



Comunidad de Soporte de Cisco en  
Español Webcast en vivo:

# Internet Protocol (IP) Multicast: Fundamentos y mejores prácticas.

Enrique Dávila  
Technical Leader Services

24 de septiembre del 2013

# Comunidad de Soporte de Cisco – Webcast en vivo

- El experto del día de hoy es: Enrique Dávila



**Enrique Dávila**

CCIE in Routing and Switching,  
Service Provider, & Security

# Internet Protocol (IP) Multicast: Fundamentos y mejores prácticas.

## Panel de Expertos (Question Manager)



**Jose Luiz Marques**

CCIE in Routing and Switching, &  
Service Provider



# Gracias por su asistencia el día de hoy

La presentación incluirá algunas preguntas a la audiencia.

Le invitamos cordialmente a participar activamente en las preguntas que le haremos durante la sesión





## Copia de la presentación

Si desea bajar una copia de la presentación de hoy, vaya a la liga indicada en el chat o use ésta dirección

<https://supportforums.cisco.com/docs/DOC-36633>



# Webcast pasados:

Usted puede encontrar todos los Webcast de la Comunidad de Soporte de Cisco en español en:

<https://supportforums.cisco.com/community/spanish/espacio-de-los-expertos/webcasts>



# Pregunta 1

## ¿Cuál es tu nivel de experiencia con Multicast?

- a) Ninguna, solamente he escuchado como funciona
- b) Básico, he estudiado la teoría.
- c) Intermedio, he estudiado y trabajado en el laboratorio
- d) Avanzado, he estudiado, trabajado en laboratorio y opero una red de multicast.

# ¡ Ahora puede realizar sus preguntas al panel de expertos!

Use el panel de preguntas y respuestas (Q&A) para preguntar a los expertos ahora. Ellos empezarán a responder.







Comunidad de Soporte de Cisco en Español Webcast en vivo:

# Internet Protocol (IP) Multicast: Fundamentos y mejores prácticas.

**Enrique Dávila**

Technical Leader Services

24 de septiembre del 2013



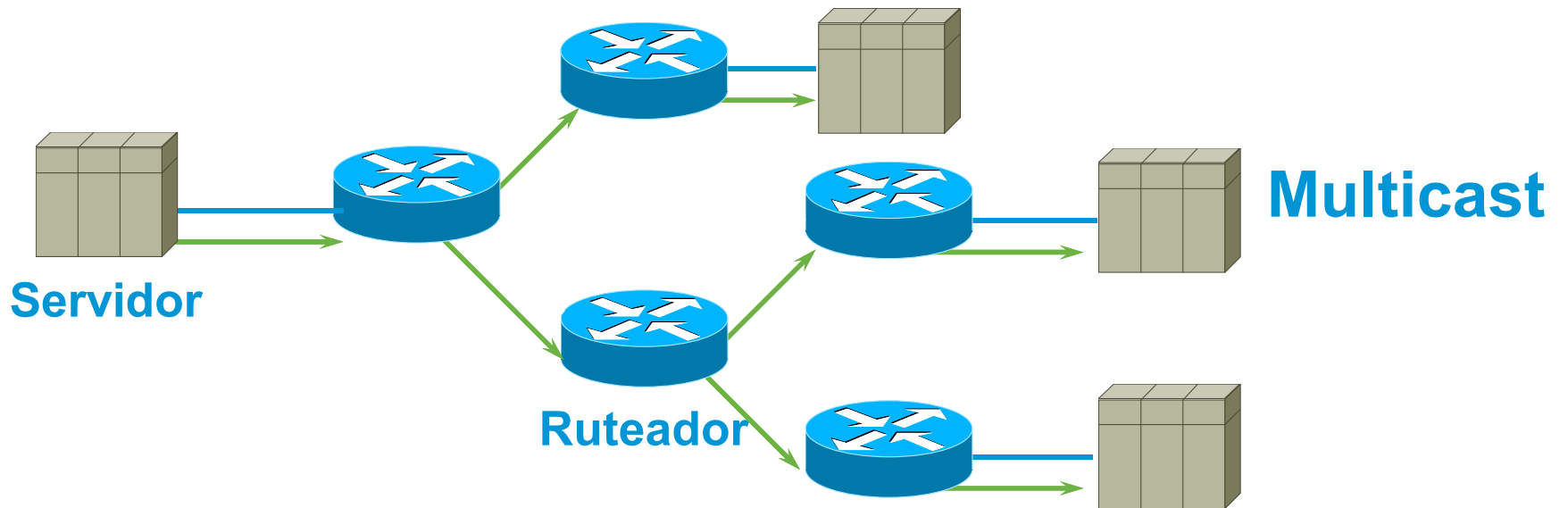
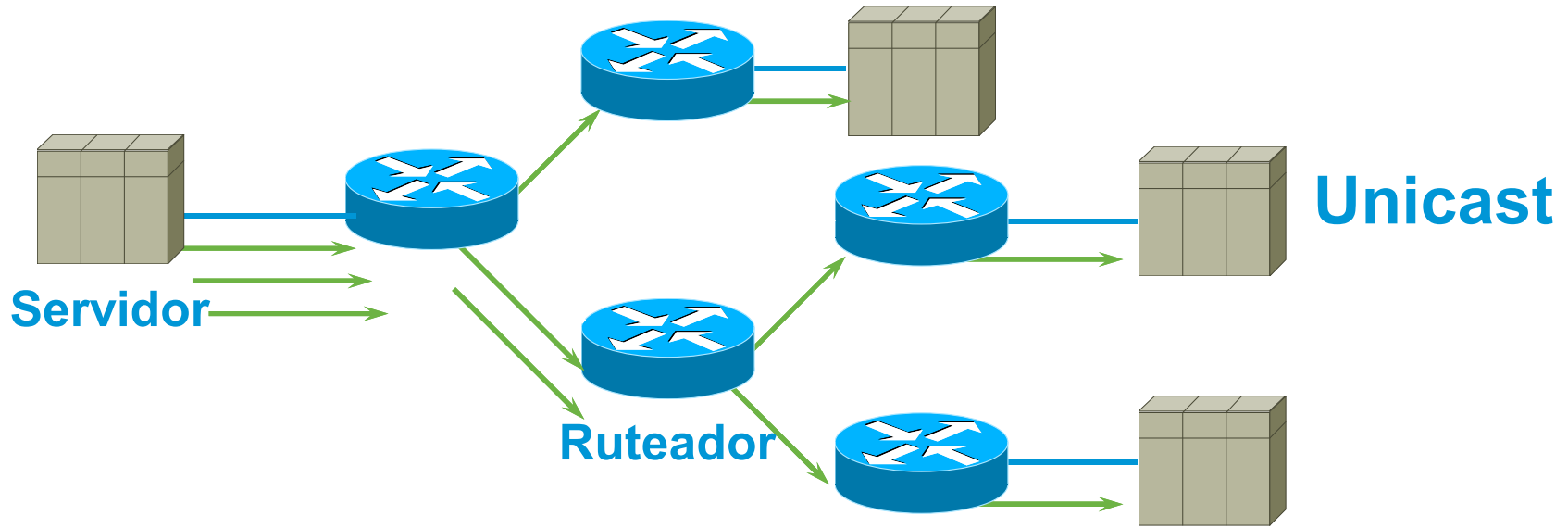
# Agenda

- ¿Por qué Multicast?
- Fundamentos de Multicast
- Multicast en capa 2
- Multicast intradominio

# ¿Por qué Multicast?



# Unicast vs. Multicast

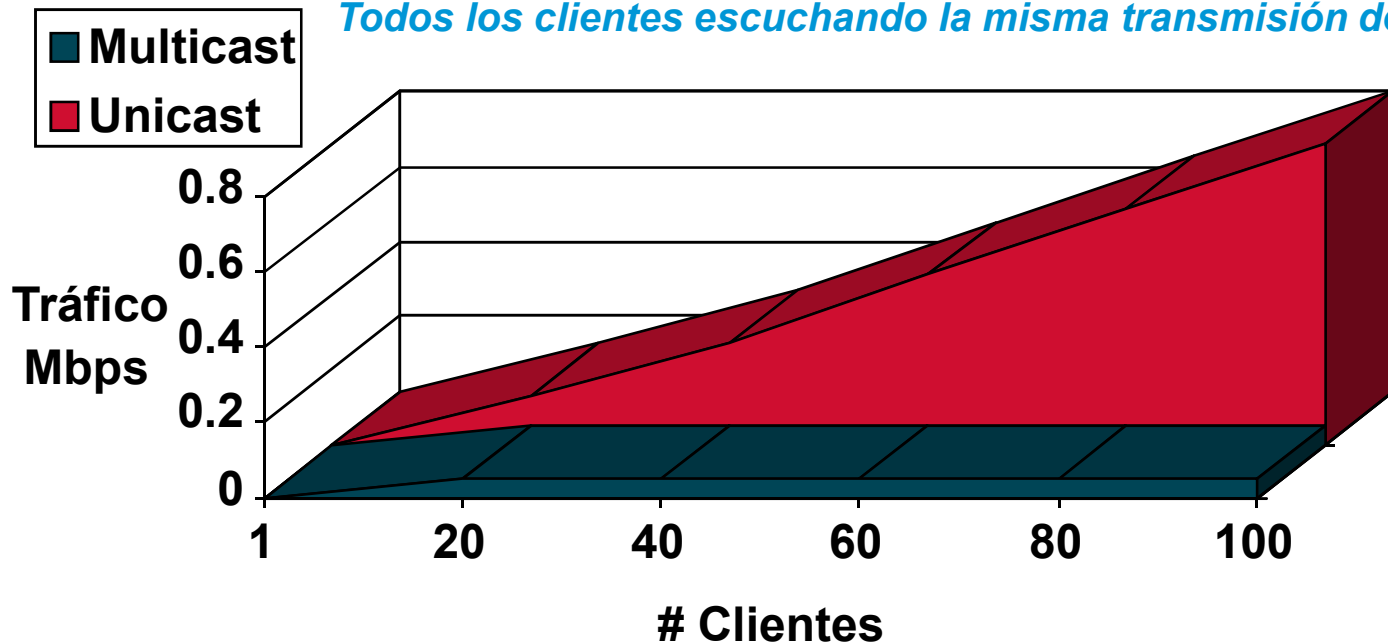


# Ventajas de Multicast

- **Eficiencia Mejorada:** Controla el tráfico en la red y reduce la carga en servidores y ciclos de CPU
- **Desempeño Optimizado:** Elimina tráfico redundante
- **Aplicaciones Distribuidas:** Permite aplicaciones multipunto.

Ejemplo: Transmisión de audio

Todos los clientes escuchando la misma transmisión de 8 kbps de audio



# Desventajas de Multicast

## ***Multicast está basado en UDP!!!***

- ***Entrega como Mejor Esfuerzo:*** Péridas son esperadas. Las aplicaciones no deben esperar que la entrega de información sea confiable y así deben deser diseñadas. El envío de multicast confiable es aún un área que requiere más investigación.
- ***No tiene mecanismos para evitar congestión:*** No cuenta con mecanismos como la ventana de TCP o el comienzo lo cual puede terminar en congestión en la red. De ser posible, las aplicaciones deben de tener la inteligencia para detectar y así evitar condiciones de congestión.
- ***Duplicados:*** Algunos mecanismos de multicast (Asserts, Registers y transiciones de SPT) pueden ocasionar la generación de paquetes duplicados. Las aplicaciones deben de ser diseñadas de tal forma en que se esperen paquetes duplicados ocasionalmente.
- ***Entrega fuera de orden:*** Algunos topologías puede terminar en envío de paquetes fuera de orden.

# Aplicaciones que se benefician de Multicast

- **Multimedia**
  - ✓ Transmisión de audio y video
  - ✓ Entrenamiento
  - ✓ Conferencias
- **Almacenamiento de información**
- **Aplicaciones financieras**
- **Cualquier aplicación que requiera comunicación de uno a muchos.**

## Pregunta 2

**¿Cuántos años de experiencia en redes tienes?**

- a) 1 a 3 años
- b) 3 a 6 años
- c) 6 a 9 años
- d) 9 a 12 años
- e) Más de 12 años



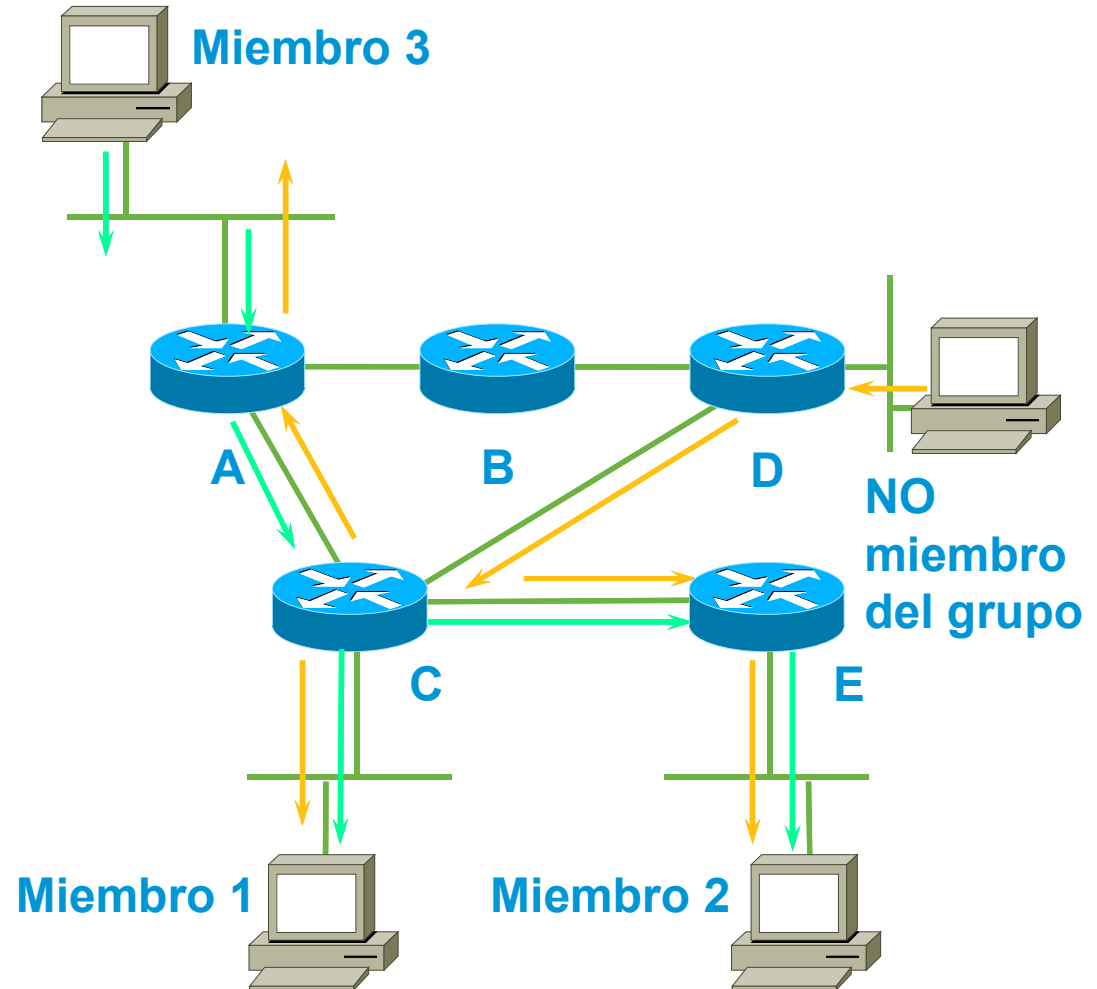
# Agenda

- ¿Por qué Multicast?
- Fundamentos de Multicast
- Multicast en capa 2
- Multicast intradominio



# Concepto de grupo Multicast

1. Si envías a una dirección de grupo, todos los miembros lo reciben.
2. Debes de ser miembro del grupo para recibir la información.
3. No tienes que ser miembro del grupo para enviar al grupo.



# Direccionamiento Multicast

- Grupo de direcciones IP Multicast 224.0.0.0 – 239.255.255.255
  - Espacio de direcciones Clase “D”
    - Los bits más significativos del primer octeto = “1110” – “1110XXXX”
- Direcciones reservadas (Direcciones Link-local)
  - 224.0.0.0 – 224.0.0.255
  - Enviados con TTL = 1
  - Ejemplos:

224.0.0.1	Todos los sistemas en el segmento
224.0.0.2	Todos los routers en el segmento
224.0.0.4	Ruteadores DVMRP
224.0.0.5	Ruteadores OSPF
224.0.0.13	Ruteadores PIMv2
224.0.0.22	Ruteadores IGMPv3

# Direccionamiento Multicast

- Rango de direcciones administrativas

239.0.0.0 – 239.255.255.255

Rango de direcciones privadas

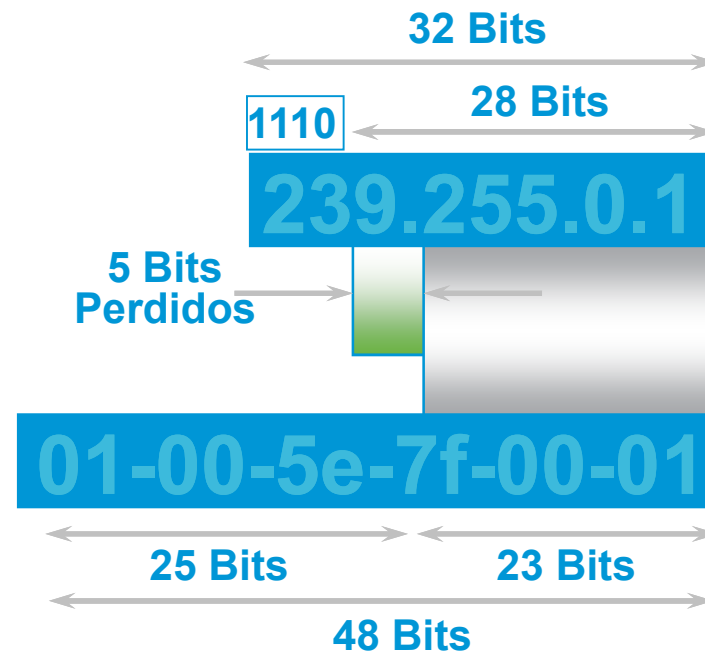
- Similar al RFC1918 para direcciones unicast.
- No utilizado para tráfico en internet
- Utilizado para limitar el alcance de tráfico multicast.
- La misma dirección puede ser utilizada en localidades distintas para otras sesiones de multicast.
- Ejemplos

Rango Site-local: 239.255.0.0/16

Rango Organization-local: 239.192.0.0/14

# Multicast Addressing

## Mapeo de dirección IP Multicast a MAC (Ethernet)



# Direccionamiento Multicast

## Mapeo de Direcciones IP Multicast a MAC (Ethernet)

Tomar en cuenta el traslape de direcciones 32:1

32 – Direcciones IP Multicast

224.1.1.1  
224.129.1.1  
225.1.1.1  
225.129.1.1  
⋮  
⋮  
238.1.1.1  
238.129.1.1  
239.1.1.1  
239.129.1.1

1 – Direcciones MAC Multicast  
(Ethernet)

0x0100.5E01.0101

# Direccionamiento Multicast

## Evitar direcciones que serán tratadas como Broadcast

Direcciones en el rango Link Local serán tratadas como broadcast

32 – Direcciones IP Multicast Addresses

224.0.0.x  
224.128.0.x  
225.0.0.x  
225.128.0.x  
⋮  
⋮  
238.0.0.x  
238.128.0.x  
239.0.0.x  
239.128.0.x

