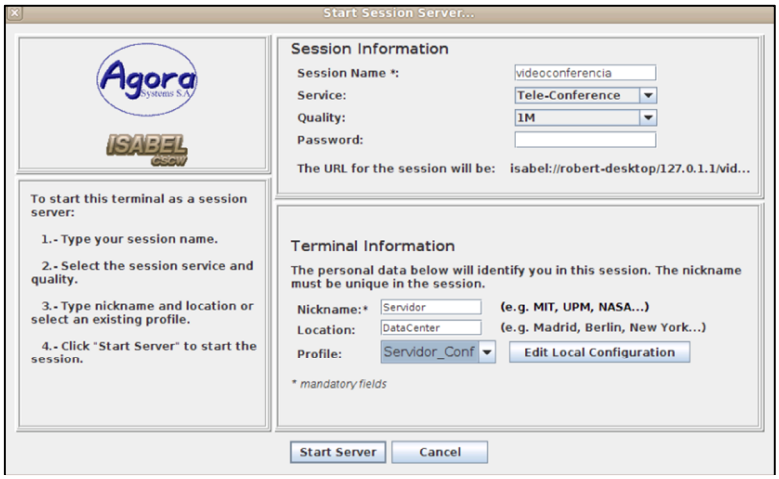


Fig. 4.13 [A]; Configuración inicio de servidor Isabela

8- Después de configurar el inició de sesión de servidor, se presiona iniciar servidor, con lo que todos los clientes que accedan al grupo de videoconferencia podrán acceder al flujo de datos de la videoconferencia multipunto.

Configuración Cliente.- Para configurar la aplicación Isabela en el cliente y participar en la videoconferencia, se ejecuta la aplicación ya instalada y se efectúa las siguientes configuraciones:

1- Para acceder a la videoconferencia como cliente, se accede a la opción Connect to session, conectar a la sesión, en el menú de operaciones de la aplicación Isabela, tal como se muestra en la Fig. 4.14.

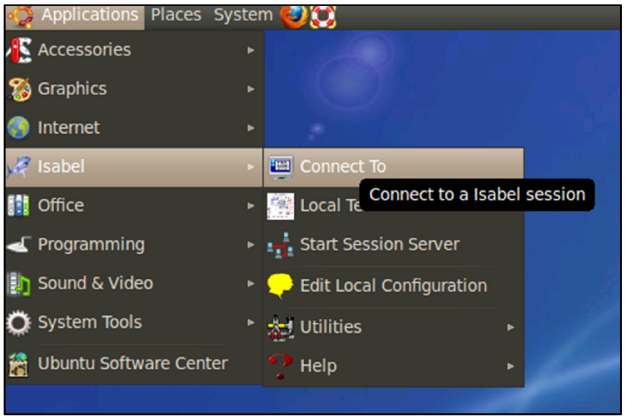


Fig. 4.14 [A]; Conectar a servidor videoconferencia

2- Desplegada la ventana de conectar a sesión, se ingresa la dirección del grupo multicast al cual se desea acceder (239.255.6.1), se escribe el nombre de usuario, ubicación, luego en la opción Profile (Perfil), que se encuentra en Default (Configuración por defecto), se presiona en editar la configuración local, aparecerá la misma ventana donde se configuró el perfil para la aplicación servidor, en la ventana de configuración local, en la opción Role (Rol) se debe seleccionar el modo Interactive (Interactivo), y en la opción Multicast se configura de manera similar a la configuración hecha en el perfil del servidor, se habilita Radiate Multicast, irradiar multicast, se accede sobre configurar, para visualizar el menú de opciones de grupo multicast y se establece el valor TTL = 2, la dirección IP del grupo multicast a la cual se va asociar, que será 239.255.6.1, luego se presiona en Done (Hecho) para salvar la configuración local. Ya en la ventana inicial se presiona conectar y se establecerá la videoconferencia, pudiendo ver y escuchar a los demás participantes, tal como se muestra en la Fig. 4.15.

Fig. 4.15 [A]; Configuración conexión cliente Isabela

CONCLUSIONES

- IP Multicast es una tecnología muy poco utilizada en aplicaciones cuya función es transmitir y en otros casos también recibir flujos de datos de un gran número de aplicaciones cliente, donde la ventaja principal de esta tecnología es el bajo consumo de ancho de banda, como si la comunicación fuese de uno a uno.

- El principio fundamental de IP Multicast radica en la utilización de un rango de direcciones, donde a cada una se asocia un grupo de direcciones IP las cuales desean pertenecer y recibir el flujo de datos inyectado a dicho grupo. De tal manera que un solo flujo de datos es recibido por un grupo de hosts clientes, en una comunicación de uno a muchos.

- El rango de direcciones Multicast está subdividido ya que se han definido varios sub rangos dependiendo del ámbito de aplicación de esta tecnología, teniendo reservado direcciones IP Multicast para aplicaciones específicas. Del mismo modo que en el direccionamiento IPV4, donde se creó un rango de direcciones privadas, para el direccionamiento dentro de la LAN, IP Multicast también aplica el mismo concepto estableciendo un rango de direcciones IP Multicast para su uso privado dentro de la LAN.

- Al establecer las direcciones IP Multicast para los grupos, se debe tener en cuenta que la dirección MAC Multicast resultante de cada grupo sea distinta, de manera que dos grupos que inyectan un flujo de datos diferente no tengan una misma dirección MAC Multicast, produciéndose errores en la entrega del flujo de datos a los clientes asociados a un grupo específico.

