PRÁCTICA 3: ROUTING MULTICAST con PIM

Autor: Santiago Felici

1.- Objetivo

Configurar en la maqueta de routers que se muestra en la figura siguiente, routing multicast utilizando PIM (Protocol Independent Multicast), tanto en modo denso (PIM-DM, dense mode), modo disperso (PIM-SM, sparse mode) y en modo disperso-denso. Para configuración de modo disperso en PIM-SM utilizaremos puntos de encuentro o "Rendezvous Point" (que se abrevia por RP). La implementación la realizaremos con routers de Cisco Systems con su sistema operativo IOS[1] que soporta PIM. Para la realización de este práctica se requiere el manejo de las aplicaciones multicast vistas en prácticas anteriores, bien SDR de las herramientas Mbone (con VIC y RAT) o bien con VideoLAN. Para ver el uso de estas herramientas ver el anexo III.

Además se pretende que el alumno se familiarice con los comandos de los routers de Cisco Systems para analizar el comportamiento multicast. Para el análisis del tráfico multicast, sería interesante que el alumno guardara en un fichero aparte, para analizar a posteriori las diferentes salidas de los comandos, dados que estos incluyen mucha información.

2.- Introducción

Una vez el router sabe por IGMP en qué grupos multicast están interesados los hosts de su LAN debe 'conspirar' o actuar como apoderado de sus clientes, con los demás routers para conseguir que dichos paquetes le lleguen desde cualquier sitio donde se estén produciendo, utilizando para ello protocolos de routing multicast. Esta conspiración tiene dos planteamientos iniciales, o que todo el mundo esté interesado en la emisión multicast o que no lo esté, lo cual da pie a funcionamiento de los protocolos de routing en modo denso y disperso respectivamente.

En el modo denso, inicialmente los datagramas multicast se propagan por toda la red siguiendo un árbol óptimo sin bucles y si algún router no está interesado envía un mensaje de podado o 'prune' (prune = podar), formando el árbol de distribución multicast. En el modo disperso, se presupone que sólo una minoría de los routers tienen miembros del grupo multicast y en principio no se le envía a ninguno; si a alguno le interesa lo debe solicitar con un mensaje explícito (join).

PIM-DM utiliza para calcular rutas a los emisores la tabla de routing unicast. El tráfico se transmite inicialmente por inundación, con lo cual los routers no interesados pueden enviar comandos Prune (podar) o Graft (injertar). La inundación (y el consiguiente podado) se repite cada 3 minutos. Tras esta primera inundación, para evitar bucles, los routers ejecutan el RPF check (Reverse Path Forwarding check).

El RPF es una forma de evitar los bucles por inundación tanto en PIM-DM (Dense Mode) y PIM-SM (Sparse Mode o modo disperso), que consiste en, que antes de reenviar por inundación un paquete el router realiza la siguiente comprobación:

1. Analiza la interfaz de entrada del paquete y su dirección de origen (unicast)
2. Consulta en la tabla de rutas la interfaz de la ruta óptima hacia la dirección de origen
3. Si la interfaz de entrada coincide con la de la ruta óptima, el paquete es aceptado y redistribuido por inundación.
4. En caso contrario el paquete se descarta ya que probablemente se trata de un duplicado

Destacar que el RPF check es incompatible con rutas asimétricas obviamente.

Aunque PIM-DM es relativamente simple, presenta problemas de escalabilidad, como que cada router de la red ha de mantener la relación de las 'ramas' que cuelgan de él en el árbol así como la relación de las ramas que han sido podadas para cada emisor y cada grupo (cada par (S,G), Source, Group). Por tanto la gran cantidad de información de estado hace difícil establecer un servicio multicast en una red grande para un número elevado de emisores y grupos.

Como alternativa a PIM-DM tenemos PIM-SM, donde no se hace inundación de la información por parte de los routers con emisores activos y para localizar a los emisores, establecemos un punto de encuentro o "Rendezvous Point" donde los emisores se registren y los receptores vayan a preguntar. De esta forma, se crean árboles compartidos con raíz común en el "Rendezvous Point", minimizando la cantidad de información de estado en los

[1] Las versiones de IOS utilizadas son IP+ o IP plus

routers, mateniendo sólo información de estado de (*,G), donde * es el "Rendezvous Point" o centro de reunión de emisores y G son los diferentes grupos multicast emitidos desde el "Rendezvous Point".

En PIM-SM, los mensajes Join o Prune se envían por la interfaz por la que apunta la ruta unicast hacia el "Rendezvous Point" (o hacia la fuente, en caso de que se esté estableciendo el árbol SPT, Shortest Path Tree, directamente con ella). La dirección de destino de esos mensajes no es el "Rendezvous Point" o la fuente, sino la dirección multicast 224.0.0.13 propia de PIMv2 (PIM versión 2; por tanto sólo se mandan al siguiente router). El siguiente router, en función del mensaje recibido y su información de estado multicast, decide si debe o no, propagar el Join o Prune al siguiente router hacia la fuente.

Además PIM-SM puede fijar un umbral de tráfico a partir del cual los routers conmutan de árbol compartido con raíz en el "Rendezvous Point", a árbol de distribución individual con raíz en la fuente multicast o SPT. En el caso de la implementación de Cisco Systems, esta conmutación se realiza con el primer paquete multicast recibido en el receptor.

Comentar finalmente que el "Rendezvous Point" se puede asignar por configuración en cada router y es posible asignar un "Rendezvous Point" diferente para diferentes rangos de direcciones multicast.

Otro elemento importante en PIM-SM es el descubrimiento automático del "Rendezvous Point" (ej, Auto-RP de Cisco Systems), de forma que para evitar la configuración manual se utilizan protocolos de descubrimiento del "Rendezvous Point" (no estandarizados) que hace uso de dos grupos multicast para distribuir sus mensajes, concretamente "RP Announce: 224.0.1.39" y "RP Discovery: 224.0.1.40". Estos dos grupos multicast han de distribuirse necesariamente en modo denso.

También, existe la posibilidad de configurar los routers multicast en modo mixto denso y disperso, de forma que si se conoce a un "Rendezvous Point" (para un rango de direcciones multicast) se trabaja en modo disperso (para el rango de direcciones multicast especificado) y si no en modo denso, llamándose este modo PIM-SM-DM.

3.- Realización de la práctica

LEER ANTES DE EMPEZAR:

En el laboratorio se van a desarrollar varias maquetas (maqueta X, donde X será 1, 2, 3, etc) cada una formada por tres routers que denominaremos RP(X), RS1(X) y RS2(X). RP(X) tiene asociados dos hosts, HP1(X) y HP2(X), mientras que RS1(X) y RS2(X) tienen asociados los hosts HS1(X) y HS2(X) respectivamente. Inicialmente las maquetas son independientes (figura 1), luego se interconectan todas entre sí (figura 2).

Los siguientes pasos se han de realizar **de forma coordinada por todos los alumnos y paso a paso** durante toda la sesión y siguiendo las instrucciones del guión. Previamente, se supone que los alumnos deben estar familiarizados con la práctica o haberse leído este documento.

Todos los alumnos que participan en una misma maqueta, deben comprobar la ejecución de los comandos en los diferentes routers de su maqueta, ya que la información de cada router es sólo parcial dentro de los árboles multicast y por tanto para analizar el comportamiento del multicast necesitamos conocer la información de cada uno de los routers que forman la maqueta.

Se recomienda tener controlado el tráfico multicast para poder observar los árboles multicast creados por PIM. **En ocasiones tendremos que utilizar un analizador de protocolos (por ejemplo Ethereal o Wireshark) para comprobar realmente el tráfico emitido por cada ordenador**. Además, las líneas serie entre los routers no permiten velocidades superiores a 128 Kb/s, por lo que es importante evitar superar los 110 Kbps como máximo, pues en caso de saturación no podrán pasar los mensajes de PIM.

También se recomienda **eliminar cualquier cortafuegos**[2] configurado, para evitar que el tráfico multicast sea filtrado.

Los pasos a realizar en esta práctica son:

Paso 0: cableado de la maqueta

[2] En Linux desactive el firewall, "**services iptables stop".** En MS Windows, mirar en la esquina inferior derecha la aplicación en ejecución del cortafuegos y pinchando con el botón derecho, seleccionar "desactivar cortafuegos".

En primer lugar comprobar la conectividad física de toda la maqueta tal como indica en la siguiente figura. En el caso de las LAN de RP(X), a la que se conecta el router y dos hosts, es preciso utilizar un hub o conmutador. En el caso que los routers dispongan de varias interfaces LAN, escoger aquella de mayor velocidad.

