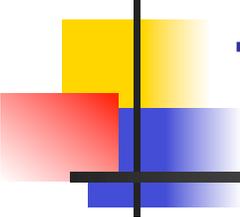
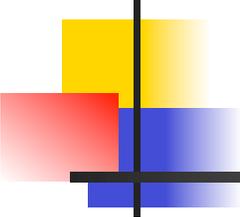


Implementando IP Multicast



Tipos de Transmisión

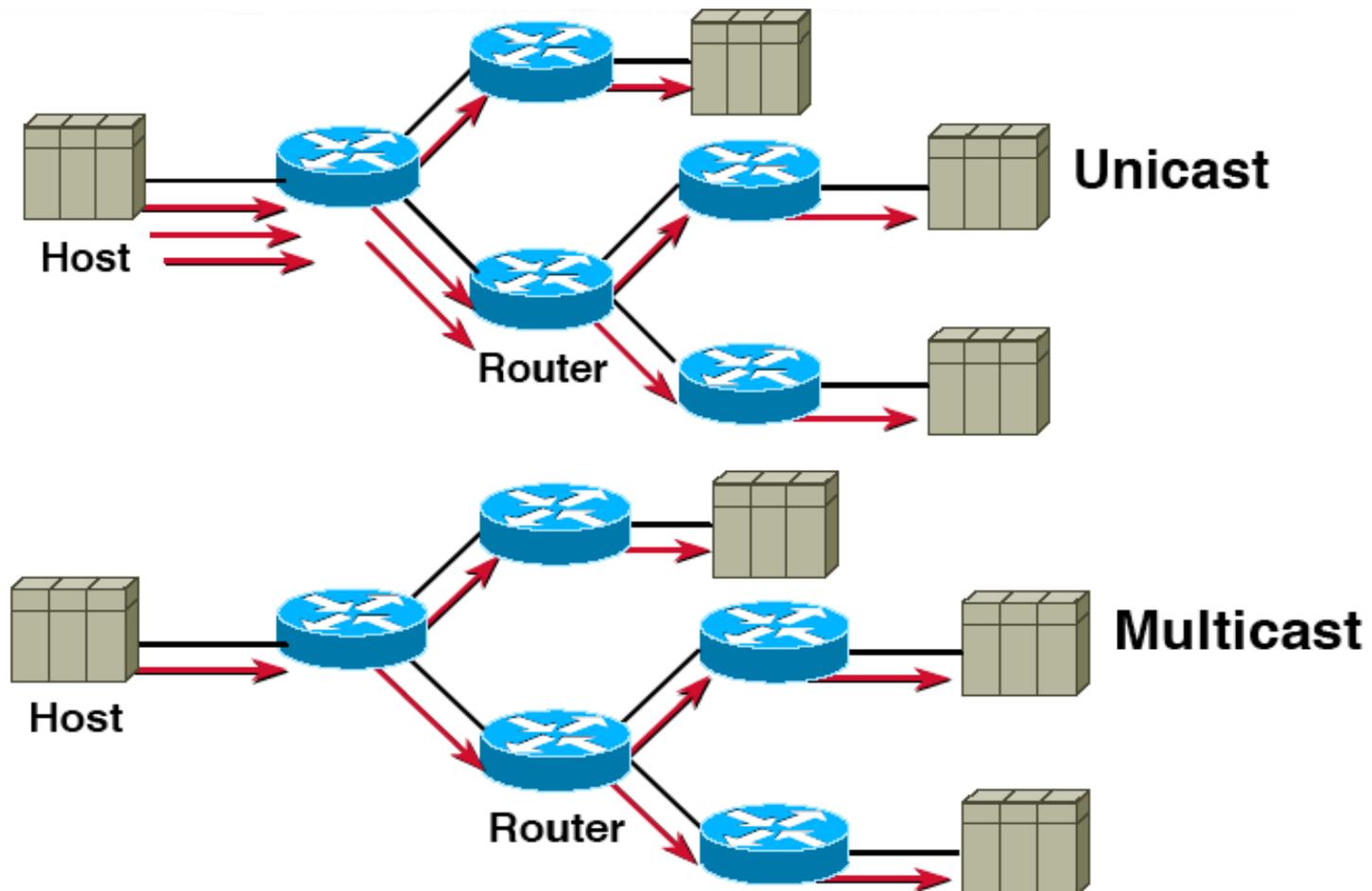
- Unicast
 - Comunicación uno a uno
- Broadcast
 - Comunicación uno a todos
- Multicast
 - Comunicación uno a miembros de un grupo que ha expresado interés
- Anycast
 - Comunicación de uno a uno con localización cercana basada en tablas de enrutamiento

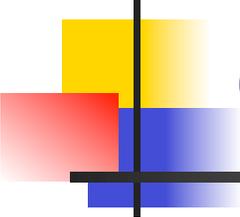


Por Qué Multicast?

- Cuando se quiere enviar los mismos datos a varios destinatarios
- Mejor uso del ancho de banda
- Menor procesamiento en los computadores y enrutadores
- Se desconoce la dirección de los destinatarios

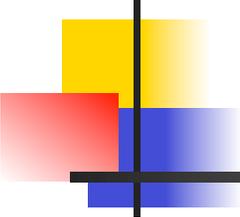
Diferencias entre Unicast y Multicast





Servicios Que Se pueden Ofrecer con Multicast

- Aplicaciones con muchos destinatarios
 - Distribución de Vídeo
 - Distribución de Informaciones de Interés Común
 - Bolsa de valores, anuncios, resultados de eventos, noticias
 - Replicación de datos
 - Juegos distribuidos



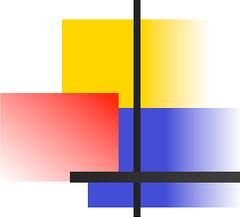
Direcciones de IP Multicast

- Direcciones tipo Clase D
 - 1110xxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx
 - 224.0.0.0 - 239.255.255.255
- Direcciones Reservadas por IANA
 - 224.0.0.0/24 para protocolos de enrutamiento en la subred local
 - 224.0.1.0/24 para aplicaciones con alcance global
 - 232.0.0.0/8 para Multicast con Origen Específico (SSM)
 - 233.0.0.0/8 para GLOP (<http://www.shepfarm.com/multicast/glop.html>)
 - 239.0.0.0/8 para grupos con restricción de distancia administrativa.

Direcciones Multicast de Capa-2 Ethernet



- El bit 0 del octeto 0 indica si la dirección está destinada a todas las estaciones (0xFFFFFFFF) o a un grupo de estaciones
- Para Ethernet las direcciones de multicast usan el prefijo de 24 bits 0x01:00:5E:xx:xx:xx
- La mitad, 23 bits del resto, están disponibles para direcciones de grupos de multicast

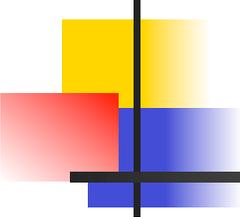


Representación de Direcciones de IP en Capa-2

- De los 32 bits para direcciones de IP multicast, cuatro son comunes (0x1110) y se pueden ignorar, esto nos deja con 28 bits
- Como sólo tenemos 23 bits en la dirección de capa-2, 5 de los 28 bits anteriores se pierden
- Los 23 bits restantes, representados en hexadecimal son agregados al OUI
0x01005E

Representación de Direcciones de IP en Capa-2



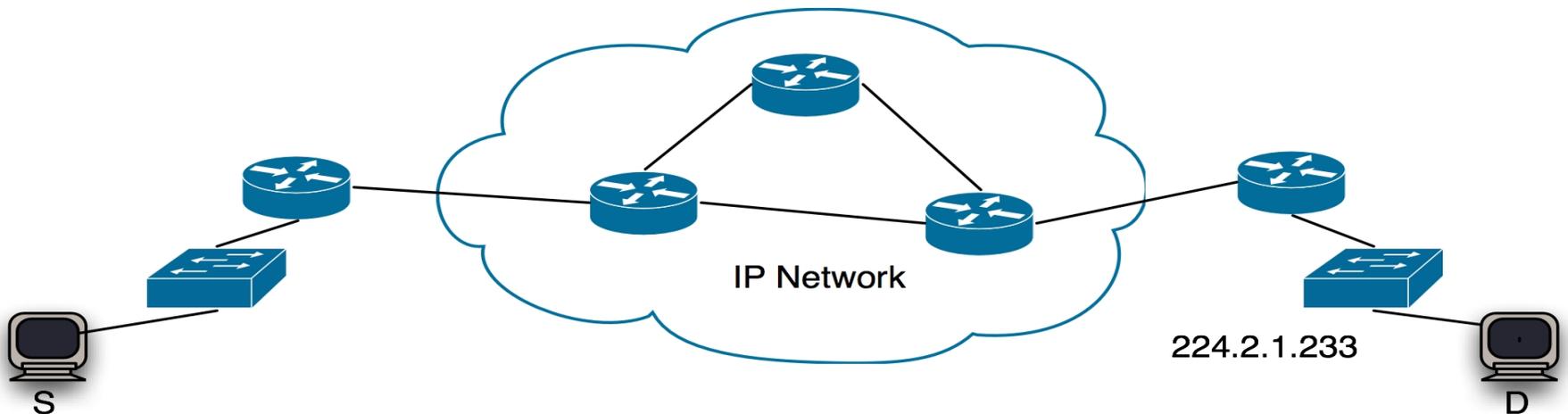


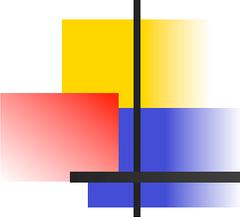
Representación de Direcciones de IP en Capa-2

- La pérdida de 5 bits en la dirección de multicast IP durante la representación a capa-2, causa que 2^5 direcciones de IP sean representadas por la misma dirección de capa-2
 - 32 direcciones IP multicast son representadas por la misma dirección multicast de capa-2
- Esta ambigüedad debe ser manejada por los niveles superiores durante el análisis de la dirección de multicast.

Terminología Básica

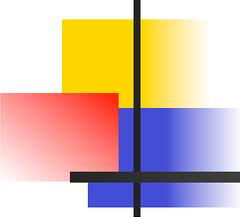
- S : Source : Origen : Dirección de origen de los paquetes de multicast
- G : Group : Grupo : Dirección de multicast del grupo que recibe los paquetes de multicast
- * : Star : Asterisco : Representa un estado para todas las direcciones de origen (fuente)





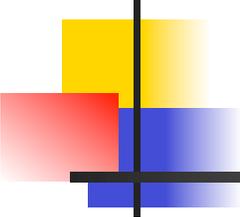
Modelo de Servicio

- Multicast utiliza UDP como protocolo de transporte
- Basado en el RFC 1112 que especifica las extensiones para el soporte de multicast en las estaciones
- Cada grupo de multicast está representado por una dirección de IP en la clase D
- Miembros del grupo pueden estar localizados en cualquier parte del Internet



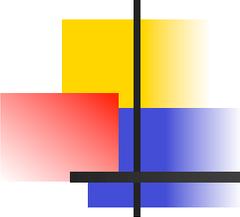
Modelo de Servicio

- Miembros pueden subscribirse y retirarse de los grupos y deben indicar estas acciones a los enrutadores que sirven el segmento de red, utilizando IGMP
- Fuentes y receptores son diferentes, por ejemplo, una fuente no tiene que ser miembro de un grupo para enviar mensajes a el grupo
- Enrutadores escuchan por todas las direcciones de multicast y usan protocolos de enrutamiento de multicast (e.g. PIM) para administrar los grupos y enviar mensajes.



Modelo de Servicio

- Enrutamiento basado en origen del paquete
 - Contrario a Unicast, donde el enrutamiento está basado en el destino del paquete
- Los enrutadores utilizan RPF para decidir hacia dónde replicar los paquetes de multicast

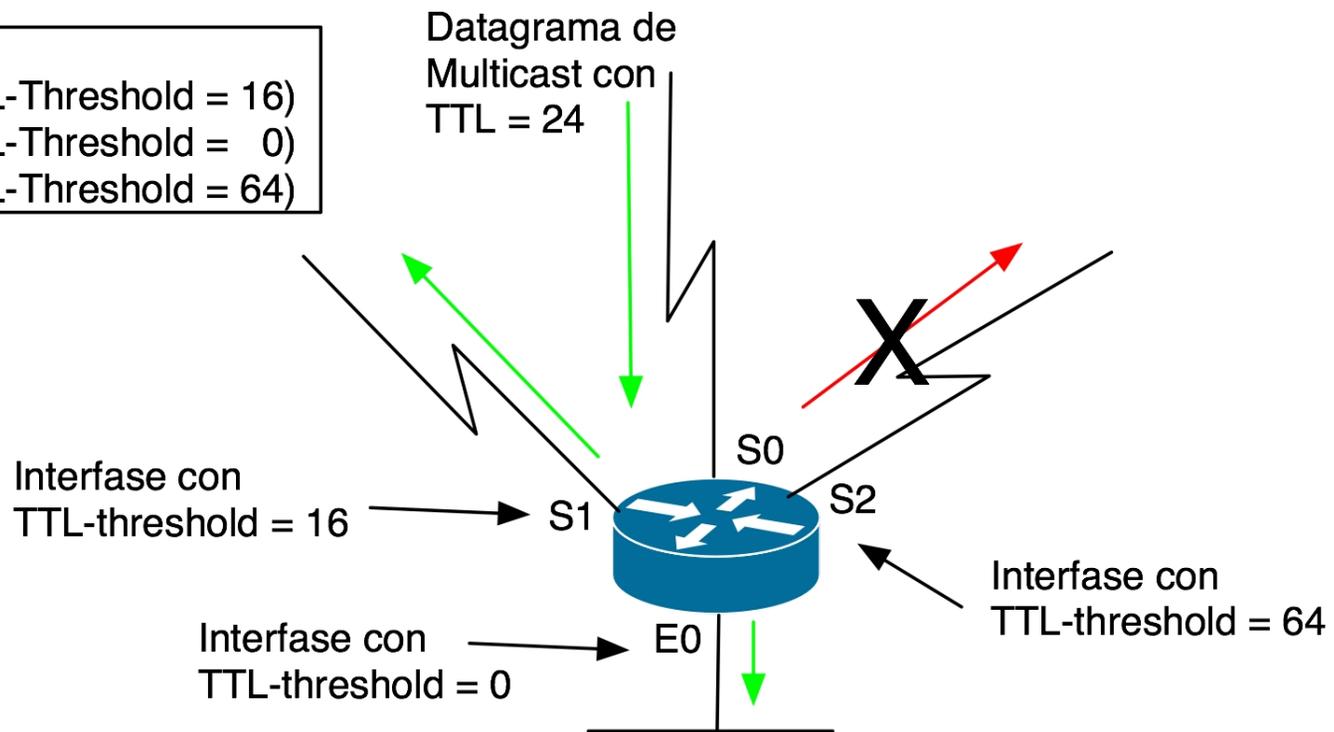


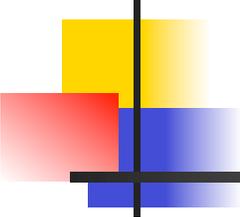
Restringiendo el Alcance

- TTL: Tiempo de vida del datagrama
 - Los datagramas de multicast deben tener un TTL > TTL asignado a la interfaz
 - Si el TTL es menor, el datagrama es descartado
 - Ejemplos de valores:
 - 0 -> limitado a la estación
 - 1 -> limitado al segmento local
 - 32 -> limitado a la misma red
 - 64 -> limitado a una región
 - 128 -> limitado al mismo continente
 - 255 -> no limitado
 - Sin embargo este no es un mecanismo confiable para limitar el alcance de los datagramas de multicast

Restringiendo el Alcance

oilst:
S1: (TTL-Threshold = 16)
E0: (TTL-Threshold = 0)
S2: (TTL-Threshold = 64)



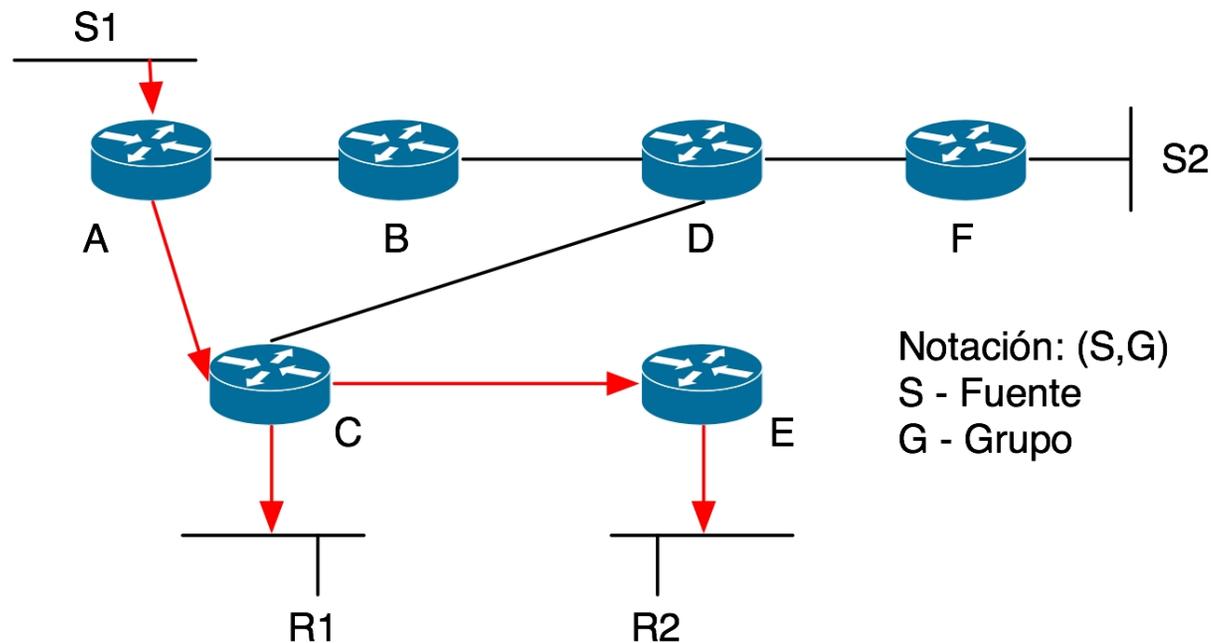


Restringiendo el Alcance

- Grupos con Restricción de Distancia Administrativa
 - Recomendadas para aplicaciones que no deben dejar un área determinada
 - El enrutador que delimita el alcance administrativo de la red deberá bloquear este rango
 - 239.0.0.0/8 (239.0.0.0 - 239.255.255.255)
 - Site-local
 - 239.255.0.0/16 (239.255.0.0 - 239.255.255.255)
 - Organization-Local
 - 239.192.0.0/14 (239.192.0.0 - 239.251.255.255)
 - Las mismas direcciones pueden ser usadas en varias instituciones
 - El concepto es similar al de las direcciones unicast privadas (RFC1918)