- El protocolo de ruteo Multicast a utilizar, depende de la aplicación a ejecutar y el número de usuarios a enganchar, es decir si se asume que se va a tener un gran número de usuarios, que por lo menos uno por subred desea obtener el tráfico Multicast, se debe utilizar el protocolo de ruteo Multicast en modo Denso de manera que se empuje el tráfico Multicast hacia los receptores. Caso contrario, si se asume que no se va a tener un gran número de usuarios, en primera instancia ningún usuario por subred desea el tráfico Multicast, se debe utilizar el protocolo de ruteo Multicast en modo Disperso de manera que el tráfico Multicast sea halado a los receptores.

- Al utilizar IP Multicast, la carga de procesamiento ya no lo soporta en su totalidad el servidor, sino todo el equipo activo de red como el router y los Switches sobre los cuales se encuentra corriendo la configuración Multicast.

- Los hosts clientes tanto para los sistemas operativos Windows como Linux ya incorporan el soporte para IP Multicast y el protocolo IGMP. Dependiendo de la versión del sistema operativo, el protocolo IGMP puede variar en su versión. Es importante tener presente la versión IGMP utilizada por los host clientes, para establecer la versión a utilizar en el router Multicast.

- La implementación de IP Multicast en ambientes LAN, es factible, y en la mayoría de los casos no representa una inversión monetaria adicional, ya que la mayoría de equipo activo de red poseen el soporte para esta tecnología, o basta con la actualización del IOS a una versión que traiga dicho soporte.

- Al ejecutar la aplicación de videoconferencia Multicast, se debe tener en cuenta que los host clientes también van a transmitir información al grupo Multicast, a diferencia del streaming de video donde sólo recibían el flujo de datos, donde la fuente Multicast

no es precisamente el servidor de videoconferencia quien actúa como MCU (Unidad de Control Multicas) o servidor de flujo Multicast, sino cada host asociado quien en un determinado lapso de tiempo inyecta al grupo Multicast la información a transmitir, mientras los demás reciben esa información, y así sucesivamente lo hará cada host que participe de la videoconferencia, todo este proceso es controlado por el servidor de flujo o MCU. Por esta razón para la ejecución de la videoconferencia Multicast todos los participantes deben pertenecer a la misma VLAN, caso contrario no podrán asociarse al grupo Multicast.

RECOMENDACIONES

- Es importante ampliar el concepto de implementación de IP Multicast dentro de la LAN haciendo uso de IPV6, ya que existe la tendencia de aplicar IPV6 dentro de la LAN por las mejoras que trae esta tecnología sobre IPV4.

- Multicast provee múltiples beneficios sobre el rendimiento de una red, razón por la cual esta tecnología ha sido acogida por diferentes clases de servicios como Multicast VPN, que permite conectar varias LAN que corren IP Multicast de manera local, aspectos que no han sido revisados en esta investigación.

- La Televisión IP, utiliza el concepto de IP Multicast, sin embargo integra otros conceptos y configuraciones para servicios como pago bajo demanda o suscripción de canales, aspectos que podría ser ampliados para diversas aplicaciones.

GLOSARIO DE TÉRMINOS

AAC	***Advanced Audio Coding***	(Codificación Avanzada de Audio)
AS	***Autonomous System***	(Sistema Autónomo)
ASM	***Any Source Multicast***	(Cualquier Fuente Multicast)
CAM	***Content Addressable Memory***	(Memoria de Contenido Direccionable)
CBT	***Core Based Tree***	(Árboles Basados en el Núcleo)
CBWFQ	***Class-Based Weighted Fair Queueing***	(Clase Basada en Colas de Peso Justo)
CGMP	***CISCO Group Management Protocol***	(Protocolo de Administración de Grupo CISCO)
COS	***Class of Service***	(Clase de Servicio)
CPU	***Central Processing Unit***	(Unidad Central de Procesamiento)
DNS	***Domain Name System***	(Sistema de Nombre de Dominio)
DSCP	***Differentiated Services Code Point***	(Servicios Diferenciados de Código de Punto)
DVMRP	***Distance Vector Multicast Routing Protocol***	(Protocolo de Ruteo Multicast de Vector Distancia)
FTP	***File Transfer Protocol***	(Protocolo de Transferencia de Archivos)
FWQ	***Weighted Fair Queuing***	(Colas de Peso Justo)
H.264	***Advanced video coding for generic audiovisual services***	(Codificación avanzada de video para servicios genéricos audiovisuales)
IEEE	***Institute of Electrical and Electronics Engineers***	(Instituto de Ingenieros Eléctricos y Electrónicos)
IETF	***Internet Engineering Task Force***	(Grupo Especial sobre Ingeniería de Internet)
IGMP	***Internet Group Management Protocol***	(Protocolo de Administración de Grupo de Internet)
IOS	***Internetwork Operating System***	(Sistema Operativo de interconexión de Redes)
IP	***Internet Protocol***	(Protocolo de Internet)
IPP	***IP Precedence***	(Prioridad IP)
LAN	***Local Area Network***	(Área Local de Red)