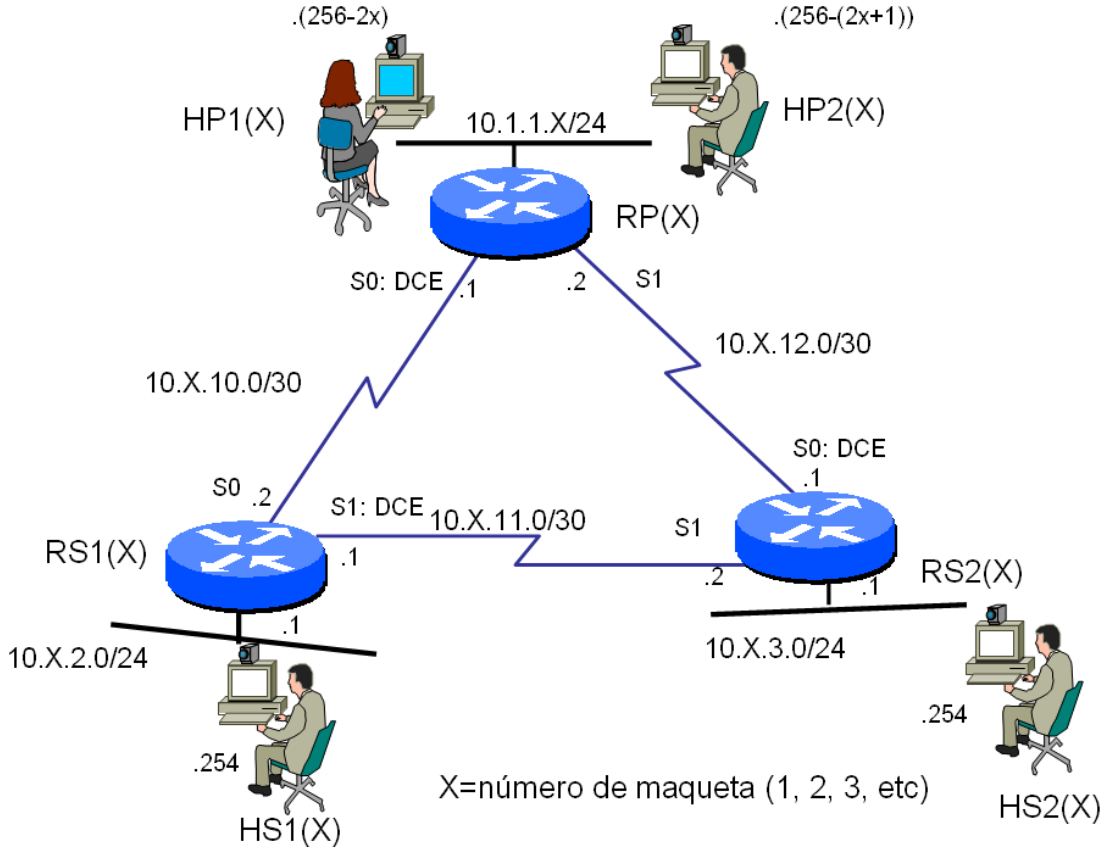

Figura 1. Maqueta independientes de tres routers en malla completa.

Paso 1: configuración de todos los routers con OSPF

En este paso vamos a configurar lógicamente la maqueta, concretamente sus routers. Como hay varias maquetas, cada maqueta vendrá identificada por un número en base al cual se realizará la asignación de direcciones IP. En concreto, la variable X que aparece en la asignación de IP hace referencia al número de maqueta (1, 2, 3, …) que asignará el profesor al inicio de la sesión.

Según la figura, la asignación de IP son

Router RP(X)
- LAN 10.1.1.X/24
- S0 (DCE) 10.X.10.1/30
- S1 10.X.12.2/30

Router RS1 (X)
- LAN 10.X.2.1/24
- S0 10.X.10.2/30
- S1 (DCE) 10.X.11.1/30

Router RS2 (X)
- LAN 10.X.3.1/24
- S0 (DCE) 10.X.12.1/30
- S1 10.X.11.2/30

Comentario DCE/DTE: por simplificación, podemos configurar como DCE todas las interfaces con "`clock rate`" y aquellas que no sean DCE ingonarán dicho comando.

***Ejemplo**: En la maqueta 2, la IP del router RS1(2) en su LAN será 10.2.2.1/24 y la IP del router RP(2) en su LAN será 10.1.1.2/24. Para el caso de los hosts conectados en LAN de RP(2), será en cada caso host HP1(2) 10.1.1.(256-2x) y host HP2(2) 10.1.1.(256-(2x+1)), y como x=2 por ser la maqueta 2, por tanto 10.1.1.252 y 10.1.1.251.*

En concreto las IP de las interfaces son:

Equipo	Interfaz	Maqueta 1	Maqueta 2	Maqueta 3	…	Maqueta x
RP	Fastethernet 0	10.1.1.1	10.1.1.2	10.1.1.3		10.1.1.x
	Serial 0	10.1.10.1	10.2.10.1	10.3.10.1		10.x.10.1
	Serial 1	10.1.12.2	10.2.12.2	10.3.12.2		10.x.12.2
HP1	Eth0	10.1.1.254	10.1.1.252	10.1.1.250		10.1.1.(256-2x)
HP2	Eth0	10.1.1.253	10.1.1.251	10.1.1.249		10.1.1.(256-(2x+1))
RS1	Fastethernet 0	10.1.2.1	10.2.2.1	10.3.2.1		10.x.2.1
	Serial 0	10.1.10.2	10.2.10.2	10.3.10.2		10.x.10.2
	Serial 1	10.1.11.1	10.2.11.1	10.3.11.1		10.x.11.1
HS1	Eth0	10.1.2.254	10.2.2.254	10.3.2.254		10.x.2.254
RS2	Fastethernet 0	10.1.3.1	10.2.3.1	10.3.3.1		10.x.3.1
	Serial 0	10.1.12.1	10.2.12.1	10.3.12.1		10.x.12.1
	Serial 1	10.1.11.2	10.2.11.2	10.3.11.2		10.x.11.2
HS2	Eth0	10.1.3.254	10.2.3.254	10.3.3.254		10.x.3.254

Los pasos para configurar los routers son:

NOTA: En ningún momento, se indica a lo largo de la práctica guardar la configuración de los routers. Con ello se simplifica el último paso de la práctica, que consiste en dejar la maqueta y los routers configurados tal como estaba en el inicio.

a.- utilizaremos la conexión de consola mediante el programa de emulación de terminal "minicom" (comando '**minicom**') o HyperTerminal en MS Windows (Programas->Accesorios->Comunicaciones->HyperTerminal). La configuración del programa de emulación debe ser la siguiente:

- Velocidad 9600 bits/s
- Sin paridad
- 8 bits de datos
- bit de parada (8N1)
- Dispositivo de entrada: ttyS0 o COM1

b.- encender el router. Debe aparecer la secuencia de mensajes de arranque. Esto nos confirma que la comunicación por el puerto de consola es correcta.

c.- Una vez ha arrancado el router debe aparecer el prompt `'Router>'`; teclear el comando **`'enable'`** para pasar a modo Privilegiado. En caso de que pida una password consultar al profesor.

d.- Ejecutar el comando "`show ip interface brief`" y tomar nota de los nombres asignados a las interfaces en cada modelo de router. El nombre de las interfaces depende del modelo y se utilizarán a continuación.

e.- Una vez en modo Privilegiado entraremos en modo Configuración Global para introducir la configuración que corresponde a cada router, siguiendo el siguiente modelo. Utilizad en cada router, el nombre para identificar a las diferentes interfaces, tal como se ha indicado anteriormente.

Ejemplo, para el router RS1 de maqueta 2 configurado sobre un router Cisco Systems 1721. Tened en cuenta que los nombres de las interfaces así como la identificación de cada uno de ellas depende según modelo. Por ese motivo, se ejecutó previamente el comando "`show ip interface brief`" para saber el nombre de las interfaces en el router y modelo utilizado.

```
Router>enable
Router#configure terminal
Router(config)#hostname RS1(2)
```

```
RS1(2) (config)#no ip domain-lookup
RS1(2) (config)#interface fastethernet 0
RS1(2) (config-if)#ip address 10.2.2.1 255.255.255.0
RS1(2) (config-if)#no shutdown
RS1(2) (config)#interface serial 0
RS1(2) (config-if)#ip address 10.2.10.2 255.255.255.252
RS1(2) (config-if)#clock rate 128000[3]
RS1(2) (config-if)#no shutdown
RS1(2) (config)#interface serial 1
RS1(2) (config-if)#ip address 10.2.11.1 255.255.255.252
RS1(2) (config-if)#clockrate 128000
RS1(2) (config-if)#no shutdown
RS1(2) (config-if)#exit
```

Como routing vamos a utilizar en este caso un protocolo estado del enlace no propietario, concretamente OSPF (OSPF, Open Shortest Path First). Para ello hay que habilitar el OSPF declarando todas las interfaces de cada router dentro del "*área 0*", es decir, vamos a configurar todas las redes como parte del área backbone (troncal) y por tanto todos los routers van a disponer de la misma información de la red. Otra forma para realizar esta configuración OSPF, sería en el caso de tener una red de mayores dimensiones, utilizando routing jerárquico, con múltiples áreas. La forma de configurar OSPF es como sigue:

Router(config)#router ospf xxx
Router(config-router)#network *d.d.d.d m.m.m.m* ***area 0***