1 - Multicast MAC Address  
(FDDI and Ethernet)

0x0100.5E00.00xx

# Agenda

- ¿Por qué Multicast?
- Fundamentos de Multicast
- **Multicast en capa 2**
- Multicast intradominio





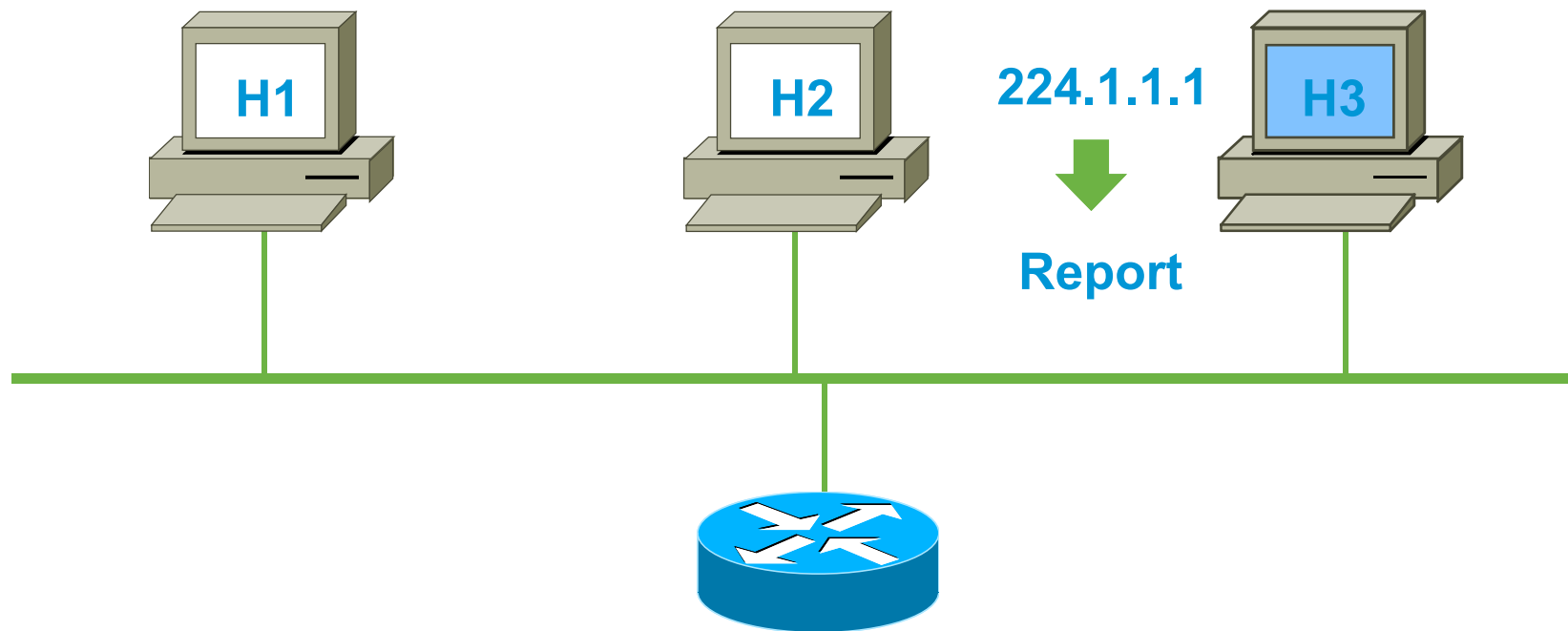
# Señalización entre hosts y Routers: IGMP

- Mecanismo que tienen los hosts para avisar a los routers que quieren unirse a un grupo.
- Ruteadores solicitan de hosts directamente conectados si quieren estar unidos a un grupo.
- **RFC 1112 especifica la versión 1 de IGMP** Soportado en Windows 95
- **RFC 2236 especifica la versión 2 de IGMP** Soportado en todos los sistemas operativos en la actualidad.
- **RFC 4604 especifica la versión 3 de IGMP**



# Señalización Host-Ruteador: IGMP

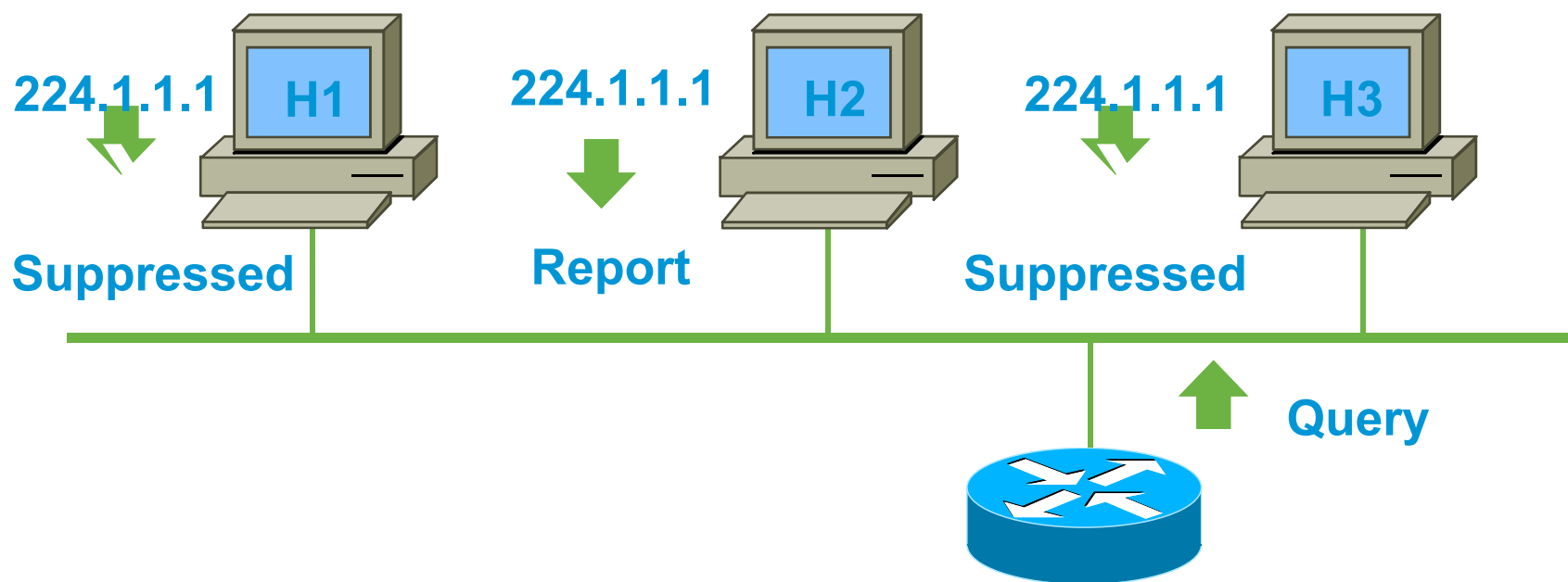
## ¿Cómo unirse a un grupo?



El host envía un “IGMP Report” para unirse al grupo

# Señalización Host-Ruteador: IGMP

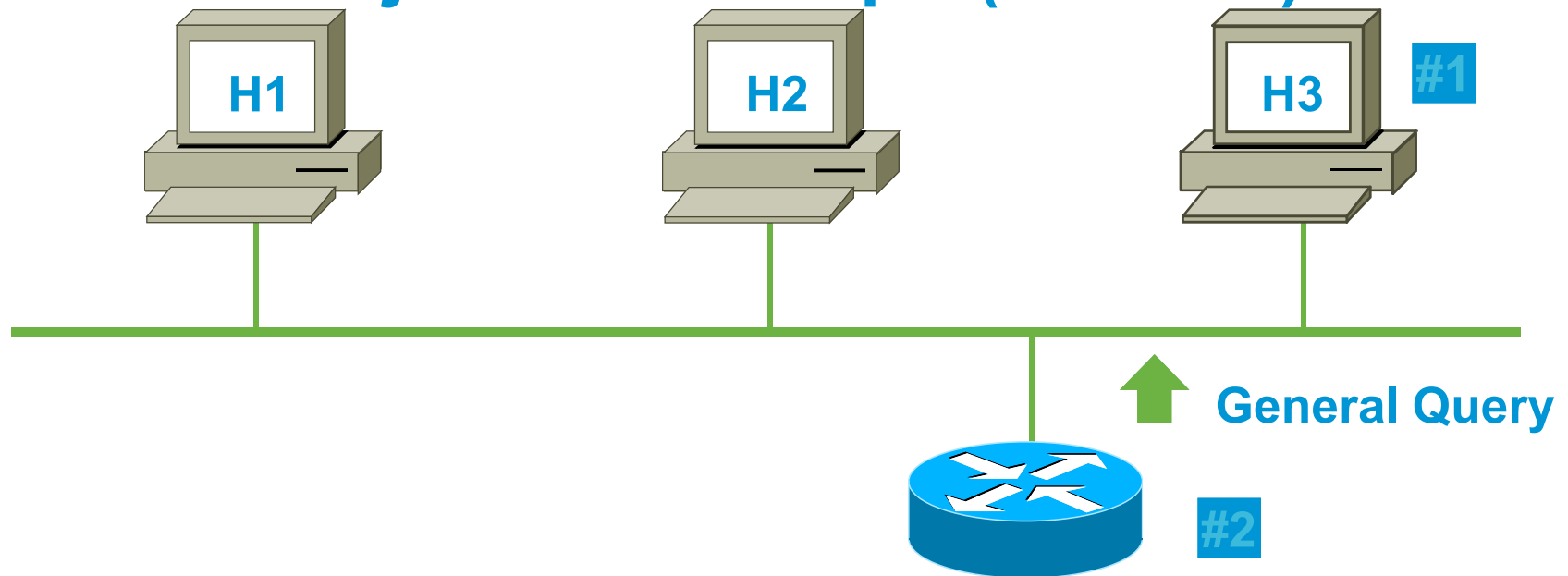
## ¿Cómo mantenemos a un grupo?



- Ruteadores envía “Queries” a la dirección 224.0.0.1
- 1 Miembro por grupo y por subred envía los “reports”
- Los otros miembros suprimen el envío de “reports”.

# Señalización Host-Ruteador: IGMP

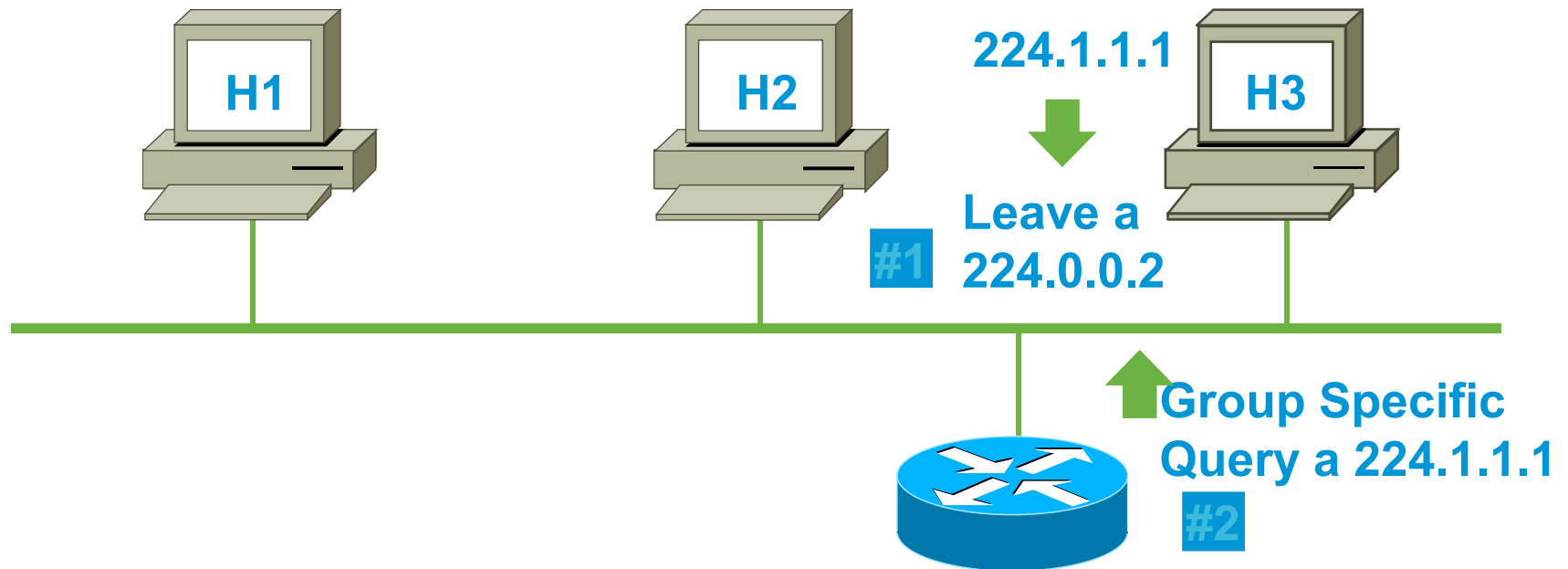
## Dejando un Grupo (IGMPv1)



- Los hosts silenciosamente dejan los grupos
- Ruteadores envían 3 “General Queries” (60 segundos)
- No se recibe un “IGMP Report” para el grupo.
- El grupo expira (Peor escenario  $\approx$  3 minutos)

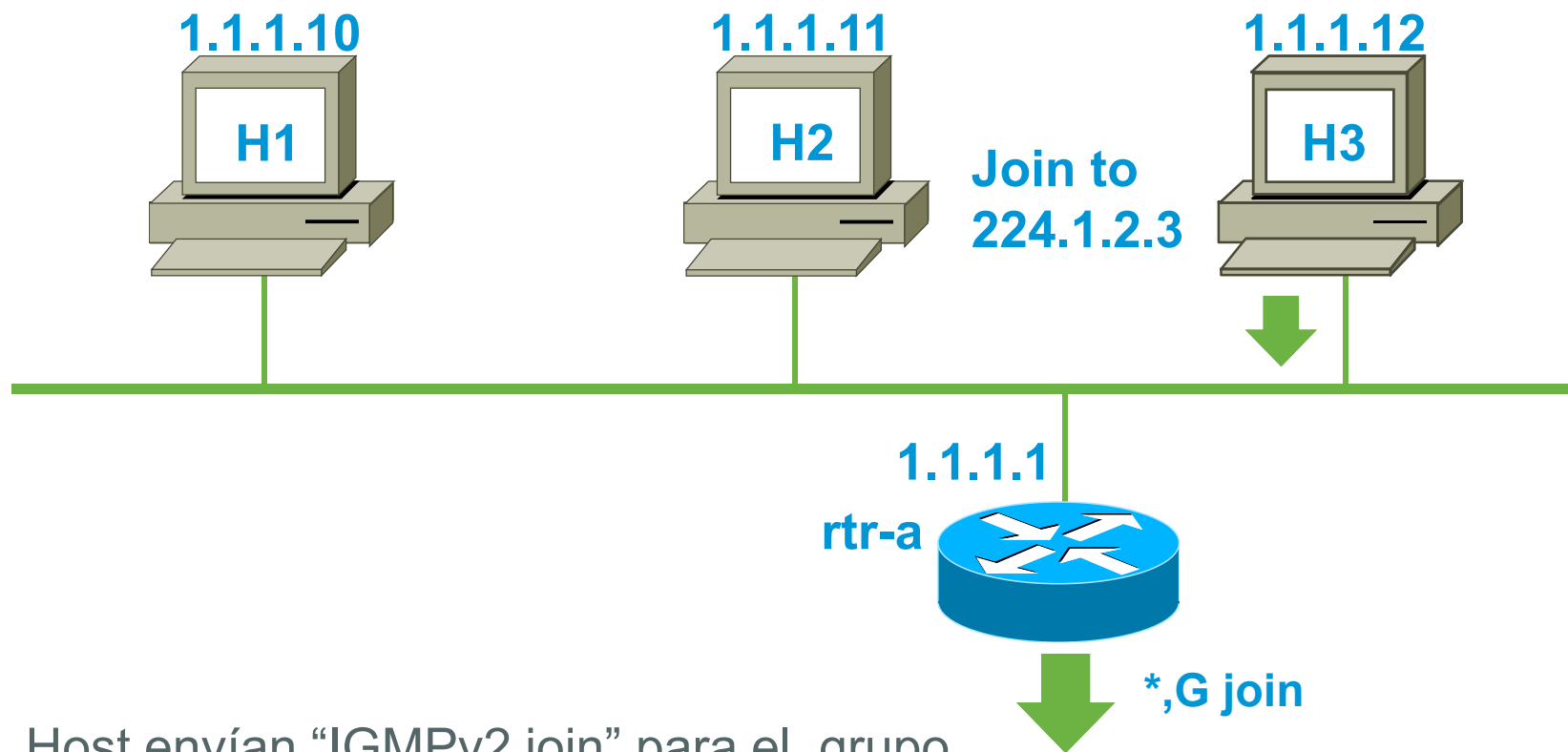
# Señalización Host-Ruteador: IGMP

## Dejando un grupo (IGMPv2)



- El Host envía un mensaje de “Leave” a 224.0.0.2
- El router envía un “Group Specific Query” a 224.1.1.1
- No se recibe ningún “IGMP Report” en ~3 segundos
- El grupo 224.1.1.1 expira

# IGMPv2



- Host envían "IGMPv2 join" para el grupo
- Los ruteadores agregan la relación con el grupo (membership)
- El ruteador envía un (\*,G) join al RP (Tiene que, no conoce la fuente)

# Señalización Host-Ruteador: IGMPv3

- RFC 4604
- Agrega el Incluir/Excluir la lista fuente.

Habilita a los hosts a escuchar solamente a un rango específico de hosts que transmiten a un grupo de multicast.

- Aplicaciones tiene que soportar el incluir dicha lista.