LLMNR	***Link Local Multicast Name Resolution***	(Resolución de Nombre Multicast de Enlace Local)
LLQ	***Low Latency Queuing***	(Cola de Baja Latencia)
MAC	***Media Access Control***	(Control de Acceso al Medio)
MCU	***Multicast Control Unit***	(Unidad de Control Multicast)
MFTP	***Multicast File Transfer Protocol***	(Protocolo de Transferencia de Archivos Multicast)
MPEG 4	***Moving Picture Experts Group 4***	(Grupo Experto en Movimiento de Cuadros 4)
MRC	***Maximum Response Code***	(Código de Respuesta Máximo)
MRT	***Maximum Time Response***	(Tiempo de Respuesta Máximo)
NIC	***Network Interface Controller***	(Controlador de Interfaz de Red)
PHB	***Per-Hop Behaviors***	(Comportamiento por Salto)
PIM	***Protocol Independent Multicast***	(Protocolo Independiente Multicast)
PIM-DM	***Protocol Independent Multicast-Dense Mode***	(Protocolo Independiente Multicast - Modo Denso)
PIM-SM	***Protocol Independent Multicast-Sparse Mode***	(Protocolo Independiente Multicast - Modo Disperso)
QoS	***Quality of Services***	(Calidad de Servicio)
QQIC	***Querier's Query Interval Code***	(Consultor de Consulta de Intervalo de Código)
QRV	***Querier Robustness Value***	(Valor de Consulta Robusto)
RFC	***Request for Comments***	(Petición de Comentarios)
RIB	***Routing Information Base***	(Base de Información de Ruteo)
RP	***Rendezvous Point***	(Punto de Encuentro)
RPF	***Reverse Path Forwarding***	(Reenvío de Enlace Inverso)
RPT	***Rendezvous Point Trees***	(Árboles de Punto de Encuentro)
RTCP	***Real Time Control Protocol***	(Protocolo de Control de Tiempo Real)
RTP	***Real Time Protocol***	(Protocolo de Tiempo Real)
SAP	***Session Announcement Protocol***	(Protocolo de Anuncio de Sesión)
SDP	***Session Description Protocol***	(Protocolo de Descripción de Sesión)

SPT	***Short Path Tree***	(Árbol de Camino más Corto)
SSM	***Specific Source Multicast***	(Fuente Específica Multicast)
TCP	***Transmission Control Protocol***	(Protocolo de Control de Transmisión)
TTL	***Time To Live***	(Tiempo de Vida)
UDP	***User Datagram Protocol***	(Protocolo de Datagrama de Usuario)
VLC	***Video LAN Converter***	(Convertidor de Video LAN)
VPN	***Virtual Private Network***	(Red Virtual Privada)

ANEXOS

ANEXO 1.- Ambiente de Pruebas Multicast Videoconferencia Multipunto

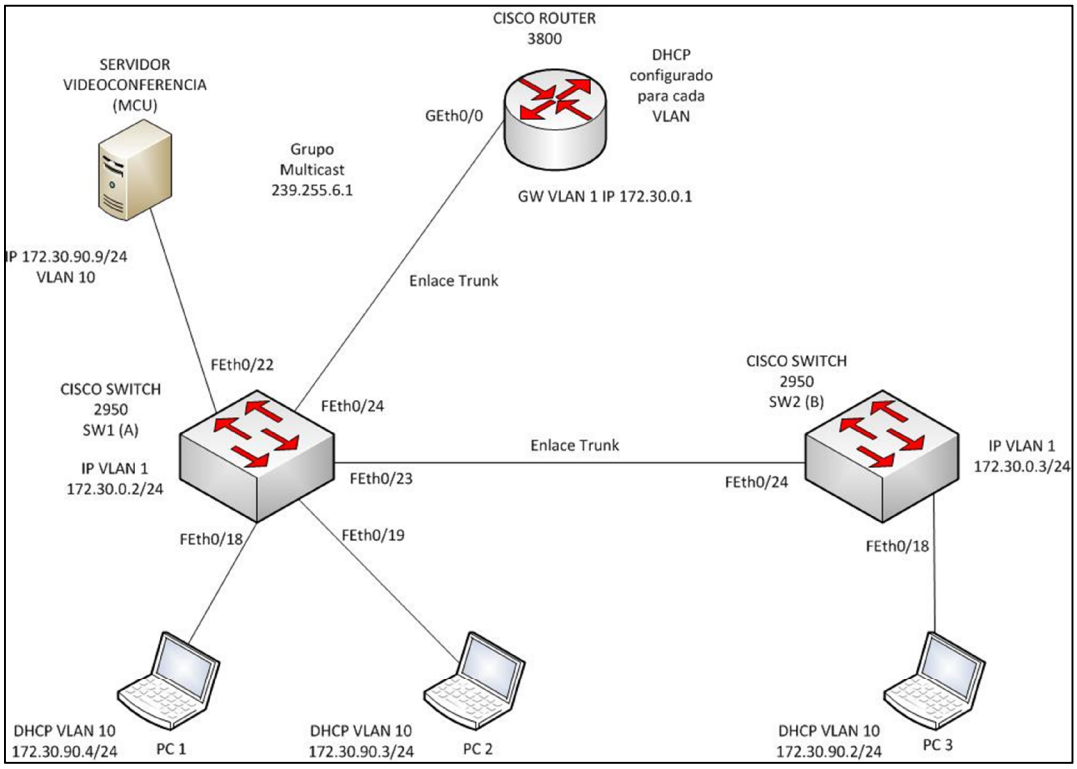
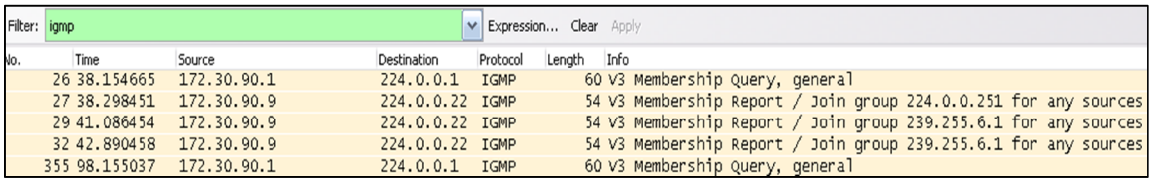


Fig. 1 [A]; Ambiente de Pruebas Multicast Videoconferencia Multipunto

En la Fig. 1 se detalla un ambiente Multicast, que permite ejecutar el servicio de videoconferencia multipunto, haciendo uso del software Isabela. En este escenario el servidor de videoconferencia funciona como una undad de control de flujo Multicast (MCU), el cual habilita el grupo IP Multicast asignado para llevar a cabo la videoconferencia, correspondiente a la dirección 239.255.6.1.