Donde xxx es un número o identificativo de proceso que ejecuta OSPF interno para el router (por ejemplo, podemos poner "`router ospf 1`" o cualquier valor), *d.d.d.d* son direcciones de red de redes directamente conectadas y *m.m.m.m* es una "*wildmask*", es decir tiene el significado inverso de la máscara, 1's en vez de 0's. Ejemplo, /24 sería 0.0.0.255 en vez de 255.255.255.0. Para poder introducir esta configuración, tenemos 2 opciones:

- Especificar la dirección de las subredes de los interfaces que se vayan a anunciar con su *wildmask* apropiada, o en su defecto declarar la clase mayor que incluye a las interfaces y dejar que el propio proceso anuncie sólo las subredes dentro de la clase mayor declarada
- Especificar la IP de las interfaces que se vayan a anunciar con *wildmask* 0.0.0.0, es decir, fijando únicamente la IP de la interfaz y dejando que el proceso tome la máscara completa de la interfaz identificada

De estos métodos, el más simple y el que vamos a utilizar es el primero en su modo por defecto con declaración de la clase mayor. Por tanto, en nuestro caso bastará declarar

(config)#router ospf 1
(config-router)#network *10.0.0.0 0.255.255.255* ***area 0***

Una vez configurado OSPF y antes de ejecutar ningún comando más, vamos a borrar las posibles rutas aprendidas si las hubiera para forzar que el router obtenga las rutas utilizando para ellos el nuevo protocolo de routing configurado. Para ello, debemos ejecutar

Router#clear ip route *

Una vez inicializada la tabla de rutas (Routing Table (RT)), contrastar la información que nos ofrece sobre OSPF los siguientes comandos:

Router# show ip protocol
Router# show ip ospf nei

Router# show ip route

¿Se ven todas las redes? En caso de no ver todas las redes comprobar que las configuraciones son correctas y que las interfaces de todos los routers están operativas. Si todo está correcto, deja un tiempo para que las tablas de rutas se estabilicen dado que OSPF tiene que hacer con los LSP (Link State Packets) el árbol unicast SPF.

Prueba a realizar *ping* a todas las interfaces de los routers. Si no funciona, ¡ resuelve los problemas!.

[3] **Comentario DCE/DTE**: por simplificación, podemos configurar como DCE todas las interfaces con "`clock rate`" y aquellas que no sean DCE ingonarán dicho comando.

Hasta que no exista conectividad IP total no podemos continuar, dado que PIM requiere conectividad IP del protocolo de routing utilizado.

Ejercicio teórico:

Antes de seguir con los siguientes pasos, vamos a realizar un ejercicio teórico previo a routing multicast, que es el árbol de distribución broadcast truncado (ABT) o Source Distribution Tree (SDT). Como sabemos PIM va a calcular estos árboles tanto para el modo denso como para el modo disperso, utilizando la información de routing unicast (que se puede deducir a través del esquema de la maqueta) en base al RPF check (Reverse Path Forwarding check).

Calculad el ABT o SDT: suponed que en todas las LAN hay receptores multicast y todos los routers ejecutan PIM. Ver figura de la maqueta para detalles de IP y conexiones.

a.- utilizando modo denso y con un emisor en la LAN del router RP(X).
-
-
-
-
-

b.- utilizando modo disperso y siendo el "Rendezvous Point", el router RP(X) y con un emisor en la LAN del router RS2(X).
-
-
-
-
-

Paso 2: configuración de los hosts

En este paso vamos a configurar los hosts, que previamente habremos conectado en sus correspondientes LANs. Debemos asignarles una dirección IP y una ruta por defecto. La configuración en los hosts es:

En el caso de utilizar Windows, utilizar "Propiedades" en "Mis conexiones de Red"y allí configurar la IP y ruta por defecto de forma manual.

Linux

```
ifconfig eth0 inet d.d.d.d netmask 255.255.255.0
route add default gw r.r.r.r
```

donde "*d.d.d.d*" es la dirección del host acorde con la figura de la maqueta de la práctica y "*r.r.r.r*" es la ruta por defecto.

Nuevamente, vamos a comprobar la conectividad de los hosts, en este caso sólo a los hosts conectados en la LAN de RP(X).

Paso 3: creación de una única sesión multicast utilizando las herramientas vistas en prácticas anteriores en un host de la LAN del router RP(X)

Una vez tenemos conectividad IP entre todos los hosts y routers de la maqueta, vamos a lanzar una única sesión multicast con un ámbito a nivel de organización o mundo y crear por tanto el emisor multicast a través de las herramientas disponibles en uno de los hosts conectados en la LAN del router RP(X).

Para ello, en primer lugar conectaremos la cámara USB, (y el auricular y micrófono para el caso de emisión de audio). Lanzamos la aplicación utilizada para creación de sesiones multicast, anotamos la IP del grupo multicast utilizada y los puertos en los que se emite. Consultar la ayuda de las herramientas en el anexo III.

En el resto de ordenadores (uno en cada LAN de todos los routers), incluido donde está el emisor vamos a configurar los receptores y tratar de sintonizar el grupo multicast anunciado.

¿Tenemos éxito?:_____
¿Por qué?:_____

Antes de continuar al siguiente paso, debemos de desconectar todos los receptores existentes y dejar sólo el único emisor conectado.

Paso 4: routing multicast con PIM-DM o PIM en Modo Denso

Una vez lanzada la sesión multicast, podemos observar que en el resto de host en otras LAN no recibimos las sesiones nuevas anunciadas, simplemente porque no tenemos todavía routing multicast. Para solucionarlo, vamos a utilizar PIM-DM. En estos momentos no debe haber ningún receptor multicast conectado, sólo el emisor del paso anterior.

Para configurar todos los routers para que ejecuten IP multicast, IGMP y PIM, hay que introducir el siguiente comando en modo global de configuración:

Router(config)#ip multicast-routing

A continuación, para activar PIM-DM, hay que ir interfaz por interfaz y en TODAS ellas y en TODOS los routers, configurar como vemos para un caso general *xxx/yyy*

Router(configf)#interface xxx/yyy
Router(config-if)#ip pim dense-mode

Es importante configurar TODAS las interfaces, dado que PIM utiliza la tabla de rutas unicast para el RPF y por tanto, si las interfaces trabajan en unicast, también lo deben de hacer para multicast.

Con la configuración de PIM-DM en los routers, tenemos disponibles en los routers los siguientes comandos, los cuales sería interesante ejecutar y tomar nota de sus diferentes salidas.

Los comandos **disponibles de la versión de IOS utilizada**, centrándonos **en las opciones multicast** las podemos ver en el Anexo I y Anexo IV.

Ahora, ejecutar los siguientes comandos. Sería interesante tomar nota (o guardar en fichero) en especial de las siguientes salidas, para analizarlas posteriormente, dado que van a aparecer diferentes direcciones IP multicast y mucha información a procesar en una única sesión. Para poder interpretar las direcciones multicast podemos hacer uso de los servidores DNS en algún host conectado a Internet, mediante preguntas con los comandos "`nslookup`" en MS Windows o "`host`" en Linux. Ejemplo en Linux "`host 224.0.0.1`" nos indica que es ALL-SYSTEMS.MCAST.NET. Además en el Anexo II existe una relación de direcciones multicast.

Además, tal como hemos comentado anteriormente, sería interesante lanzar un analizador de protocolos (por ejemplo Ethereal o Wireshark) para ver el tráfico IP multicast generado por los host de cada LAN, para ver la coherencia de los comandos ejecutados a continuación, por ejemplo con el comando "`src net 10.1.1.0/24 and ip multicast`" para ver los paquetes multicast con origen la LAN de RP(1).

Otra forma de comprobar el tráfico multicast en la LAN es a través de IGMP. Ya que son los routers quienes gestionan IGMP, podemos ver las solicitudes/abandonos de tráfico multicast con:

`Router#debug ip igmp`
(para desactivarlo ejecutamos "`undebug all`")

Aunque no existan receptores en el grupo del emisor multicast creado en el paso anterior, podemos comprobar como los routers siguen participando en diferentes grupos multicast. En particular, el grupo creado anteriormente, si no existen receptores, no debe aparecer.

Pasemos en primer lugar a ejecutar en todos los routers (las salidas van a ser diferentes para cada router), los siguientes comandos:

Los siguientes comandos nos dan información de IGMP, su estado en cada interfaz y los grupos que gestiona.

```
Router#show ip igmp groups
IGMP Connected Group Membership
Group Address    Interface                Uptime    Expires   Last Reporter
-
-
-
-
-
```

```
Router#show ip igmp interface
-
-
-
-
-
```

El siguiente comando nos da información de los árboles multicast. Detalle de este comando lo tenemos en el Anexo IV. La salida de este comando está estructurada por los diferentes grupos multicast (*, G) y luego el detalle de las diferentes fuentes (S, G). En modo denso, nos indica que no hay "Rendezvous Point" con RP 0.0.0.0 y con RPF nbr (Reverse Path Forwarding neighbor) la IP del router en la rama siguiente del árbol multicast. Para el grupo (*, G) mantiene activo el flag D de denso. Para las fuentes (S, G) nos indica con el flag T que está trabajando con el árbol SPT.