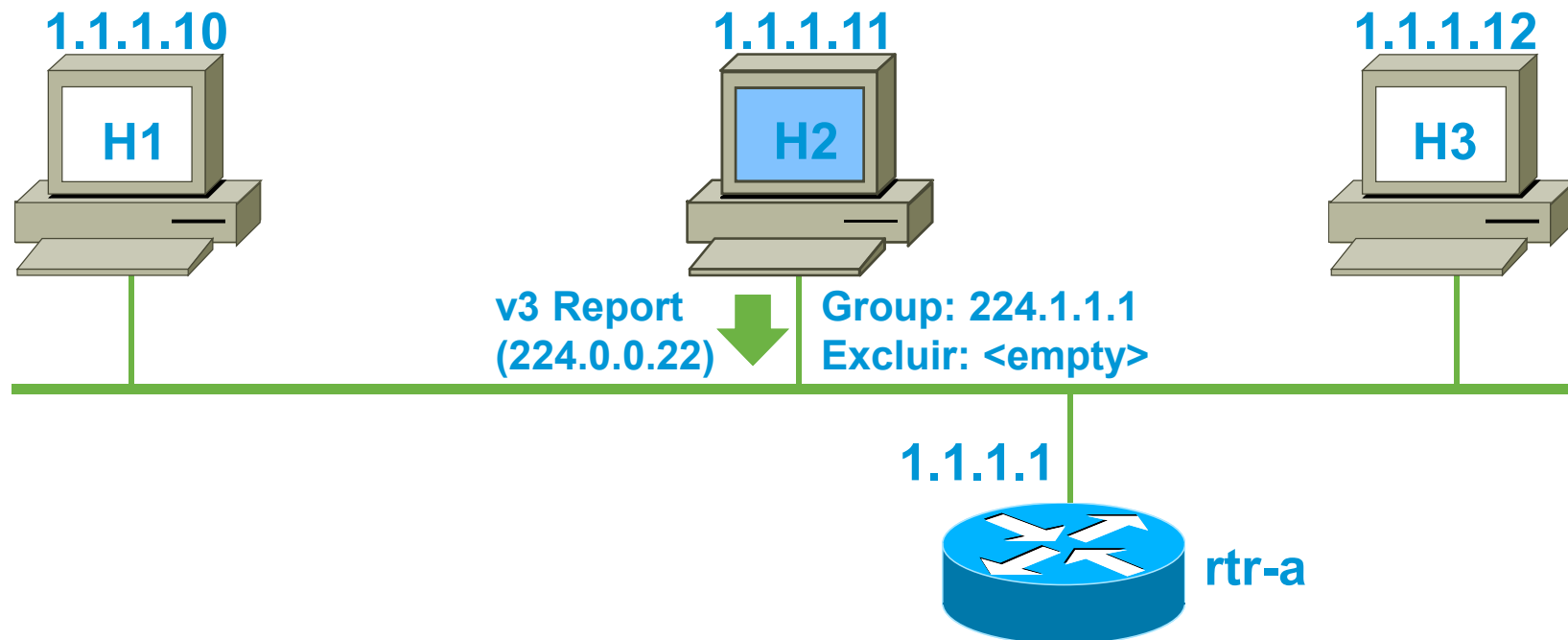
# Señalización Host-Ruteador: IGMPv3

- Nueva dirección para envío de “Membership Reports”  
224.0.0.22 (IGMPv3 Ruteadores)
  - Todos los hosts con IGMPv3 envían “reports” a esta dirección.
  - Todos los ruteadores habilitados con IGMPv3 escuchan esta dirección.
  - Los hosts no escuchan ni responden a esta dirección.
  - No hay “Report Suppression”
  - Todos los hosts en el segmento responden a “Queries”
  - El intervalo de respuesta puedes ser configurado

Útil cuando hay muchos hosts

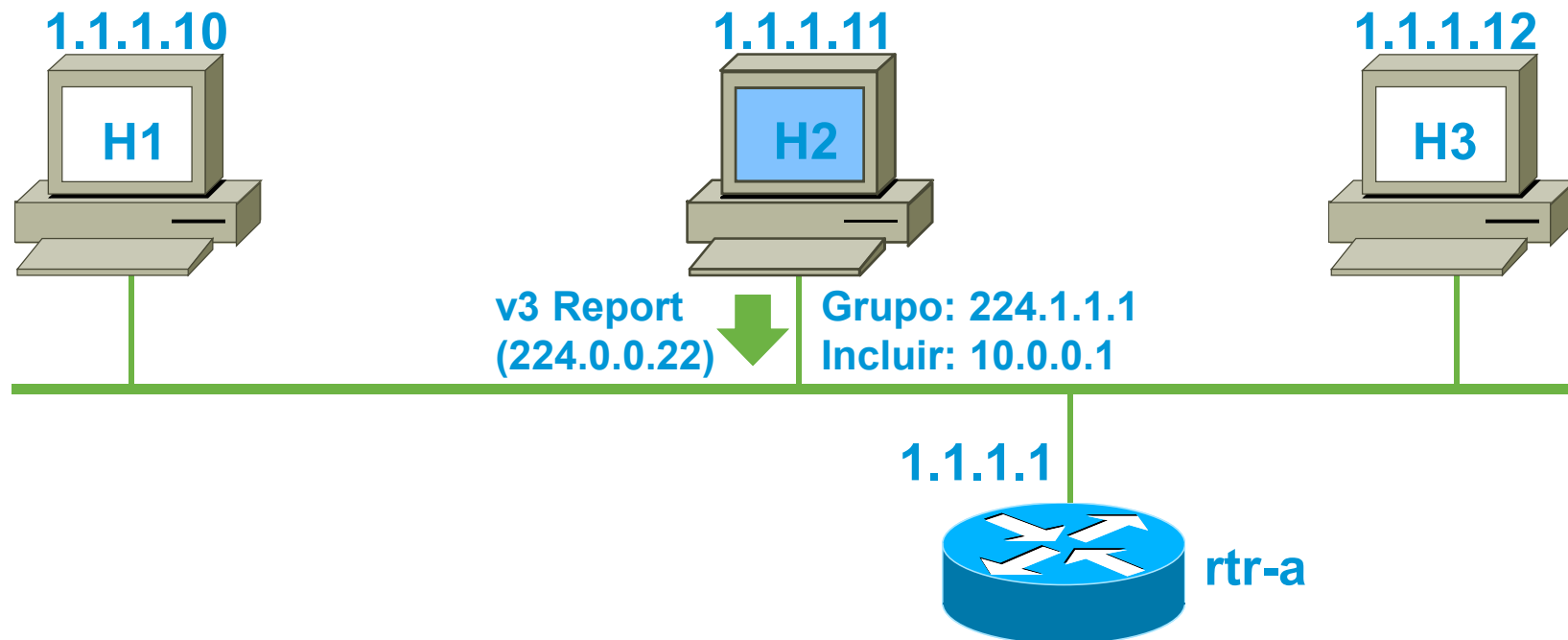


# IGMPv3— Uniéndose a un grupo



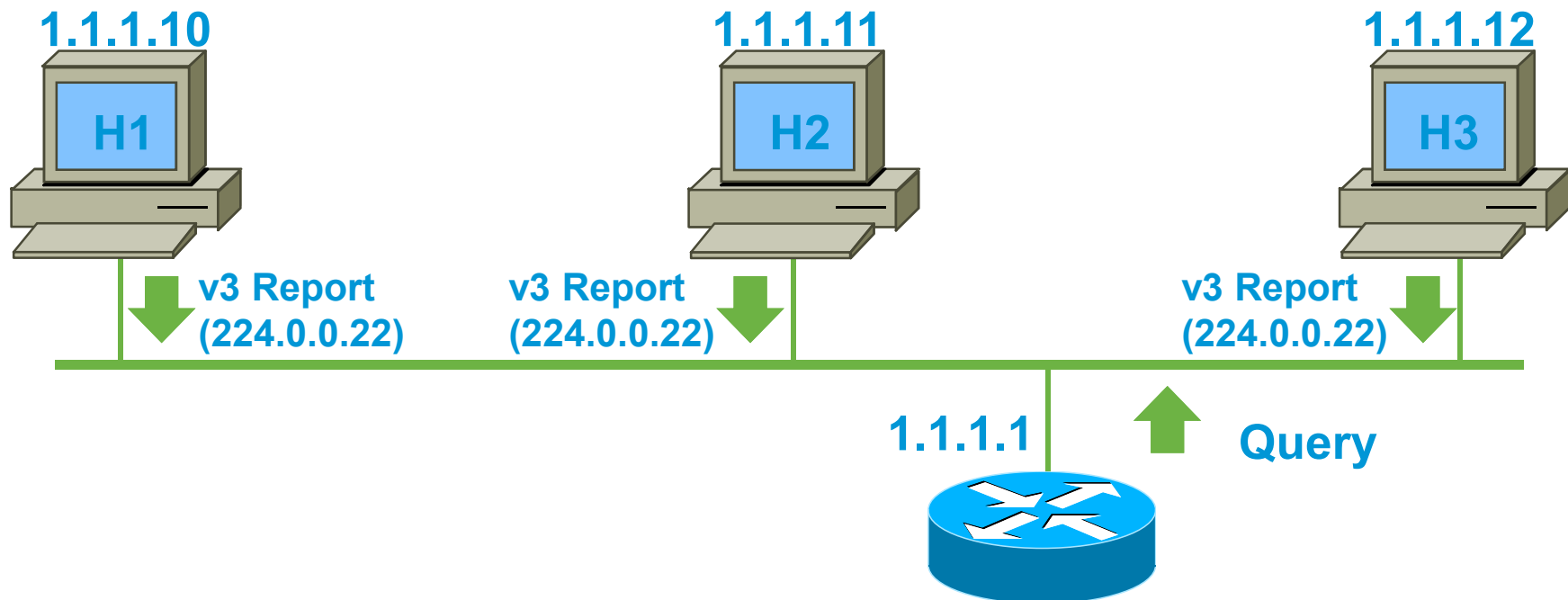
- El miembro envía un “IGMPv3 Report” a la dirección 224.0.0.22 sin esperar un query del router.

# IGMPv3— Uniéndose a fuente(s) específica(s)



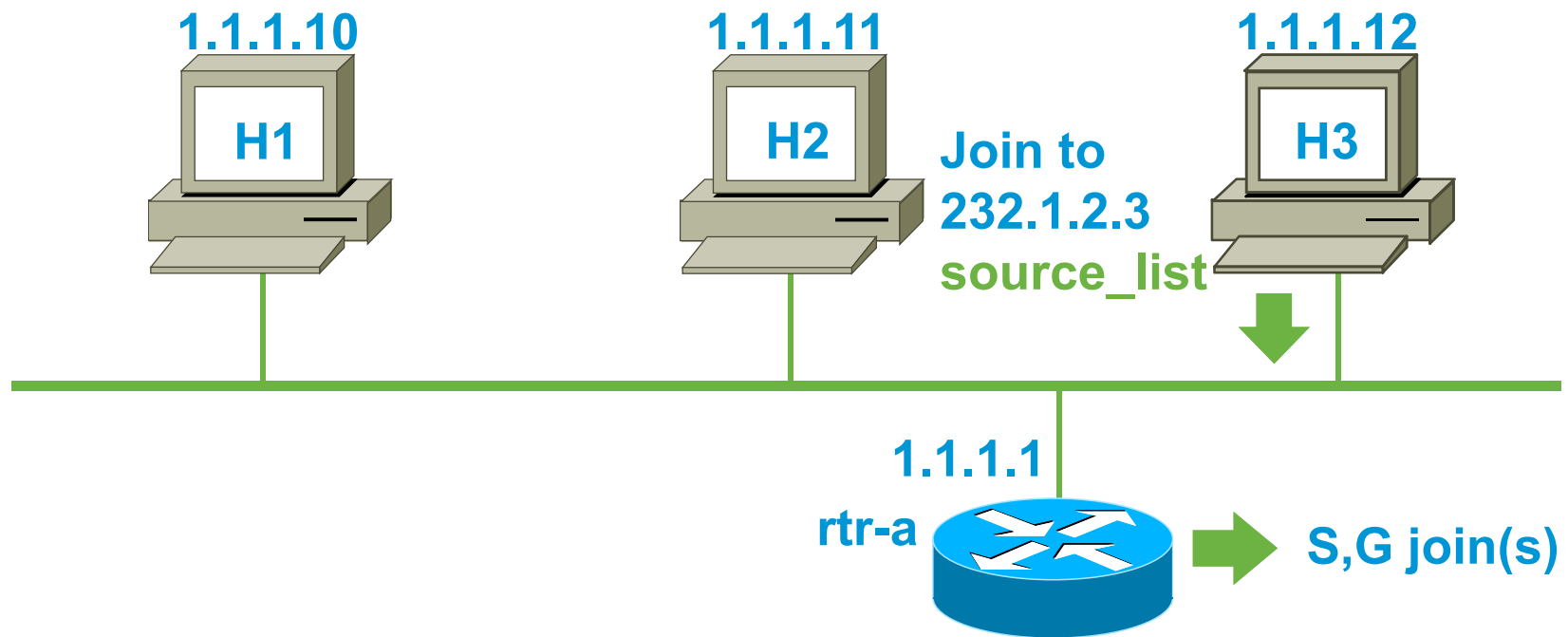
- El “IGMPv3 Report” incluye la fuente deseada dentro de la lista.
- Solamente se unirá a las transmisiones que estén en la “included list”

# IGMPv3—Manteniendo el estado



- Ruteadores envían “Queries” periódicos.
- Todos los miembros de IGMPv3 responderán
  - Los “reports” contienen multiples “Group state Records”.

# IGMPv3

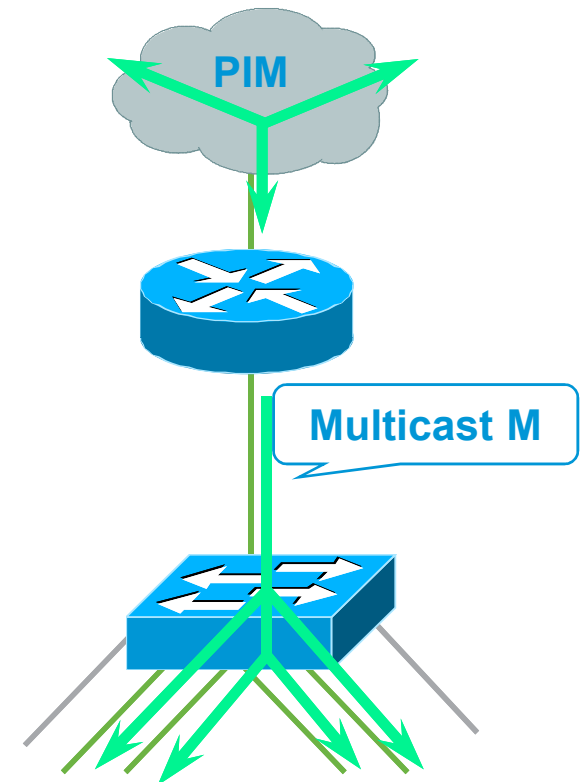


- El host envía un “IGMPv3 join” para el grupo en donde puede especificar la lista de fuentes que quiere incluir.
- Los ruteadores agregan la relación con el grupo “membership”
- El router envía un “(S,G) join” directamente a las fuentes que se tienen en el “source\_list”, ya no es necesario enviar el “(\*,G) join” al RP.

# Multicast Frame Switching en Capa 2

## Problema: Inundación de multicast frames de capa 2

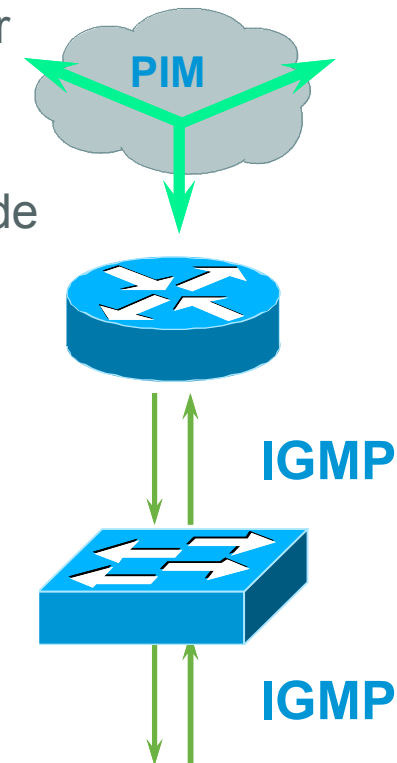
- Típicamente, switches de capa 2 tratan el tráfico de multicast como desconocido o como broadcast y éste es inundado en todos los puertos.
- Entradas estáticas pueden ser algunas veces configuradas para especificar que puertos deben de recibir que grupos de multicast.
- La configuración dinámica de estas entradas disminuiría la carga administrativa.



# Multicast Frame Switching en capa 2

## Solución: IGMPv1-v2 Snooping

- Los switches deben soportar IGMP
- Los paquetes de IGMP son interceptados por el NMP o por ASICs especiales.
  - Requiere de HW especial para mantener el throughput.
- El switch debe de examinar el contenido de los mensajes de IGMP para determinar que puertos quieren qué tráfico.
  - IGMP membership reports
  - IGMP leave messages
- Tiene impacto en switches de capa 2 de baja capacidad.
  - Debe de procesar todos los paquetes de multicast de capa 2.
  - La carga administrativa incrementa con la carga de tráfico de multicast.
  - Puede terminar afectando drásticamente el desempeño del Switch!!!!



# Multicast Frame Switching en capa 2

- Impacto de IGMPv3 en IGMP Snooping

Mensajes de “IGMPv3 Reports” son enviados a un grupo distinto (224.0.0.22)

Switches escuchan solamente este grupo.

Solamente IGMP – no tráfico

*Reduce sustancialmente la carga en el CPU del switch.*

Permite switches de baja capacidad implementar IGMPv3 snooping.

No hay “Report Suppression” en IGMPv3

Habilita el seguimiento individual de cada miembro

IGMPv3 soporta “Includes/Excludes” de fuentes específicas.

Permite que el estado (S,G) sea mantenido por el switch.

Actualmente NO implementado en switches

Puede llegar a ser necesario para tener la funcionalidad completa de IGMPv3

# Resumen —Frame Switches

## IGMP snooping

- Switches que tengan HW/ASICs con visibilidad de capa 3  
Mantiene un alto desempeño con relación al throughput  
Incrementa el costo de los switches
- Switches que no tengan HW/ASICs con visibilidad de capa 3
- Sufren una gran degradación en su desempeño
- NO debería afectar con tal magnitud cuando IGMPv3 es implementado.