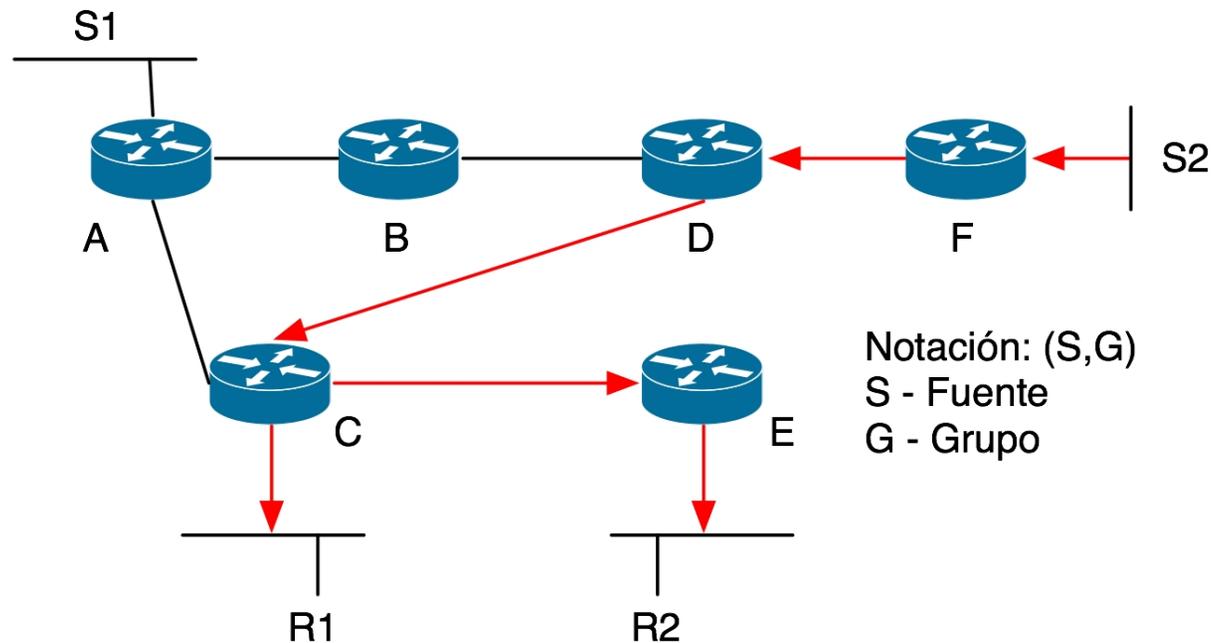
Arboles de Distribución

- Arbol de Camino Más Corto (Source/ Shortest Path Tree - SPT)



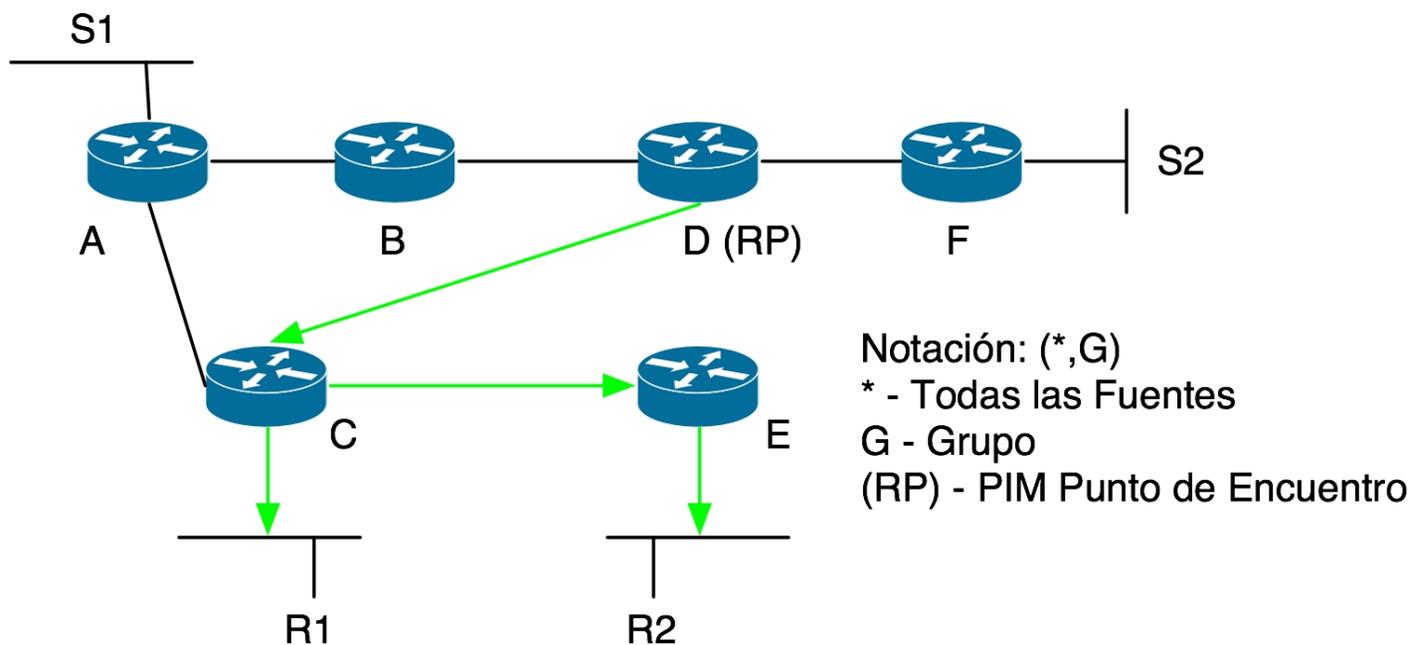
Arboles de Distribución

- Arbol de Camino Más Corto (Source/ Shortest Path Tree - SPT)



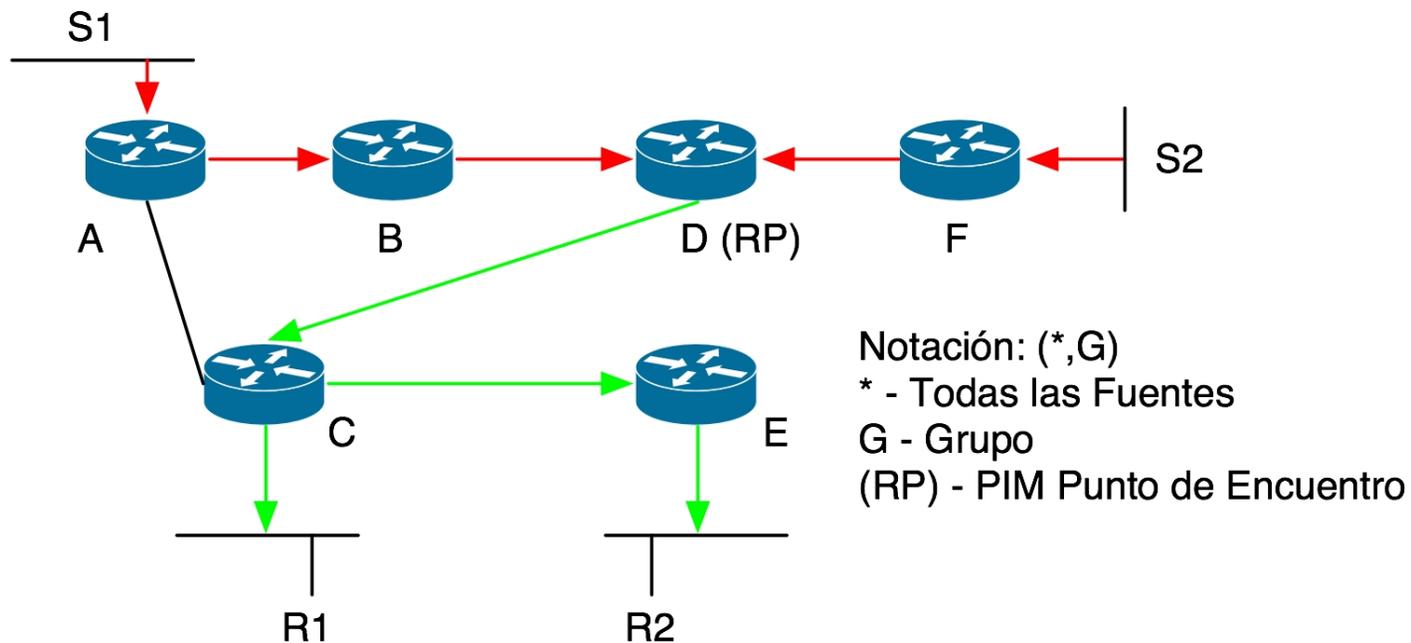
Arboles De Distribución

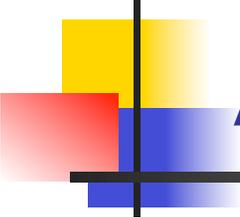
- Arbol de Distribución Compartido (Shared/Core Distribution Tree - RPT)



Arboles De Distribución

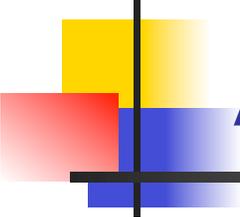
- Arbol de Distribución Compartido (Shared/Core Distribution Tree - RPT)





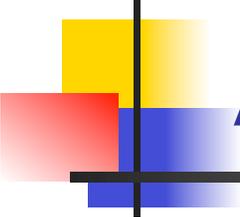
Arboles De Distribución

- Arbol de Camino Más Corto (SPT)
 - Usa más memoria, $O(S \times G)$
 - ofrece los caminos más óptimos desde las fuentes hasta los destinos
 - Minimiza retardos
 - Mejor para distribución de uno a muchos



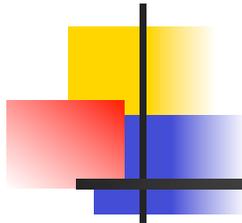
Arboles De Distribución

- Arbol de Distribución Compartido
 - Usa menos memoria, $O(G)$
 - Dependiendo de la topología, los caminos desde las fuentes hacia los destinos podrían ser sub-óptimos
 - Podría introducir retardos
 - La localización del RP y el tipo de dispositivo podrían afectar rendimiento
 - Mejor para distribuciones de muchos a muchos
 - Dependiendo de configuración, podría ser necesario para el descubrimiento de las fuentes



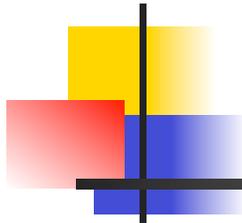
Arboles De Distribución

- Como se pueden construir los árboles de distribución?
 - **PIM**: utiliza tablas de enrutamiento unicast existentes además de un mecanismo para juntar/cortar/insertar nodos
 - **DVMRP**: usa la tabla de enrutamiento de DVMRP además de un mecanismo de envenenamiento invertido(poison-reverse)
 - **MOSPF**: usa extensiones del mecanismo de estado del enlace en OSPF
 - **CBT**: utiliza tablas de enrutamiento unicast existentes además de un mecanismo para juntar/cortar/insertar nodos



RPF

- Qué es RPF?
 - Un enrutador sólo envía los datagramas si éstos han sido recibidos en la interfaz hacia la estación de origen (S)
- Verificación de RPF
 - La tabla de enrutamiento para multicast es comparada con la dirección de origen en el datagrama
 - Si el datagrama arribó en la interfaz especificada en la tabla de enrutamiento para la dirección de origen; entonces la verificación de RPF es satisfactoria
 - Sino; la verificación de RPF falla

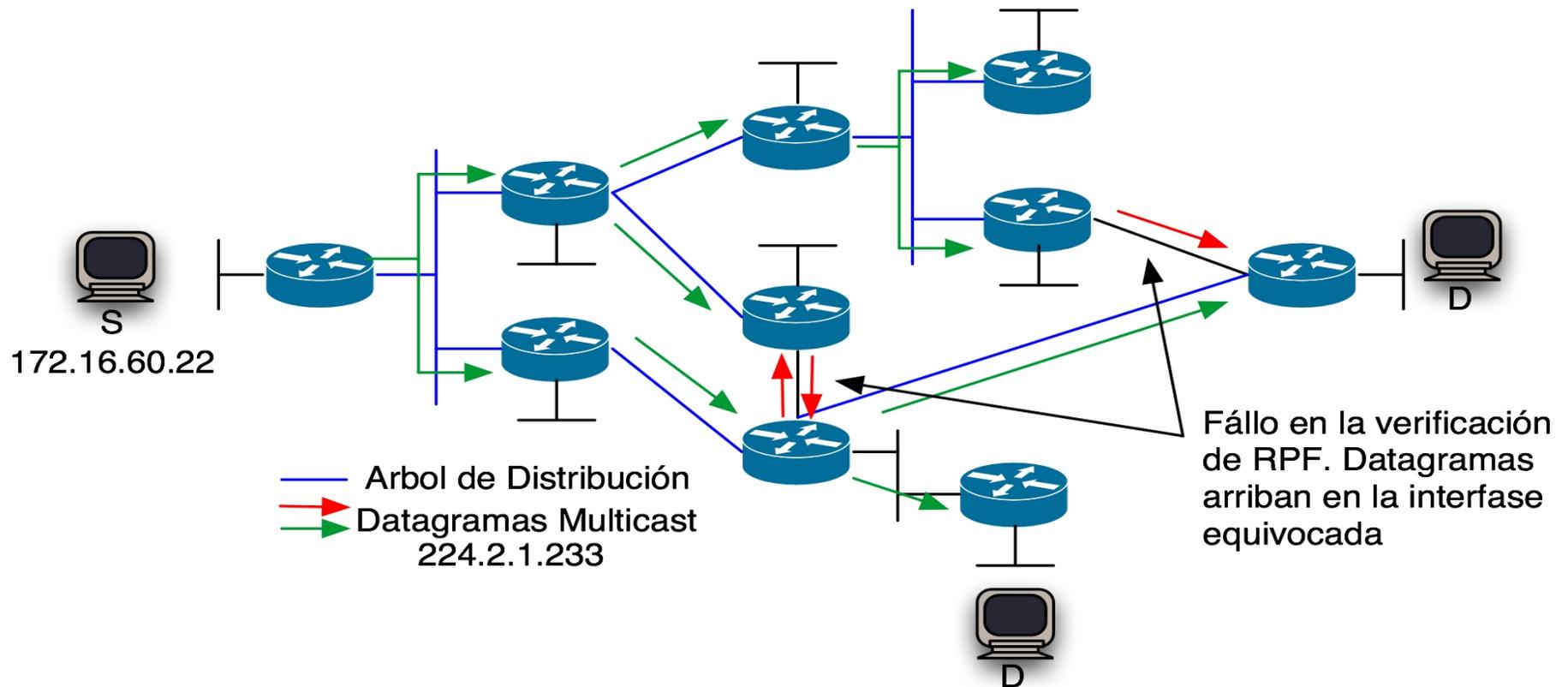


RPF

- Si la verificación de RPF es satisfactoria, el datagrama es replicado
- Si la verificación de RPF falla, el datagrama es descartado en silencio
- Cuando un datagrama es replicado, es enviado por todas las interfaces en la lista de interfaces de salida para el grupo
- El datagrama **NUNCA** debe ser enviado por la misma interfaz en que arribó al enrutador (la interfaz RPF)