Para cada (S, G) nos determina además las interfaces del router que participan en el árbol.

```
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, s - SSM
Outgoing interface flags: H - Hardware switched
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode
-
-
-
-
-
```

Otros comandos interesantes y complementarios al anterior son con la opción de resumen (`summary`) y con la opción de "`active`" para visualizar sólo aquellas fuentes que emiten tráfico mayor que un cierto umbral:

```
Router#show ip mroute summary
Router#show ip mroute active
```

El siguiente comando nos permite ver los interfaces configurados para multicast con PIM. Deben ser todos como hemos dicho anteriormente.

```
Router#show ip pim interface
-
-
-
-
-
```

El siguiente comando nos permite ver el tráfico multicast de entrada y salida por las interfaces del router.

```
Router#show ip pim interface count
-
-
-
-
-
```

El siguiente comando nos permite ver los vecinos que ejecutan PIM.
Router#show ip pim nei
-
-
-
-
-

Para comprobar las adyacencias establecidas por el protocolo PIM podemos lanzar el modo depuración:
Router#debug ip pim
(para desactivarlo ejecutamos "`undebug all`")

Ahora podríamos comprobar que las sesiones multicast se pueden visualizar en cualquier host de cualquier LAN, si tenemos la maqueta bien configurada. Pero para probarlo, lo haremos a través de las siguientes pruebas, ejecutando en cada una de ellas los comandos vistos anteriormente.

Otro comentario para poder analizar los diferentes resultados, es que **los usuarios suscritos a un grupo multicast, de forma indirecta participan como emisores multicast** al enviar paquetes con el protocolo RTCP, por tanto en una emisión si se utiliza RTP que es lo habitual, habrá tantos emisores como receptores y viceversa, es decir tanto árboles como LAN con hosts en el grupo multicast.

Pasemos a realizar las siguientes pruebas e interpretar los resultados correspondientes, en todos los routers de la maqueta. Tened en cuenta que los cambios a producir pueden llevar su tiempo (del orden de minutos), tal como se indicó en la introducción.

En particular el comando "**`show ip mroute [source][group]`**" permite observar las rutas multicast para un origen (source) o grupo (group) en concreto. En nuestro caso particular, puede ser útil fijar "`source`", como la IP del emisor multicast en la LAN de RP(X).

Realice las siguientes pruebas:

a.- comprobar el árbol de distribución cuando sólo tenemos un emisor y un receptor, por ejemplo en la LAN del router RP(X). ¿Coincide con el estimado previamente?

b.- una vez visto el árbol de distribución creado, desconectar el receptor. Esperar el tiempo necesario hasta que el árbol de distribución se haya modificado, ¿cuál es el nuevo árbol?

c.- ahora conectar en cada LAN un receptor y analizar cuál es el nuevo árbol de distribución

d.- una vez tenemos todo el árbol, ¿qué pasaría si desconectáremos el emisor?

Paso 5: routing multicast con PIM-SM o PIM en Modo Disperso

Uno de los inconvenientes de PIM-DM es la cantidad innecesaria de tráfico que se realiza.

¿Por qué?
-
-
-
-
-

Para solucionarlo, planteamos utilizar PIM-SM. En primer lugar vamos a eliminar cualquier tipo de configuración relacionada con PIM-DM simplemente con el comando:

*Router(config)# **no** ip multicast-routing*

Una vez borrada la configuración, volvemos a proceder como en el paso anterior.

Router(config)#ip multicast-routing

Y a continuación, activamos PIM-SM, en TODAS las interfaces de los routers, que para un caso general *xxx/yyy*

Router(configf)#interface xxx/yyy
Router(config-if)#ip pim sparse-mode

Otro elemento necesario y característico de los modos de routing multicast en modo disperso para PIM-SM, es especificar el lugar de cita de los emisores multicast o sesiones multicast, en lo que hemos llamado ("Rendezvous Point"). Para configurar el "Rendezvous Point" en los routers, debemos de introducir en todos los routers

Router(config)#ip pim rp-address "d.d.d.d"

donde en este caso "*d.d.d.d*" es la dirección de un router que realizará el papel de "Rendezvous Point". En nuestro caso configuraremos cualquiera de las IP de las interfaces del router RP(X). En el mismo RP(X), podemos bien no configurar nada o configurarse a él como su propio "Rendezvous Point".

Una vez realizada la configuración anterior, comprobar que todas las interfaces están en modo disperso.

Ejecutar los siguientes comandos. Sería interesante tomar nota (o guardar en fichero) en especial de las siguientes salidas, para analizarlas. Destacar que la versión de PIM-SM en Cisco Systems conmuta rápidamente (con el primer paquete) del ABT con "Rendezvous Point" al modo SPT.

```
Router#show ip igmp groups
IGMP Connected Group Membership
Group Address    Interface                Uptime    Expires   Last Reporter
-
-
-
-
-

Router#show ip igmp interface
-
-
-
-
-
```

El siguiente comando nos da información de los árboles multicast. Detalle de este comando lo tenemos en el Anexo IV. La salida de este comando está estructurada por los diferentes grupos multicast (*, G) y luego el detalle de los diferentes fuentes (S, G).

En modo disperso, nos indica para (*, G) el "Rendezvous Point" con RP y la IP, además el flag S nos indica que estamos en modo Sparse. Con RPF nbr (Reverse Path Forwarding neighbor) la IP del router en la rama ascendente del árbol multicast. Para (S, G) se puede observar los flags de T o J, que nos dan información de si la ruta es según SPT en el caso de T o si el ABT ha conmutado a SPT por superar el umbral de tráfico en caso de J. Dado que la conmutación de ABT a SPT por defecto es con 0 Kbps, no observaremos los árboles con raíz en el "Rendezvous Point", aunque sí nos indicará que ha sido el punto de encuentro.

Para cada (S, G) nos determina además las interfaces del router que participan en el árbol.

```
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, s - SSM
Outgoing interface flags: H - Hardware switched
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode
-
-
-
-
-

Router#show ip mroute summary
Router#show ip mroute active
```

Router#show ip pim interface
-
-
-
-
-

Router#show ip pim interface count
-
-
-
-
-

Router#show ip pim nei
-
-
-
-
-

Router#debug ip pim
(para desactivarlo ejecutamos "`undebug all`")

Ahora, vamos a comprobar el mapeo de "Rendezvous Point" y su funcionamiento. Para ello, ejecutamos
Router#show ip pim rp mapping
-
-
-
-
-

Router#debug ip pim auto-rp
(para desactivarlo ejecutamos "`undebug all`"). En este caso, el mapeo es estático, aunque no por ello el router trata de buscar anuncios de RP.
-
-
-
-
-

Trata de describir en base a los comandos anteriores, las diferencias más evidentes entre PIM-DM y PIM-SM.
-
-
-
-
-
¿Cuáles son los nuevos árboles de distribución creados cuando utilizamos "Rendezvous Point"?
-
-
-
-
-

Realizar las mismas pruebas que en el apartado anterior, para ver como evoluciona el routing multicast.

¿Afectaría para algo en PIM si utilizáramos EIGRP en vez de OSPF?
-
-

¿Qué versión de PIM utilizan los routers de la práctica?
-
-

Paso 6: PIM-SM-DM

Como hemos comentado anteriormente, se puede prever en esta maqueta una configuración mixta de PIM-DM y PIM-SM, de forma que si se conoce un RP se trabaje como PIM-SM y si no como PIM-DM.

Para ello debemos de configurar los interfaces que puedan conocer a un RP de la siguiente forma para un caso general *xxx/yyy*

Router(configf)#interface xxx/yyy
Router(config-if)#ip pim sparse-dense-mode

Por lo general, las interfaces WAN se suelen asociar al modo SM dado que disponen de un menor ancho de banda y las interfaces LAN al modo DM.

Paso 7: PIM-SM y conexión de TODAS las maquetas

Para poder observar los árboles con mayor número de nodos, vamos a interconectar las diferentes maquetas utilizando para ello la LAN de los routers RP(X), conectando por tanto RP(1), RP(2), RP(3), … tal como se muestra en la siguiente figura. Para ello utilizaremos cables cruzados para conectar cada conmutador de las maquetas en las mesas laterales con el conmutador de la mesa central. En definitiva, lo que hacemos en unir los routers RP(X) y los hosts HP1(X) y HP2(X) en una misma LAN.

Tal como hemos asignado las direcciones en el paso 1, las IP de los diferentes routers interconectados serán (si lo hemos realizado correctamente) 10.1.1.1/24, 10.1.1.2/24, 10.1.1.3/24, etc…. respectivamente para RP(1), RP(2), RP(3), …

Para realizar las dos uniones entre el conmutador y la maqueta 3 (router RP(3) y host HP1(3)) sin tener que mover equipos ni cruzar cables por el laboratorio utilizaremos dos puentes que hay establecidos entre la mesa central y la lateral, concretamente entre las rosetas números 538 y 557 y entre la 547 y 559.