Se debe tener en cuenta que para el funcionamiento del servicio de videoconferencia multicast, es necesario que los hosts clientes se encuntren en la misma VLAN que el servidor, ya que los clientes al asociarse al grupo IP Multicast, estos no sólo reciben el flujo de datos multicast, sino también emiten información al grupo. Todo este proceso de emisión y recepsión del flujo de datos del grupo IP Multicast, es controlado por el servidor de videoconferencia MCU.

En la Fig. 2 se mustra una captura de tráfico en el lado del servidor, en la cual se puede observar la publicación del grupo IP Multicast, a ser utilizado para el servicio de videoconferencia, de la comunicación establecida, haciendo uso del protocolo IGMP, entre el servidor y el router multicast.

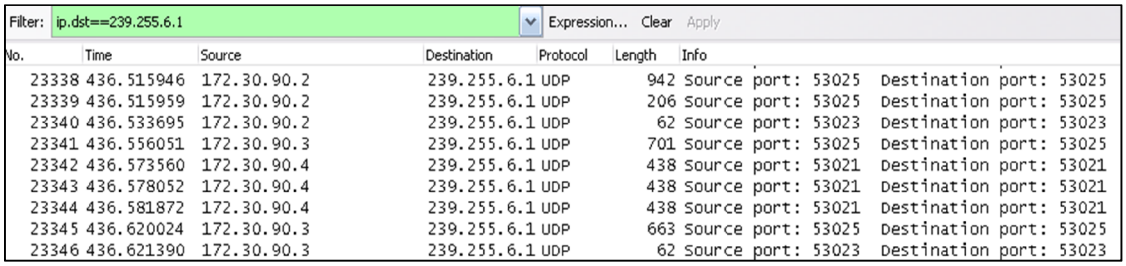

Filter: igmp Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
26	38.154665	172.30.90.1	224.0.0.1	IGMP	60	V3 Membership Query, general
27	38.298451	172.30.90.9	224.0.0.22	IGMP	54	V3 Membership Report / Join group 224.0.0.251 for any sources
29	41.086454	172.30.90.9	224.0.0.22	IGMP	54	V3 Membership Report / Join group 239.255.6.1 for any sources
32	42.890458	172.30.90.9	224.0.0.22	IGMP	54	V3 Membership Report / Join group 239.255.6.1 for any sources
355	98.155037	172.30.90.1	224.0.0.1	IGMP	60	V3 Membership Query, general

Fig. 2 [A]; Captura de tráfico en el Servidor de Videoconferencia inicio del servicio

A diferencia del streaming de video, el servidor de videoconferencia no emitirá información al flujo de datos del grupo multicast, en cuanto funcionará sólo como un servidor de control de flujo multicast, manteniendo la administración de la videoconferencia y el estado de los participantes, esto se logra mediante una comunicación unicast con cada uno de ellos, cada cierto tiempo, proporcionando información de control, para que cada participante pueda inyectar información al flujo de datos multicast. Por esta razón el servidor de videoconferencia, al no ser fuente de emisión de datos directa al grupo IP Multicast, también se debe asociar al grupo para resivir el flujo de datos y controlar la información que se esta emitiendo.

En la Fig. 3 se muestra una captura de tráfico en el lado del servidor, en la cual se puede observar a los tres participantes de la videoconferencia inyectando información al grupo IP Multicast, de manera coordinada. Cabe resaltar que cada participante asociado a la videoconferencia, pasará a ser fuente en un determinado tiempo, y en otro receptor del flujo de datos del grupo. Todo este proceso es controlado por el servidor de videoconferencia.



Filter: ip.dst==239.255.6.1 Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
23338	436.515946	172.30.90.2	239.255.6.1	UDP	942	Source port: 53025 Destination port: 53025
23339	436.515959	172.30.90.2	239.255.6.1	UDP	206	Source port: 53025 Destination port: 53025
23340	436.533695	172.30.90.2	239.255.6.1	UDP	62	Source port: 53023 Destination port: 53023
23341	436.556051	172.30.90.3	239.255.6.1	UDP	701	Source port: 53025 Destination port: 53025
23342	436.573560	172.30.90.4	239.255.6.1	UDP	438	Source port: 53021 Destination port: 53021
23343	436.578052	172.30.90.4	239.255.6.1	UDP	438	Source port: 53021 Destination port: 53021
23344	436.581872	172.30.90.4	239.255.6.1	UDP	438	Source port: 53021 Destination port: 53021
23345	436.620024	172.30.90.3	239.255.6.1	UDP	663	Source port: 53025 Destination port: 53025
23346	436.621390	172.30.90.3	239.255.6.1	UDP	62	Source port: 53023 Destination port: 53023

Fig. 3 [A]; Captura de tráfico en el Servidor de Videoconferencia Participantes

En la Fig. 4 se muestra las rutas creadas en el router multicast, para la transmisión y recepsión del flujo de datos del grupo IP Multicast.

```
Router#show ip mroute 239.255.6.1
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 239.255.6.1), 01:35:04/stopped, RP 0.0.0.0, flags: DC
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    GigabitEthernet0/0.10, Forward/Dense, 00:10:45/00:00:00

(172.30.90.2, 239.255.6.1), 00:00:44/00:02:15, flags: PT
  Incoming interface: GigabitEthernet0/0.10, RPF nbr 0.0.0.0
  Outgoing interface list: Null

(172.30.90.3, 239.255.6.1), 00:01:32/00:01:27, flags: PT
  Incoming interface: GigabitEthernet0/0.10, RPF nbr 0.0.0.0
  Outgoing interface list: Null

(172.30.90.4, 239.255.6.1), 00:02:52/00:00:07, flags: PT
  Incoming interface: GigabitEthernet0/0.10, RPF nbr 0.0.0.0
  Outgoing interface list: Null
```

Fig. 4 [A]; Rutas Multicast Servicio de Videoconferencia

En la Fig. 4 se puede observar cuatro rutas para el grupo IP Multicast 239.255.6.1, una ruta es de salida del flujo de datos multicast correspondiente a una fuente cualquiera, y tres rutas de entrada del flujo de datos multicast correspondiente a cada participante

de la videoconferencia que actuarán en un determinado tiempo como fuente del grupo IP Multicast.