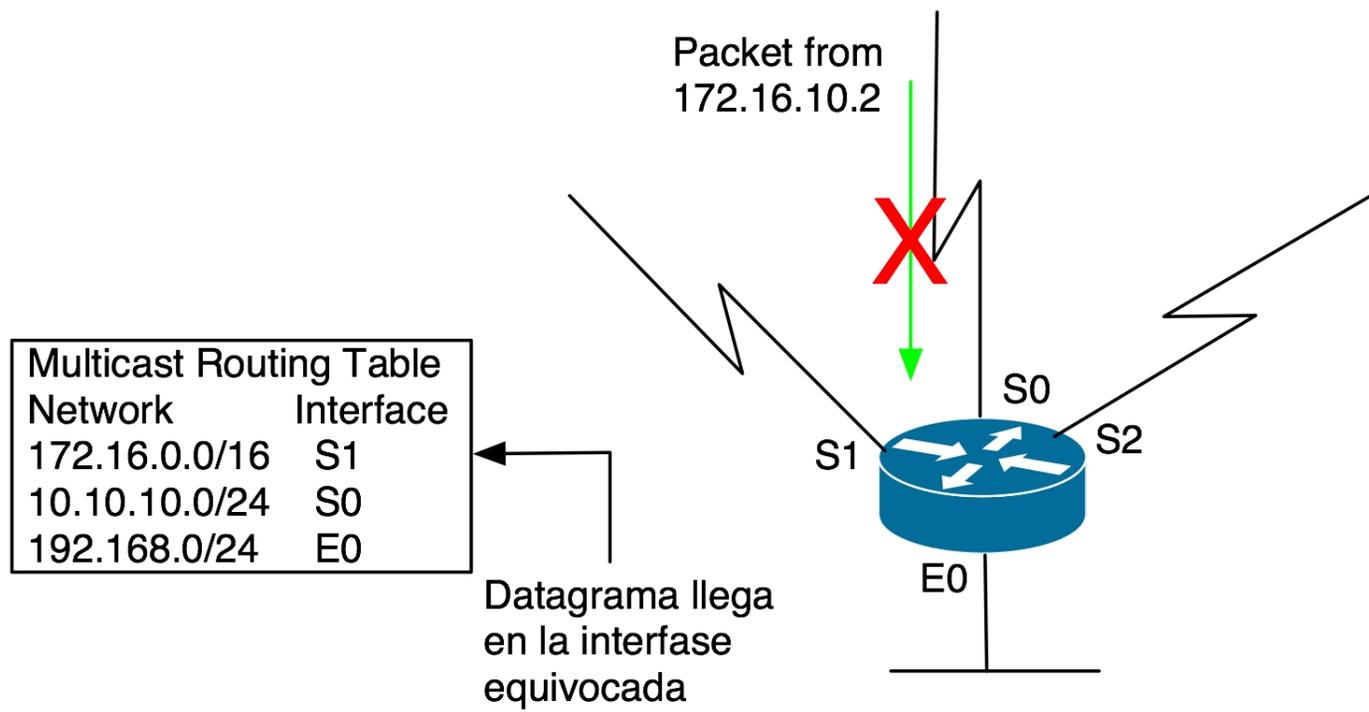
RPF

■ Verificación de RPF



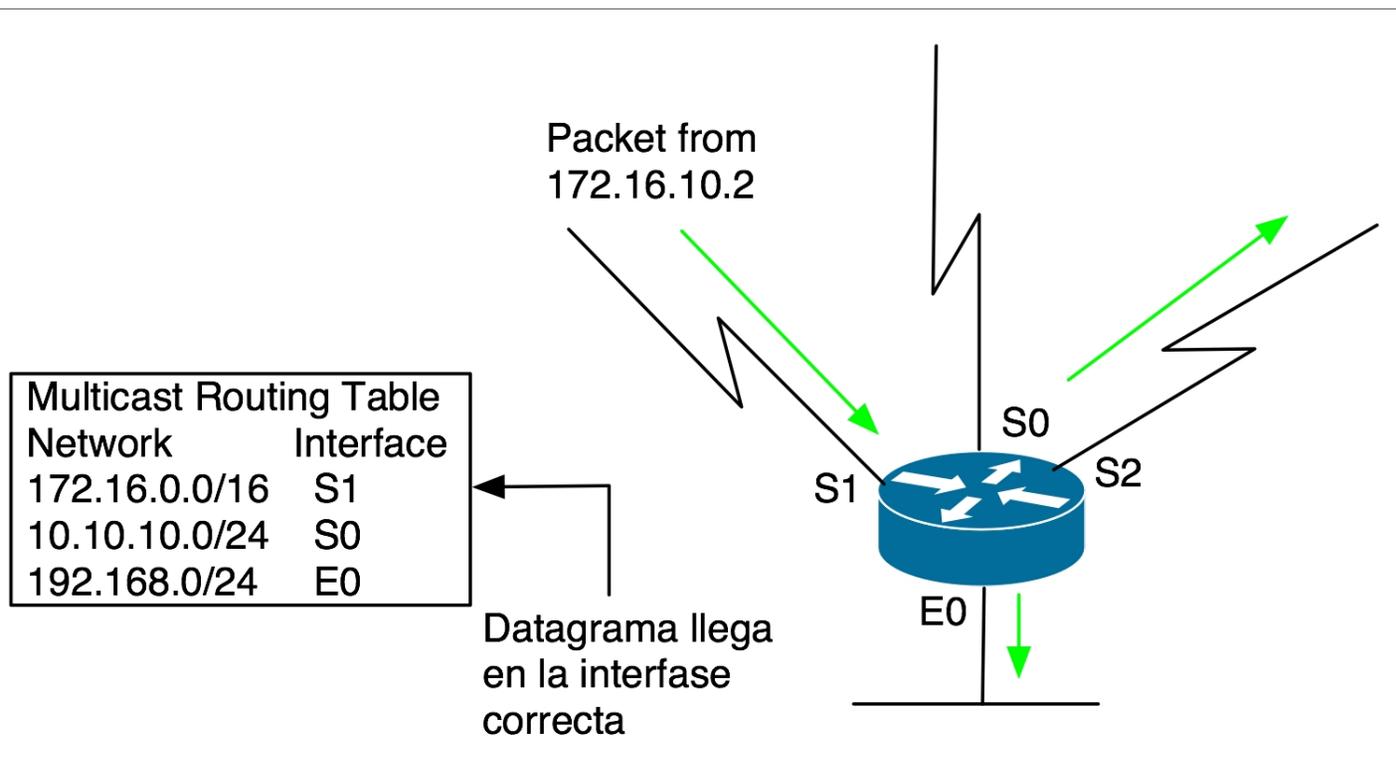
RPF

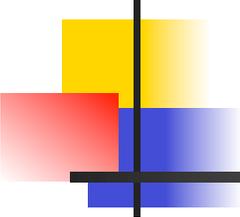
- Fallo en la verificación de RPF



RPF

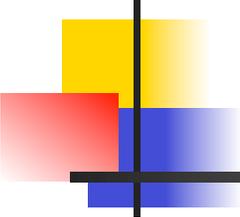
■ Verificación Satisfactoria de RPF





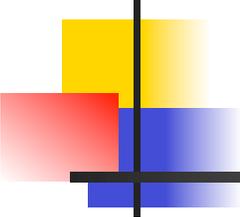
Asignación de Direcciones de Multicast

- IANA asigna las direcciones de multicast
 - Si las direcciones van a ser utilizadas por un protocolo o aplicación.
 - 224.0.0.0/24: bloque de control de la red
 - 224.0.1.0/24: bloque de control entre redes
 - Asignaciones a Instituciones ad-hoc
 - 224.0.2.0 - 224.0.255.255



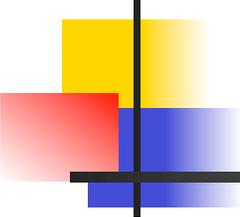
Asignación de Direcciones de Multicast

- Asignación Dinámica para uso en el Protocolo de Descripción de Sesiones (SDP) y el Protocolo de Anuncio de Sesiones (SAP)
 - SDR es una de las aplicaciones que implementan estos protocolos
 - 224.2.0.0/16 (224.2.0.0 - 224.2.255.255)



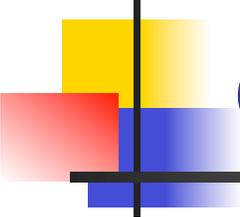
Asignación de Direcciones de Multicast

- Direcciones de Multicast desde Orígenes Específicos (SSM)
 - 232.0.0.0/8 (232.0.0.0 - 232.255.255.255)
 - FF3x::/32 en IPv6
 - FF3x::/96 está disponible hoy día
 - Direcciones son prácticamente ilimitadas puesto que ahora el origen y la dirección del grupo definen el canal
 - Está siendo definido en el IETF
 - RFC3569
 - draft-ietf-ssm-arch-04.txt



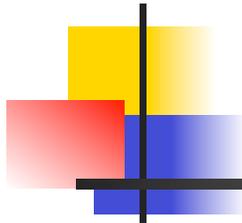
Asignación de Direcciones de Multicast

- GLOP
 - BCP definido en RFC3180
 - 233.0.0.0/8 (233.0.0.0 - 233.255.255.255)
 - Los 16 bits del número de sistema autónomo son integrados en el segundo y tercer octeto de la dirección de multicast
 - AS 3582
 - 3582 = x0D FE
 - 233.13.254.0/24
 - Provee 255 direcciones únicas por cada sistema autónomo



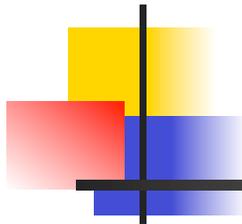
Protocolo de Administración de Grupos de Internet (IGMP)

- Utilizado por las estaciones para indicar a los enrutadores del interés de recibir el tráfico de cierto grupo
- Los enrutadores solicitan reportes de membresía de las estaciones directamente conectadas al segmento
- Tres (3) versiones
 - IGMPv1 (RFC1112)
 - IGMPv2 (RFC2236)
 - IGMPv3 (RFC3376)



IGMP

- **Funciones básicas de las estaciones**
 - Escucha en la dirección de capa-2 que representa la dirección de IP multicast
 - Reporta su interés de asociarse a un grupo enviando un mensaje de reporte de membresía, el cual causa que uno de los enrutadores cree el árbol de propagación
 - Los mensajes de reportes son enviados a:
 - la dirección de multicast del grupo (IGMPv1, IGMPv2)
 - la dirección 224.0.0.22 (IGMPv3)
 - Para evitar inundar la red con tráfico duplicado, las estaciones esperan un momento aleatorio de tiempo antes de responder a los mensajes del enrutador
 - Si una estación escucha un mensaje de reporte de otra estación entonces suprime el envío de su mensaje
 - Envía mensajes de retiro a todos los enrutadores (224.0.0.2)

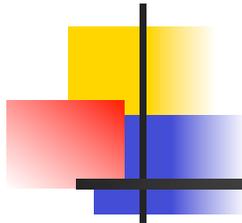


IGMP

- **Funciones básicas de los enrutadores**
 - Si existe más de un enrutador en el segmento, el que tenga la dirección de IP menor es elegido como el encargado de hacer las solicitudes (Querier) para ese segmento
 - Envía mensajes de solicitud de reporte a todas las estaciones en el segmento (224.0.0.1) con TTL=1
 - Los demás enrutadores suprimen el envío de mensajes de solicitud de reporte pero continúan escuchando y actualizando sus tablas
 - Escucha por mensajes de reporte de membresía y mantiene tablas de membresía para cada interfaz

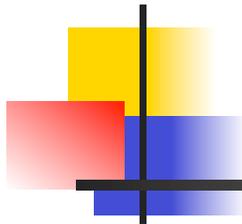
IGMP Connected Group Membership

Group Address	Interface	Uptime	Expires	Last Reporter
224.2.162.67	GigabitEthernet9/2	6d10h	00:02:24	128.223.157.16
224.2.250.29	GigabitEthernet9/2	09:13:13	00:02:24	128.223.157.17
224.2.198.47	GigabitEthernet9/2	12:22:16	00:02:26	128.223.157.109
224.2.245.25	GigabitEthernet9/2	02:28:24	00:02:25	128.223.157.21

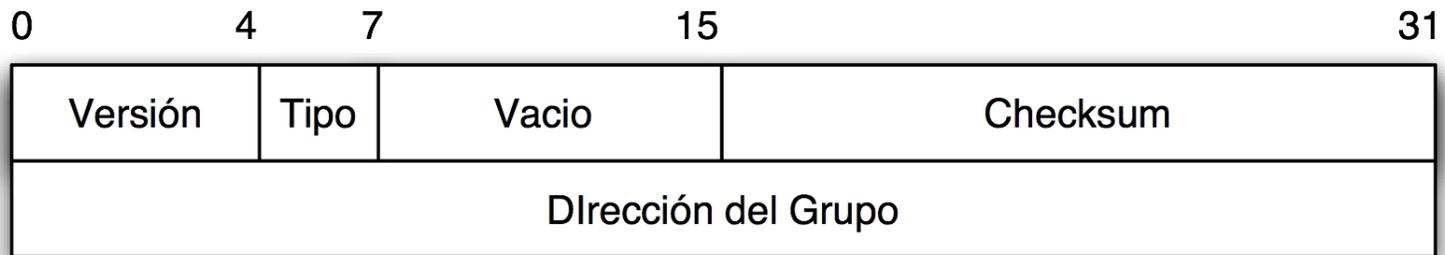


IGMP

- Para cada interfaz mantiene una tabla con:
 - Lista de todos los grupos que tiene estaciones interesadas en el segmento
 - La dirección de IP de la última estación que expresó interés en recibir el grupo
 - Tiempo de expiración para cada entrada en la tabla (GMI)
- $GMI = (\text{variable de robustez} \times \text{intervalo de solicitud}) + \text{intervalo de respuesta a las solicitudes}$
 - **Variable de Robustez:** define el número de solicitudes que se pueden enviar sin recibir una respuesta antes de que la entrada expire (valor por defecto es 2). Incrementado este valor ayuda cuando hay errores
 - **Intervalo de Solicitud:** es intervalo entre el envío de solicitudes por el enrutador encargado de hacer las solicitudes (valor por defecto es 125s)
 - **Intervalo de Respuesta:** es la cantidad de tiempo que las estaciones tienen para responder a las solicitudes (valor por defecto es 10s). El valor es parte del mensaje de IGMP y es utilizado por las estaciones para calcular cuándo responder

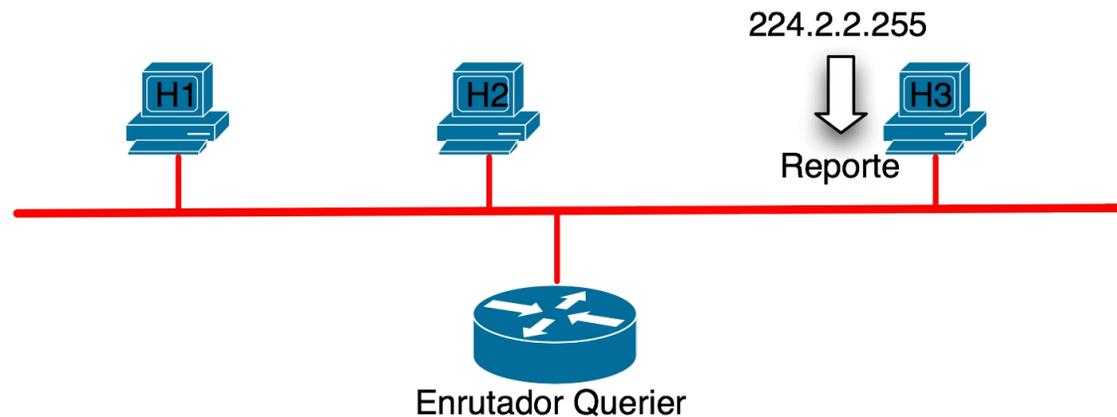


IGMPv1



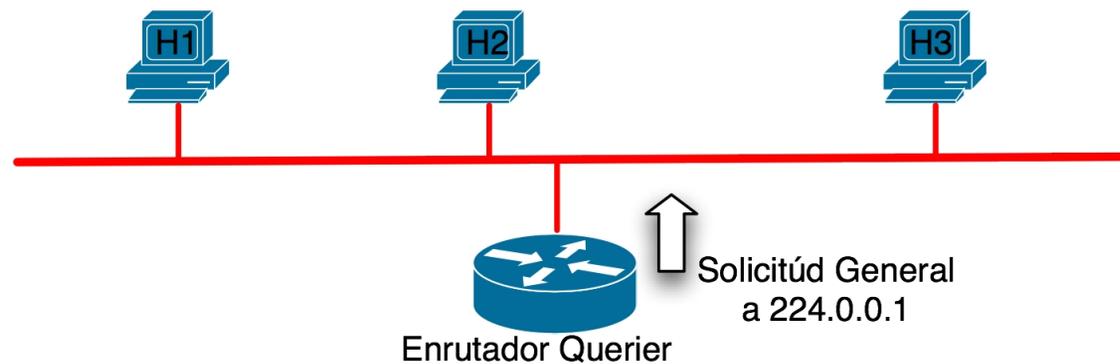
- Versión: 0x1
- Tipo
 - 0x1 = Solicitud de Membresía
 - 0x2 = Reporte de Membresía
- Dirección de Multicast al que se refiere el mensaje

IGMPv1: Reporte de Membresía



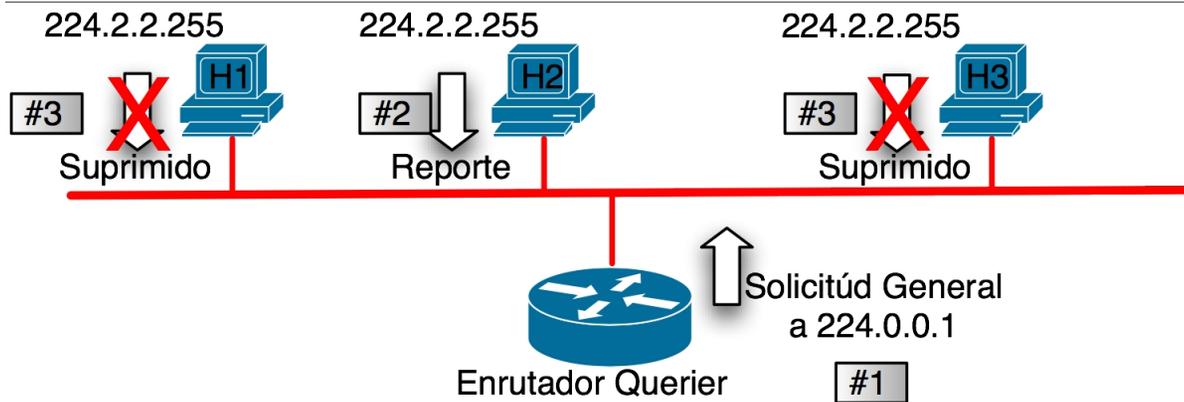
- La estación envía un reporte de membresía para indicar su interés de recibir datagramas para un grupo de multicast
- El mensaje es enviado la dirección de multicast del grupo (224.2.2.255)

IGMPv1: Solicitud de Membresía



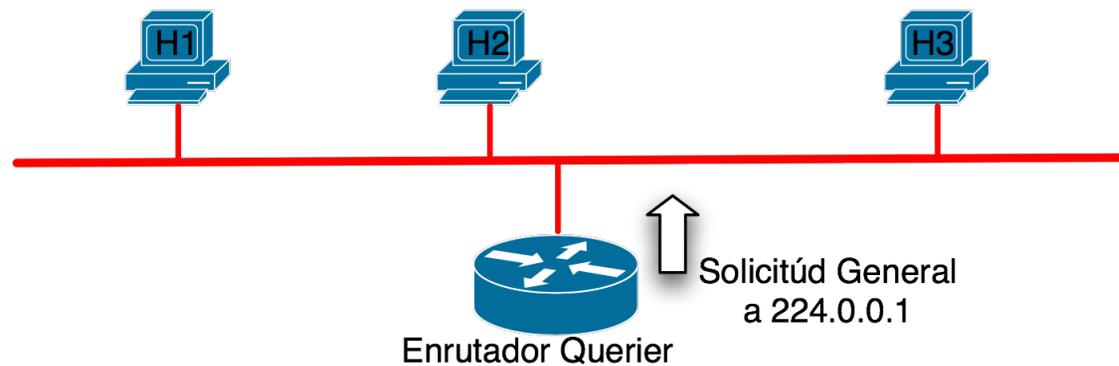
- Periódicamente el enrutador envía mensajes de solicitud de membresía (por defecto cada 60s)
- Los mensajes son enviados a la dirección 224.0.0.1
- En IGMPv1 no existe un proceso para la elección del enrutador encargado de enviar las solicitudes, lo cual podría causar repeticiones