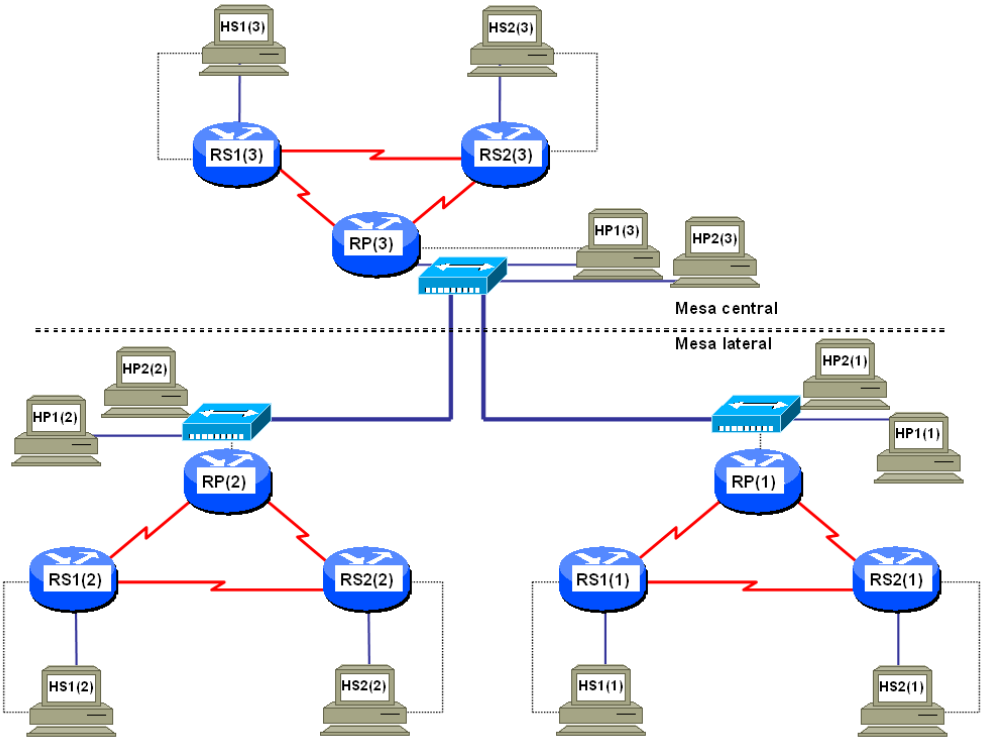

Figura 2. Maqueta completa de unión de todas las maquetas independientes.

Una vez cableado todo, debemos observar TODAS las rutas unicast en TODOS los routers y para ello ejecutaremos los siguientes comandos:

Router#clear ip route *

Una vez borrada los restos de la anterior tabla de rutas, observemos la nueva tabla creada con:

Router# show ip route

En caso de no ver todas las redes comprobar que las configuraciones son correctas y que las interfaces de todos los routers están operativas y no hay IP duplicadas. Si todo está correcto, deja un tiempo para que las tablas de rutas se estabilicen dado que OSPF tiene que recibir todos los LSP's (Link State Packets) y calcular el árbol unicast SPF, en base al cual crea la tabla de rutas en el router.

Para poder trabajar conjuntamente vamos a configurar un único lugar de cita de los emisores multicast o sesiones multicast o "Rendezvous Point".

Vamos a fijar en todos los routers como "Rendezvous Point" a RP(1).

Para ello, tal como hemos realizado anteriormente, debemos de introducir en todos los routers

Router(config)#ip pim rp-address "d.d.d.d"

donde en este caso "*d.d.d.d*" es cualquiera de las IP de las interfaces del router RP(1). En el mismo RP(1), podemos bien no configurar nada o configurarla a él como su propio "Rendezvous Point".

Además, volvermos a configurar PIM-SM, para ello debemos de configurar los interfaces para un caso general *xxx/yyy*

Router(configf)#interface xxx/yyy
Router(config-if)#ip pim sparse--mode

Una vez realizada la configuración anterior, comprobar que todas las interfaces están en modo disperso.

Ahora sólo el host HP1(1) realizará una emisión multicast que todos los demás hosts recibirán. Recordemos no superar el caudal máximo de 110 Kb/s. No debe haber ningún otro emisor.

Ejecutar los siguientes comandos. Sería interesante tomar nota en especial de las siguientes salidas, para analizarlas:

```
Router#show ip igmp interface
-
-
-
-
-

Router#show ip igmp groups
IGMP Connected Group Membership
Group Address    Interface                Uptime    Expires   Last Reporter
-
-
-
-
-

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, s - SSM
Outgoing interface flags: H - Hardware switched
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode
-
-
-
-
-
```

Router#show ip pim interface
-
-
-
-
-

Router#show ip pim interface count
-
-
-
-
-

Router#show ip pim nei
-
-
-
-
-

Router#debug ip pim
(para desactivarlo ejecutamos "`undebug all`")

Ahora, vamos a comprobar el mapeo de "Rendezvous Point" y su funcionamiento. Para ello, ejecutamos
Router#show ip pim rp mapping
-
-
-
-
-

Router#debug ip pim auto-rp
(para desactivarlo ejecutamos "`undebug all`")
-
-
-
-
-

Paso 8: dejarlo todo como al principio

Finalizada la práctica, dejaremos la configuración de los equipos y la maqueta tal como esta al principio de empezar la práctica.

ANEXO I: Comandos IP multicast en IOS c1700-sy-mz.122-11.T11

```
Router#show ip ?
  dvmrp                DVMRP information
  igmp                 IGMP information
  mpacket              Display possible duplicate multicast packets
  mrm                  IP Multicast Routing Monitor information
  mroute               IP multicast routing table
  msdp                 Multicast Source Discovery Protool (MSDP)
  mtag                 IP Multicast Tagswitching TIB
  pim                  PIM information

Router#show ip msdp[4] ?
  count     SA count per AS
  peer      MSDP Peer Status
  sa-cache  MSDP Source-Active Cache
  summary   MSDP Peer Summary

Router#show ip pim ?
  autorp      Global AutoRP information
  bsr-router  Bootstrap router (v2)
  interface [count]  PIM interface information
  neighbor    PIM neighbor information
  rp          PIM "Rendezvous Point" (RP) information
  rp-hash     RP to be chosen based on group selected

Router#debug ip ?
  cgmp       CGMP protocol activity
  dvmrp      DVMRP protocol activity
  igmp       IGMP protocol activity
  mbgp       MBGP information
  mhbeat     IP multicast heartbeat monitoring
  mpacket    IP multicast packet debugging
  mrm        IP Multicast Routing Monitor
  mrouting   IP multicast routing table activity
  msdp       Multicast Source Discovery Protocol (MSDP)
  mtag       IP multicast tagswitching activity
  pim        PIM protocol activity

Router#show ip igmp ?
  groups      IGMP group membership information
  interface   IGMP interface information
  membership  IGMP membership information for forwarding
  tracking    IGMP Explicit Tracking information
  udlr        IGMP undirectional link multicast routing information
```

[4] MSDP Multi Source Discovery Protocol, es un protocolo para descubrimiento de RP entre diferentes sistemas autónomos.

Anexo II: Relación de direcciones multicast y asignación

Rango	**Uso**
224.0.0/24	Bloque de control de la red local. No propagado por los routers. Asignado por la IANA
224.0.1/24	Bloque de control para la Internet. Asignado por la IANA
224.0.2/24 – 224.0.255/24	Bloque para asignaciones ad-hoc
224.1/16	Grupos multicast Stream Protocol
224.2/16	**Bloque SDP/SAP (MBone)**
232/8	Multicast específico de la fuente (SSM)
233/8	Reservado para 'glop addressing', que incluye byte 2 y 3 con el sistema autónomo.
239/8	Multicast con ámbito limitado por la dirección
255.255.255.255/32	Broadcast confinado a la LAN

Scope IPv6	**Ámbito**	**Direcciones IPv4 (RFC 2365)**
0	Reservado	
1	Nodo	
2	**Nivel de enlace (LAN)**	**224.0.0.0/24 239.255.0.0/16**
3	(sin asignar)	
4	(sin asignar)	
5	Ubicación (ej. Campus)	
6	(sin asignar)	
7	(sin asignar)	
8	**Organización**	**239.192.0.0/14**
9	(sin asignar)	
A	(sin asignar)	
B	(sin asignar)	
C	(sin asignar)	
D	(sin asignar)	
E	Global	224.0.1.0-238.255.255.255
F	Reservado	

Dirección	**Uso**
224.0.0.0	**Reservada**
224.0.0.1	**Hosts con soporte multicast**
224.0.0.2	**Routers con soporte multicast**
224.0.0.4	**Routers DVMRP (routing multicast)**
224.0.0.5	**Routers OSPF**
224.0.0.6	**Routers OSPF designados**
224.0.0.9	**Routers RIP v2**
224.0.0.10	**Routers IGRP**

224.0.0.11	**Agentes móviles**
224.0.0.12	**Agentes DHCP server/relay**
224.0.0.13	**Routers PIMv2 (routing multicast)**
224.0.0.15	**Routers CBT (routing multicast)**
224.0.0.22	**Routers IGMP v3 (Memb. Report)**
255.255.255.255	**Todos los hosts**

Dirección	**Uso**
224.0.1.1	**NTP – Network Time Protocol**
224.0.1.7	**Audio News**
224.0.1.12	**IETF-1-Video**
224.0.1.16	**Music-Service**
224.0.1.39	**RP Announce (PIM)**
224.0.1.40	**RP Discovery (PIM)**
224.0.1.41	**Gatekeepers (H.323)**
224.0.1.52	**Directorio VCR de MBone**
224.0.1.68	**Protocolo MADCAP**
224.2.127.254	**Anuncio de sesiones SAP (SDR)**

Anexo III: Herramientas multicast: Mbone tools y VLC

Mbone tools

Las herramientas MBone son un conjunto de programas que permiten realizar videoconferencias multicast a través de Internet. El software es de libre distribución y puede obtenerse de http://www-mice.cs.ucl.ac.uk/multimedia/software/. De la multitud de herramientas disponibles nosotros utilizaremos el SDR y el VIC.