En la Fig. 5 se muestra los puertos asociados al grupo IP Multicast, y la dirección MAC utilizada por el grupo además de otra información referente al protocolo de comunicación IGMP, obtenida en el Switch 1 (A).

```
SwitchA#show ip igmp snooping group
  vlan  Show group address information in a Catalyst Vlan
  |     Output modifiers
  <cr>

SwitchA#show ip igmp snooping group
Vlan      Group           Version     Port List
------------------------------------------------------------
10        239.255.6.1     v3          Fa0/18, Fa0/19, Fa0/22, Fa0/23


SwitchA#show mac-address-table multicast
Vlan    Mac Address       Type        Ports
----    -----------       ----        -----
  10    0100.5e7f.0601    IGMP        Fa0/18, Fa0/19, Fa0/22,
                                      Fa0/23, Fa0/24
```

Fig. 5 [A]; Información obtenida SwitchA servicio de Videoconferencia

En la Fig. 6 se muestra los puertos asociados al grupo IP Multicast, y la dirección MAC utilizada por el grupo además de otra información referente al protocolo de comunicación IGMP, obtenida en el Switch 2 (B).

```
SwitchB#show ip igmp snooping group
Vlan      Group           Version     Port List
------------------------------------------------------------
10        239.255.6.1     v3          Fa0/18


SwitchB#show mac-address-table multicast
Vlan    Mac Address       Type        Ports
----    -----------       ----        -----
  10    0100.5e7f.0601    IGMP        Fa0/18, Fa0/24
```

Fig. 6 [A]; Información obtenida SwitchB servicio de Videoconferencia

ANEXO 2.- Configuración Router Cisco 3800.

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$yQxF$uuLFe4fz6ebAxccYqrq2G1
!
no aaa new-model
ip cef
!
!
no ip dhcp use vrf connected
ip dhcp excluded-address 172.30.10.1
ip dhcp excluded-address 172.30.20.1
ip dhcp excluded-address 172.30.30.1
ip dhcp excluded-address 172.30.40.1
ip dhcp excluded-address 172.30.50.1
ip dhcp excluded-address 172.30.60.1
ip dhcp excluded-address 172.30.70.1
ip dhcp excluded-address 172.30.80.1
ip dhcp excluded-address 172.30.90.1
ip dhcp excluded-address 172.30.90.9
ip dhcp excluded-address 172.30.90.10
!
ip dhcp pool DHCP_FIE
   network 172.30.10.0 255.255.255.0
   default-router 172.30.10.1
   domain-name 198.6.1.1
!
ip dhcp pool DHCP_FSP
   network 172.30.20.0 255.255.255.0
   default-router 172.30.20.1
   domain-name 198.6.1.1
!
ip dhcp pool DHCP_FM
   network 172.30.30.0 255.255.255.0
   default-router 172.30.30.1
   domain-name 198.6.1.1
!
ip dhcp pool DHCP_FC
   network 172.30.40.0 255.255.255.0
   default-router 172.30.40.1
   domain-name 198.6.1.1
!
ip dhcp pool DHCP_FRN
   network 172.30.50.0 255.255.255.0
   default-router 172.30.50.1
   domain-name 198.6.1.1
!
ip dhcp pool DHCP_FCP
```

```
   network 172.30.60.0 255.255.255.0
   default-router 172.30.60.1
   domain-name 198.6.1.1
!
ip dhcp pool DHCP_FADE
   network 172.30.70.0 255.255.255.0
   default-router 172.30.70.1
   domain-name 198.6.1.1
!
ip dhcp pool DHCP_Administrativos
   network 172.30.80.0 255.255.255.0
   default-router 172.30.80.1
   domain-name 198.6.1.1
!
ip dhcp pool DHCP_Serv
   network 172.30.90.0 255.255.255.0
   default-router 172.30.90.1
   domain-name 198.6.1.1
!
!
ip multicast-routing
!
username roberto privilege 15 password 7 03094E071206224D5D1D
!
!
!
class-map match-all high_priority_data
 match  dscp af21
class-map match-all call_signaling
 match  dscp af31
class-map match-all video_conferencing
 match  dscp cs4
class-map match-all voice
 match  dscp ef
!
!
policy-map qos_clases
 class video_conferencing
  priority percent 20
 class voice
  priority percent 10
 class call_signaling
  bandwidth percent 10
 class high_priority_data
  bandwidth percent 20
 class class-default
  fair-queue 16
!
!
!
interface GigabitEthernet0/0
 description CONEXION LAN
 no ip address
 duplex auto
 speed auto
 media-type rj45
 service-policy output qos_clases
!
interface GigabitEthernet0/0.1
```