IGMPv1: Respuesta a Solicitud

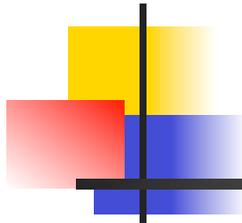


- #1: Enrutador envía solicitudes periódicamente
- #2: Un miembro del grupo responde por segmento
- #3: Los demás miembros suprimen sus reportes

IGMPv1: Retiro

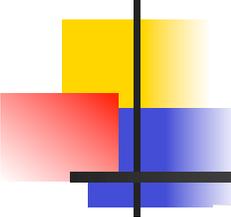


- Las estaciones no tienen que reportar que no quieren recibir un grupo
- El enrutador deja de enviar mensajes si no ha escuchado una respuesta a sus mensajes de solicitud y el temporizador ha expirado

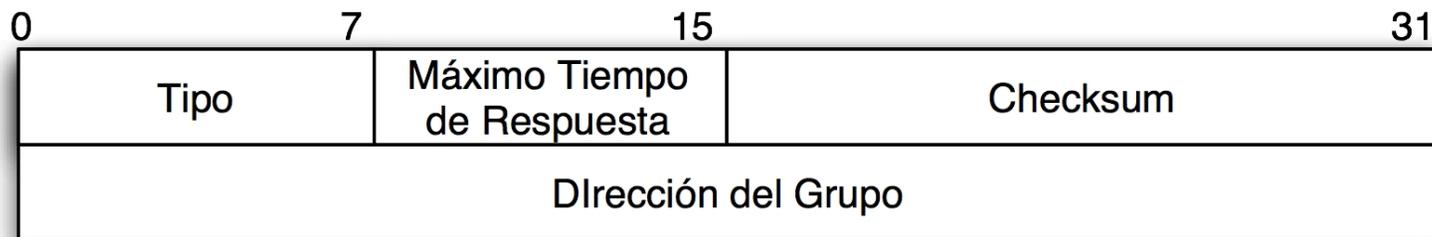


IGMPv1

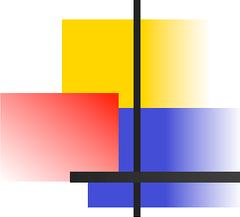
- No es suficiente para lo que se quiere hacer
- Se inician los trabajos de definición de IGMPv2



IGMPv2



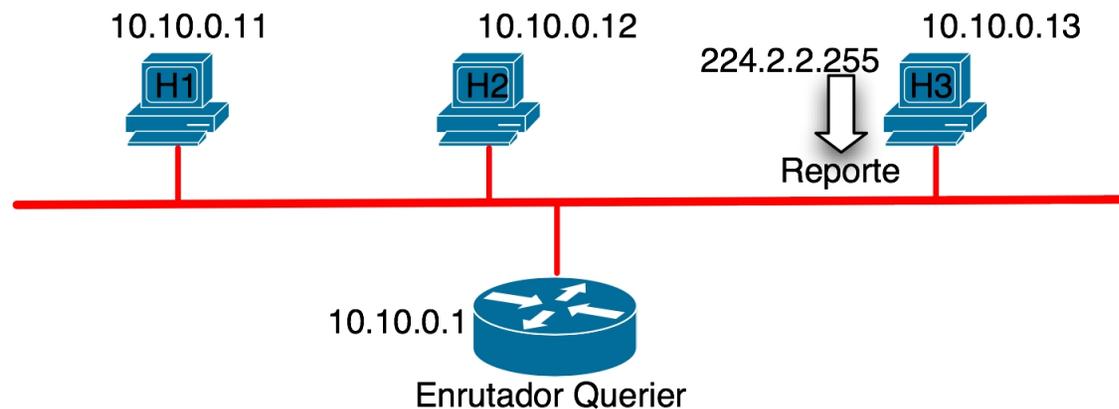
- Tipo
 - 0x11 = Solicitud de Membresía
 - 0x12 = Reporte de Membresía (IGMPv1)
 - 0x16 = Reporte de Membresía (IGMPv2)
 - 0x17 = Retiro de Grupo
- Máximo tiempo de respuesta en $1/10^{\text{mo}}$ de segundos
- Dirección del Grupo
 - 0.0.0.0 para solicitudes generales



IGMPv2 Vs IGMPv1

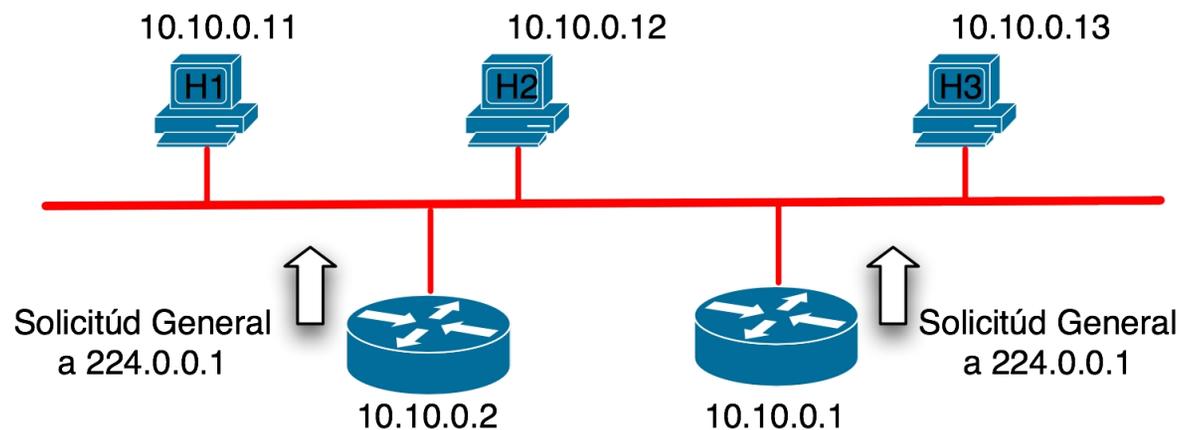
- Mecanismo para la selección del enrutador encargado de hacer las solicitudes (querier)
 - EL enrutador con la menor dirección de IP es seleccionado
 - Sólo este router puede enviar solicitudes de membresía
- Se ha agregado un campo especificando el tiempo máximo que los clientes tienen para responder a solicitudes
- Compatible con IGMPv1 debido a la asignación dada a los tipos de mensajes

IGMPv2: Reporte de Membresía

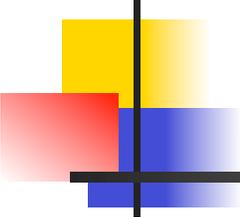


- Igual que en IGMPv1
- La estación envía un reporte de membresía para indicar su interés de recibir datagramas para un grupo de multicast
- El mensaje es enviado la dirección de multicast del grupo (224.2.2.255)

IGMPv2: Solicitud de Membresía

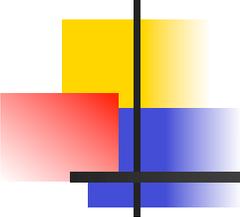


- Inicialmente todos los enrutadores envían mensajes de solicitud de membresía
- Si un enrutador escucha un mensaje de un enrutador con una IP menor entonces deja de enviar mensajes
- Los enrutadores pueden enviar solicitudes de membresía para grupos específicos
 - Mensaje enviado a la dirección del grupo en lugar de a 224.0.0.1



IGMPv2: Elección de Enrutador Mensajero (Querier)

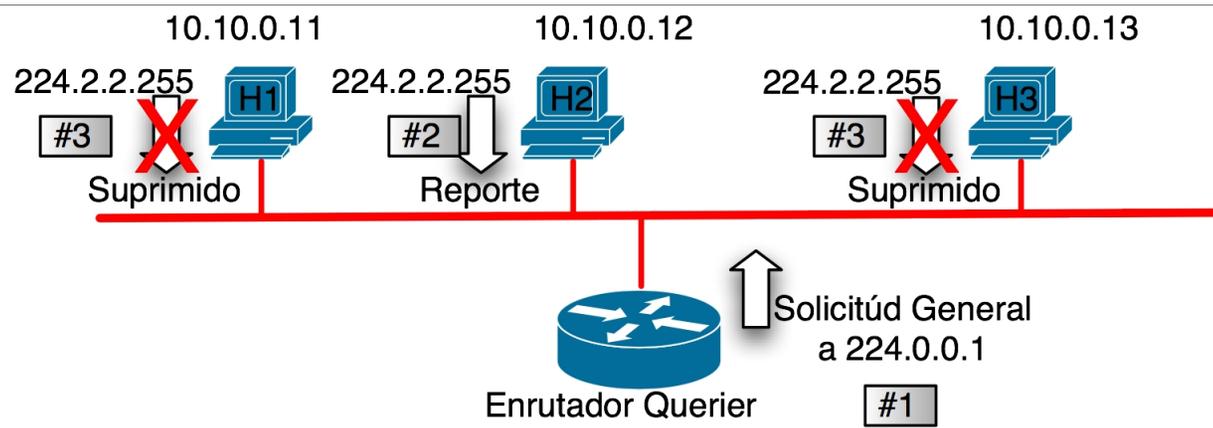
```
uonet2-gw#sh ip igmp int gig 5/1
GigabitEthernet5/1 is up, line protocol is up
Internet address is 128.223.2.2/24
IGMP is enabled on interface
Current IGMP host version is 2
Current IGMP router version is 2
IGMP query interval is 60 seconds
IGMP querier timeout is 120 seconds
IGMP max query response time is 10 seconds
Last member query count is 2
Last member query response interval is 1000 ms
Inbound IGMP access group is not set
IGMP activity: 3 joins, 0 leaves
Multicast routing is enabled on interface
Multicast TTL threshold is 0
Multicast designated router (DR) is 128.223.2.9
IGMP querying router is 128.223.2.1
Multicast groups joined by this system (number of users):
  224.2.127.254(1) 239.255.255.255(1)
```



IGMPv2: Elección de Enrutador Mensajero (Querier)

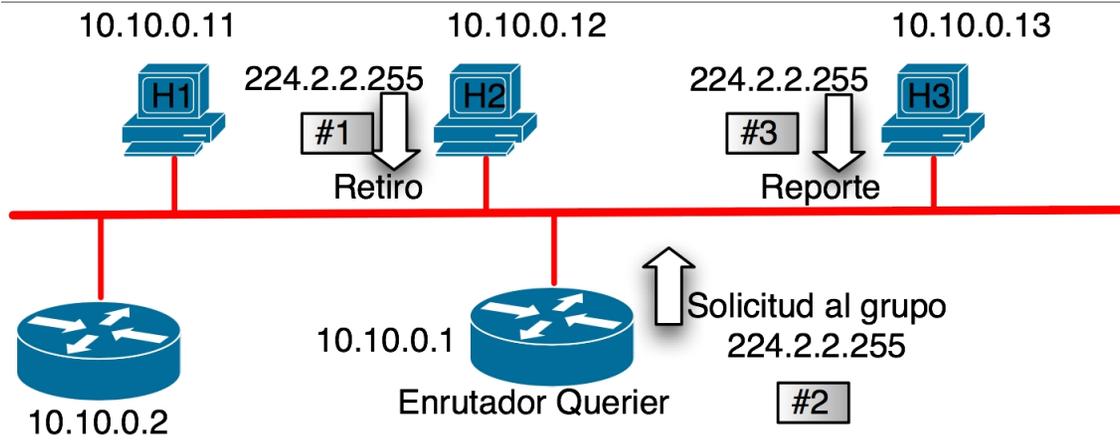
```
uonet1-gw#sh ip igmp int gig 5/1
GigabitEthernet5/1 is up, line protocol is up
Internet address is 128.223.2.1/24
IGMP is enabled on interface
Current IGMP host version is 2
Current IGMP router version is 2
IGMP query interval is 60 seconds
IGMP querier timeout is 120 seconds
IGMP max query response time is 10 seconds
Last member query count is 2
Last member query response interval is 1000 ms
Inbound IGMP access group is not set
IGMP activity: 8 joins, 5 leaves
Multicast routing is enabled on interface
Multicast TTL threshold is 0
Multicast designated router (DR) is 128.223.2.9
IGMP querying router is 128.223.2.1 (this system)
URL Rendezvousing is on.
No multicast groups joined by this system
```

IGMPv2: Respuesta a Solicitud



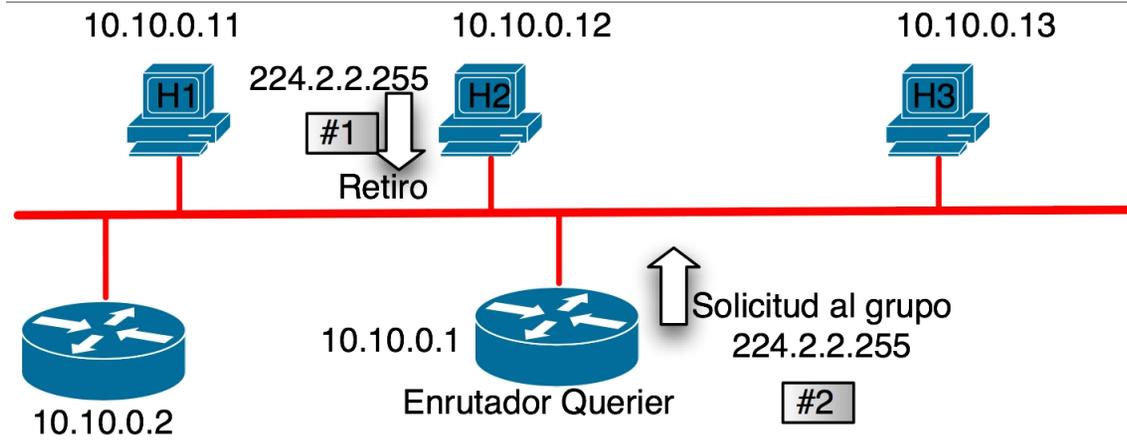
- Similar al proceso en IGMPv1
- #1: Enrutador envía solicitudes periódicamente
- #2: Un miembro del grupo responde por segmento
- #3: Los demás miembros suprimen sus reportes

IGMPv2: Retiro

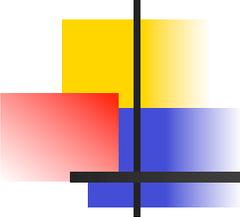


- #1: H2 envía un mensaje de retiro
- #2: El enrutador envía una solicitud de membresía para un grupo específico
- #3: H3 responde a la solicitud
- El grupo se mantiene activo

IGMPv2: Retiro



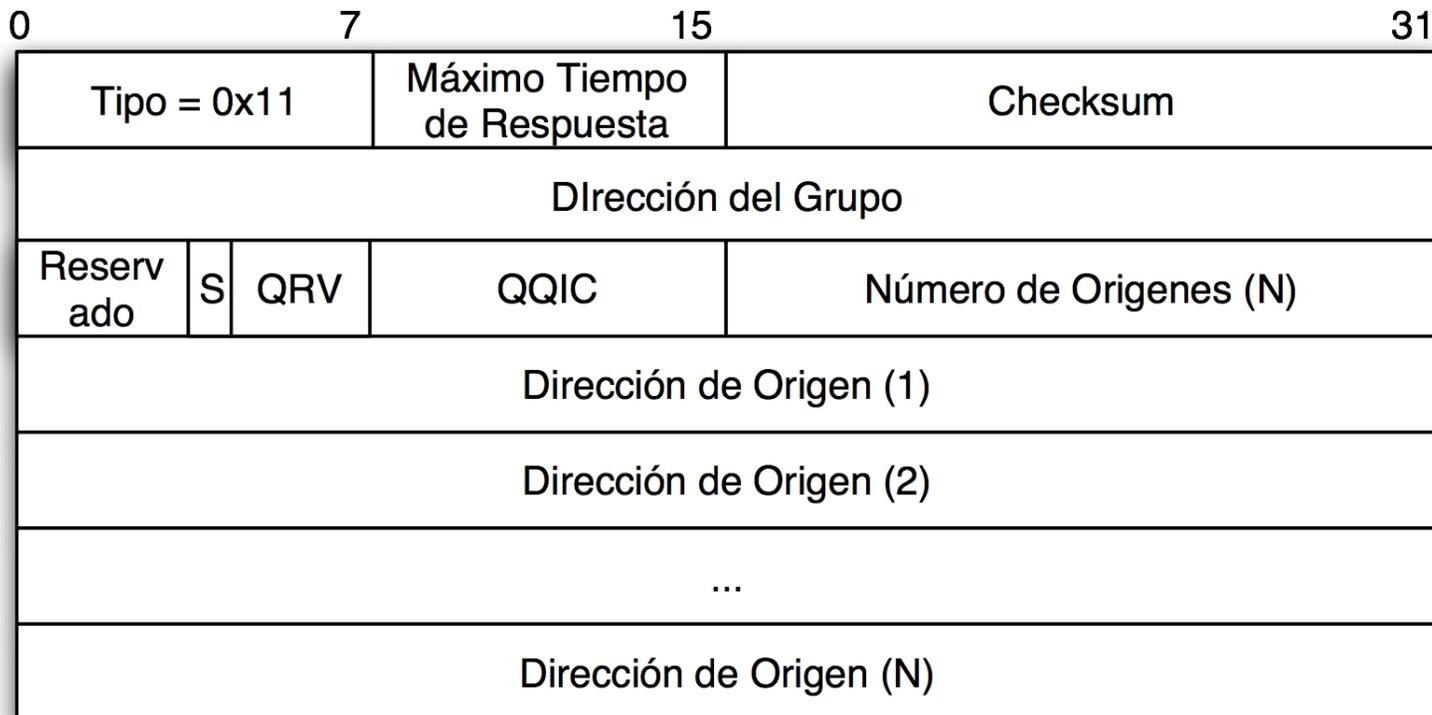
- #1: H2 envía un mensaje de retiro
- #2: El enrutador envía una solicitud de membresía para un grupo específico
- Como nadie responde el enrutador dejará de enviar datagramas para el grupo