SDR (Session Directory) permite crear y anunciar sesiones multicast, así como unirnos a otras ya existentes.

Recibir la lista de emisiones de Internet con SDR

Para ejecutar el SDR debemos hacer doble clic en el icono correspondiente, o bien seleccionar **'Inicio' -> 'Todos los programas'**, de la lista seleccionar '**Mbone Tools**' y una vez allí '**sdr**'. A continuación aparece una ventana con la lista de sesiones. Para ver una sesión la seleccionamos mediante doble clic.

Realizar emisiones propias con SDR

Para crear una emisión multicast, en la ventana de sesiones del SDR '**New**' y a continuación '**Create advertised session**'. Se entra entonces en un diálogo con varias etapas:

0. En la etapa 0 asigna a la sesión un nombre de la sesión; además le asignará una descripción (es obligatorio asignar una).
1. En la etapa 1 elegirá el valor por defecto (sesión tipo Test).
2. En la etapa 2 también elegirá los valores por defecto (sesión de dos horas de duración a empezar de forma inmediata).
3. En la etapa 3, '**Select the Distribution Scope**', elegirá 'IPv4 Local Scope' con lo que la sesión recibirá una dirección del rango 239.255.0.0/16 que tiene restringido el alcance al ámbito local.
4. En la etapa 4 elegirá audio y vídeo (aunque el audio no funciona esto nos permitirá ver lgunos aspectos interesantes).
5. En la etapa 5 '**Provide Contact Details**' dejará los valores por defecto.
6. En la etapa 6 '**Select security parameters for this session**' también dejará los valores por defecto.
7. Aceptar

Una vez creada la sesión cualquier ordenador puede unirse a ella simplemente seleccionándola de la lista que muestra la ventana de SDR. En la ventana que aparece debemos hacer clic en '**Join**'. Como SDR ha asignado una dirección multicast diferente al audio y al vídeo nos da opción de unirnos independientemente a uno de ambos medios, o a los dos. Si nos unimos al vídeo el SDR arrancará el programa VIC y si nos unimos al audio arrancará el RAT.

Para generar nuestra propia emisión seleccionaremos el menú '**Transmit**' y en '**Device…**' el dispositivo '**USB camera**'. Después pulsamos el botón '**Transmit**' y a partir de ese momento estaremos emitiendo vídeo. Podemos utilizar los mandos del '**Rate Control**' para regular el caudal (en Kb/s) y el número de fotogramas por segundo que generamos.

Herramientas VLC

VideoLAN es un software de dominio público que permite realizar distribución de vídeo streaming por Internet. El software incorpora tanto las funciones de servidor como de cliente.

El procedimiento para arrancar el **cliente VideoLAN** es el siguiente:

1- Arrancar el programa '**VLC media player**' mediante doble clic en el icono correspondiente.
2- Seleccionar en la ventana que aparece el menú '**Archivo:F**'
3- Elegir de la lista la opción '**Abrir Aparato de Captura…**'
4- En la ventana '**Abrir…**' seleccionar la pestaña '**Red**'
5- En la lista de botones radio seleccionar '**UDP/RTP Multiemisión**'. En ese momento se habilitan los campos '**Dirección**' y '**Puerto**'. La direccion la podemos prefijar previamente dentro del rango RFC 2365 para ámbito de organización 239.192.0.0/14.Ambos cliente y servidor utilizarán la misma dirección y puerto. El campo '**Puerto**' debe quedar con su valor por defecto (1234).
6- Pulsar el botón '**OK**'

A partir de este momento el cliente ya está preparado para recibir cualquier emisión multicast que ocurra en esa dirección y la tarjeta de red está preparada para capturar cualquier trama ethernet cuya dirección MAC de destino coincida con la MAC de mapeo de la dirección IP que hemos seleccionado.

El procedimiento para poner en marcha la emisión en **el servidor VideoLAN con streaming desde fichero**, es el siguiente:

1. Arrancar el programa '**VLC media player'** mediante doble clic en el icono correspondiente.
2. Seleccionar el menú '**Archivo:F'**
3. Elegir de la lista la opción '**Abrir Volcado de Red…: N'**
4. En la ventana '**Abrir…**' seleccionar la pestaña '**Archivo'**
5. Pulsar el botón '**Explorar'** y seleccionar el fichero correspondiente ('**Ethernet.mpg'**)
6. Marcar la casilla '**Volcado/Salvar'** y pulsar el botón 'Opciones'.
7. En la ventana '**Volcado de salida'** marcar la casilla '**RTP'**. En ese momento se habilitan los campos '**Dirección'** y '**Puerto'**.
8. En el campo '**Dirección'** poner la dirección que utilizará el servidor para la emisión multicast del rango RFC 2365 para ámbito de organización, 239.192.0.0/14 .El campo '**Puerto'** debe quedar con su valor por defecto (1234).
9. Además, especificar el campo TTL, dado que por defecto las emisiones se realizan con TTL 1 y por tanto este ámbito es de LAN. Modificar ese campo a 63 o 127 por ejemplo.
10. Pulsar el botón 'OK'

El procedimiento para poner en marcha la emisión en **el servidor VideoLAN con emision en directo**, es el siguiente:

1. Arrancar el programa '**VLC media player'**.
2. Seleccionar el menú '**Archivo:F'**
3. Elegir de la lista la opción '**Abrir Volcado de Red…: N'**
4. En la ventana '**Abrir**…' seleccionar la pestaña '**DirectShow'**

5. En la línea donde aparece ‘**Nombre del aparato de vídeo’** pulsar el botón ‘**Refresh list’**, desplegar la lista que aparece a la izquierda y seleccionar la cámara. Si no aparece esta opción debemos pulsar nuevamente el botón ‘Refresh list’ hasta que aparezca.
6. Comprobar que no estén marcadas las casillas ‘Propiedades del aparato’ y ‘Propiedades del sintonizador’.
7. Marcar la casilla ‘**Volcado/Salvar’** y pulsar el botón ‘**Opciones’**.
8. En la ventana ‘**Volcado de salid**a’ marcar la casilla ‘RTP’.
9. En el campo ‘**Dirección’** poner la dirección que utilizará el servidor para la emisión multicast del rango RFC 2365 para ámbito de organización, 239.192.0.0/14 .El campo ‘**Puerto’** debe quedar con su valor por defecto (1234).
10. Marca la casilla ‘**Códec de vídeo’**. Seleccionar ‘mp1v’. En ‘Tasa de bits (kb/s)’ seleccionar ‘512’. En ‘Escala’ dejar el valor por defecto (1).
11. Además, especificar el campo TTL, dado que por defecto las emisiones se realizan con TTL 1 y por tanto este ámbito es de LAN. Modificar ese campo a 63 o 127 por ejemplo.
12. Pulsar el botón ‘OK’.

Anexo IV: Relación extensa de comandos utilizados

Información original pública extraída de Cisco Systems para la versión de IOS utilizada en la práctica, respecto a los comandos utilizados en el desarrollo de la práctica.

show ip igmp groups
show ip igmp interface
show ip mroute
show ip pim interface
show ip pim neighbor
show ip pim rp

show ip igmp groups

Next table describes the significant fields shown in the displays.

show ip igmp groups Field Descriptions	
Field	**Description**
Group Address	Address of the multicast group.
Interface	Interface through which the group is reachable.
Uptime	How long (in weeks, days, hours, minutes, and seconds) this multicast group has been known.
Expires	How long (in hours, minutes, and seconds) until the entry expires. If an entry expires, then it will (for a short period) show the word "now" before it is removed. The word "never" indicates that the entry will not time out, because a local receiver is on this router for this entry. The word "stopped" indicates that timing out of this entry is not determined by this expire timer. If the router is in INCLUDE mode for a group, then the whole group entry will time out after the last source entry has timed out (unless the mode is changed to EXCLUDE mode before it times out).
Last Reporter	Last host to report being a member of the multicast group. Both IGMP v3lite and URD require a v2-report.
Group mode:	Can be either INCLUDE or EXCLUDE. The group mode is based on the type of membership reports received on the interface for the group. In the output for the **show ip igmp groups detail** command, the EXCLUDE mode also shows the "Expires:" field for the group entry (not shown in the output).
CSR Grp Exp	This field is shown for multicast groups in the Source Specific Multicast (SSM) range. It indicates the time (in hours, minutes, and seconds) since the last received group membership report was received. Cisco IOS software needs to use these reports for the operation of URD and IGMP v3lite, but they do not indicate group membership by themselves.
Group source list:	Provides details of which sources have been requested by the multicast group.
Source Address	IP address of the source.
Uptime	Indicates the time since the source state was created.
v3 Exp	Indicates the time (in hours, minutes, and seconds) until the membership for the source will time out according to IGMP operations. The word "stopped" is shown if no member uses IGMPv3 (but only IGMP v3lite or URD).