# Pregunta 3

**¿Qué temas de multicast te gustaría profundizar?**

- a) Multicast VPN
- b) Multicast LDP
- c) MSDP
- d) Troubleshooting de Multicast
- e) IPv6 Multicast

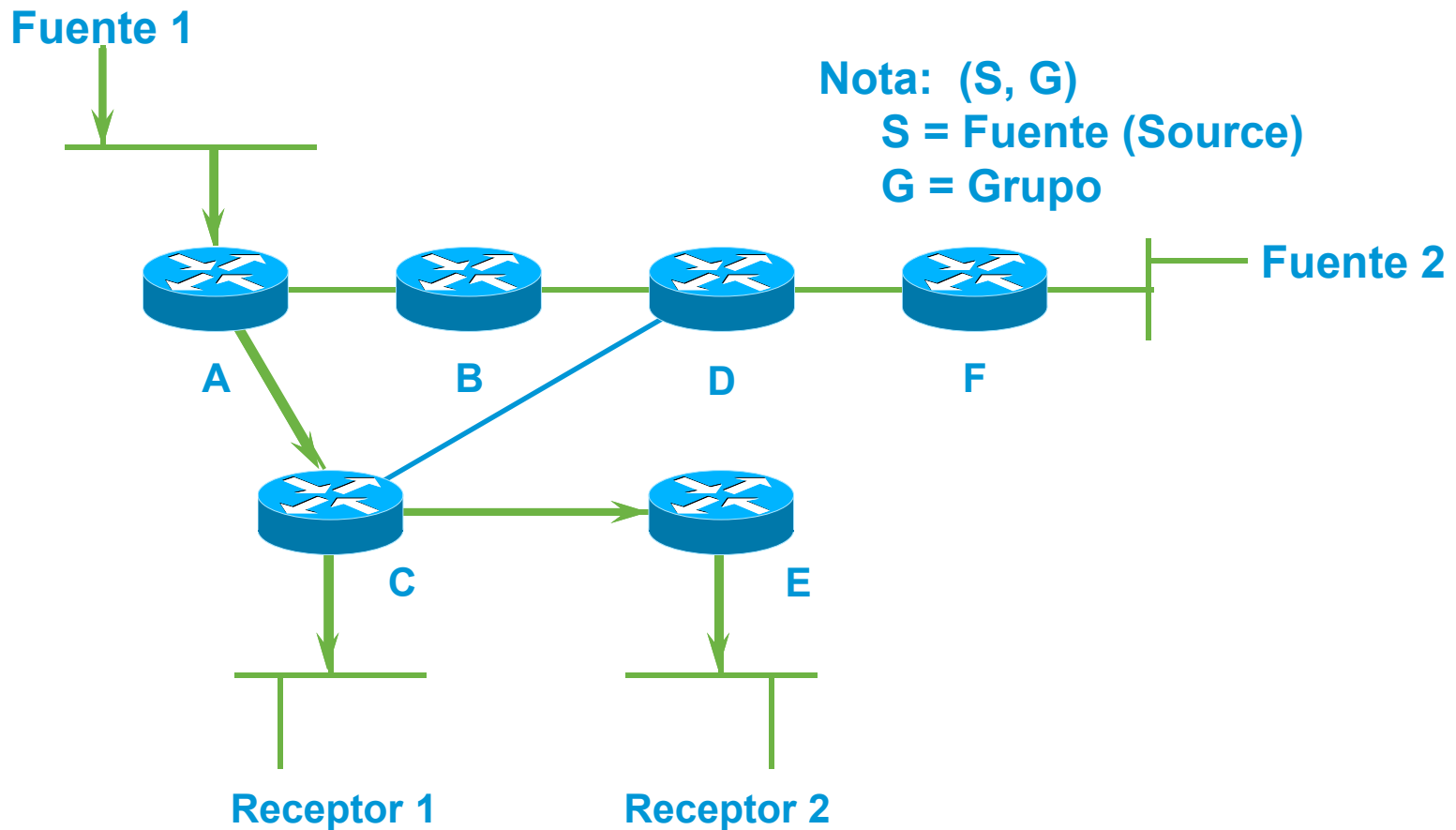
# Agenda

- ¿Por qué Multicast?
- Fundamentos de Multicast
- Multicast en capa 2
- **Multicast intradominio**



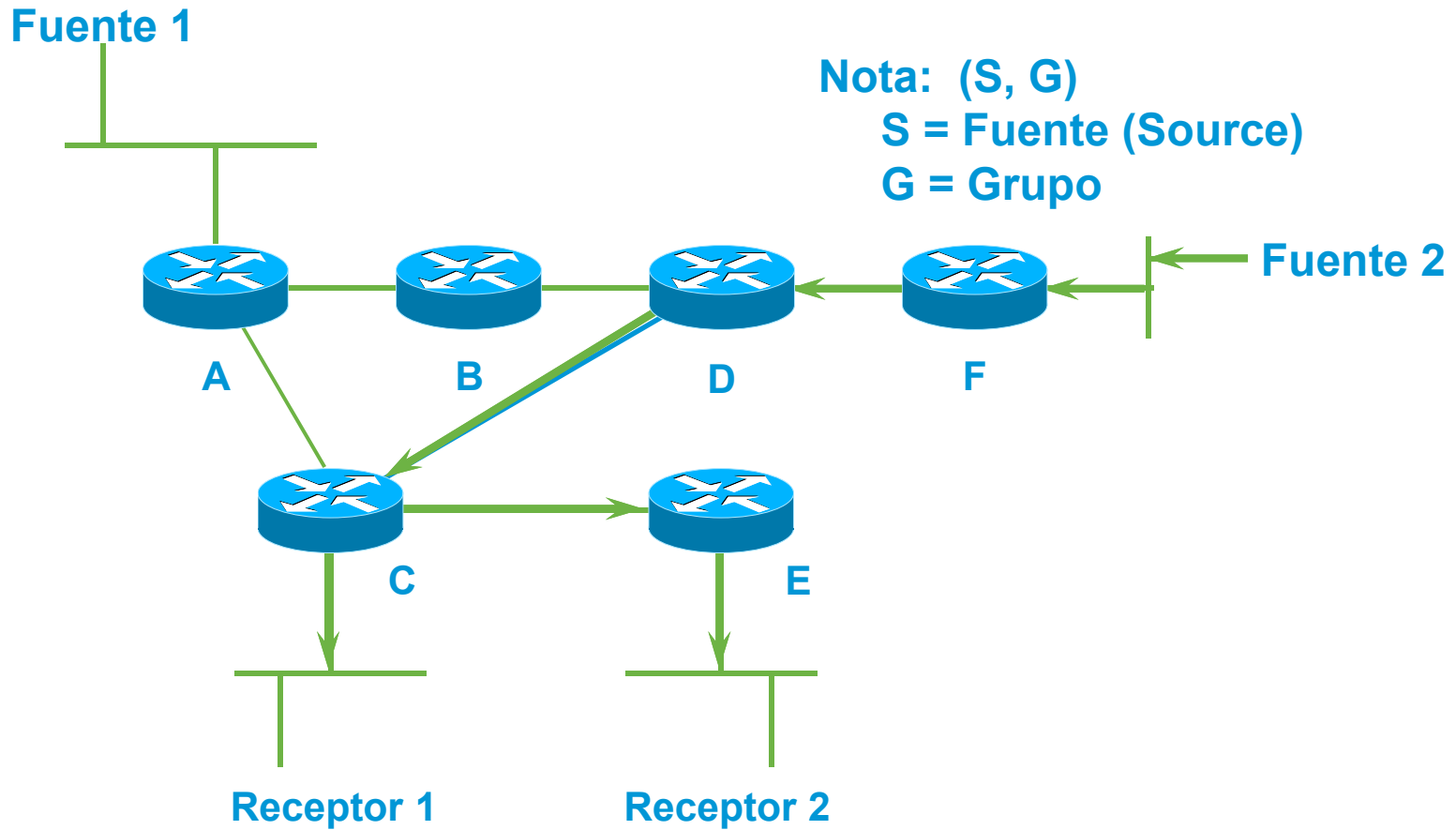
# Multicast Distribution Trees

“Shortest Path” o “Source Distribution Tree”



# Multicast Distribution Trees

## “Shortest Path o Source Distribution Tree”



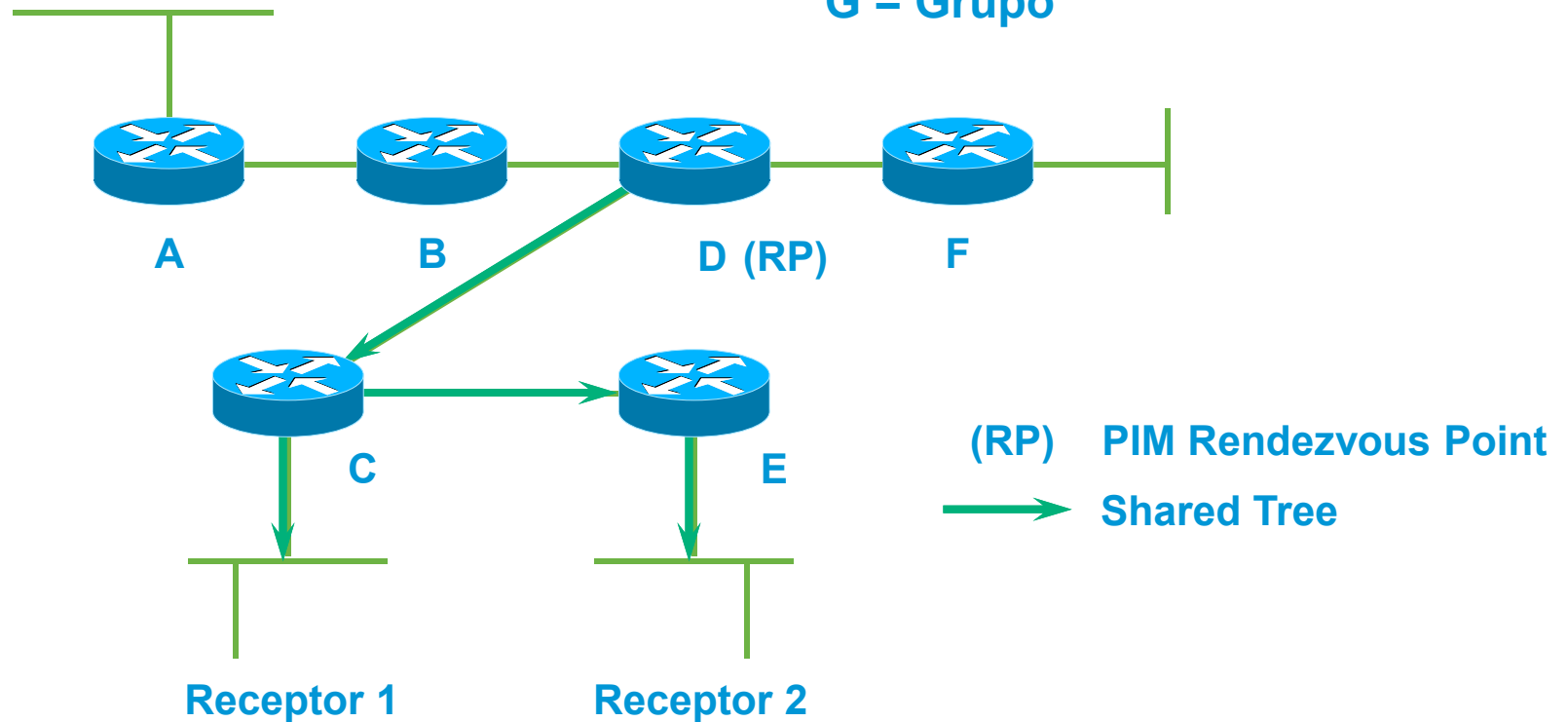
# Multicast Distribution Trees

## Shared Distribution Tree

Nota: (\*, G)

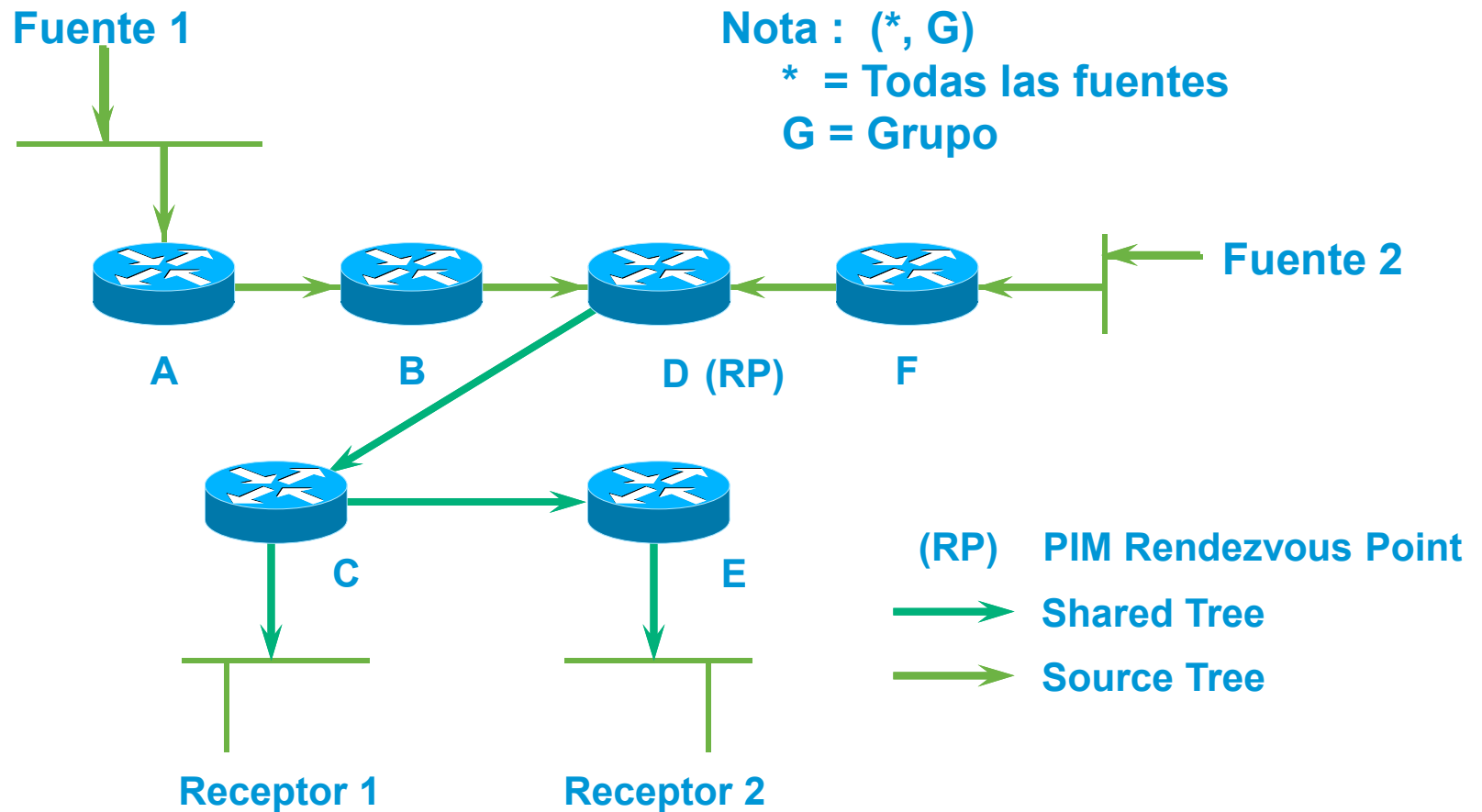
\* = Todas las fuentes

G = Grupo



# Multicast Distribution Trees

## Shared Distribution Tree



# Multicast Distribution Trees

## Características de los “Distribution Trees”

- **Source o Shortest Path trees**

Utilizan más memoria (S, G) pero dan trayectorías óptimas de la fuente a sus receptores minimizando el retraso.

- **Shared trees**

Utilizan menos memoria (\*, G) pero obtienen trayectorias subóptimas de la fuente a los receptores pudiendo introducir retraso adicional a la transmisión.

# Conmutación de Multicast

- El ruteo de tráfico multicast es al revez de como se rutea el tráfico unicast.

El ruteo de tráfico unicast está enfocado a dónde el paquete va.

El ruteo de tráfico multicast está enfocado de donde viene el paquete.

- El ruteo de Multicast utiliza “Reverse Path Forwarding”



# Conmutación de Multicast

## Reverse Path Forwarding (RPF)

- **¿Qué es RPF?**

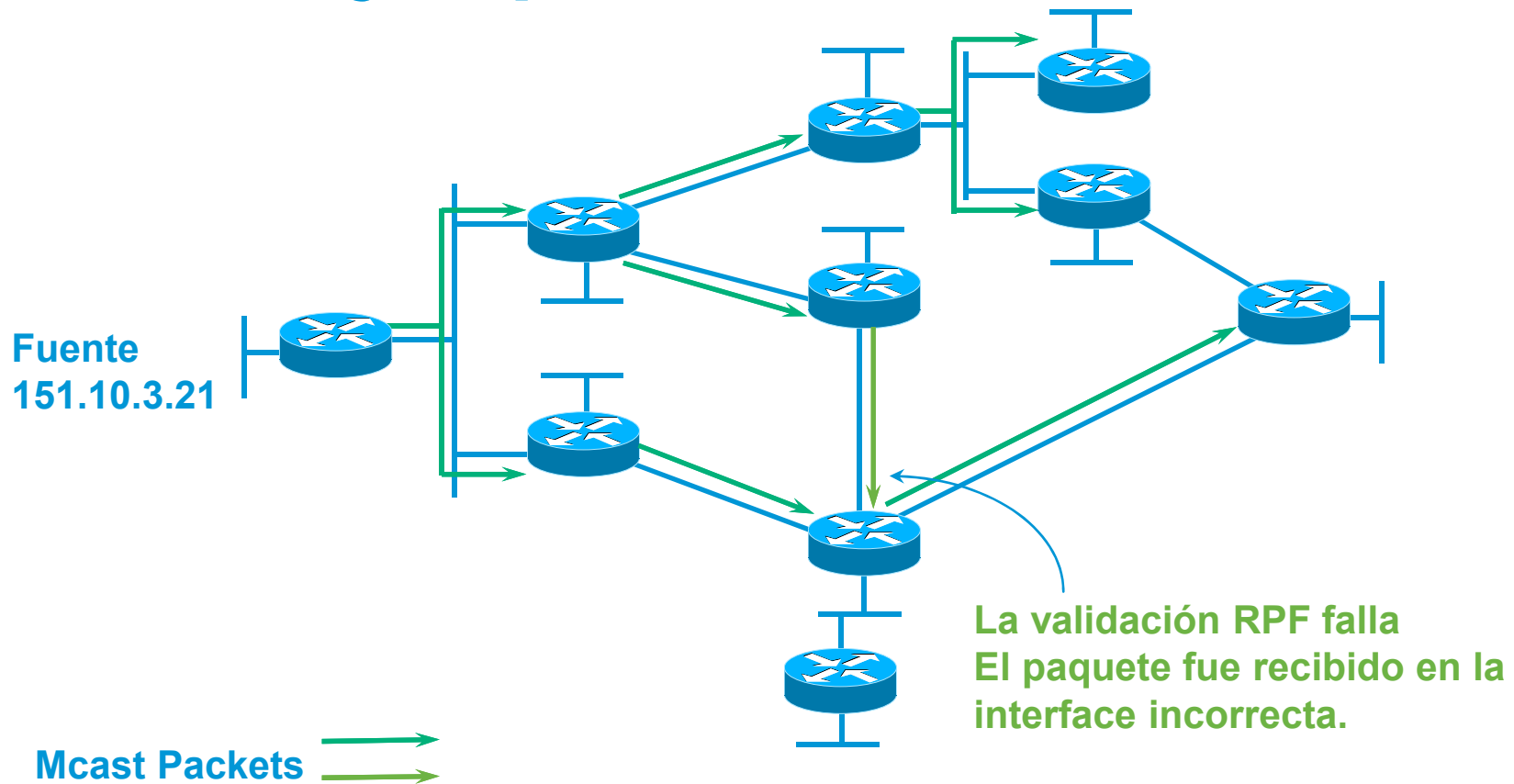
Un router conmuta un paquete de multicast solamente si fue recibido por la interface que ve a la fuente. (ejemplo: sigue al “distribution tree”).

- **La validación de “RPF”**

- La tabla de ruteo es utilizada para hacer la validación sobre la dirección fuente del paquete.
- Si el paquete se recibió en la interface que indica la tabla de ruteo de cómo llegar a la fuente, entonces la validación de RPF es exitosa.
- De no ser así, la validación de RPF falla y el paquete se tira.