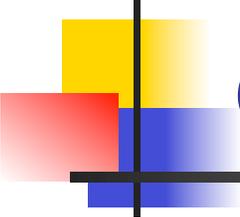


IGMPv3

- Se comenzó a definir antes de que IGMPv2 se convirtiera en estándar
- Los mensajes de reportes son enviados a la dirección de multicast 224.0.0.22 y todos los enrutadores que soportan IGMPv3 deben escuchar por estos mensajes
- Los mensajes de solicitud se siguen enviando a:
 - 224.0.0.1 para las solicitudes generales
 - Dirección del grupo de IP multicast para solicitudes de grupos u origen/grupo específicos
- Ideal para aplicaciones de SSM

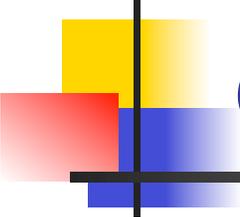
IGMPv3: Formato de Mensaje de Solicitud de Membresía





IGMPv3: Mensaje de Solicitud de Membresía

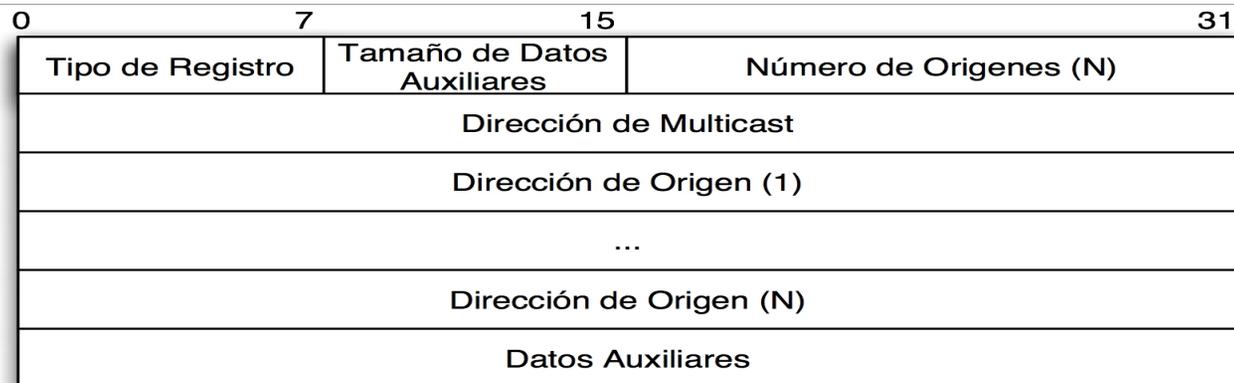
- Tipo es 0x11
- S es un indicador de que el enrutador ha dejado de procesar este grupo
- QRV es el valor de robustez del enrutador que envía solicitudes (querier)
- QQIC es el valor del intervalo de solicitudes del enrutador que envía solicitudes (querier)

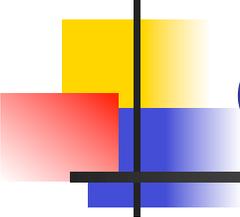


IGMPv3: Mensaje de Solicitud de Membresía

- Los mensajes se pueden enviar para
 - Solicitudes Generales
 - Solicitudes de un grupo específico
 - Solicitudes de un origen/grupo específico

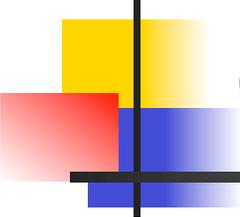
IGMPv3: Formato de Mensaje de Reporte de Membresía





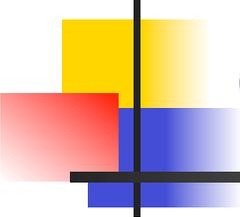
IGMPv3: Formato de Mensaje de Reporte de Membresía

- Tipo de registro
 - 0x1 = indica que el modo es inclusivo
 - La lista de orígenes representa los que se quieren recibir
 - 0x2 = indica que el modo es exclusivo
 - La lista de orígenes representa la lista de los que se quieren excluir
 - 0x3 = indica un cambio a inclusivo
 - Cambio de exclusivo a inclusivo para los orígenes listados
 - 0x4 = indica un cambio a exclusivo
 - Cambio de inclusivo a exclusivo para los orígenes listados
 - 0x5 = indica adición de nuevos orígenes
 - Si la lista original era inclusiva agrega los orígenes
 - Si la lista original era exclusiva excluye los orígenes
 - 0x6 = indica exclusión de orígenes previamente definidos
 - Si la lista original era inclusive se remueven los orígenes
 - Si la lista original era exclusive se agregan los orígenes



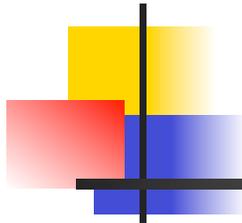
Consideraciones de la Capa-2

- Cambios en la topología podrían ser necesarios
 - Localizar los servidores de multicast cerca de los enrutadores para evitar el envío de paquetes innecesarios a través de los switches
- IGMP Snooping
 - Es un requisito para instalaciones con mucho tráfico de multicast
 - Los switches instalan entradas en su CAM para los grupos de multicast y envían datagramas solo a los puertos que han reportado suscripción a un grupo



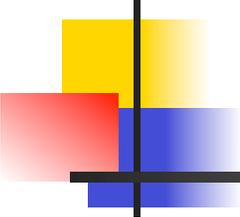
Consideraciones de la Capa-2

- PIM Snooping
 - Ideal para instalaciones en puntos de intercambio o en backbones donde no existen estaciones que envíen mensajes de reporte de membresía
- Inundación de 224.0.0.x
 - Hay que verificar que los switches entienden que deben inundar los puertos con datagramas para este rango para evitar la interrupción de tráfico necesario por otros protocolos
- Tener en cuenta la duplicación de direcciones
 - Seleccionar las direcciones de multicast tratando de evitar duplicados de direcciones de capa-2
 - Evitar el uso de direcciones en el rango x.0.0.x y x.128.0.x (ver mas arriba)



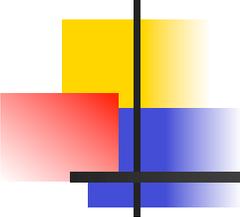
Paradigmas

- Multicast desde Cualquier Origen (ASM)
 - Orientado a comunicaciones de muchos a muchos
- Multicast desde Orígenes Específicos (SSM)
 - Orientado a comunicaciones de uno a muchos



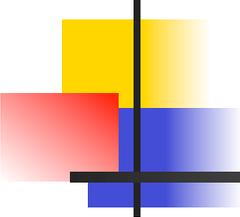
Protocolos de Enrutamiento para Multicast: PIM

- Nos vamos a concentrar en PIM que se ha convertido en el estándar por defecto
- Existen dos versiones
 - PIM-DM: Modo denso
 - PIM-SM: Modo escaso



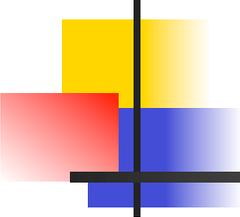
PIM-DM

- Este modelo asume que todas las estaciones quieren recibir todos los grupos de multicast
- La última especificación definida en draft-ietf-pim-dm-new-v2-04.txt que expira en Marzo, 2004
- Los enrutadores inundan todas las interfaces con tráfico de multicast si:
 - Existe otro enrutador corriendo PIM-DM
 - Existe una estación suscrita al grupo
 - La interfaz ha sido configurada manualmente para recibir el grupo
- Ramas sin miembros envían mensajes de recorte
 - Luego de 3 minutos el enrutador vuelve e inunda la interfaz y el proceso se repite



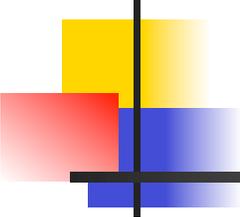
PIM-DM

- El plano de control y el plano de datos es el mismo
 - Estado (S,G) y el árbol de camino más corto (SPT) son creados en el momento que arriban los datos
 - El estado y arbol son removidos si no se reciben datagramas por 3 minutos
 - No existe un árbol compartido
- Recomendado cuando se tiene mucho ancho de banda en todos los enlaces debido al uso excesivo de tráfico innecesario
 - O en situaciones donde todo el mundo debe recibir datagramas para un grupo



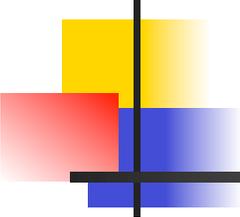
PIM - Reglas Generales

- 1) Siempre que se crea estado (S,G) se crea estado (*,G) si éste no existe
- 2) Interfaz RPF es calculada como la interfaz con el menor costo hacia el origen. Si varias interfaces tienen el mismo costo, se selecciona la interfaz con la dirección de IP mas alta
- 3) Cuando el estado (S,G) es creado, la lista de interfaces de salida es creada con la lista en el estado (*,G)
- 4) La interfaz de entrada (RPF) nunca debe aparecer en la lista de interfaces de salida



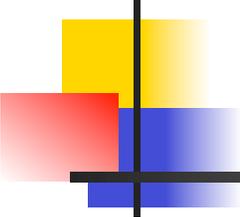
PIM - Reglas Generales

- 5) La interfaz de entrada (RPF) para cada entrada en la tabla de estado es recalculada cada 5 minutos y la tabla de salida es ajustada apropiadamente basado en la regla #4
- 6) Las adiciones y remociones a la lista de interfaces de salida de (*,G) duplicadas para todas las entradas (S,G) para el grupo



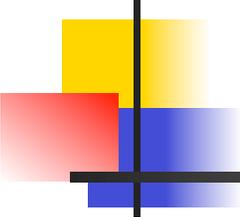
PIM-DM - Reglas

- 1) La lista de interfaces de salida para estado (*,G) contiene interfaces con vecinos PIM-DM o con clientes
- 2) Las interfaces de salida de una entrada (S,G) en PIM-SM no son removidas como resultado de los recortes. En su lugar estas son marcadas como recortadas y se mantienen en la lista de interfaces de salida



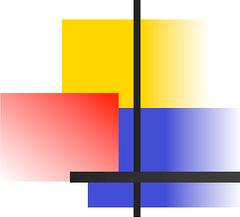
PIM-SM

- El enfoque de la presentación es utilizar PIM-SM como el protocolo para la creación de las tablas de enrutamiento para multicast
- La última especificación esta definida en draft-ietf-pim-sm-v2-new-09.txt que una vez aprobada reemplazará el RFC2362
- Define un punto de encuentro a donde todos los intentos de unión a un grupo de multicast deben ser enviados
- Usa uniones explicitas puesto que asume que nadie quiere recibir los datagramas
- Los datagramas de multicast y los mensajes de unión son enviados al punto de encuentro (RP) para el encuentro inicial
- Todos los enrutados en el dominio PIM deben tener una definición del RP que sirve el dominio
 - Pudiese usar AnycastRP - draft-ietf-pim-anycast-rp-00.txt



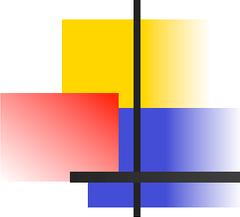
PIM-SM

- Cuando la carga excede el límite, el árbol de distribución cambia a SPT (por defecto es 1 datagrama)
- La cantidad de datos en la tabla de estados se incrementa proporcionalmente al número de orígenes y grupos
- El estado del árbol de distribución es actualizado cuando los datagramas son enviados y con mensajes de control de unión (join) o recorte (prune)



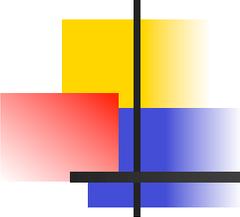
PIM - Reglas Generales

- 1) Siempre que se crea estado (S,G) se crea estado (*,G) si este no existe
- 2) interfaz RPF es calculada como la interfaz con el menor costo hacia el origen. Si varias interfaces tienen el mismo costo, se selecciona la interfaz con la dirección de IP mas alta
- 3) Cuando estado (S,G) es creado, la lista de interfaces de salida es creada con la lista en el estado (*,G)
- 4) La interfaz de entrada (RPF) nunca debe aparecer en la lista de interfaces de salida



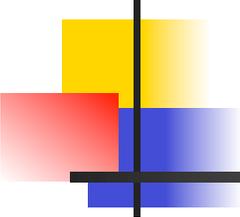
PIM - Reglas Generales

- 5) La interfaz de entrada (RPF) para cada entrada en la tabla de estado es recalculada cada 5 minutos y la tabla de salida es ajustada apropiadamente basado en la regla #4
- 6) Las adiciones y remociones a la lista de interfaces de salida de (*,G) duplicadas para todas las entradas (S,G) para el grupo



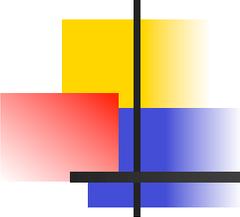
PIM-SM - Reglas

- 1) Una entrada (*,G) es creada como resultado de una operación explícita de unión (join)
- 2) La lista de interfaces de entrada para una entrada (*,G) siempre apunta hacia el árbol de distribución compartido hacia el RP
- 3) Una entrada (S,G) es creada si se da una de las siguientes condiciones
 - Recepción de un mensaje de unión/recorte
 - Cuando el enrutador final (last-hop) cambia al árbol SPT
 - Cuando se recibe tráfico (S,G) y no existe una entrada (*,G)
 - En el RP cuando un mensaje de registro (register) es recibido



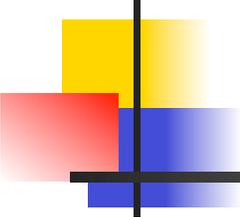
PIM-SM - Reglas

- 4) Una interfaz es agregada a la lista de interfaces de salida de una entrada $(*,G)$ o (S,G) cuando se cumple una de las siguientes condiciones
 - Un mensaje de unión para el $(*,G)$ o (S,G) es recibido
 - Existe una estación directamente conectada que quiere recibir el grupo (usando IGMP)
- 5) Una interfaz es removida de la lista de interfaces de salida para una entrada $(*,G)$ o (S,G) cuando
 - Un mensaje de recorte para la entrada $(*,G)$ o (S,G) apropiada es recibido vía la interfaz ya definida (y no existen estaciones directamente conectadas a la interfaz interesadas en recibir el grupo)
 - El temporizador de expiración de la interfaz ha llegado a cero



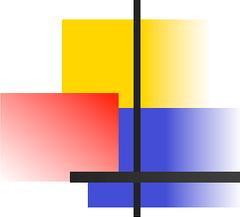
PIM-SM - Reglas

- 6) El temporizador de una interfaz es reinicializado a 3 minutos como resultado de una de las siguientes condiciones:
 - Un mensaje de unión (join) para la entrada (*,G) o (S,G) es recibido vía esta interfaz
 - Un mensaje IGMP de reporte membresía de una estación directamente conectada es recibido
- 7) Enrutadores enviarán un mensaje de retiro (prune) para una entrada (S,G), con el bit de RP inicializado, por el árbol de distribución compartido, cuando el vecino de RPF para la entrada (S,G) es diferente del vecino RPF para la entrada (S,G)
 - Esto pasa cuando un enrutador ha logrado establecer un árbol SPT
- 8) La interfaz de entrada (RPF) para una entrada (S,G) es calculada usando la dirección del origen, excepto cuando el bit de RP está inicializado, en cuyo caso se utiliza la dirección de IP del RP



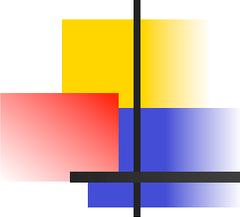
PIM-SM - Operación

- Elección del enrutador designado (DR)
 - Todos los enrutadores envían mensajes de hello periódicamente
 - Cuando se reciben los mensajes de hello, el enrutador mantiene una lista con la dirección de IP del vecino y su prioridad para convertirse en DR
 - El enrutador con la mayor prioridad es elegido
 - Si las prioridades son iguales entonces el enrutador dirección de IP más alta es elegido
 - Cuando el DR tiene problemas, un nuevo enrutador deberá ser seleccionado como el DR
 - El enrutador DR está encargado de enviar
 - Mensajes de unión/recorte (join/prune) hacia el RP de la red de destino
 - Mensajes de registro (register) hacia el RP desde la red de origen



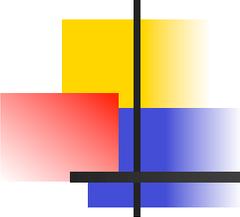
Indicadores usados en PIM

- **S**: indica que el grupo es de PIM-SM (solo aparece en (*,G))
- **C**: indica que hay miembros del grupo directamente conectados a este enrutador - aparece en ambos (*,G) y (S,G)
- **L**: indica que el enrutador es miembro del grupo - aparece en ambos (*,G) y (S,G)
- **P**: indica que la lista de interfaces de salida está vacía y se deben enviar mensajes de retiro para (*,G) o (S,G)
- **T**: indica que el tráfico está siendo recibido a través del SPT - aparece solo en (S,G)
- **X**: indica que el temporizador para el proxy-timer está corriendo - solo aparece en (S,G)
- **J**: para (*,G), este indicador es inicializado cuando la tasa de recepción de tráfico ha sobrepasado el límite preestablecido
- **J**: para (S,G), indica que este origen fue removido del SPT y le indica a PIM que debe chequear el volumen de tráfico a través del SPT y compararlo con el límite para ver si se debe unir al RPT
- **F**: indica que se deben enviar mensajes de registro para el tráfico de (S,G)
- **R**: denominado RP-bit, indica que la información en la entrada (S,G) aplica al RPT. Entradas con este indicador inicializado son utilizadas para recortar el tráfico a través del RPT porque se ha creado el SPT