CSR Exp	Indicates the time (in hours, minutes, and seconds) until the membership for the source will time out according to IGMP v3lite or URD reports. The word "stopped" is shown if members use only IGMPv3.
Fwd	Indicates whether the router is forwarding multicast traffic due to this entry.
Flags	Information about the entry. The Remote flag indicates that an IGMPv3 report has been received by this source. The C flag indicates that an IGMP v3lite or URD report was received by this source. The U flag indicates that a URD report was received for this source.

show ip igmp interface

Next table describes the significant fields shown in the display.

show ip igmp interface Field Descriptions	
Field	**Description**
Ethernet0 is up, line protocol is up	Interface type, number, and status.
Internet address is... subnet mask is...	Internet address of the interface and subnet mask being applied to the interface, as specified with the **ip address** command.
IGMP is enabled on interface	Indicates whether IGMP has been enabled on the interface with the **ip pim** command.
IGMP query interval is 60 seconds	Interval at which the Cisco IOS software sends Protocol Independent Multicast (PIM) router query messages, as specified with the **ip igmp query-interval** command.
Inbound IGMP access group is not set	Indicates whether an IGMP access group has been configured with the **ip igmp access-group** command.
Multicast routing is enabled on interface	Indicates whether multicast routing has been enabled on the interface with the **ip pim** command.
Multicast TTL threshold is 0	Packet time-to-threshold, as specified with the **ip multicast ttl-threshold** command.
Multicast designated router (DR) is...	IP address of the designated router for this LAN segment (subnet).
No multicast groups joined	Indicates whether this interface is a member of any multicast groups and, if so, lists the IP addresses of the groups.

show ip mroute

To display the contents of the IP multicast routing table, use the **show ip mroute** command in EXEC mode.

show ip mroute [*group-address* | *group-name*] [*source-address* | *source-name*] [*type number*] [**summary**] [**count**] [**active** *kbps*]

Syntax Description

group-address | *group-name*	(Optional) IP address or name multicast group as defined in the Domain Name System (DNS) hosts table.
source-address | *source-name*	(Optional) IP address or name of a multicast source.
type number	(Optional) Interface type and number.
summary	(Optional) Displays a one-line, abbreviated summary of each entry in the IP multicast routing table.

count	(Optional) Displays statistics about the group and source, including number of packets, packets per second, average packet size, and bytes per second.
active *kbps*	(Optional) Displays the rate that active sources are sending to multicast groups. Active sources are those sending at the *kbps* value or higher. The *kbps* argument defaults to 4 kbps.

Usage Guidelines

If you omit all optional arguments and keywords, the **show ip mroute** command displays all entries in the IP multicast routing table.

The Cisco IOS software populates the multicast routing table by creating (S, G) entries from (*, G) entries. The asterisk (*) refers to all source addresses, the "S" refers to a single source address, and the "G" is the destination multicast group address. In creating (S, G) entries, the software uses the best path to that destination group found in the unicast routing table (that is, through Reverse Path Forwarding [RPF]).

The output for the **show ip mroute** command with the **active** keyword will display either positive or negative numbers for the rate pps. The router displays negative numbers when RPF packets fail or when the router observes RPF packtets with an empty OIF list. This type of activity may indicate a multicast routing problem.

Next table describes the significant fields shown in the displays.

show ip mroute Field Descriptions	
Field	**Description**
Flags:	Provides information about the entry.
D - Dense	Entry is operating in dense mode.
S - Sparse	Entry is operating in sparse mode.
B - Bidir Group	Indicates that a multicast group is operating in bidirectional mode.
s - SSM Group	Indicates that a multicast group is within the SSM range of IP addresses. This flag is reset if the SSM range changes.
C - Connected	A member of the multicast group is present on the directly connected interface.
L - Local	The router itself is a member of the multicast group. Groups are joined locally by the **ip igmp join-group** command (for the configured group), the **ip sap listen** command (for the well-known session directory groups), and rendezvous point (RP) mapping (for the well-known groups 224.0.1.39 and 224.0.1.40). Locally joined groups are not fast switched.
P - Pruned	Route has been pruned. The Cisco IOS software keeps this information so that a downstream member can join the source.
R - RP-bit set	Indicates that the (S, G) entry is pointing toward the RP. This is typically prune state along the shared tree for a particular source.
F - Register flag	Indicates that the software is registering for a multicast source.
T - SPT-bit set	Indicates that packets have been received on the shortest path source tree.
J - Join SPT	For (*, G) entries, indicates that the rate of traffic flowing down the shared tree is exceeding the SPT-Threshold set for the group. (The default SPT-Threshold setting is 0 kbps.) When the

	J - Join shortest path tree (SPT) flag is set, the next (S, G) packet received down the shared tree triggers an (S, G) join in the direction of the source, thereby causing the router to join the source tree. For (S, G) entries, indicates that the entry was created because the SPT-Threshold for the group was exceeded. When the J - Join SPT flag is set for (S, G) entries, the router monitors the traffic rate on the source tree and attempts to switch back to the shared tree for this source if the traffic rate on the source tree falls below the SPT-Threshold of the group for more than 1 minute. **Note** The router measures the traffic rate on the shared tree and compares the measured rate to the SPT-Threshold of the group once every second. If the traffic rate exceeds the SPT-Threshold, the J - Join SPT flag is set on the (*, G) entry until the next measurement of the traffic rate. The flag is cleared when the next packet arrives on the shared tree and a new measurement interval is started. If the default SPT-Threshold value of 0 kbps is used for the group, the J - Join SPT flag is always set on (*, G) entries and is never cleared. When the default SPT-Threshold value is used, the router immediately switches to the shortest path source tree when traffic from a new source is received.
M - MSDP created entry	Indicates that a (*, G) entry was learned through a Multicast Source Discovery Protocol (MSDP) peer. This flag is only applicable for a rendezvous point (RP) running MSDP.
X - Proxy Join Timer Running	Indicates that the proxy join timer is running. This flag is only set for (S, G) entries of an RP or "turnaround" router. A "turnaround" router is located at the intersection of a shared path (*, G) tree and the shortest path from the source to the RP.
A - Advertised via MSDP	Indicates that an (S, G) entry was advertised through an MSDP peer. This flag is only applicable for an RP running MSDP.
U - URD	Indicates that a URL Rendezvous Directory (URD) channel subscription report was received for the (S, G) entry.
I - Received Source Specific Host Report	Indicates that an (S, G) entry was created by an (S, G) report. This (S, G) report could have been created by Internet Group Management Protocol Version 3 (IGMPv3), URD, or IGMP v3lite. This flag is only set on the designated router (DR).
Outgoing interface flags:	Provides information about the entry.
H - Hardware switched	Indicates that a Multicast Multilayer Switching (MMLS) forwarding path has been established for this entry.
Timers:Uptime/Expires	"Uptime" indicates per interface how long (in hours, minutes, and seconds) the entry has been in the IP multicast routing table. "Expires" indicates per interface how long (in hours, minutes, and seconds) until the entry will be removed from the IP multicast routing table.
Interface state:	Indicates the state of the incoming or outgoing interface.
Interface	Indicates the type and number of the interface listed in the incoming or outgoing interface list.
Next-Hop or VCD	"Next-hop" specifies the IP address of the downstream neighbor. "VCD" specifies the virtual circuit descriptor number. "VCD0" means the group is using the static map

	virtual circuit.
State/Mode	"State" indicates that packets will either be forwarded, pruned, or null on the interface depending on whether there are restrictions due to access lists or a Time To Live (TTL) threshold. "Mode" indicates whether the interface is operating in dense, sparse, or sparse-dense mode.
(*, 224.0.255.1) and (198.92.37.100/32, 224.0.255.1)	Entry in the IP multicast routing table. The entry consists of the IP address of the source router followed by the IP address of the multicast group. An asterisk (*) in place of the source router indicates all sources. Entries in the first format are referred to as (*, G) or "star comma G" entries. Entries in the second format are referred to as (S, G) or "S comma G" entries. (*, G) entries are used to build (S, G) entries.
RP	Address of the RP router. For routers and access servers operating in sparse mode, this address is always 0.0.0.0.
flags:	Information about the entry.
Incoming interface:	Expected interface for a multicast packet from the source. If the packet is not received on this interface, it is discarded.
RPF neighbor or RPF nbr	IP address of the upstream router to the source. Tunneling indicates that this router is sending data to the RP encapsulated in register packets. The hexadecimal number in parentheses indicates to which RP it is registering. Each bit indicates a different RP if multiple RPs per group are used. If an asterisk (*) appears after the IP address in this field, the RPF neighbor has been learned through an assert.
Dvmrp	Indicates if the RPF information is obtained from the Distance Vector Multicast Routing Protocol (DVMRP) routing table. If "Mroute" is displayed, the RPF information is obtained from the static mroutes configuration.