```
 encapsulation dot1Q 1 native
 ip address 172.30.0.1 255.255.255.0
 ip access-group seguridad_vlan1_in in
 ip access-group seguridad_vlan1_out out
 no ip redirects
!
interface GigabitEthernet0/0.2
 encapsulation dot1Q 2
 ip address 172.30.10.1 255.255.255.0
 ip access-group bloqueo_IGMP_VLAN2 in
 ip access-group seguridad_vlan3_out out
 no ip redirects
 ip pim dense-mode
 ip igmp access-group igmp-join-filter
 ip igmp version 3
 ip sap listen
!
interface GigabitEthernet0/0.3
 encapsulation dot1Q 3
 ip address 172.30.20.1 255.255.255.0
 ip access-group seguridad_vlan3_in in
 ip access-group seguridad_vlan3_out out
 no ip redirects
 ip pim dense-mode
 ip igmp access-group igmp-join-filter
 ip igmp version 3
 ip sap listen
!
interface GigabitEthernet0/0.4
 encapsulation dot1Q 4
 ip address 172.30.30.1 255.255.255.0
 ip access-group seguridad_vlan4_in in
 ip access-group seguridad_vlan4_out out
 no ip redirects
 ip pim dense-mode
 ip igmp access-group igmp-join-filter
 ip igmp version 3
 ip sap listen
!
interface GigabitEthernet0/0.5
 encapsulation dot1Q 5
 ip address 172.30.40.1 255.255.255.0
 ip access-group seguridad_vlan5_in in
 ip access-group seguridad_vlan5_out out
 no ip redirects
 ip pim dense-mode
 ip igmp access-group igmp-join-filter
 ip igmp version 3
 ip sap listen
!
interface GigabitEthernet0/0.6
 encapsulation dot1Q 6
 ip address 172.30.50.1 255.255.255.0
 ip access-group seguridad_vlan6_in in
 ip access-group seguridad_vlan6_out out
 no ip redirects
 ip pim dense-mode
 ip igmp access-group igmp-join-filter
 ip igmp version 3
```

```
 ip sap listen
!
interface GigabitEthernet0/0.7
 encapsulation dot1Q 7
 ip address 172.30.60.1 255.255.255.0
 ip access-group seguridad_vlan7_in in
 ip access-group seguridad_vlan7_out out
 no ip redirects
 ip pim dense-mode
 ip igmp access-group igmp-join-filter
 ip igmp version 3
 ip sap listen
!
interface GigabitEthernet0/0.8
 encapsulation dot1Q 8
 ip address 172.30.70.1 255.255.255.0
 ip access-group seguridad_vlan8_in in
 ip access-group seguridad_vlan8_out out
 no ip redirects
 ip pim dense-mode
 ip igmp access-group igmp-join-filter
 ip igmp version 3
 ip sap listen
!
interface GigabitEthernet0/0.9
 encapsulation dot1Q 9
 ip address 172.30.80.1 255.255.255.0
 ip access-group seguridad_vlan9_in in
 ip access-group seguridad_vlan9_out out
 no ip redirects
 ip pim dense-mode
 ip igmp access-group igmp-join-filter
 ip igmp version 3
 ip sap listen
!
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 172.30.90.1 255.255.255.0
 ip access-group seguridad_vlan10_in in
 ip access-group seguridad_vlan10_out out
 no ip redirects
 ip pim dense-mode
 ip igmp access-group igmp-join-filter
 ip igmp version 3
 ip sap listen
!
interface GigabitEthernet0/1
 description CONEXION INTERNET
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
!
ip forward-protocol nd
!
ip http server
!
ip access-list standard igmp-join-filter
```

```
 permit 239.255.6.1
 permit 239.0.0.10
 deny   any
!
ip access-list extended bloqueo_IGMP_VLAN2
 deny   igmp 172.30.10.0 0.0.0.255 any log
 permit ip host 0.0.0.0 host 255.255.255.255 log
 permit ip 172.30.10.0 0.0.0.255 any log
 deny   ip any any
ip access-list extended seguridad_vlan10_in
 permit ip host 0.0.0.0 host 255.255.255.255 log
 permit ip 172.30.90.0 0.0.0.255 any log
 deny   ip any any
ip access-list extended seguridad_vlan10_out
 permit ip any 172.30.90.0 0.0.0.255 log
 permit ip any 239.0.0.0 0.255.255.255 log
 deny   ip any any
ip access-list extended seguridad_vlan1_in
 permit ip host 0.0.0.0 host 255.255.255.255 log
 permit ip 172.30.0.0 0.0.0.255 any log
 deny   ip any any
ip access-list extended seguridad_vlan1_out
 permit ip any 172.30.0.0 0.0.0.255 log
 deny   ip any any
ip access-list extended seguridad_vlan2_in
 permit ip host 0.0.0.0 host 255.255.255.255 log
 permit ip 172.30.10.0 0.0.0.255 any log
 deny   ip any any
ip access-list extended seguridad_vlan2_out
 permit ip any 172.30.10.0 0.0.0.255 log
 permit ip any 239.0.0.0 0.255.255.255 log
 deny   ip any any
ip access-list extended seguridad_vlan3_in
 permit ip host 0.0.0.0 host 255.255.255.255 log
 permit ip 172.30.20.0 0.0.0.255 any log
 deny   ip any any
ip access-list extended seguridad_vlan3_out
 permit ip any 172.30.20.0 0.0.0.255 log
 permit ip any 239.0.0.0 0.255.255.255 log
 deny   ip any any
ip access-list extended seguridad_vlan4_in
 permit ip host 0.0.0.0 host 255.255.255.255 log
 permit ip 172.30.30.0 0.0.0.255 any log
 deny   ip any any
ip access-list extended seguridad_vlan4_out
 permit ip any 172.30.30.0 0.0.0.255 log
 permit ip any 239.0.0.0 0.255.255.255 log
 deny   ip any any
ip access-list extended seguridad_vlan5_in
 permit ip host 0.0.0.0 host 255.255.255.255 log
 permit ip 172.30.40.0 0.0.0.255 any log
 deny   ip any any
ip access-list extended seguridad_vlan5_out
 permit ip any 172.30.40.0 0.0.0.255 log
 permit ip any 239.0.0.0 0.255.255.255 log
 deny   ip any any
ip access-list extended seguridad_vlan6_in
 permit ip host 0.0.0.0 host 255.255.255.255 log
 permit ip 172.30.50.0 0.0.0.255 any log
```