PIM-SM - RP

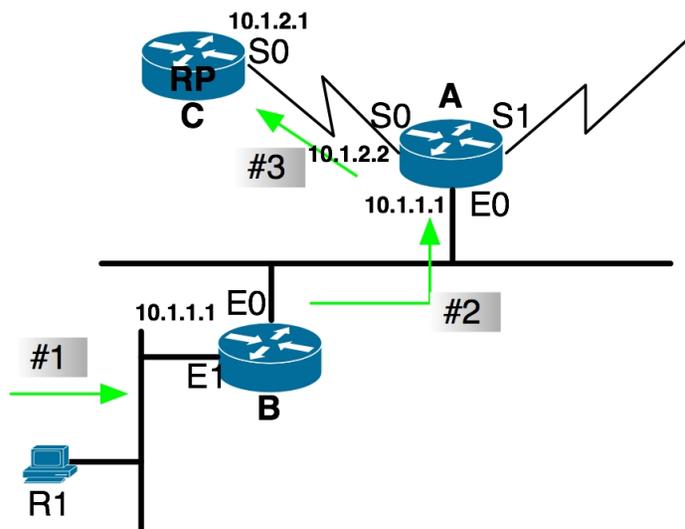
- El punto de encuentro (RP)
 - Sirve para conectar orígenes y receptores
 - Provee descubrimiento de orígenes
 - Es la raíz del árbol de distribución compartido (RPT)
- Típicamente usa un RPT y luego cambia a un SPT
- Las direcciones del RP puede ser aprendidas a través de
 - Configuración estática (Recomendado)
 - Auto-RP (Cisco)
 - Enrutador de Inicialización de PIMv2 (Bootstrap router)



PIM-SM - RP

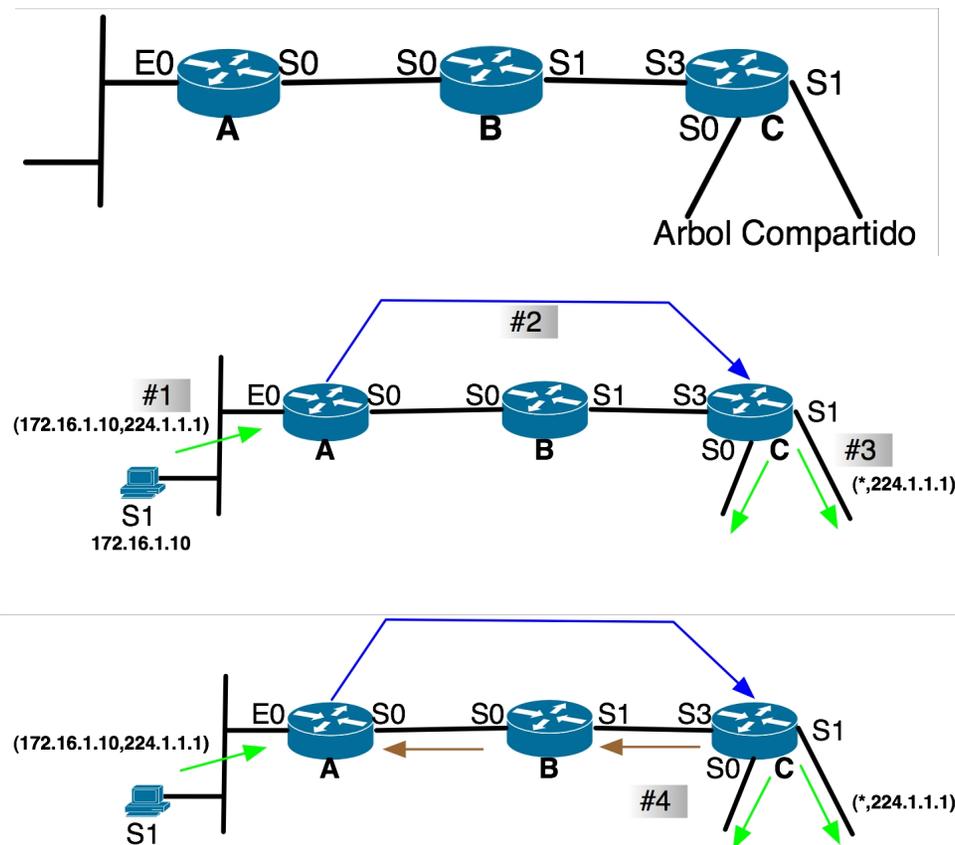
- Donde colocar el RP dependerá de muchas cosas, entre ellas
 - La localización de los receptores del grupo
 - La cantidad de tráfico que pasará por el RP
 - La localización de los creadores de tráfico para el grupo
 - La necesidad de reducir tiempo de respuesta (latency) en la red
 - Requerimientos de redundancia y recuperación de fallos del RP
- Para la mayoría de las redes el RP puede ser el enrutador en el borde
 - Para grandes ISP este podría estar localizado en el centro de la red o el área de más tráfico de multicast
 - Una solución para redes grandes es utilizar Anycast-RP

Proceso de Unión (PIM Join)



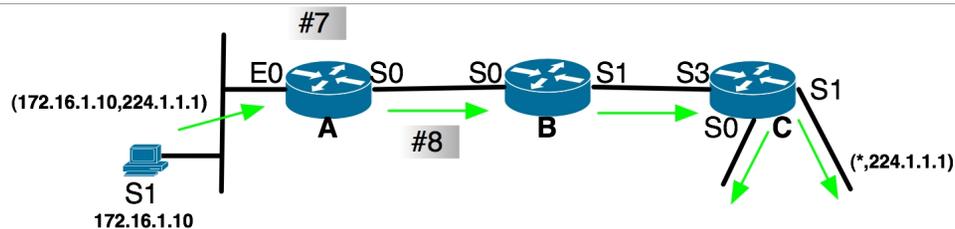
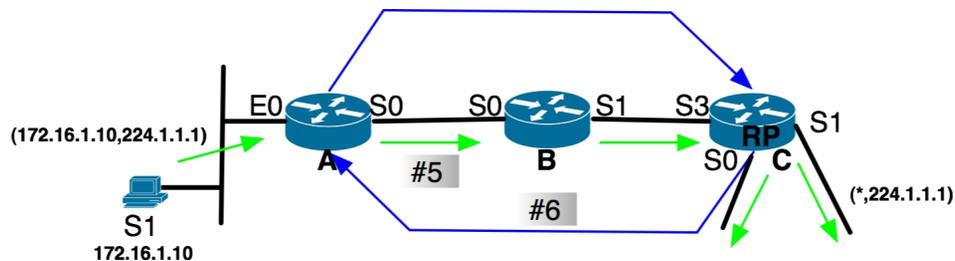
- #1: R1 envía un mensaje IGMP de reporte de membresía indicando que quiere recibir 224.1.1.1 (IGMP Join)
- Si el DR (B en este caso) no tiene estado para (*, 224.1.1.1), lo crea (Regla 1)
 - interfaz entrada: E0
 - interfaz salida: E1
- #2: Porque B creó una entrada (*,G), debe enviar un mensaje de unión hacia el vecino RPF (datagrama PIM de multicast con la dirección del vecino en el mensaje y solo el vecino lo procesa)
- Cuando A recibe el mensaje, este crea estado (*, 224.1.1.1) por la misma regla 1
 - interfaz entrada: S0
 - interfaz salida: E0
- #3: Porque A creó una entrada (*,G), debe enviar un mensaje de unión hacia el vecino RPF (C, que también es el RP)
- Cuando C recibe el mensaje, este también crea estado (*, 224.1.1.1) por la regla 1
 - interfaz entrada: Null
 - interfaz salida: S0

Proceso de Registro - PIM Register (Orígenes no Existen)



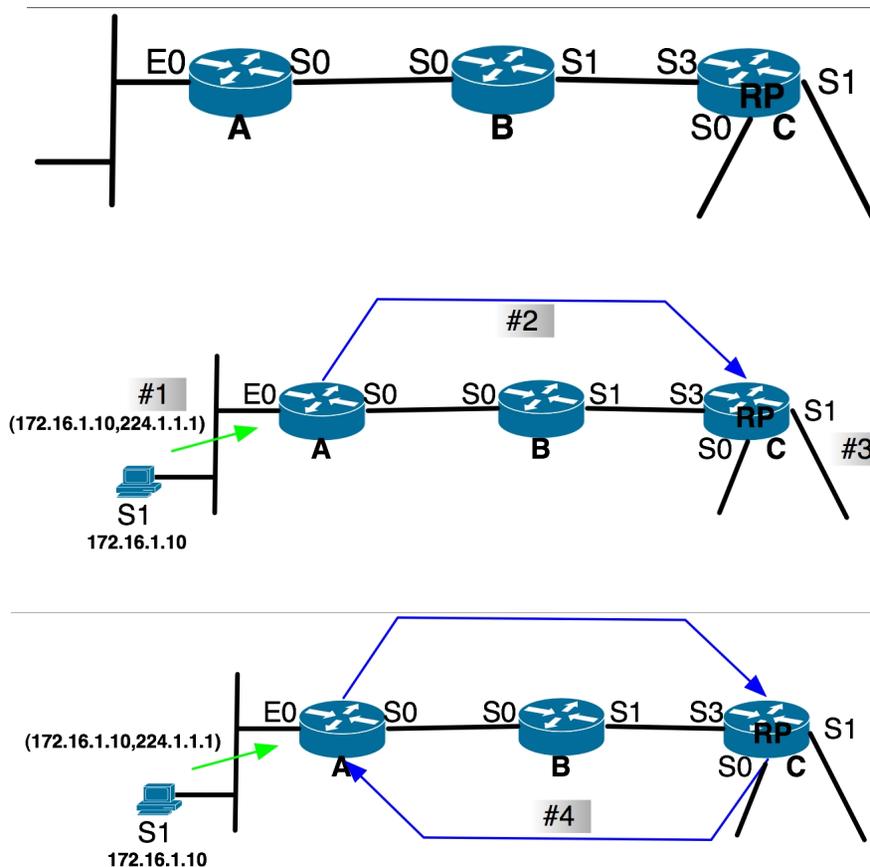
- #1: El origen comienza a enviar datagramas para el grupo 224.1.1.1
- #2: Enrutador A encapsula los datagramas en mensajes de registro (Register Messages) y los envía usando unicast hacia el RP
- #3: El RP de-encapsula los datagramas y los envía por el árbol compartido (RPT)
- #4: El RP envía mensajes de unión (Join) para (S,G) hacia el origen, creando el SPT

Proceso de Registro - PIM Register (Orígenes no Existen)



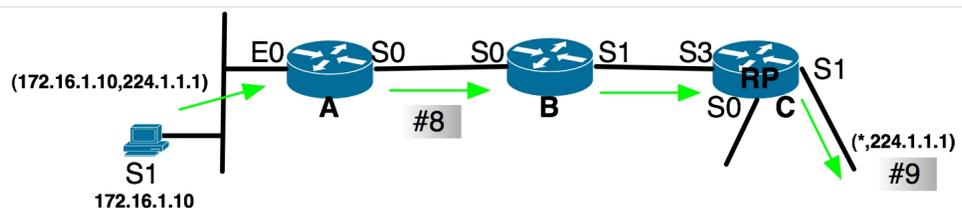
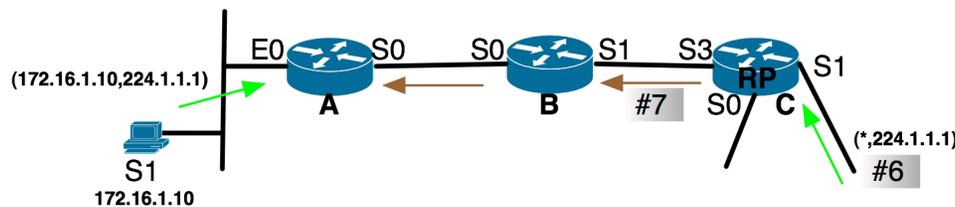
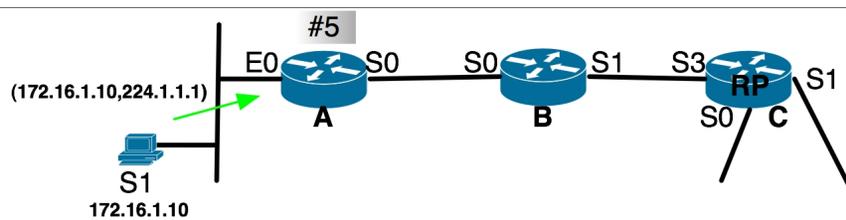
- #5: El RP comienza a recibir datagramas (S,G) a través del SPT
- #6: El RP envía un mensaje de paro de registro (Register Stop) hacia el enrutador A
- #7: El enrutador A deja de encapsular el tráfico en mensajes de registro
- #8: El tráfico (S,G) se mantiene llegando usando solo el SPT hacia el RP

Proceso de Registro - PIM Register (Receptores no Existen)



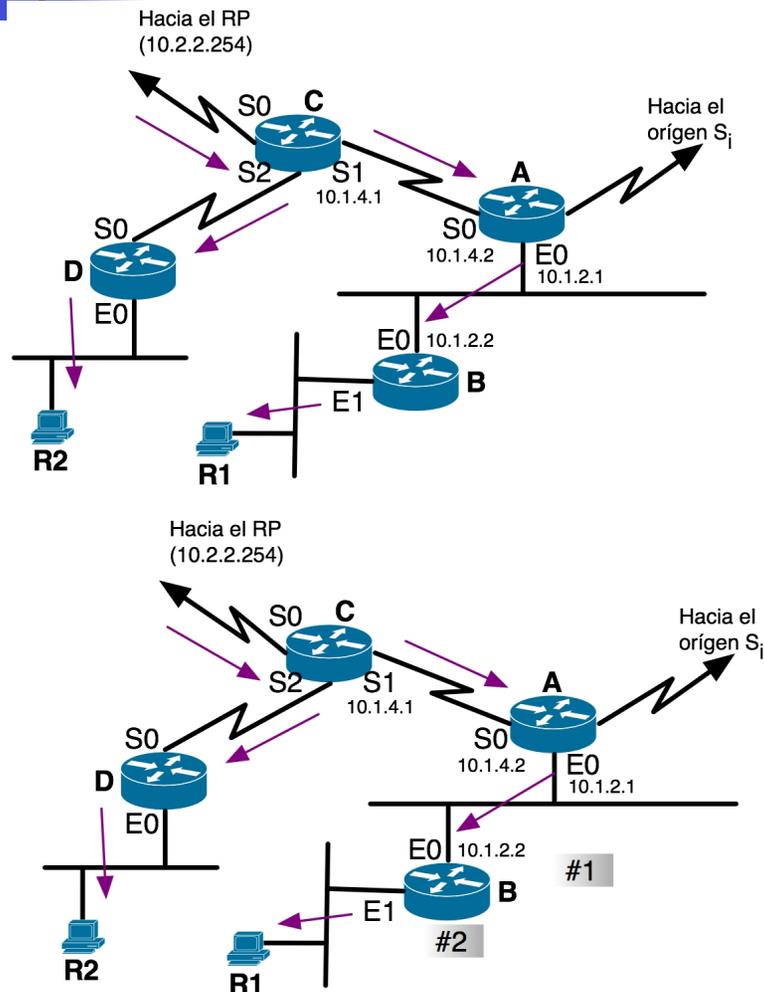
- #1: El origen comienza a enviar tráfico para el grupo 224.1.1.1
- #2: El enrutador A encapsula los datagramas en mensajes de Registro y los envía usando unicast hacia el RP
- #3: El RP no tiene receptores/ clientes en el arbol compartido y descarta los datagramas
- #4: El RP envía un mensaje de paro de registro hacia el enrutador A

Proceso de Registro - PIM Register (Receptores no Existen)



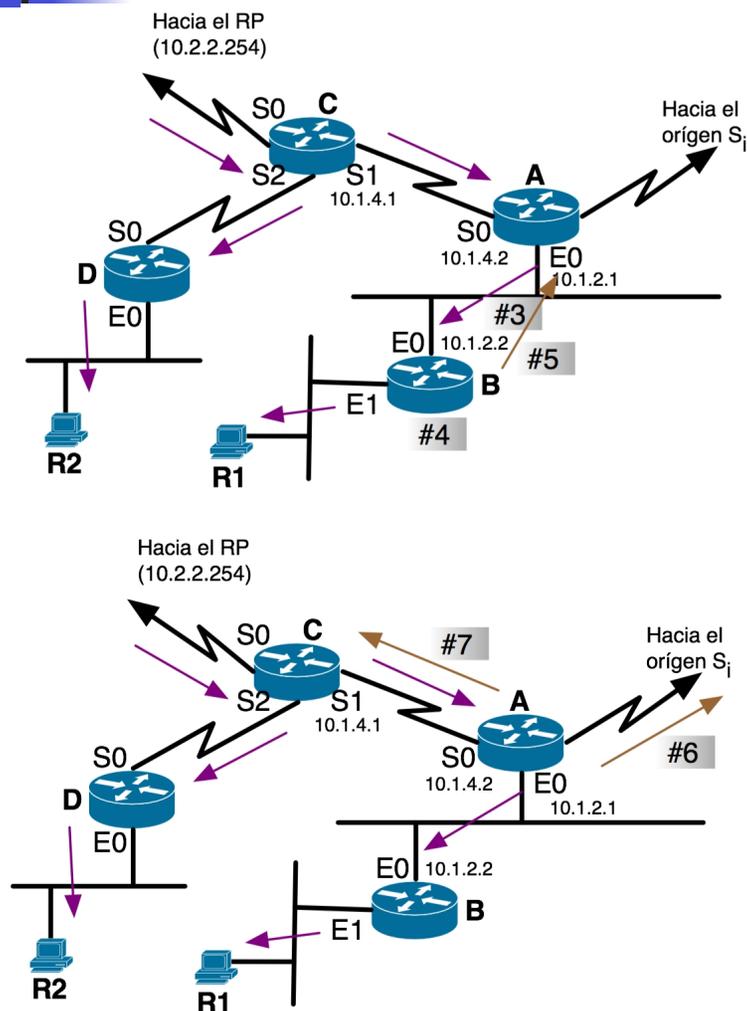
- #5: El enrutador A deja de encapsular los datagramas en mensajes de registro y descarta los subsecuentes paquetes del origen
- #6: El enrutador C recibe un mensaje de unión (*,G) desde un cliente en el RPT
- #7: El RP envía un mensaje de unión (S,G) a todos los orígenes conocidos para el grupo
- #8: El RP comienza a recibir datagramas de (S,G) a través del SPT
- #9: El RP envía el tráfico (S,G) hacia los clientes usando el RPT