Next table describes the significant fields shown in the display for the **count option.**

show ip mroute count Field Descriptions	
Field	**Description**
Group:	Summary statistics for traffic on an IP multicast group G. This row is displayed only for non-SSM groups.
Forwarding Counts:	Statistics on the packets that are received and forwarded to at least one interface. **Note** There is no specific command to clear only the forwarding counters; you can clear only the actual multicast forwarding state with the **clear ip mroute** command. Issuing this command will cause interruption of traffic forwarding.
Pkt Count/	Total number of packets received and forwarded since the multicast forwarding state to which this counter applies was created.
Pkts per second/	Number of packets received and forwarded per second. On an IP multicast fast-switching platform, this number is the number of packets during the last second. Other platforms may use a different approach to calculate this number. Please refer to the platform documentation for more information.
Avg Pkt Size/	Total number of bytes divided by the total number of packets for this multicast forwarding state. There is no direct display for the total number

	of bytes. You can calculate the total number of bytes by multiplying the average packet size by the packet count.
Kilobits per second	Bytes per second divided by packets per second divided by 1000. On an IP multicast fast switching platform, the number of packets per second is the number of packets during the last second. Other platforms may use a different approach to calculate this number. Please refer to the platform documentation for more information.
Other counts:	Statistics on the received packets. These counters include statistics about the packets received and forwarded and packets received but not forwarded.
Total/	Total number of packets received.
RPF failed/	Number of packets not forwarded due to a failed RPF or acceptance check (when bidir-PIM is configured).
Other drops(OIF-null, rate-limit etc)	Number of packets not forwarded for reasons other than an RPF or acceptance check (such as the OIF list was empty or because the packets were discarded because of a configuration, such as **ip multicast rate-limit**, was enabled).
Group:	Summary information about counters for (*, G) and the range of (S, G) states for one particular group G. The following RP-tree: and Source: output fields contain information about the individual states belonging to this group. **Note** For SSM range groups, the Group: displays are statistical. All SSM range (S, G) states are individual, unrelated SSM channels.
Source count:	Number of (S, G) states for this group G. Individual (S, G) counters are detailed in the Source: output field rows.
Packets forwarded:	The sum of the packets detailed in the Forwarding Counts: fields for this IP multicast group G. This field is the sum of the RP-tree and all Source: fields for this group G.
Packets received:	The sum of packets detailed in the Other counts fields for this IP multicast group G. This field is the sum of the Other count: Pkt Count fields of the RP-tree: and Source: rows for this group G.
RP-tree:	Counters for the (*, G) state of this group G. These counters are displayed only for groups that have a forwarding mode that do not forward packets on the shared tree. These (*,G) groups are bidir-PIM and PIM-SM groups. There are no RP-tree displays for PIM-DM and SSM range groups.
Source:	Counters for an individual (S, G) state of this group G. There are no (S, G) states for bidir-PIM groups.

show ip pim interface

Next table describes the significant fields shown in the displays.

show ip pim interface Field Descriptions	
Field	**Description**
Address	Interface IP address of the next hop router.
Interface	Interface type and number that is configured to run PIM.
Mode	Multicast mode in which the Cisco IOS software is operating. This can be dense mode or sparse mode. "DVMRP" indicates that a Distance Vector Multicast Routing Protocol tunnel is configured.
Neighbor Count	Number of PIM neighbors that have been discovered through this

	interface. If the Neighbor Count is 1 for a DVMRP tunnel, the neighbor is active (receiving probes and reports).
Query Interval	Frequency, in seconds, of PIM router query messages, as set by the **ip pim query-interval** interface configuration command. The default is 30 seconds.
DR	IP address of the designated router on a network. Note that serial lines do not have designated routers, so the IP address is shown as 0.0.0.0.
FS	An asterisk (*) in this column indicates that fast switching is enabled.
Mpackets In/Out	Number of packets into and out of the interface since the router has been up.
RP	IP address of the RP.
DF Winner	IP address of the elected DF.
Metric	Unicast routing metric to the RP announced by the DF.
Uptime	Length of time the RP has been up, in days and hours. If less than 1 day, time is expressed in hours:minutes:seconds.
State	Indicates whether the specified interface is an elected DF.
Offer count is	Number of PIM DF election offer messages that the router has sent out the interface during the current election interval.
Current DF ip address	IP address of the current DF.
DF winner up time	Length of time the current DF has been up, in days and hours. If less than 1 day, time is expressed in hours:minutes:seconds.
Last winner metric preference	The preference value used for selecting the unicast routing metric to the RP announced by the DF.
Last winner metric	Unicast routing metric to the RP announced by the DF.

show ip pim neighbor

Next table describes the significant fields shown in the display.

show ip pim neighbor Field Descriptions	
Field	**Description**
Neighbor Address	IP address of the PIM neighbor.
Interface	Interface type and number on which the neighbor is reachable.
Uptime/Expires	Uptime shows how long (in hours:minutes:seconds) the entry has been in the PIM neighbor table. Expires shows how long (in hours:minutes:seconds or in milliseconds) until the entry will be removed from the IP multicast routing table.
Ver	PIM protocol version.
DR Prio/Mode	Priority and mode of the designated router (DR). Possible modes are S (state refresh capable), B (bidirectional PIM capable), and N (neighbor doesn't include the DR-Priority Option in its Hello messages).

show ip pim rp

To display active rendezvous points (RPs) that are cached with associated multicast routing entries, use the **show ip pim rp** command in EXEC mode.

show ip pim rp [**mapping** | [**elected** | **in-use**] | **metric**] [*rp-address*]

Syntax Description

mapping	(Optional) Displays all group-to-RP mappings of which the router is aware (either configured or learned from Auto-RP).
elected	(Optional) Displays only the elected Auto RPs.
in-use	(Optional) Displays the learned RPs in use.
metric	(Optional) Displays the unicast routing metric to the RPs configured statically or learned via Auto-RP or the bootstrap router (BSR).
rp-address	(Optional) RP IP address.

Defaults

If no RP is specified, all active RPs are displayed.

Usage Guidelines

The Protocol Independent Multicast (PIM) version known for an RP influences the type of PIM register messages (version 1 or version 2) that the router sends when acting as the designated router (DR) for an active source. If an RP is statically configured, the PIM version of the RP is not set and the router, if required to send register packets, first tries to send PIM version 2 register packets. If that fails, the router sends PIM version 1 register packets.

The version of the RP displayed in the **show ip pim rp** command output can change according to the operations of the router. When the group is created, the version shown is for the RP in the RP mapping cache. Later, the version displayed by this command may change. If this router is acting as a DR for an active source, the router sends PIM register messages. The PIM register messages are answered by the RP with PIM register stop messages. The router learns from these PIM register stop messages the actual PIM version of the RP. Once the actual PIM version of the RP is learned, this command displays only this version. If the router is not acting as a DR for active sources on this group, then the version shown for the RP of the group does not change. In this case, the PIM version of the RP is irrelevant to the router because the version of the RP influences only the PIM register messages that this router must send.

When you enter the **show ip pim rp mapping** command, the version of the RP displayed in the output is determined only by the method through which an RP is learned. If the RP is learned from Auto-RP then the RP displayed is either "v1" or "v2, v1." If the RP is learned from a static RP definition, the RP version is undetermined and no RP version is displayed in the output. If the RP is learned from the BSR, the RP version displayed is "v2."

Use the **elected** keyword on an Auto-RP Mapping Agent to limit the output to only the elected RPs that the mapping agent will advertise to all other routers in the network via Auto-RP. This is useful when comparing the output of the **show ip pim rp mapping** command on non mapping agent routers with the output of the **show ip pim rp mapping elected** command on a mapping agent to verify that the Group-to-RP mapping information is consistent.

Next table describes the significant fields shown in the displays.

show ip pim rp Field Descriptions	
Field	**Description**
Group	Address of the multicast group about which to display RP information.
RP	Address of the RP for that group.

v2	Indicates that the RP is running PIM version 2.
v1	Indicates the RP is running PIM version 1.
next RP-reachable in...	Indicates the time the next RP-reachable message will be sent. Time is expressed in hours:minutes:seconds.
bidir	Indicates that the RP is operating in bidirectional mode.
Info source	RP mapping agent that advertised the mapping.
(?)	Indicates that no Domain Name System (DNS) name has been specified.
via Auto-RP	Indicates that RP was learned via Auto-RP.
Uptime	Length of time the RP has been up (in days and hours). If less than 1 day, time is expressed in hours:minutes:seconds.
expires	Time in (hours: minutes: and seconds) in which the entry will expire.
Metric Pref	The preference value used for selecting the unicast routing metric to the RP announced by the designated forwarder (DF).
Metric	Unicast routing metric to the RP announced by the DF.
Flags	Indicates the flags set for the specified RP. The following are descriptions of possible flags: • C—RP is configured. • L—RP learned via Auto-RP or the BSR.
RPF Type	Routing table from which this route was obtained, either unicast, Distance Vector Multicast Routing Protocol (DVMRP), or static mroute.
Interface	Interface type and number that is configured to run PIM.