```
 deny   ip any any
ip access-list extended seguridad_vlan6_out
 permit ip any 172.30.50.0 0.0.0.255 log
 permit ip any 239.0.0.0 0.255.255.255 log
 deny   ip any any
ip access-list extended seguridad_vlan7_in
 permit ip host 0.0.0.0 host 255.255.255.255 log
 permit ip 172.30.60.0 0.0.0.255 any log
 deny   ip any any
ip access-list extended seguridad_vlan7_out
 permit ip any 172.30.60.0 0.0.0.255 log
 permit ip any 239.0.0.0 0.255.255.255 log
 deny   ip any any
ip access-list extended seguridad_vlan8_in
 permit ip host 0.0.0.0 host 255.255.255.255 log
 permit ip 172.30.70.0 0.0.0.255 any log
 deny   ip any any
ip access-list extended seguridad_vlan8_out
 permit ip any 172.30.70.0 0.0.0.255 log
 permit ip any 239.0.0.0 0.255.255.255 log
 deny   ip any any
ip access-list extended seguridad_vlan9_in
 permit ip host 0.0.0.0 host 255.255.255.255 log
 permit ip 172.30.80.0 0.0.0.255 any log
 deny   ip any any
ip access-list extended seguridad_vlan9_out
 permit ip any 172.30.80.0 0.0.0.255 log
 permit ip any 239.0.0.0 0.255.255.255 log
 deny   ip any any
!
snmp-server community TeSiS RO
snmp-server location Laboratorio_Pruebas
snmp-server contact Ing. Roberto Larrea
snmp-server enable traps snmp authentication linkdown linkup coldstart
warmstart
snmp-server enable traps vrrp
snmp-server enable traps ds1
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps ds3
snmp-server enable traps envmon
snmp-server enable traps icsudsu
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps isdn chan-not-avail
snmp-server enable traps isdn ietf
snmp-server enable traps ds0-busyout
snmp-server enable traps ds1-loopback
snmp-server enable traps atm subif
snmp-server enable traps cnpd
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps hsrp
snmp-server enable traps ipmulticast
snmp-server enable traps msdp
```

```
snmp-server enable traps mvpn
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-
change
snmp-server enable traps ospf cisco-specific state-change shamlink
interface-old
snmp-server enable traps ospf cisco-specific state-change shamlink
neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps pim neighbor-change rp-mapping-change
invalid-pim-message
snmp-server enable traps pppoe
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps syslog
snmp-server enable traps l2tun session
snmp-server enable traps vtp
!
control-plane
!
!
line con 0
 password 7 00161C0401491F091B245F471A4B554643
 logging synchronous
 login
line aux 0
line vty 0 4
 password 7 0833434C0C0B1118060E1F0D3979747962
 login
!
scheduler allocate 20000 1000
!
end
```

ANEXO 3.- Configuración Switch1 (A) Cisco Catalyst 2950.

```
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname SwitchA
!
enable secret 5 $1$NpFM$9TN/vr5X2ul3UxUnDJrJc0
!
username roberto privilege 15 password 7 1308021E1F05072B3830
clock timezone GMT 0
clock summer-time GMT recurring last Sun Mar 1:00 last Sun Oct 2:00
wrr-queue bandwidth 20 20 80 0
wrr-queue cos-map 1 0 1 2
wrr-queue cos-map 2 4
wrr-queue cos-map 3 3 6 7
wrr-queue cos-map 4 5
ip subnet-zero
no ip igmp snooping report-suppression
!
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
!
!
!
interface FastEthernet0/1
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 3
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 3
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 4
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 4
 switchport mode access
```

```
!
interface FastEthernet0/8
 switchport access vlan 5
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 5
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 6
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 6
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 7
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 7
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 8
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 8
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 9
 switchport mode access
!
interface FastEthernet0/17
 switchport access vlan 9
 switchport mode access
!
interface FastEthernet0/18
 switchport access vlan 10
 switchport mode access
 mls qos cos 4
 mls qos cos override
!
interface FastEthernet0/19
 switchport access vlan 10
 switchport mode access
 mls qos cos 4
 mls qos cos override
!
interface FastEthernet0/20
 switchport access vlan 10
 switchport mode access
 mls qos cos 4
 mls qos cos override
!
```

```
interface FastEthernet0/21
 switchport access vlan 10
 switchport mode access
 mls qos cos 4
 mls qos cos override
!
interface FastEthernet0/22
 switchport access vlan 10
 switchport mode access
 mls qos cos 4
 mls qos cos override
!
interface FastEthernet0/23
 description CONEXION SWITCHB
 switchport mode trunk
 mls qos trust cos pass-through dscp
!
interface FastEthernet0/24
 description CONEXION ROUTER
 switchport mode trunk
 mls qos trust cos pass-through dscp
!
interface Vlan1
 ip address 172.30.0.2 255.255.255.0
 no ip route-cache
!
ip default-gateway 172.30.0.1
ip http server
snmp-server community maestria RO
snmp-server community TeSiS RO
snmp-server location Laboratorio Pruebas
snmp-server contact Ing. Roberto Larrea
snmp-server enable traps snmp authentication warmstart linkdown linkup
coldstart
snmp-server enable traps config
snmp-server enable traps copy-config
snmp-server enable traps syslog
snmp-server enable traps entity
snmp-server enable traps flash insertion removal
snmp-server enable traps bridge
snmp-server enable traps stpx
snmp-server enable traps rtr
snmp-server enable traps c2900
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps MAC-Notification
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps hsrp
snmp-server enable traps cluster
snmp-server enable traps vlan-membership
!
line con 0
 password 7 06140023495C1D16111201021F567A7A75
 logging synchronous
 login
line vty 0 4
 password 7 044904040A3358411D1C161E01595C557B
```

```
 login
line vty 5 15
 login
!
!
end
```

ANEXO 4.- Configuración Switch2 (B) Cisco Catalyst 2950.