# Conmutación de Multicast

## Ejemplo: Validación RPF



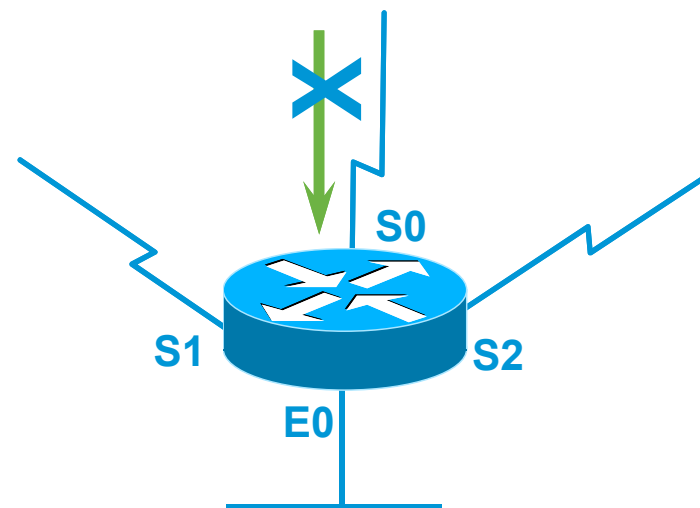
# Conmutación de Multicast

## Visto de Cerca: Validación RPF falla

Paquete de multicast de la fuente  
151.10.3.21

Validación RPF falla

Tabla de Ruteo Unicast	
Red	Interface
151.10.0.0/16	<b>S1</b>
198.14.32.0/24	S0
204.1.16.0/24	E0

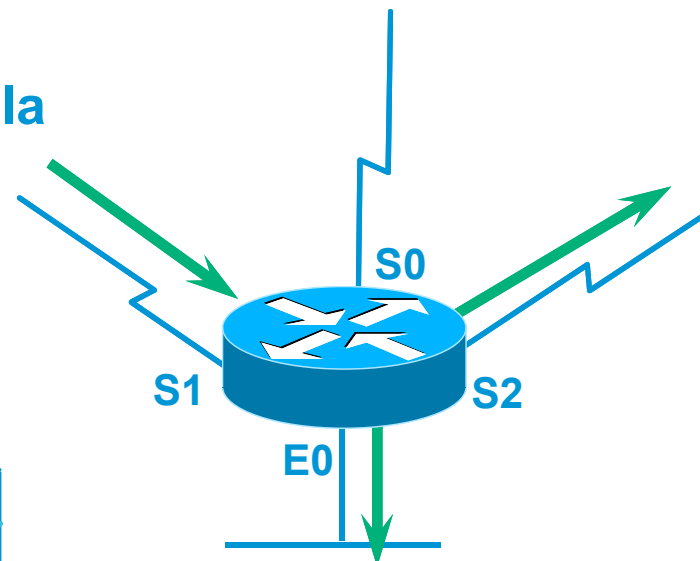


El paquete llegó por la interface incorrecta  
Por lo tanto el paquete se descarta

# Conmutación de Multicast

## Visto de Cerca: Validación RPF exitosa

Paquete multicast de la fuente 151.10.3.21



RPF Check Succeeds!

Tabla de Ruteo Unicast	
Network	Interface
151.10.0.0/16	<b>S1</b>
198.14.32.0/24	S0
204.1.16.0/24	E0

El paquete es recibido por la interface correcta

El paquete se conmutará a todas las interfaces de mi OIL.

(Ej. Hacia el “distribution tree”)

# Tipos de protocolos de Multicast

- Dense-mode
  - Utiliza un modelo “Push”
  - El tráfico es inundado (Flooded) a toda la red.
  - Es cortado (pruned) en donde no se quiere
  - Tiene un comportamiento de Flood & Prune (típicamente cada 3 minutos)
- Sparse-mode
  - Utiliza un modelo “Pull”
  - El tráfico es enviado solamente donde es solicitado.
  - Comportamiento de “Joins” explícitos.

# Protocolo Multicast

- Protocolos de ruteo multicast más comunes
  - ✓ PIM-Dense Mode
  - ✓ PIM-Sparse Mode
  - ✓ PIM-Source Specific Multicast
  - ✓ Bidirectional PIM
  - ✓ Others (DVMRP, MOSPF, etc.)

# PIM-DM

- Protocol Independent

Soporta todos los protocolos de ruteo unicast incluyendo: rutas estáticas, RIP, IGRP, EIGRP, ISIS, BGP y OSPF

- Utiliza “reverse path forwarding”

**Inunda** la red y **corta** el tráfico basado en los miembros de grupos de multicast.

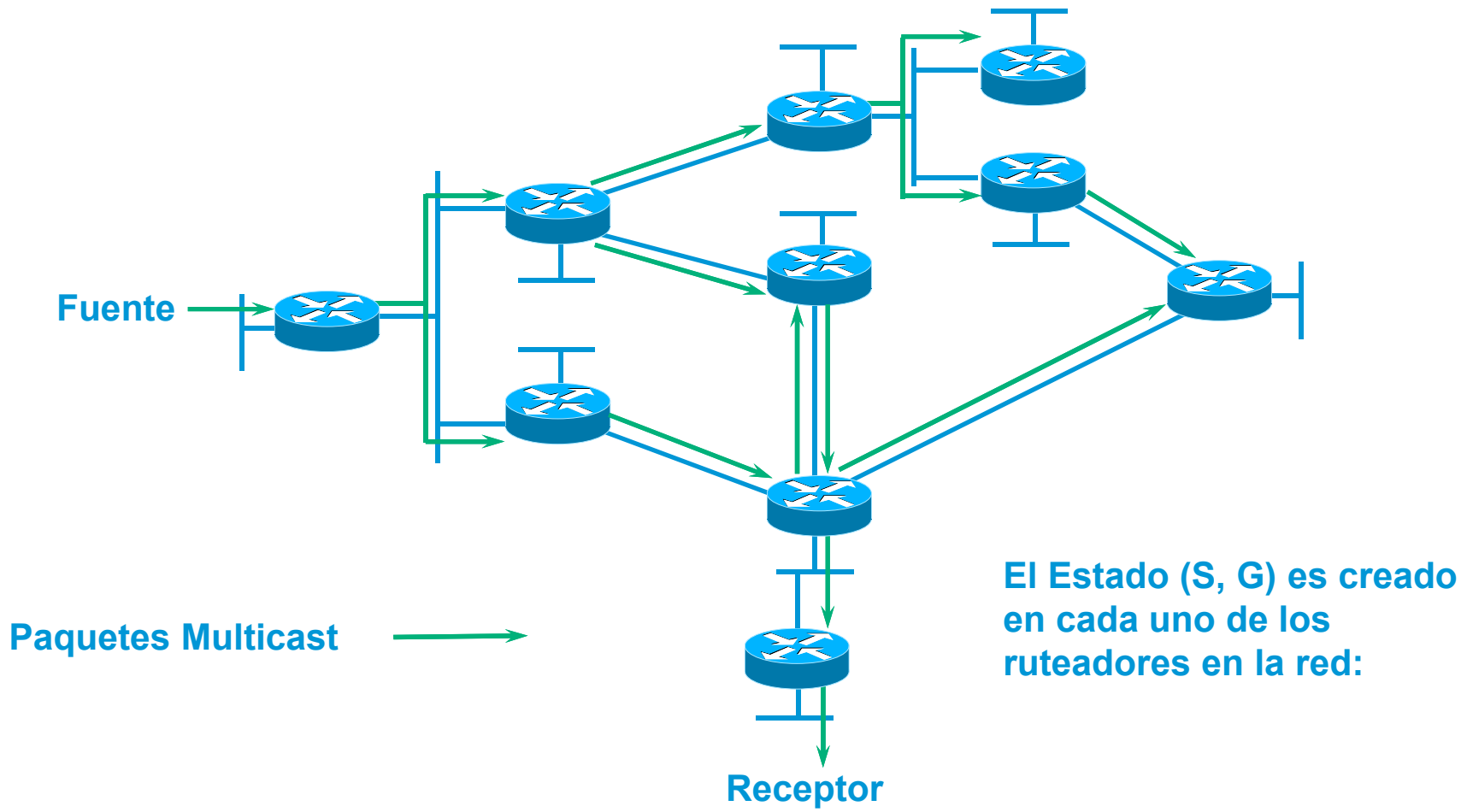
Mecanismo de “Assert” es utilizado para cortar (prune) flujos redundantes.

- Apropiado para

Pequeñas implementaciones y redes piloto

# PIM-DM Flood y Prune

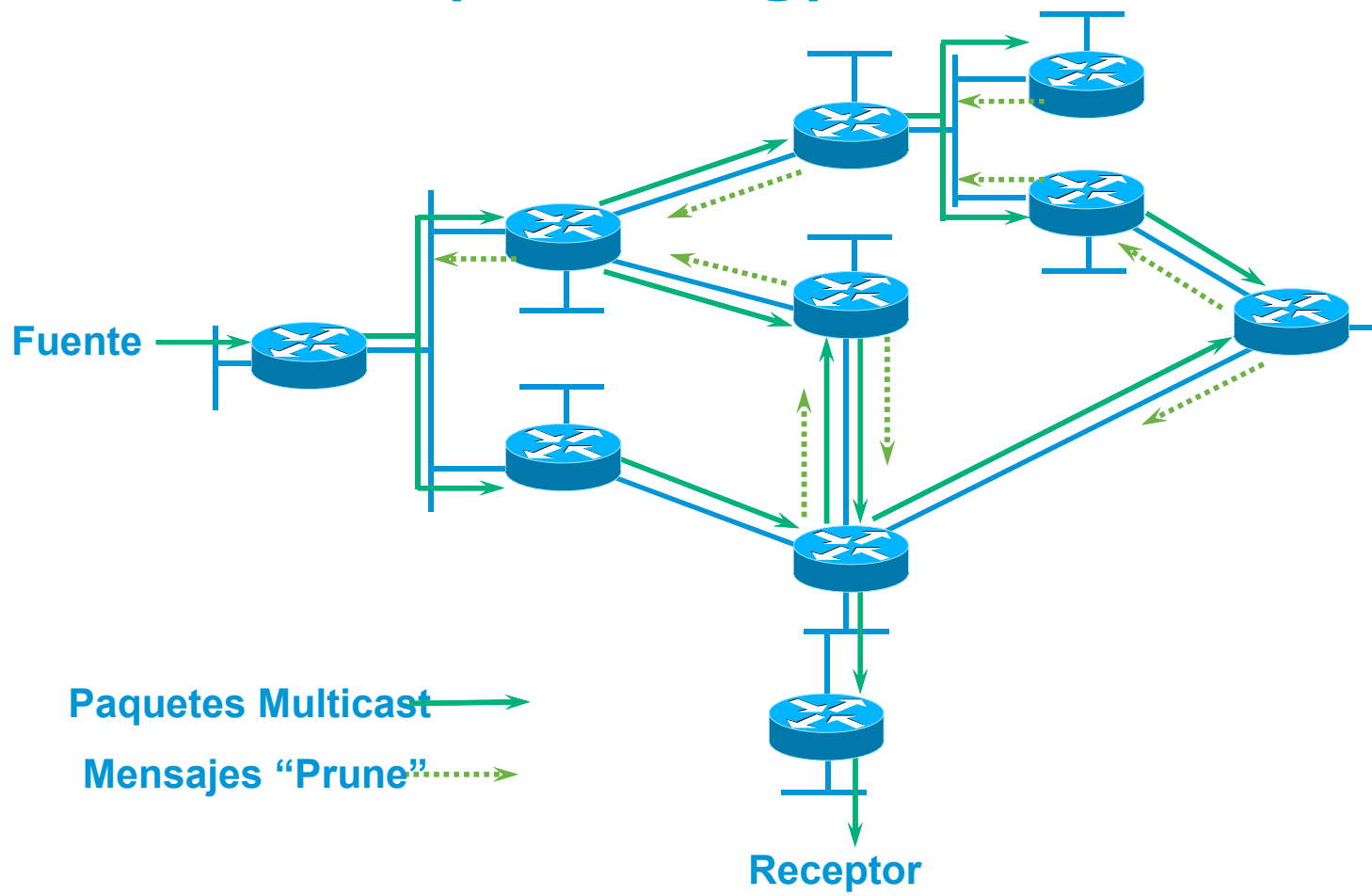
## Flooding Inicial





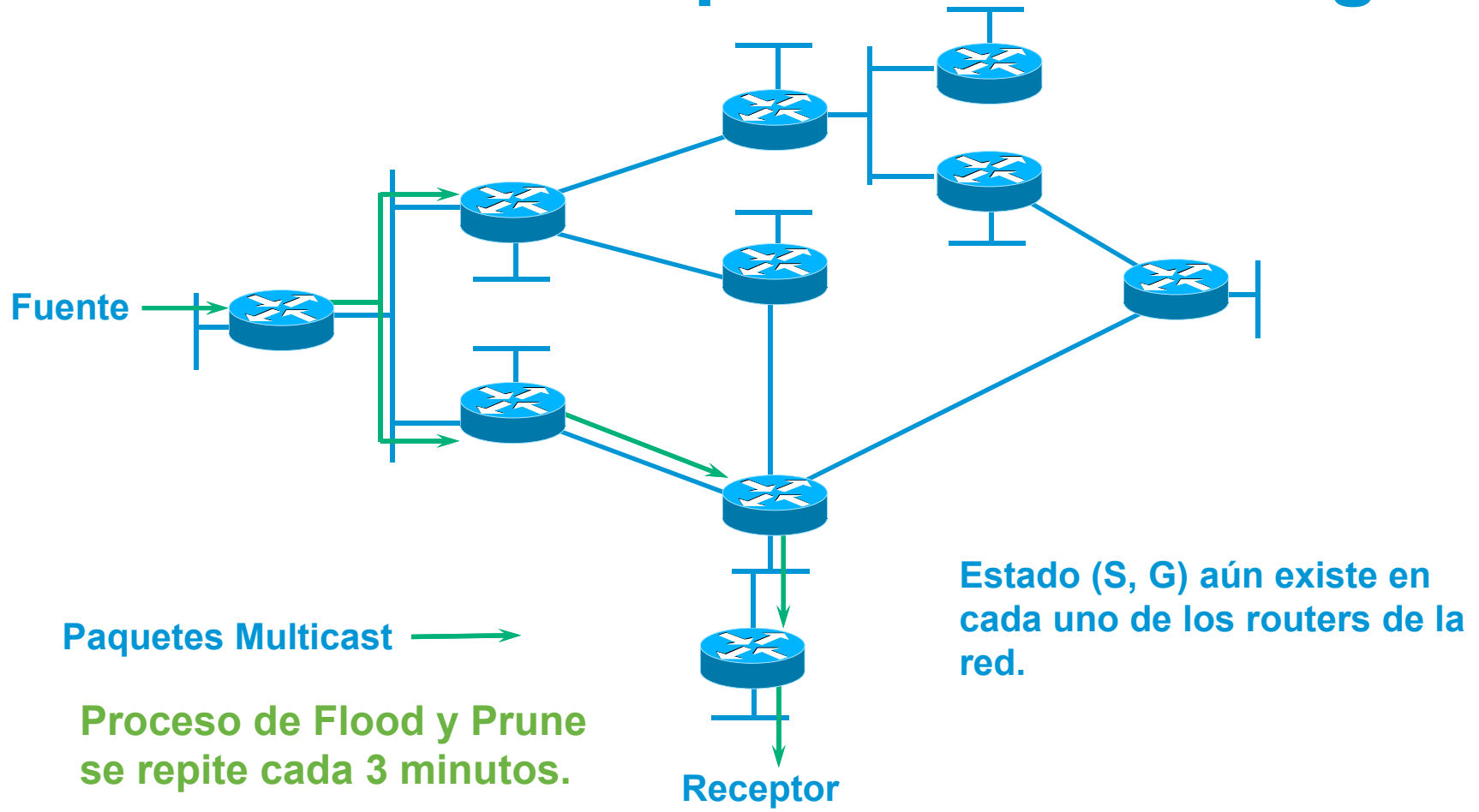
# PIM-DM Flood y Prune

## Cortando (Pruning) Tráfico no deseado



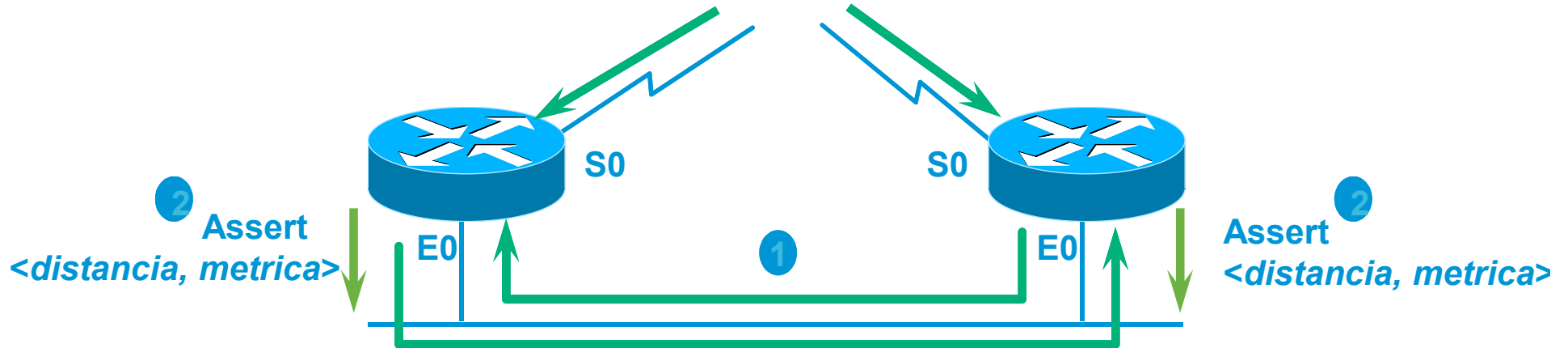
# PIM-DM Flood y Prune

## Resultados después de “Pruning”



# PIM-DM Mecanismo de “Assert”

Paquetes Multicast de Entrada  
(Validación de RPF Existosa)



- 1 Si los Ruteadores reciben paquetes en una interface que está en el OIList:  
Solamente un ruteador deberá enviar los paquetes para evitar paquetes duplicados
- 2 Los ruteadores envían mensajes “PIM Assert”  
Se compara la distancia y valores de métrica  
El ruteador con mejor ruta a la fuente gana  
Si la métrica y la distancia son iguales, la dirección más alta gana.  
El ruteadore que pierde, deja de enviar tráfico (Hace un “prune” de la int)

# PIM-DM — Evaluación

- Efectivo en redes pequeñas piloto
- Ventajas:
  - Fácil de configurar – dos comandos
  - Mecanismo sencillo de Inundación y corte (Flood y Prune)
- Problemas potenciales
  - Mecanismo de “Flood y Prune” ineficiente
  - El mecanismo de “Assert” es complejo
  - Hay una combinación del plano de control y el plano de datos. Resulta en tener una tabla de estados (S, G) en cada uno de los routers de la red.  
Puede resultar comportamientos topológicos no determinísticos
  - No soporta “shared trees”

# PIM-SM (RFC 2362)

- Soporta “Source y shared trees”

Asume que ningún “host” quiere tráfico multicast a menos que se solicite específicamente.

- Utiliza un **Rendezvous Point (RP)**

Las fuentes y receptores se unen en el RP para saber la existencia de uno y otro.