Proceso de Cambio Hacia el SPT



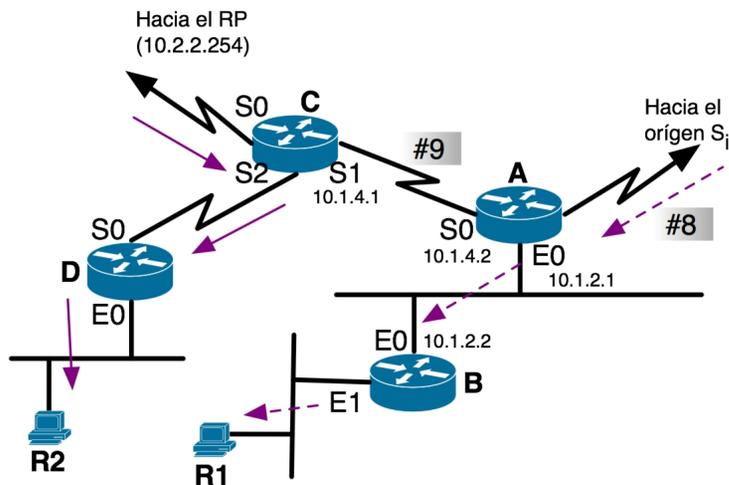
- Tráfico está utilizando el RPT para el envío de los paquetes para (*,G)
- #1: La tasa de arribo de paquetes para el grupo G excede el límite para el enrutador B
- #2: El enrutador B inicializa el indicador J y espera por el próximo datagrama de (S_i,G)

Proceso de Cambio Hacia el SPT



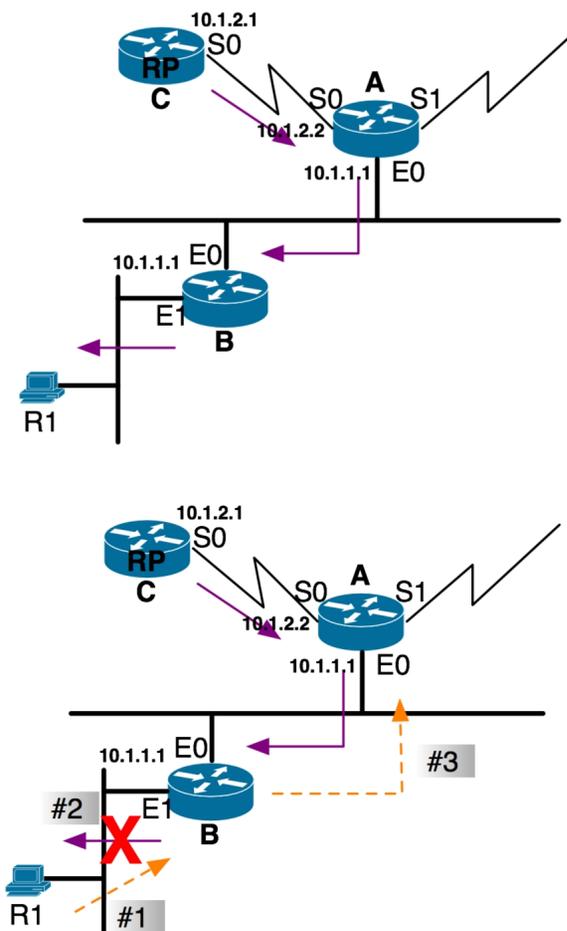
- #3: Un datagrama de (S_i, G) arriba por el RPT
- #4: Remueve el indicador J para $(*, G)$
- #5: Envía (S_i, G) hacia el origen S_i
- #6: La ruta del SPT es diferente de la ruta del RPT; el enrutador A envía un mensaje de unión para (S_i, G) hacia el origen S_i
- #7: El enrutador A inicia un mensaje de retiro para (S_i, G) con el el indicador del bit de RP hacia el RP

Proceso de Cambio Hacia el SPT



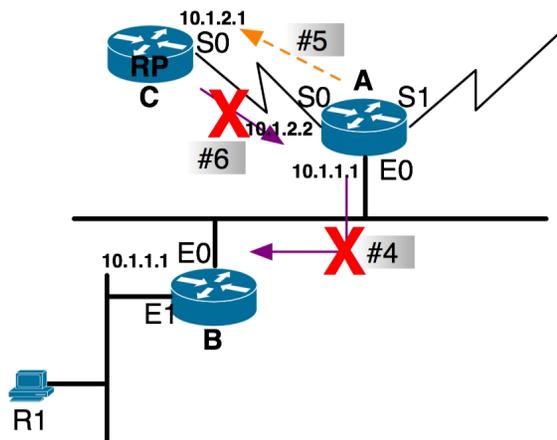
- #8: El tráfico de (S_i, G) comienza a llegar a través del SPT
- #9: El tráfico innecesario a deja de fluir por el RPT

Proceso de Recorte del RPT



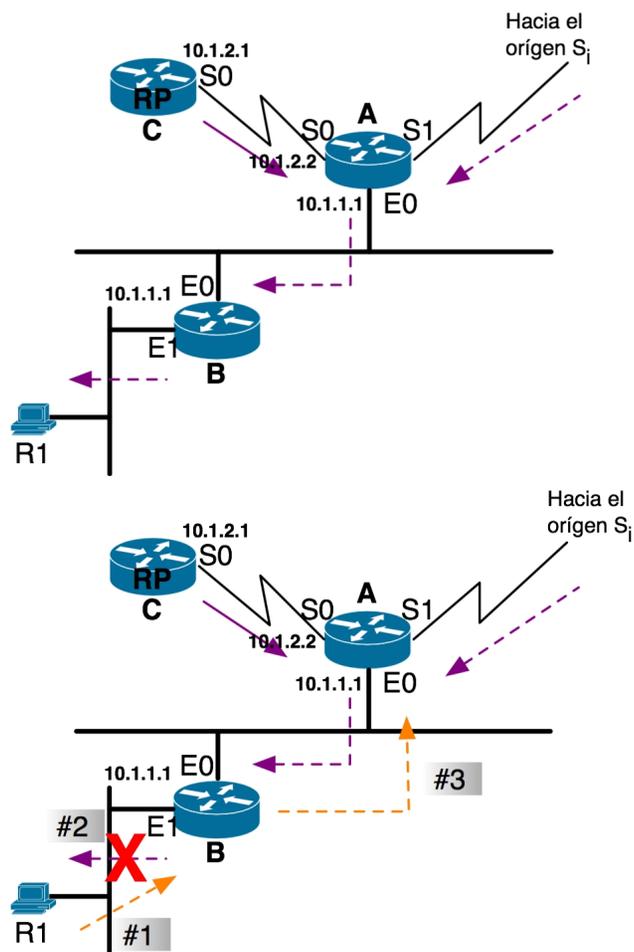
- El RPT ha sido creado en un proceso anterior
- #1: El enrutador B es un nodo final del árbol y el último cliente R1 deja de escuchar por el grupo G
- #2: El enrutador B remueve a E1 de las listas de interfaces de salida de (*,G) y cualquier otro (S_i,G)
- #3: La lista de interfaces de salida de B para (*,G) ahora está vacía y envía un mensaje de retiro (*,G) hacia el RP

Proceso de Recorte del RPT



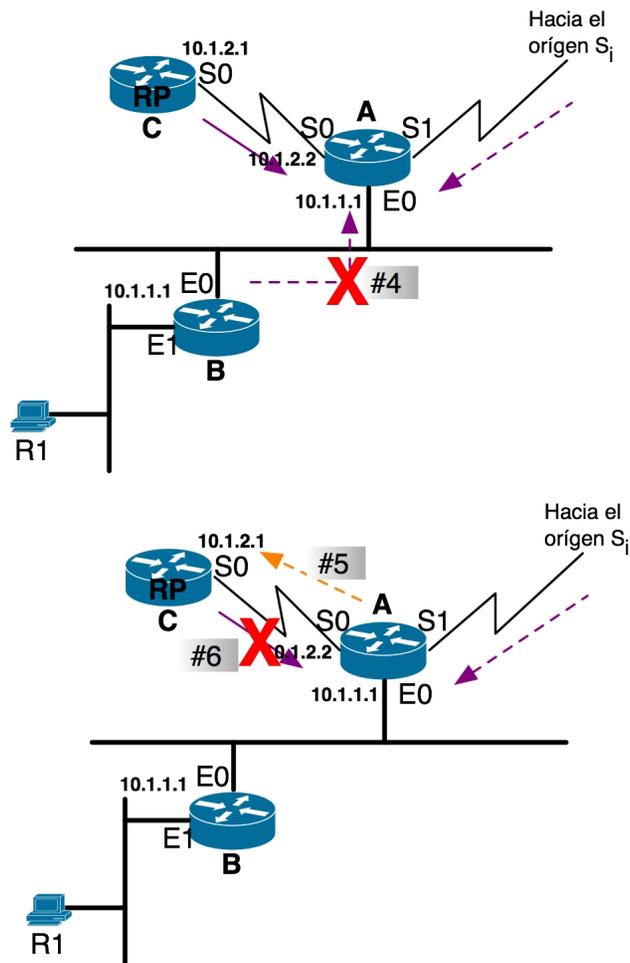
- #4: El enrutador A recibe el mensaje de retiro; remueve a E0 de la lista de interfaces de salida para (*,G)
- #5: La lista de interfaces de salida del enrutador A ahora está vacía y envía un mensaje de retiro para (*,G) hacia el RP
- #6: El proceso de retiro continúa hasta llegar al RP

Proceso de Recorte del SPT



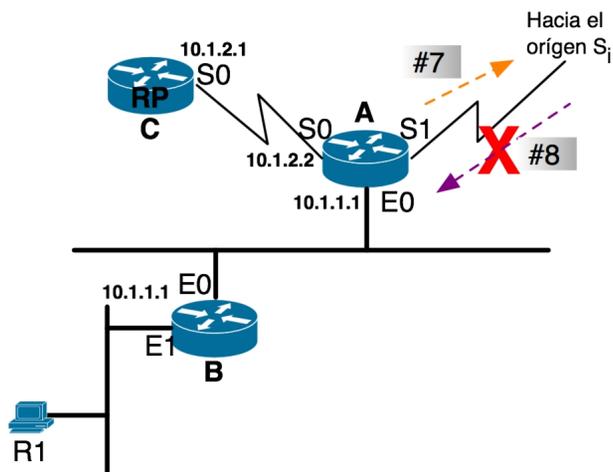
- El árbol SPT ha sido creado en un proceso anterior
- #1: El enrutador B es un nodo final del árbol y el último cliente R1 deja de escuchar por el grupo G
- #2: El enrutador B remueve a E1 de las listas de interfaces de salida de (*,G) y cualquier otro (S_i,G)
- #3: La lista de interfaces de salida de B para (*,G) ahora está vacía y envía un mensaje de retiro (*,G) hacia el RP

Proceso de Recorte del SPT



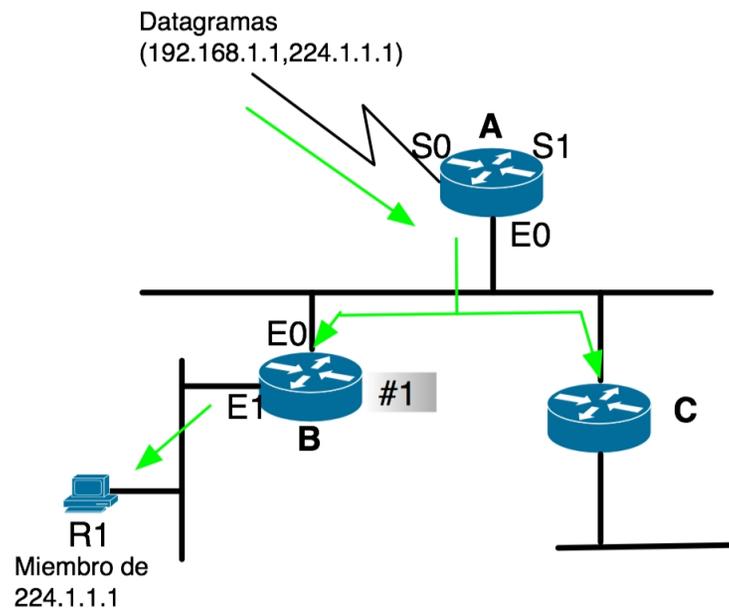
- #4: El enrutador B deja de enviar mensajes periódicos de unión para (S,G)
- #5: El enrutador A recibe el mensaje de retiro y remueve E0 de la lista de interfaces de salido para (*,G)
- #6: La lista de interfaces de salida del enrutador A ahora está vacía y envía un mensaje de retiro para (*,G) hacia el RP

Proceso de Recorte del SPT

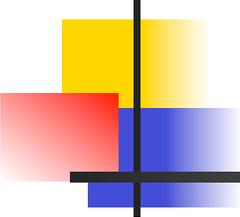


- #7: El estado para (S_i, G) expira en el enrutador A y envía un mensaje de retiro para (S_i, G) hacia S_i
- #8: El tráfico para (S_i, G) deja de fluir por el SPT

Creación de Estado (*,G) Debido al Arribo de (S,G)

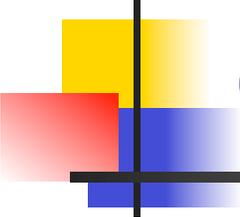


- Hay veces que estado (*,G) es creado debido a circunstancias ajenas los mecanismos de unión o retiro
- Cuando un enrutador (C) es parte de un segmento donde existen enrutadores (A,B) con miembros para un grupo este puede recibir paquetes que están destinados a un cliente en otro enrutador (B)
- El arribo de estos paquetes causará que el enrutador C cree estado (*,G) en sus tablas



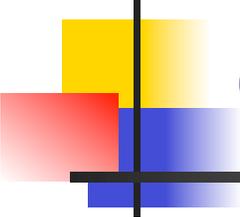
MBGP

- Extensiones para Multiprotocolos en BGP es definido por RFC2283
- Ayuda a resolver parte del problema de cómo escalar Multicast hacia conexiones entre diferentes sistemas autónomos
- Es utilizado para popular una tabla de enrutamiento para evaluar RPF entre sistemas autónomos cuando se envían ciertos mensajes de PIM-SM y decidir si se aceptan mensajes de MSDP-SA
- Permite que las rutas para unicast y multicast puedan ser diferentes
- Cuando se necesita
 - Para conexiones entre ISPs
 - Cuando tienes más de una conexión a más de un proveedor
- Cuando no es necesario
 - Si solo tienes una sola conexión



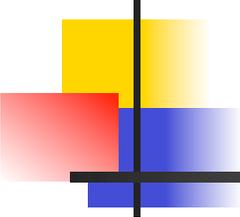
Operación de MBGP

- Puede manejar dos tipos de rutas
 - Unicast
 - Multicast
- Ambos tipos son intercambiados en la misma sesión de BGP
- MBGP no propaga información de estado para los (*,G) y (S,G)
- Tiene las mismas opciones disponibles para definir políticas
 - AS-PATH, Comunidades, MED, LOCAL-PREF, etc.



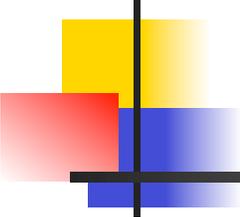
Operación de MBGP

- Nuevos Atributos (opcionales y no transitivos)
 - MP_REACH_NLRI (tipo 14)
 - MP_UNREACH_NLRI (tipo 15)
- Valores del campo de identificación de la familia de protocolos (SAFI) en el NLRI
 - SAFI=1: información para unicast
 - SAFI=2: información para multicast
 - SAFI=3: información para ambos, unicast y multicast
- Esta identificación permite el definir diferentes políticas para multicast de las que se usan para multicast



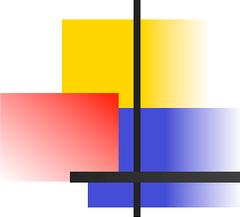
Operación de MBGP: Negociación de Capacidades

- Cuando los enrutadores tratan de abrir una sesión de BGP utilizando mensajes de OPEN, estos pueden negociar varias características.
- Para soportar MBGP, los enrutadores pueden negociar si usan:
 - Extensiones para Multiprotocolos
 - Múltiples rutas para el mismo destino
- A la vez los enrutadores se pueden configurar para que reciban uno o ambos de los NLRI (unicast y/o multicast)
 - Si un vecino configura ambos o solo un subconjunto, la intercepción de los subconjuntos es utilizada en ambas direcciones
 - Si la intercepción esta vacía, se envía una notificación y la sesión es terminada
 - Si el vecino no incluye parámetros de negociación en el mensaje de OPEN, entonces la sesión se re-inicializa sin parámetros de capacidades
 - La sesión sube solo para unicast