```
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname SwitchB
!
enable secret 5 $1$NpFM$9TN/vr5X2ul3UxUnDJrJc0
!
username roberto privilege 15 password 7 1308021E1F05072B3830
clock timezone GMT 0
clock summer-time GMT recurring last Sun Mar 1:00 last Sun Oct 2:00
wrr-queue bandwidth 20 20 80 0
wrr-queue cos-map 1 0 1 2
wrr-queue cos-map 2 4
wrr-queue cos-map 3 3 6 7
wrr-queue cos-map 4 5
ip subnet-zero
no ip igmp snooping report-suppression
!
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
!
!
!
interface FastEthernet0/1
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 3
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 3
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 4
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 4
 switchport mode access
```

```
!
interface FastEthernet0/8
 switchport access vlan 5
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 5
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 6
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 6
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 7
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 7
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 8
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 8
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 9
 switchport mode access
!
interface FastEthernet0/17
 switchport access vlan 9
 switchport mode access
!
interface FastEthernet0/18
 switchport access vlan 10
 switchport mode access
 mls qos cos 4
 mls qos cos override
!
interface FastEthernet0/19
 switchport access vlan 10
 switchport mode access
 mls qos cos 4
 mls qos cos override
!
interface FastEthernet0/20
 switchport access vlan 10
 switchport mode access
 mls qos cos 4
 mls qos cos override
!
```

```
interface FastEthernet0/21
 switchport access vlan 10
 switchport mode access
 mls qos cos 4
 mls qos cos override
!
interface FastEthernet0/22
 switchport access vlan 10
 switchport mode access
 mls qos cos 4
 mls qos cos override
!
interface FastEthernet0/23
 description CONEXION ANOTHER SWITCH
 switchport mode trunk
 mls qos trust cos pass-through dscp
!
interface FastEthernet0/24
 description CONEXION SWITCHA
 switchport mode trunk
 mls qos trust cos pass-through dscp
!
interface Vlan1
 ip address 172.30.0.3 255.255.255.0
 no ip route-cache
!
ip default-gateway 172.30.0.1
ip http server
snmp-server community maestria RO
snmp-server community TeSiS RO
snmp-server location Laboratorio Pruebas
snmp-server contact Ing. Roberto Larrea
snmp-server enable traps snmp authentication warmstart linkdown linkup
coldstart
snmp-server enable traps config
snmp-server enable traps copy-config
snmp-server enable traps syslog
snmp-server enable traps entity
snmp-server enable traps flash insertion removal
snmp-server enable traps bridge
snmp-server enable traps stpx
snmp-server enable traps rtr
snmp-server enable traps c2900
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps MAC-Notification
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps hsrp
snmp-server enable traps cluster
snmp-server enable traps vlan-membership
!
line con 0
 password 7 06140023495C1D16111201021F567A7A75
 logging synchronous
 login
line vty 0 4
 password 7 044904040A3358411D1C161E01595C557B
```

```
 login
line vty 5 15
 login
!
!
end
```

BIBLIOGRAFÍA

[A].-ROBERTO A. LARREA L., Estudio de Requerimientos Técnicos para la Implementación de Redes Ip Multicast en Ambientes LAN, 2012. 173p.

[B].-LAURENCE HARTE, Introduction to Data Multicasting, 1ra ed, Fuquay-Varina: ALTHOS, 2008. 64p.

[C].-CISCO SYSTEMS, KnowledgeNet Implementing Cisco Multicast (MCAST), 1ra ed: CISCO, 2003. p. 597-646

[D].-CISCO SYSTEMS, Developing IP Multicast Networks, 1ra ed: CISCO, 2000. p. 412-443

[E].-GCYC, IP Multicast, 1ra ed: CREATIVE COMMONS ATTRIBUTION SHARE-ALIKE, 2009. 6p.

[F].-CISCO SYSTEMS, Cisco LAN Switching Configuration Handbook, 2da ed, Indianapolis: CISCO, 2009. p. 141-147

[G].-CISCO SYSTEMS, Cisco IOS IP Configuration Guide, 1ra ed. CISCO, 2006. p. 443 - 592

[H]-CISCO SYSTEMS, CCIE Routing and Switching, 4ta ed. CISCO, 2000. p. 168 – 184

[I].-JUNIPER NETWORKS, Introduction to IGMP for IPTV Networks, White Paper. JUNIPER, 2006. 18p.

[J].-CISCO, Multicast Deployment Made Easy, Design Implementation Guide. CISCO, 1999. 20p.

Páginas de Internet:

[1].- Guía de configuración rápida Multicast

http://www.cisco.com/en/US/tech/tk828/technologies_tech_note09186a00

80094821.shtml

20120130

[2].- Configuración de Ruteo IP Multicast IOS Release 12.0

http://www.cisco.com/en/US/docs/ios/12_0/np1/configuration/guide/1c

multi.html

20120130

[3].- Matriz de soporte Multicast en Switch Catalyst

http://www.cisco.com/en/US/tech/tk828/technologies_tech_note09186a00

80122a70.shtml

20120130

[4].- Referencia de Comandos CISCO IOS IP Multicast

http://www.cisco.com/en/US/docs/ios/ipmulti/command/reference/imc_b

ook.html

20120130

[5].- Guía de configuración Switch Catalyst 2950

http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/re

lease/12.1_6_ea2c/configuration/guide/scg.html

20120130

[6].- Calidad de Servicio QoS Diseño

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/

QoS_SRND/QoSIntro.html

20120130

[7].- Aplicación VLC Funciones

http://www.videolan.org/streaming-features.html

20120130

[8].- Aplicación de Videoconferencia Isabel

http://isabel.dit.upm.es/wiki/index.php

20120130