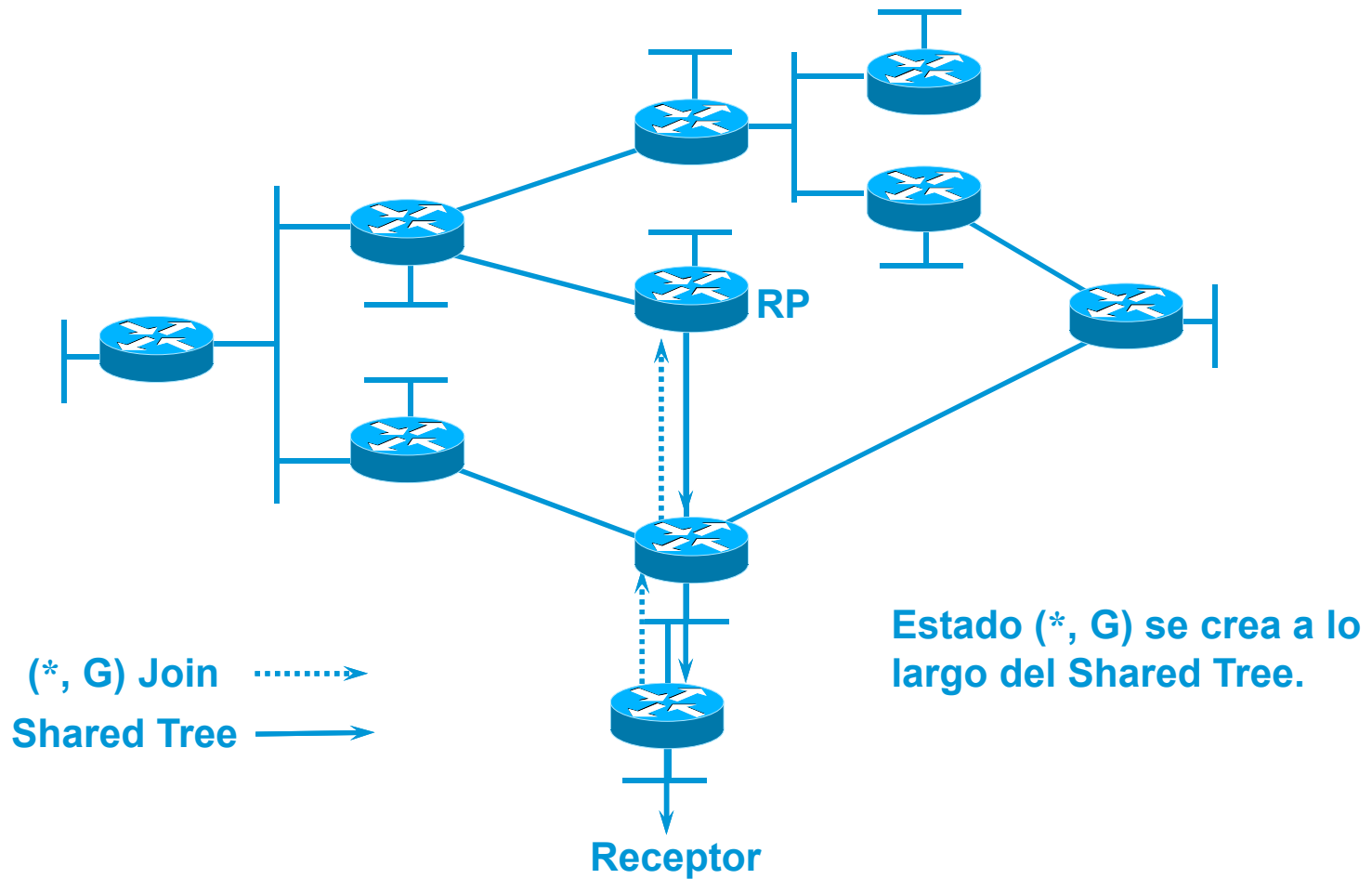
Las fuentes se registran con el RP a través de su ruteador directamente conectado.

Los receptores se unen al “shared tree” a través de su ruteador designado (DR)

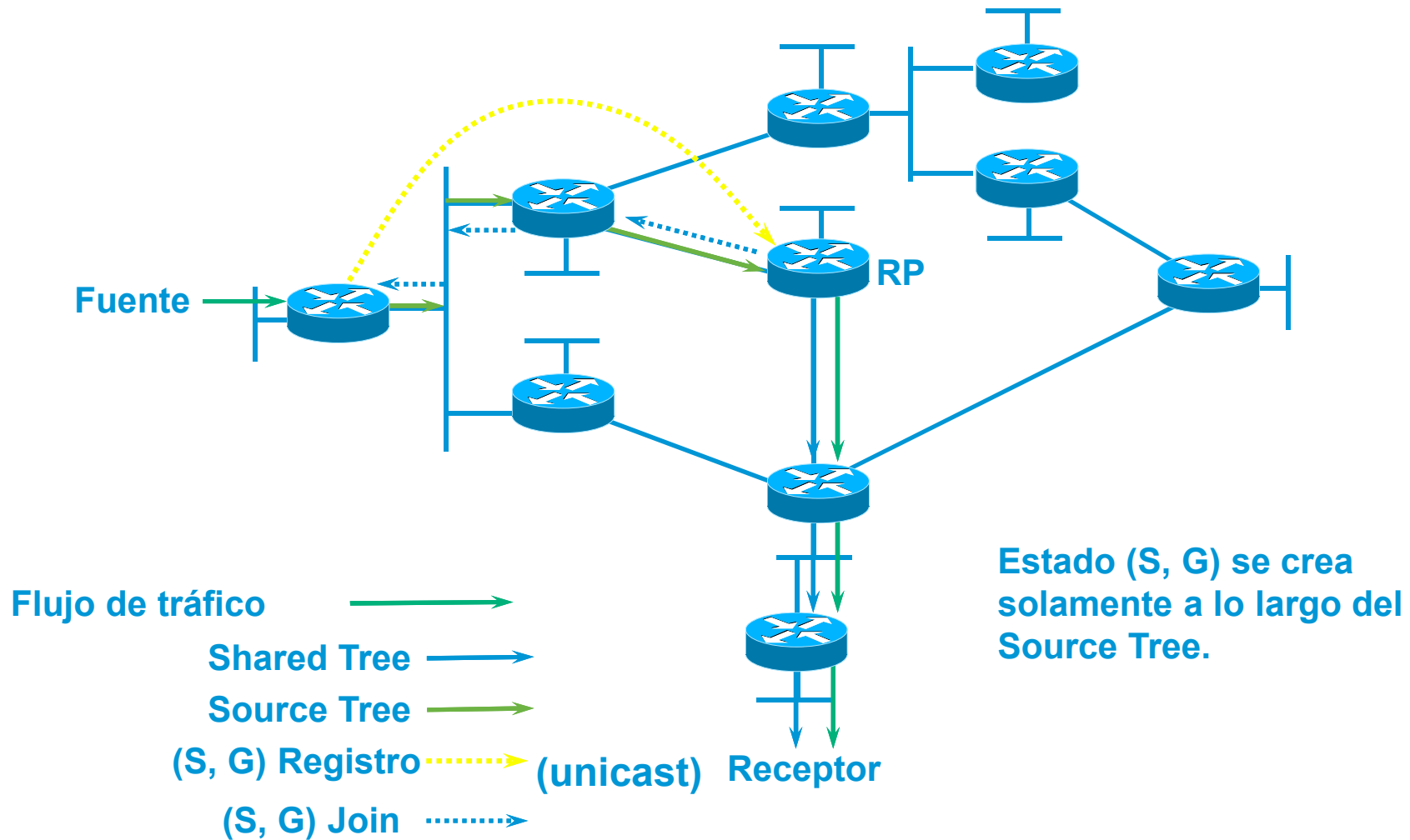
- Apropiado en:

- ✓ Implementaciones grandes tanto para grupos con una densidad alta de usuarios o grupos esparcidos dentro de la red.
- ✓ Es la elección óptima para todas las redes en producción sin importar el tamaño y número de miembros.