MSDP

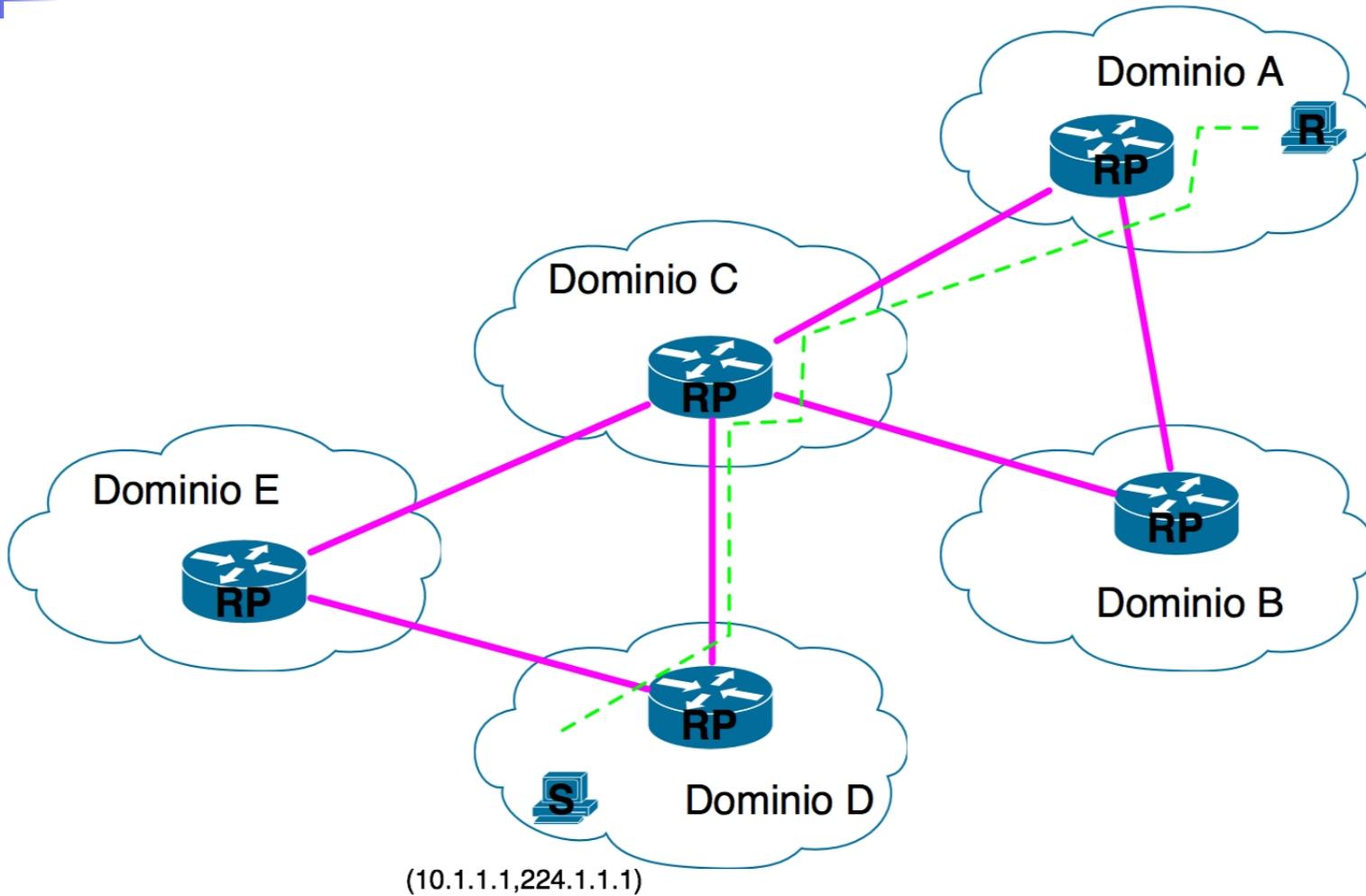
- Uno de los problemas con Multicast entre sistemas autónomos es como determinar quien están transmitiendo y como se llega hasta ellos sin muchos retardos
- MSDP describe un mecanismo para conectar dominios de PIM-SM
- Cada dominio de PIM-SM debe tener su propio RP y no deberá depender de un RP en otro dominio
- Beneficios:
 - No hay dependencia en recursos manejados por terceros (el dominio PIM-SM solo tiene que depender de su propio RP)
 - Dominios con solo receptores pueden existir si la necesidad de que tengan que anunciar globalmente su deseo de recibir un grupo

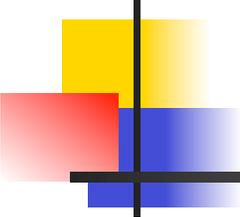


MSDP

- Interconecta RPs en diferentes dominios con una conexión TCP para intercambiar mensajes de origen activo (SA)
- También puede ser utilizado dentro de un dominio para proveer redundancia del RP cuando se usa en conjunción con Anycast-RP
- Los RPs envían mensajes de SAs para los orígenes internos hacia los otros vecinos de MSDP
- Los mensajes de SA deben pasar las pruebas de RPF antes de estos puedan ser aceptados o enviados más adelante
- Los RPs aprenden sobre fuentes externas vía los mensajes de SAs y pueden iniciar mensajes de unión (S,G) a favor de receptores locales
- Las conexiones de MSDP típicamente se hacen en paralelo con conexiones de MBGP

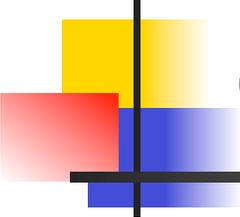
MSDP





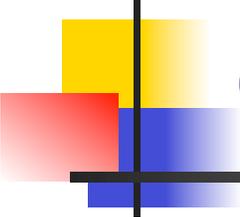
Mensajes SA de MSDP

- El mensaje SA inicial es enviado cuando el origen se registra con su RP
 - Es posible que también encapsule el primer datagrama
- Subsecuentemente envía mensajes cada 60 segundos mientras la fuente se mantenga transmitiendo
- Otros vecinos de MSDP no originan mensajes para ese SA sino que lo transmiten hacia otros vecinos de MSDP
- Los mensajes de SA son almacenados en el enrutador en el caso de que haya nuevos miembros locales que quieran recibir ese grupo
 - Ayuda a reducir el tiempo de unión
 - Previene la propagación de tormentas de SAs



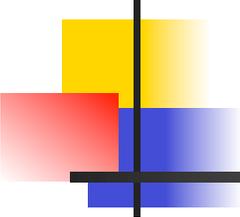
Operación de MSDP

- Los vecinos de MSDP utilizan conexiones TCP al puerto 639
 - El vecino con la dirección más alta es el que escucha, el otro inicia la conexión
- Utiliza el concepto de inundación y unión (Flood & Join)
 - Periódicamente envía mensajes de SA (fuente activa) a los otros vecinos MSDP indicando
 - La dirección de origen de los flujos activos
 - La dirección del grupo de multicast al a que se están enviando los mensajes
 - La dirección de IP del RP del origen
 - Únicamente se originan mensajes de SA para las fuentes/orígenes en el dominio local
- Los mensajes de SA que se reciben son verificados contra el RPF del RP en el mensaje
 - Si pasa la verificación una entrada es creada en las tablas de estado y el mensaje enviado a los otro vecinos de MSDP (ver mas adelante)
- Si existe estado (*,G) con una lista de interfaces de salida no vacía, se pueden enviar mensajes de unión (S,G) hacia el origen y de esta forma se crean SPTs entre dominios



Operación de MSDP: Vecinos

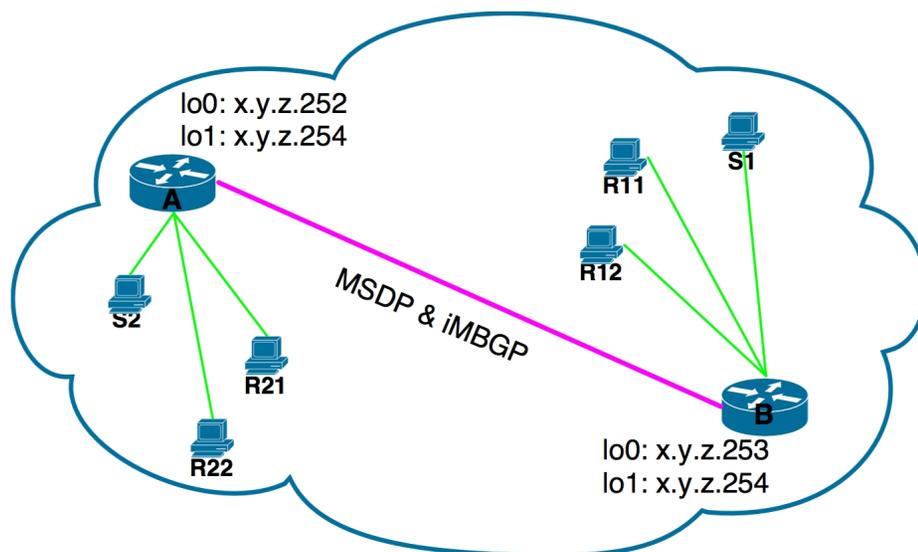
- Ya habíamos visto que los vecinos se conectan usando TCP 639
- Cada 60 segundos se envían mensajes para mantener la sesión (keepalives)
- Los vecinos terminan la sesión si pasan 74 segundos sin recibir mensajes de MSDP o keepalives
- Los vecinos de MSDP también deben correr MBGP
 - Puede correr eMBGP, iMBGP o ambos
 - Requerido para el proceso de verificación de RPF de la dirección del RP en el SA y así evitar círculos (loops)
 - La excepción es cuando solo se tiene un vecino de MSDP y entonces BGP no es necesario y se puede usar la ruta por defecto



MSDP: Procesamiento de los Mensajes de SA

- El proceso de verificación RPF es ignorado y acepta el SA si:
 - El vecino de MSDP desde donde se recibió el mensaje el único vecino (vecino por defecto -- default-peer)
 - El vecino de MSDP desde donde se recibió el mensaje es miembro del mismo grupo malla (mesh-group)
- Para cada mensaje SA ejecuta la verificación RPF
 - Si el vecino de MSDP es el RP que origina el SA
 - Acepta el SA
 - Sino, busca la mejor ruta MBGP hacia el RP en el mensaje SA
 - Si no encuentra una ruta
 - La verificación falla
 - Ignora el SA
 - Si el vecino de MSDP que envía el mensaje también es un vecino de MBGP
 - Es la mejor ruta hacia el RP a través de este vecino?
 - El proceso de verificación RPF es satisfactorio
 - Procesa el SA
 - Sino, es el primer AS en el mejor camino hacia el RP el mismo que el primer AS en el mejor camino hacia el vecino de MSDP
 - El proceso de verificación RPF es satisfactorio
 - Procesa el SA
 - Sino, el proceso de verificación falla y se descarta el SA

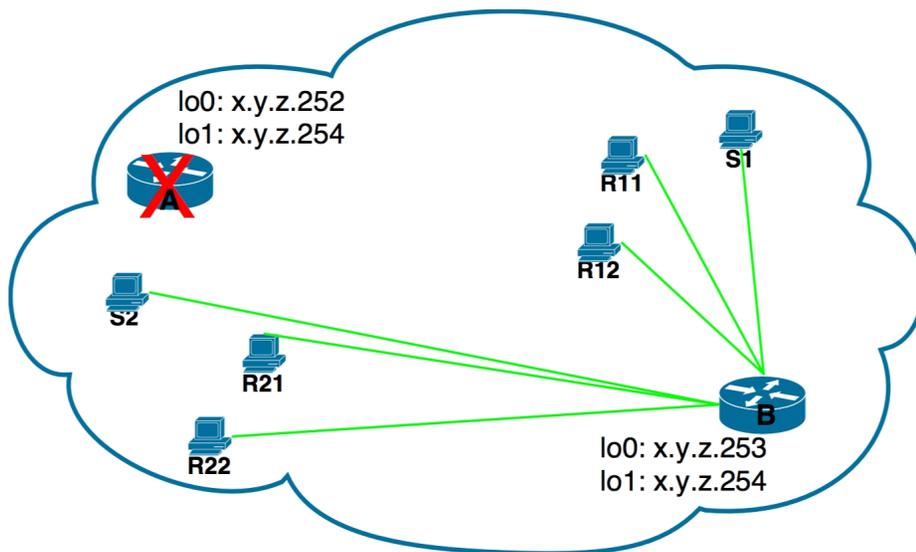
Anycast-RP

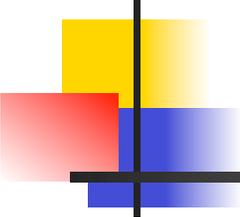


- Una forma de proveer redundancia y distribuir la carga de los RP es utilizar Anycast-RP (RFC3446)
- Anycast-RP es utilizado en redes con PIM-SM, MSDP y MBGP
- La dirección del RP es asignada a una interfaz de loopback
 - Esta dirección debe ser asignada a cada enrutador que va a proveer funciones de RP en el dominio
- Los clientes y orígenes serán registrados con el RP mas cercano basado en la métrica de IGP
- De esta forma clientes cercanos a A se asocian con A y clientes cercanos a B se asocian con B
- Los dos RPs deben establecer sesiones de MSDP. Una sesión de MBGP no es un requerimiento

Anycast-RP

- Si por alguna razón el enrutador A falla, el enrutador B será el único anunciando el prefijo x.y.z.254/32 y por lo tanto todo el estado es transferido

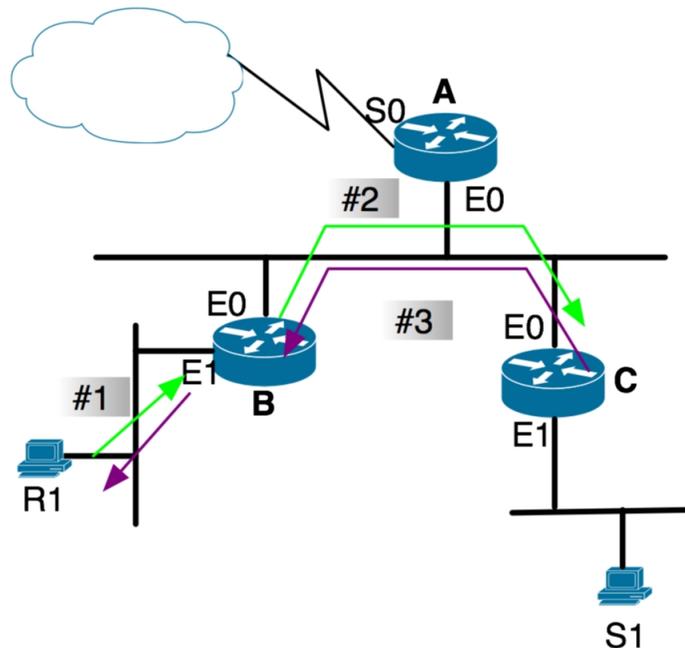




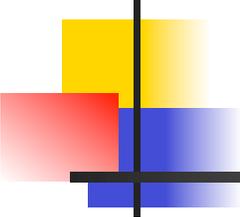
PIM-SSM

- Varias modificaciones han sido realizadas para soportar el paradigma de multicast desde orígenes específicos
 - No se requiere la creación de árboles RPT
 - No se necesita enviar mensajes de registro (Register Messages)
 - No hay necesidad de mantener una tabla de grupo a RP, pues no se requiere un RP
 - No hay necesidad de MSDP para descubrir los orígenes. Estos son especificados como parte de los mensajes de reporte de IGMPv3
 - Requiere el uso de IGMPv3 para poder informarle al enrutador inicial cuales son los árboles SPT que se deben crear
 - Se puede definir el rango de direcciones que se pueden utilizar
 - IANA ha asignado el rango 232.0.0.0/8 para SSM

Recibiendo Grupo Usando PIM-SSM

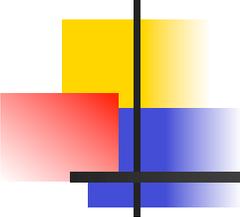


- La estación R1 ha determinado el origen que quiere escuchar por algún otro medio externo (e.g. Una página web)
- #1: La estación R1 quiere recibir el grupo G y envía un mensaje de reporte de membresía indicando los orígenes que desea recibir
- #2: El DR recibe el mensaje, crea el estado (S,G) necesario y envía un mensaje de unión (Join) hacia el origen S1 usando la interfaz de RPF
- Este proceso se repite hasta que los mensajes de unión llegan al último enrutador donde el origen está conectado
- #3: El SPT es completado y tráfico para (S,G) comienza a fluir a siguiendo el SPT



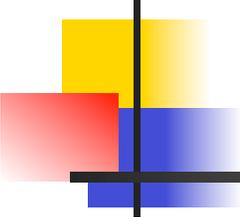
Requerimientos

- **IGMP**: es utilizado por las estaciones y enrutadores para intercambiar mensajes sobre membresía
- **PIM-SM**: es utilizado para propagar estado de membresía entre los enrutadores
- **MBGP**: es utilizado entre dominios de PIM (o sistemas autónomos) para intercambiar información de rutas para las verificaciones de RPF
- **MSDP**: es utilizado por los RP en ASM para transmitir información sobre orígenes
- **SSM**: provee modificaciones en la funcionalidad PIM-SM para construir SPT directamente hacia el origen sin necesidad de un RP o MSDP



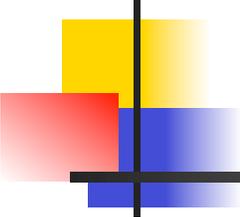
Resolviendo Problemas en Multicast

- Requerimientos:
 - Por lo menos un origen/fuente activo
 - Por lo menos un receptor/cliente activo
- Comenzar cerca del receptor
 - Identificar el enrutador PIM designado (DR)
 - Verificar el estado IGMP en el DR
 - Buscar por estado (S,G) en el DR



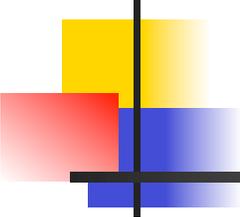
Resolviendo Problemas en Multicast

- Sigue el camino RPF desde el DR hacia el origen
- Verificar que PIM-SM ha sido configurado en cada interfaz en el camino RPF, porque esto determina la topología del árbol de distribución
- Verificar el estado (S,G) en cada enrutador
- Verificar los contadores para (S,G) en cada enrutador



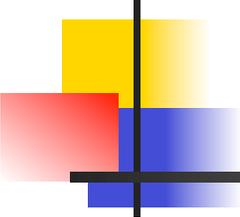
Resolviendo Problemas en Multicast

- Si el origen es externo a su dominio
 - Verificar que se tiene un mensaje MSDP de SA
 - Verificar que el próximo salto de acuerdo a las tablas de MBGP es:
 - Un vecino PIM-SM
 - Un vecino de MSDP
 - Verificar que realmente se está seleccionando la ruta con NLRI=Multicast como el camino de verificación RPF
 - Verificar la distancia administrativa de BGP



Resolviendo Problemas en Multicast

- Que pasa si nadie escucha tus transmisiones?
 - Verificar que tienes estado (S,G) en tu RP
 - Verificar que tu RP esta anunciando SA a través de MSDP y que este anuncio aparece en las tablas SA de tu vecino MSDP
 - Verificar que tiene continuidad (adjacency) con tu vecino
 - Verificar que la interfaz del vecino aparece en la lista de interfaces de salida para el (S,G)
 - Verificar que los contadores de paquetes muestran tráfico de salida



Referencias/Fuentes

- Cisco (<http://www.cisco.com>)
- Juniper (<http://www.juniper.net>)
- Procket (<http://procket.com>)
- Libros:
 - Developing IP Multicast Networks: Volumen 1
 - Interdomain Multicast Routing
 - Interdomain Multicast Solutions Guide
- Documentos del IETF:
 - RFC1700, RFC1112, RFC1771, RFC2236, RFC2362, RFC2858, RFC3180, RFC3376, RFC3446, RFC3618
 - draft-ietf-pim-dm-new-v2-04.txt
 - draft-ietf-pim-sm-v2-new-09.txt