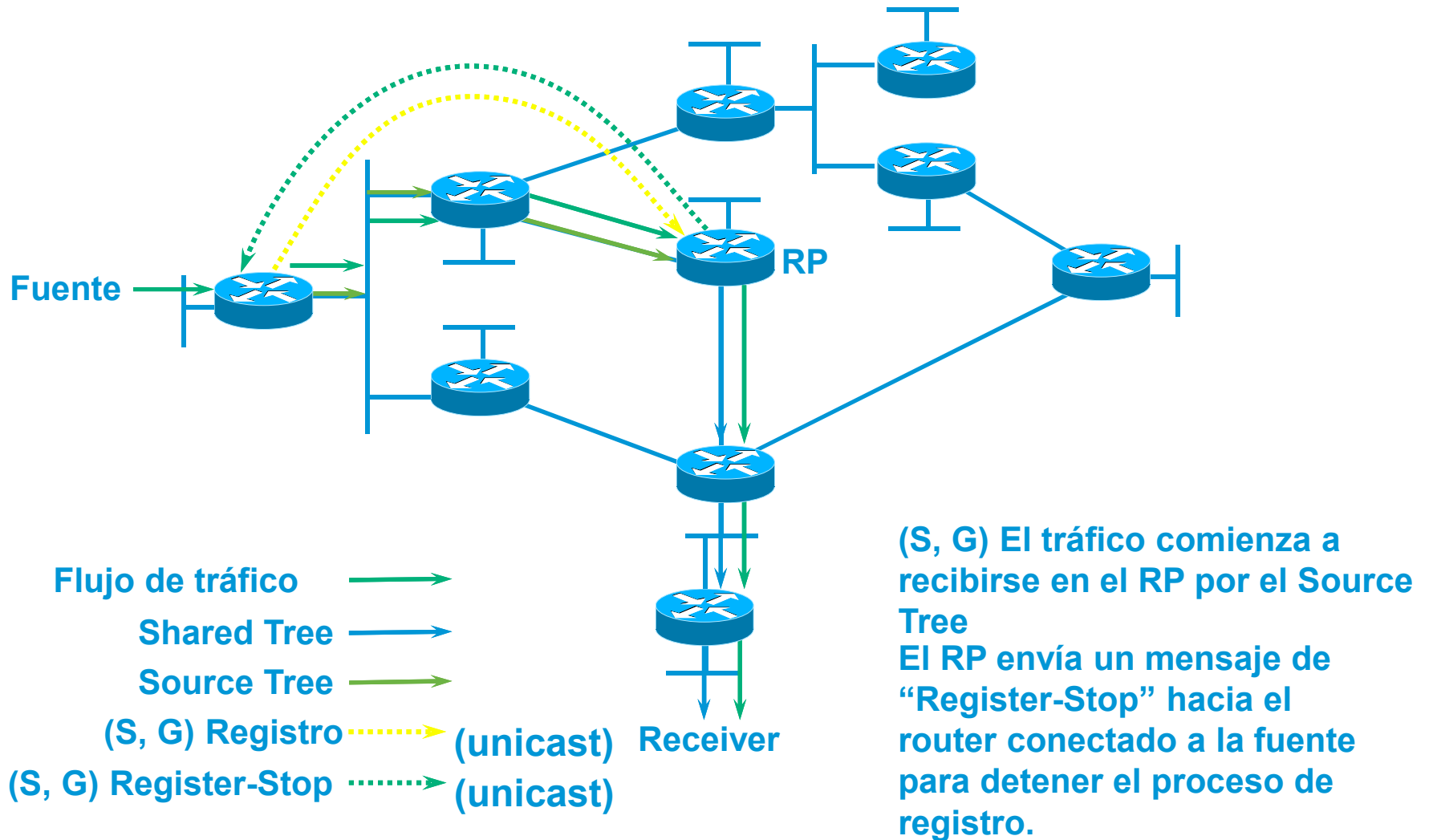
# PIM-SM Shared Tree Join



# PIM-SM Registro de la Fuente

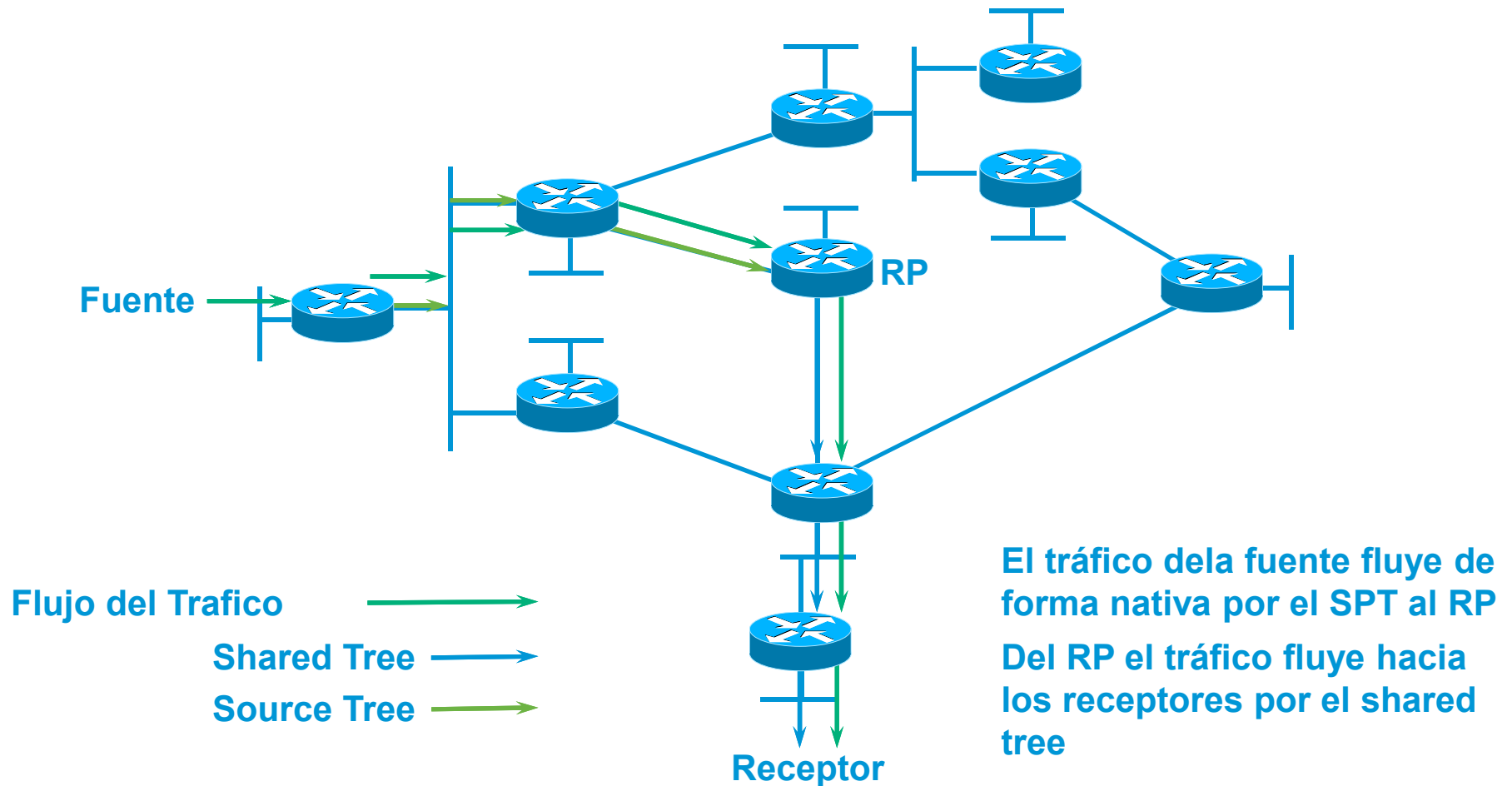


# PIM-SM Registro de la fuente

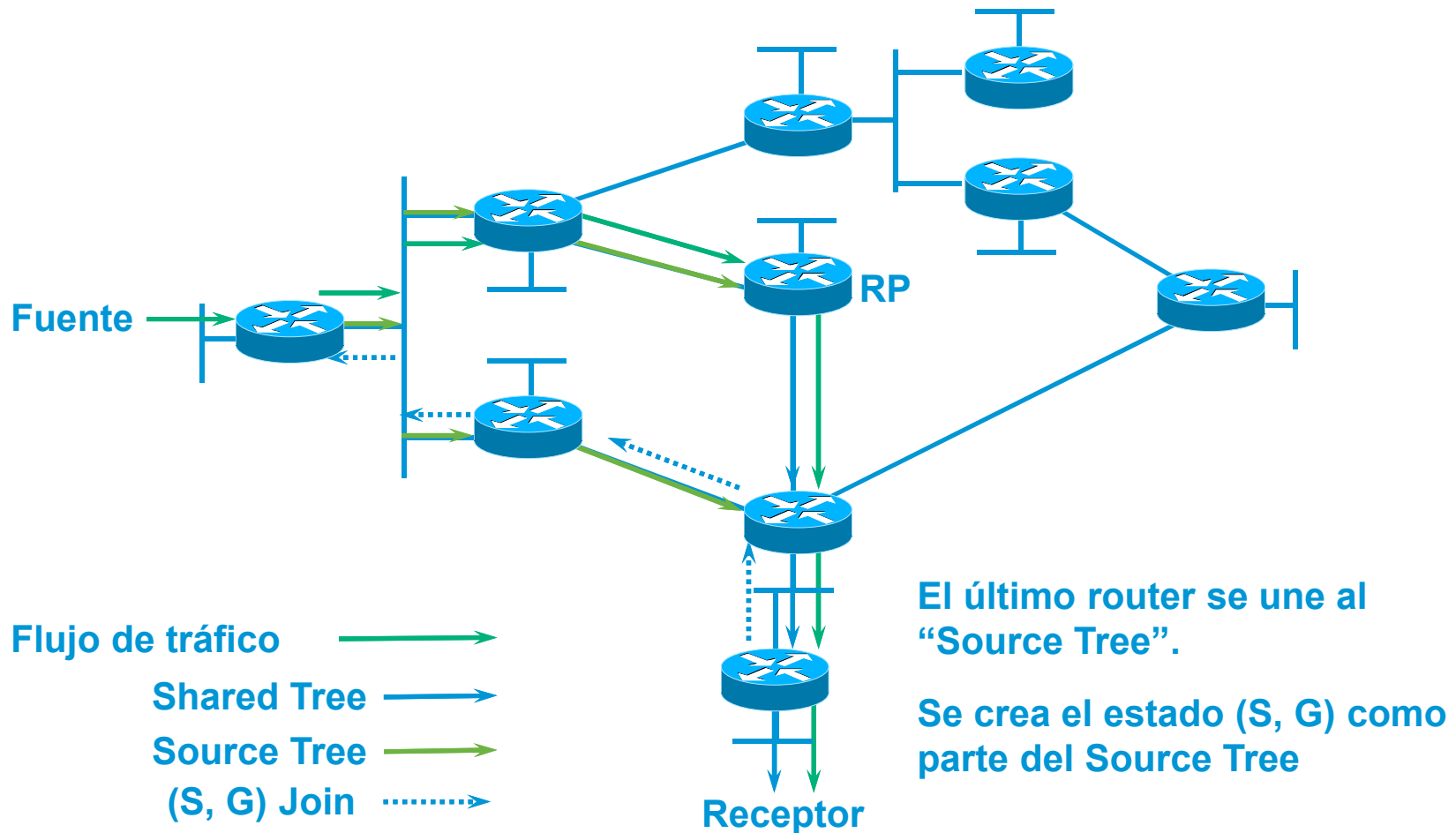




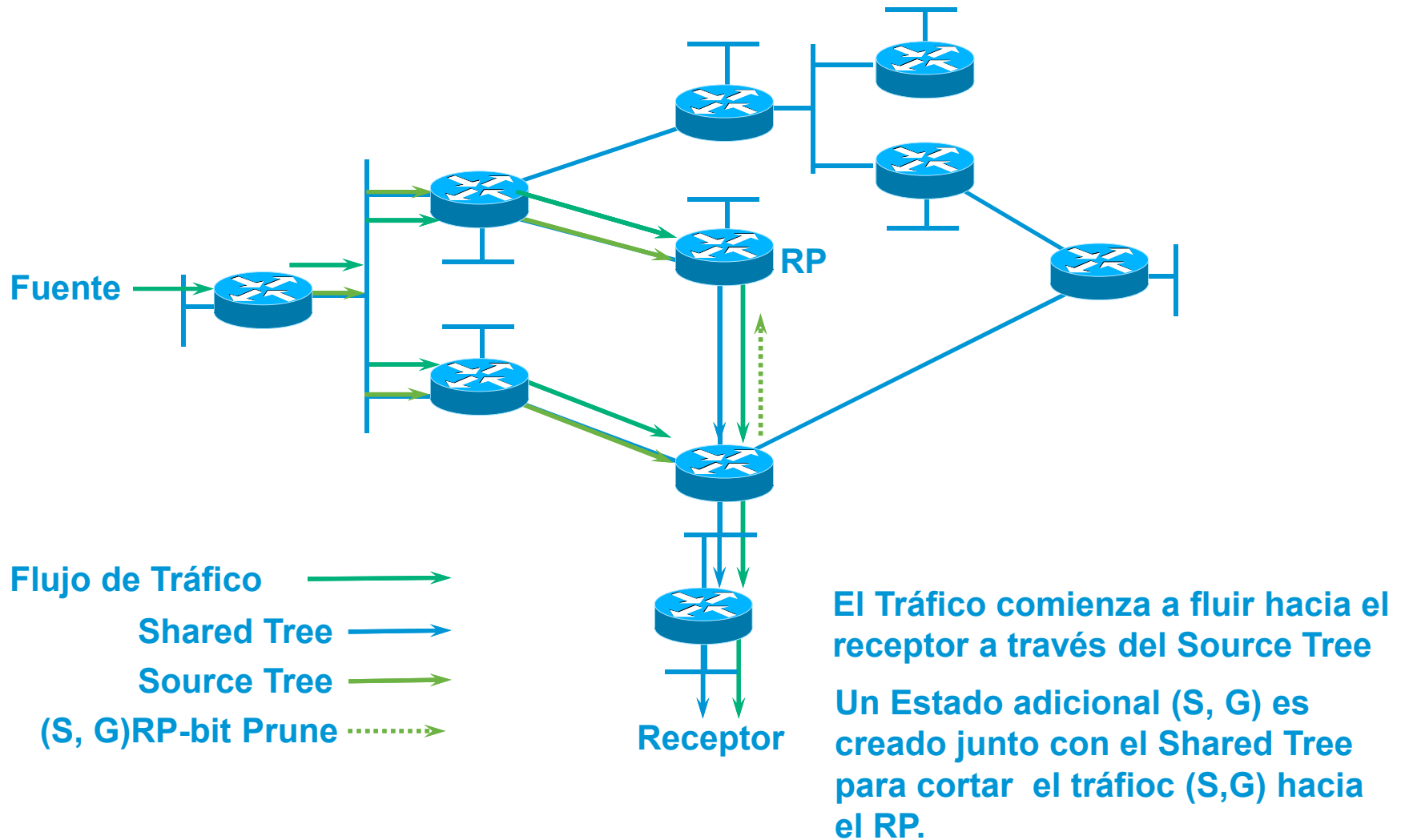
# PIM-SM Registro de la Fuente



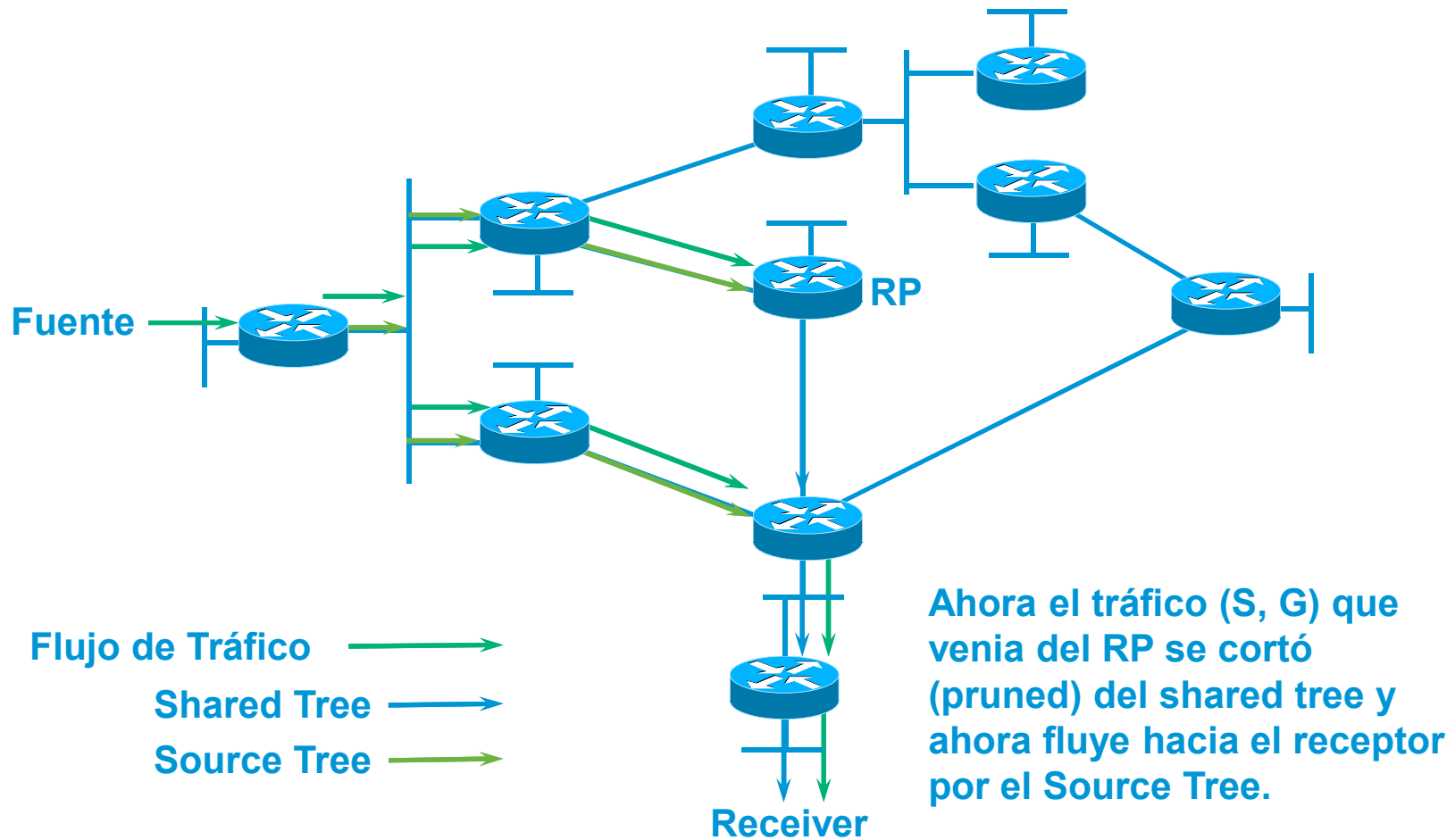
# PIM-SM SPT Switchover



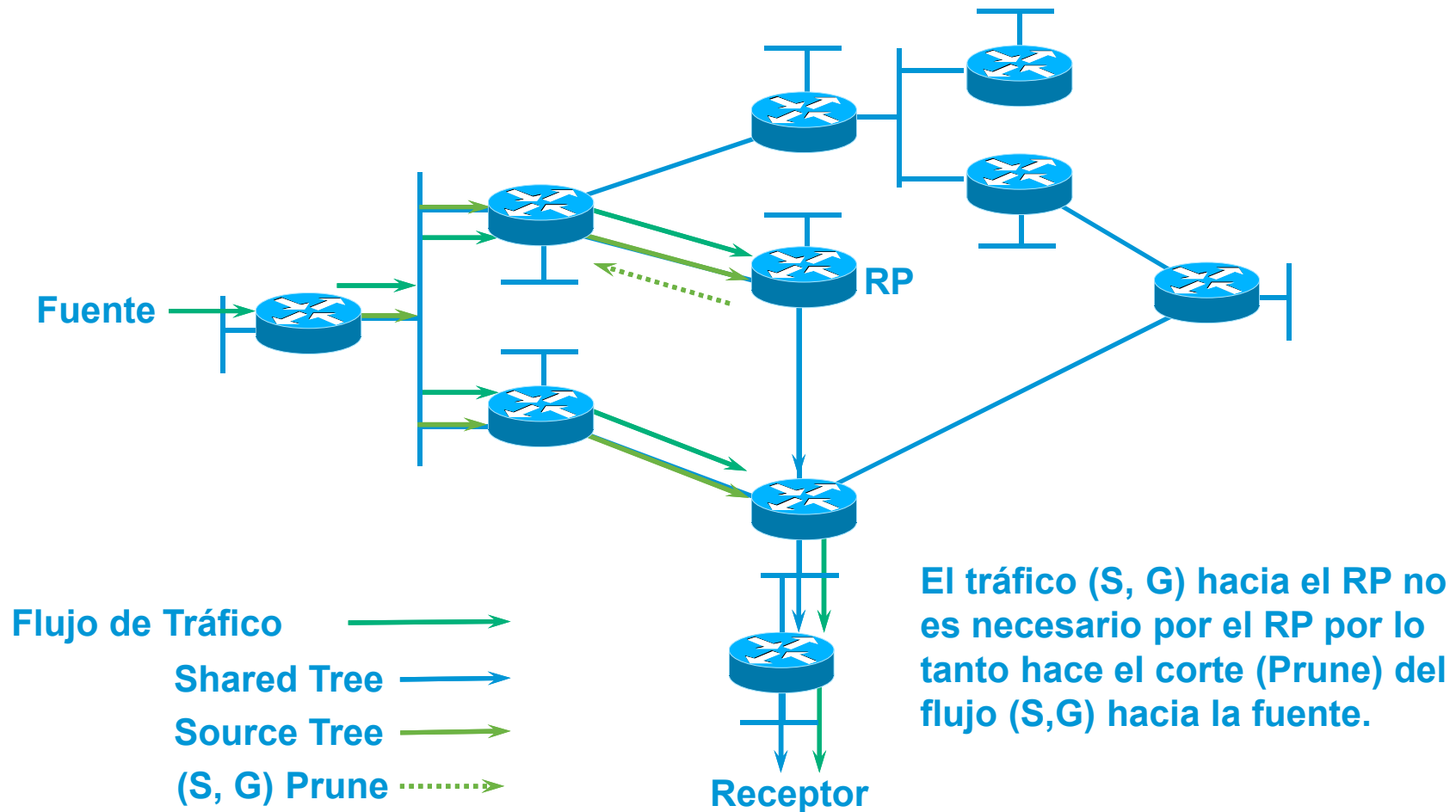
# PIM-SM SPT Switchover



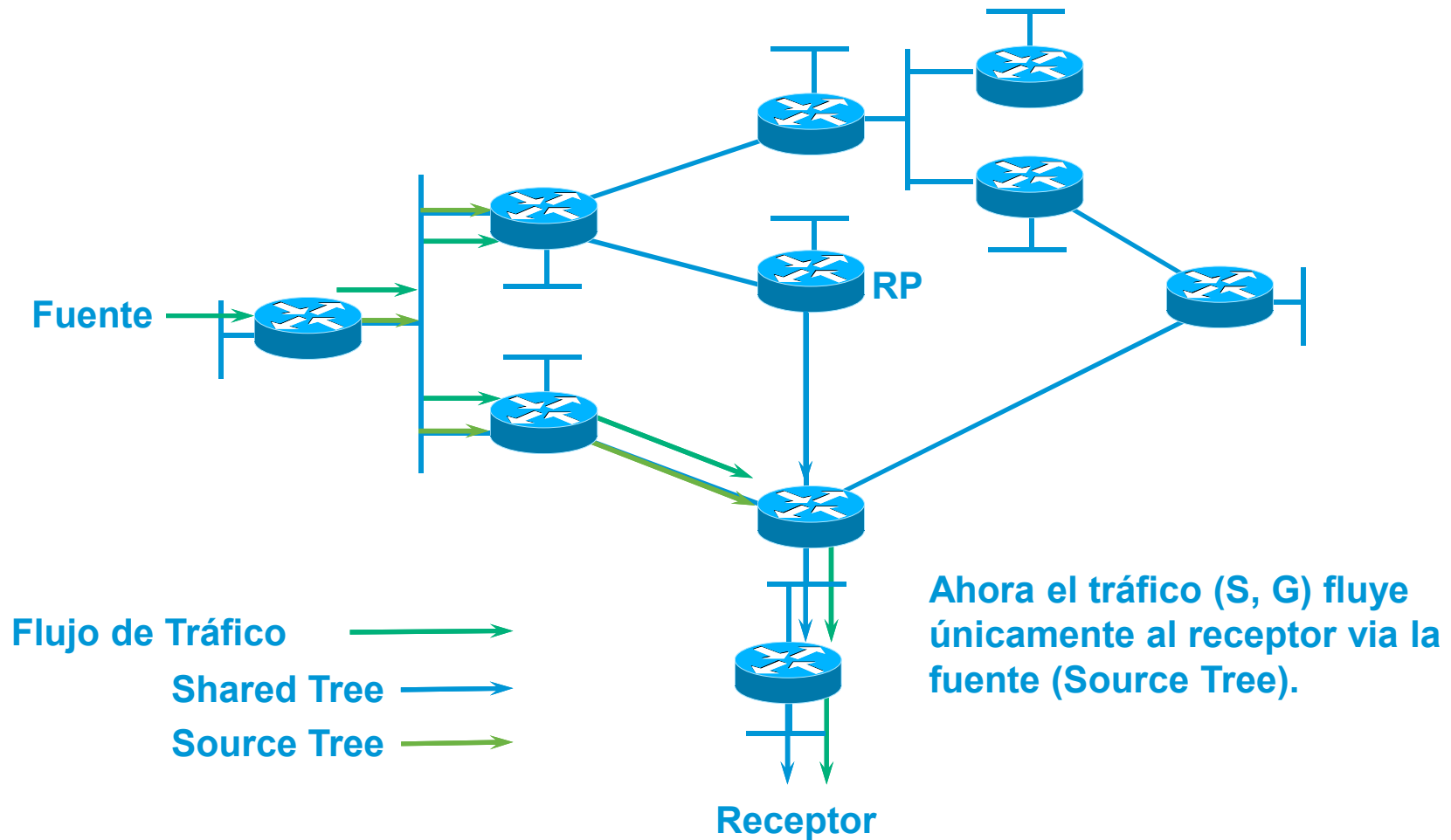
# PIM-SM SPT Switchover



# PIM-SM SPT Switchover



# PIM-SM SPT Switchover



# PIM-SM

## *PIM-SM Hecho Frecuentemente Olvidado*

---

El comportamiento de *defecto* de PIM-SM en el IOS de Cisco, es que los ruteadores con miembros directamente conectados se unirán al Shortest Path Tree tan pronto detecten una nueva fuente.

---

# PIM-SM—Evaluación

- Efectivo para redes con una distribución esparcida o densa de receptores de multicast.

- Ventajas:

El tráfico es únicamente enviado a hosts que hayan decidido unirse “joined”.

Puede conmutar de forma óptima y dinámica al “source-tree” para fuentes con carga alta de tráfico.

Independiente al protocolo de ruteo utilizado en unicast.

Es la base para ruteo multicast interdominio

Cuando se utiliza con MPBGP y MSDP



# Problema en los estados Many-to-Many

- Crea un número alto de estados (S,G)

El mantenimiento de estado se dispara.

Un número alto de OILs pueden empeorar el problema.

El desempeño de los ruteadores comienzan a sufrir.

- Utilizando solamente Shared-Trees

Permite disminuir algunos estados (S,G)

Resulta en un estado (S,G) junto con el SPT hacia el RP

Frecuentemente de cualquier forma se tienen muchos estados (S,G)

Se necesitaría una solución que solamente utilice estados (\*,G)

# Eliminando el estado (S,G)

- Shared-Trees bidireccionales

Permite a la información viajar hacia el “Shared Tree”

El tráfico de la fuente sigue al “shared tree” para llegar al RP y a todos los receptores en el “shared tree”

No puede utilizar las reglas actuales de RPF para (\*,G)

Se debe tener cuidado para evitar loops de multicast

Requiere un “Designated Forwarder (DF)”

Es el responsable de enviar el tráfico hacia el “shared tree”

El “DF” aceptará tráfico en las interfaces que estén en su OIL.

Después lo enivará en todas sus otras interfaces (Incluyendo la IIF)



# Bidirectional (Bidir) PIM

- Idea:

Utiliza el mismo árbol de las fuentes hacia el RP y del RP hacia los receptores.

- Beneficios:

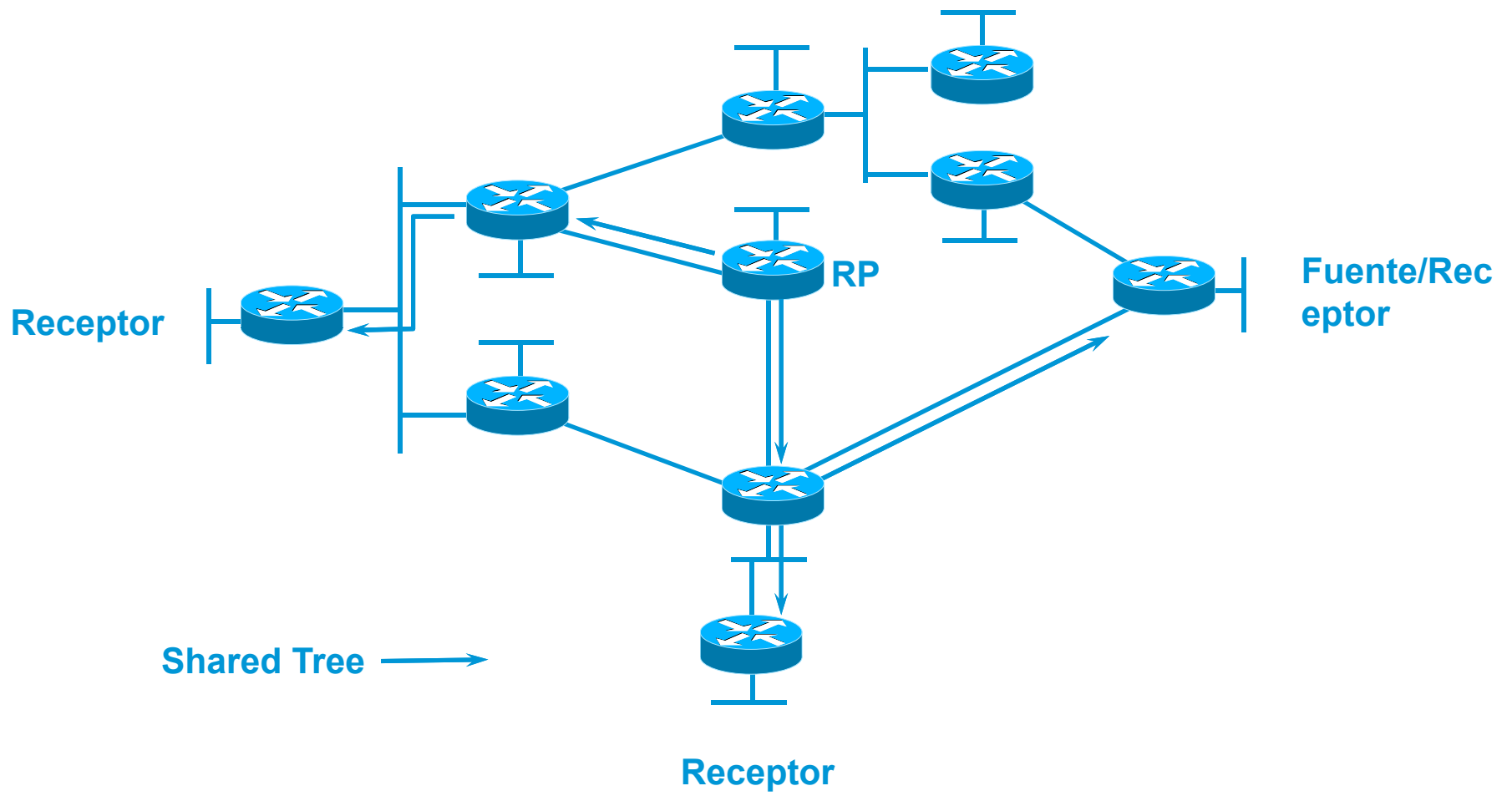
Menos estados en los ruteadores

- Solamente (\*,G) se utiliza
- El tráfico de la fuente sigue al “Shared Tree”

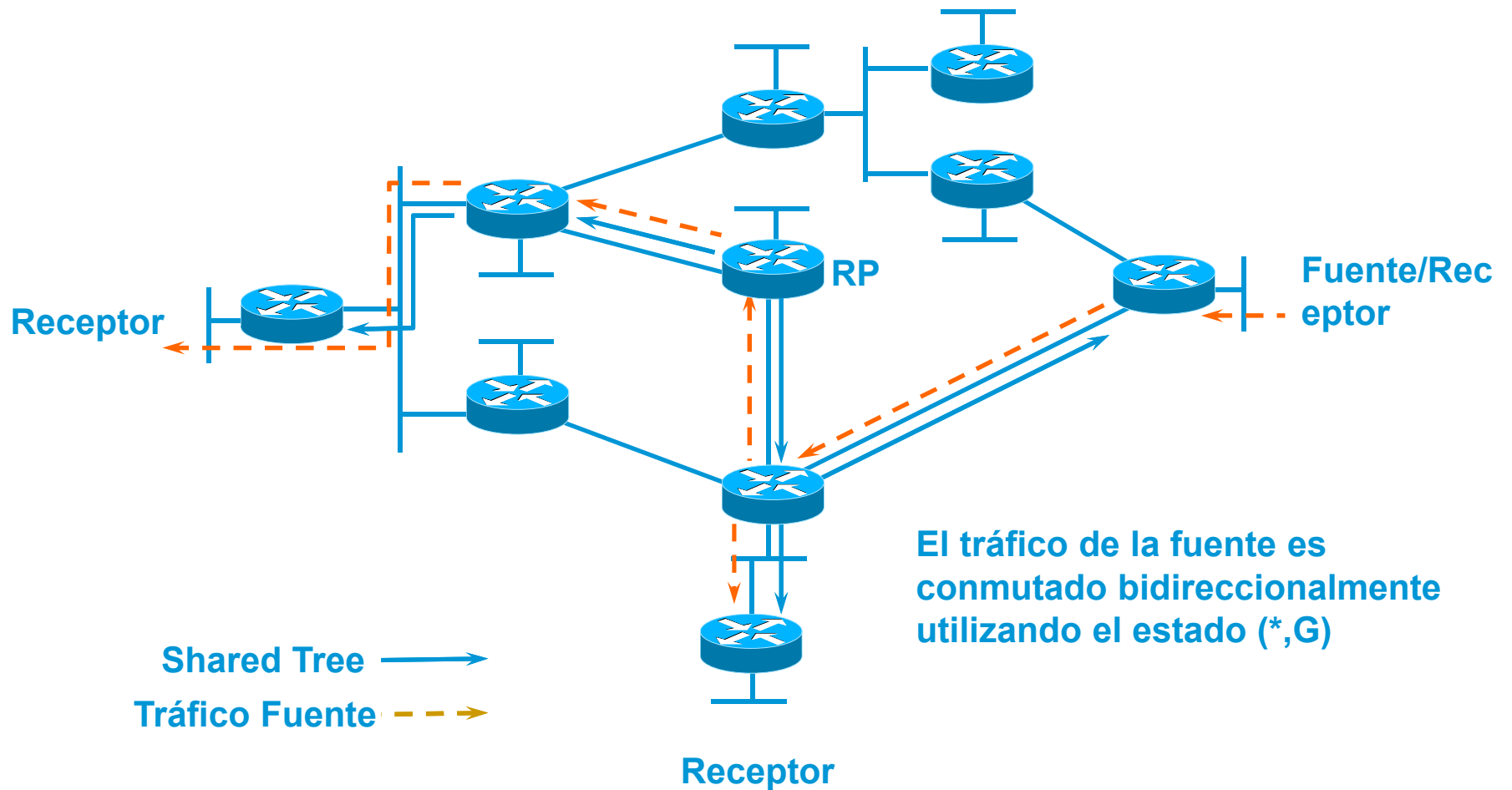
Fluye hacia el “shared tree” para alcanzar al RP

Fluye del RP hacia los receptores siguiendo el “Shared Tree”

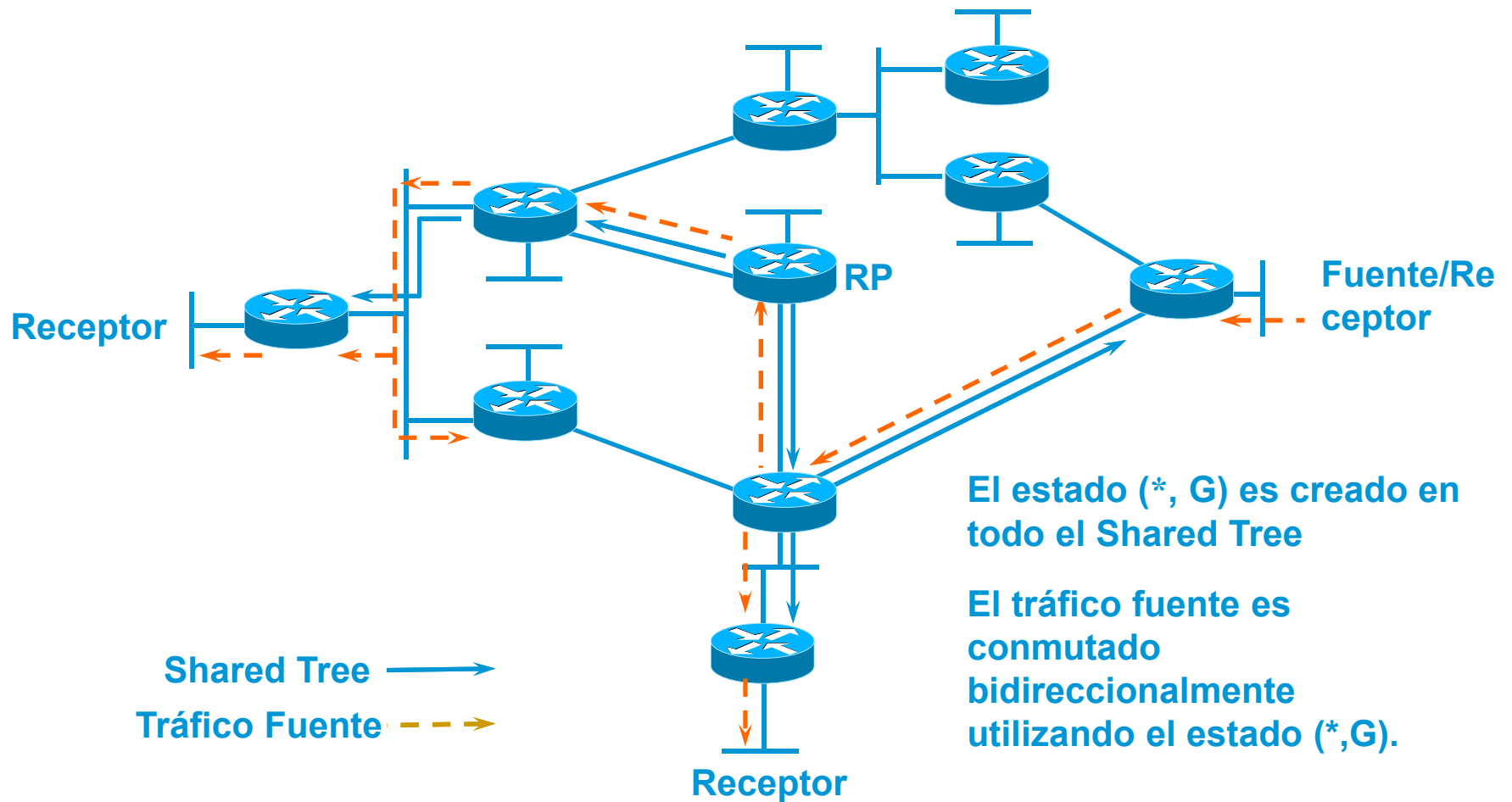
# Bidirectional PIM – Overview



# Bidirectional PIM – Overview



# Bidirectional PIM – Overview



# Modificaciones de PIM para la operación de BIDIR

- Designated Forwarders (DF)

En cada enlace el ruteador con la mejor trayectoria al RP is seleccionado como DF.

Nota: Designated Routers (DR) no son utilizados para grupos de bidir

El DF es responsable de conmutar el tráfico hacia el RP.

No hay tratamiento especial para fuentes locales.

# Bidir PIM– Evaluación

- Ideal para aplicaciones muchos a muchos
- Reduce drásticamente los estados en la tabla mroute

Elimina todos los estados (S,G) en la red

SPs son eliminados entre las fuentes y el RP

El tráfico fuente fluye hacia y desde el shared tree

Permite que aplicaciones de muchos-a-muchos escalen.

Permite virtualmente un número ilimitado de fuentes.



# RPs estáticos

- Se debe fijar la dirección del RP

Se debe configurar en cada ruteador

Todos los ruteadores deben de tener la misma dirección del RP.

No es posible tener redundancia con RPs estáticos

Excepción: Cuando se utiliza Anycast RPs:

El grupo nunca caera en “Dense Mode”

- Comando

```
ip pim rp-address <address> [group-list <acl>] [override]
```

De forma opcional se puede especificar la lista para el rango de grupos.

Rango de Defecto = 224.0.0.0/4 *(Incluye grupos de auto RP!!!!)*

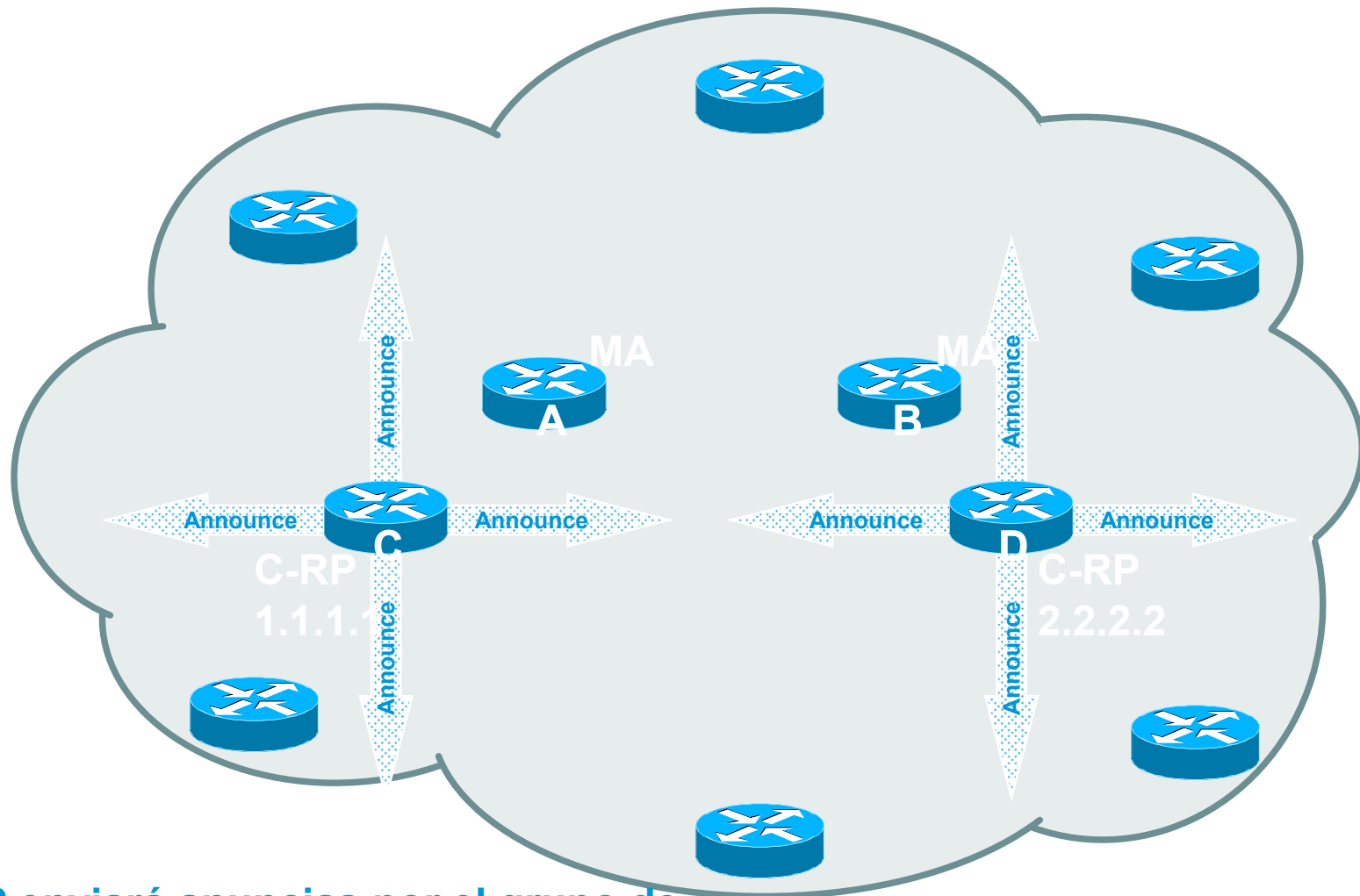
Override “reescribe ” información de Auto-RP

Comportamiento de Defecto: Lo que se aprende por Auto-RP toma precedencia.

# Auto-RP Overview

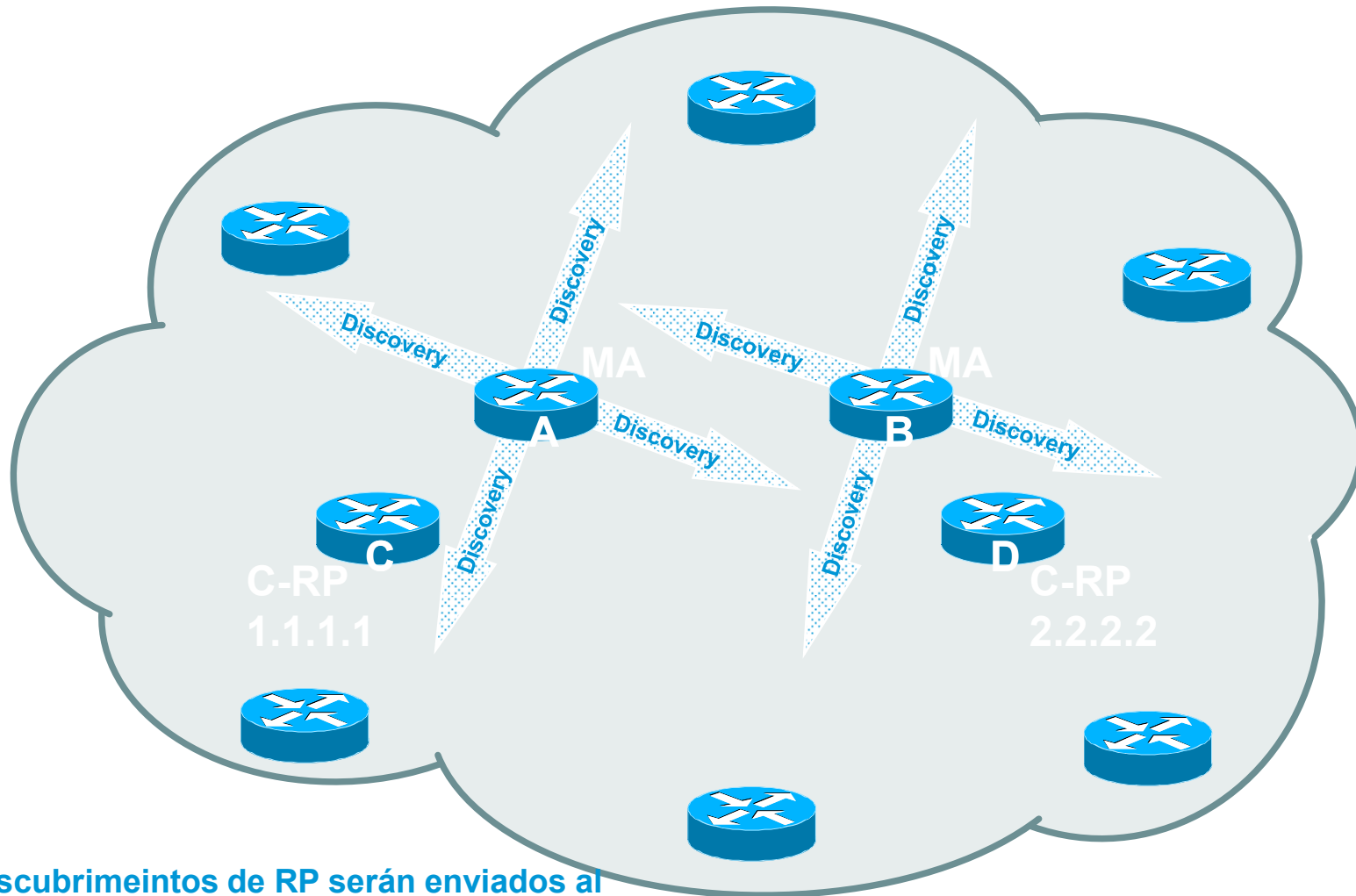
- Todos los routers aprenden direcciones de RP
  - Solamente se necesita configurar en
    - Candidate RPs
    - Mapping Agents
- Hace uso de multicast para distribuir la información
  - Dos grupos específicos asignados por IANA
    - Cisco-Announce - 224.0.1.39
    - Cisco-Discovery - 224.0.1.40
  - Estos grupos operarán normalmente en “Dense Mode”
- Permite configurar un RP de respaldo
  - Warning: Puede caer en “Dense Mode” si está mal configurado*
- Se puede utilizar con el rango de “admin-scope”

# Auto-RP— Visto en un alto nivel



El RP enviará anuncios por el grupo de multicast (224.0.1.39) "Cisco Announce"

# Auto-RP—Visto en un alto nivel



Los descubrimientos de RP serán enviados al grupo de multicast (224.0.1.40) Cisco Discovery

# BSR Overview

- Un ruteador Bootstrap (BSR) es elegido

Multiples candidatos a BSR's (C-BSR) pueden ser configurados

Da la habilidad de tener respaldo en caso de que falle el BSR elegido

C-RPs envian anuncios (C-RP) al BSR

Los anuncios de C-RP son enviados via unicast

El BSR almacena los anuncios C-RP en el "RP-set"

El BSR envía periódicamente mensajes a todos los ruteadores.

Los mensajes BSR tienen la información de "RP-SET" y la dirección IP del BSR.

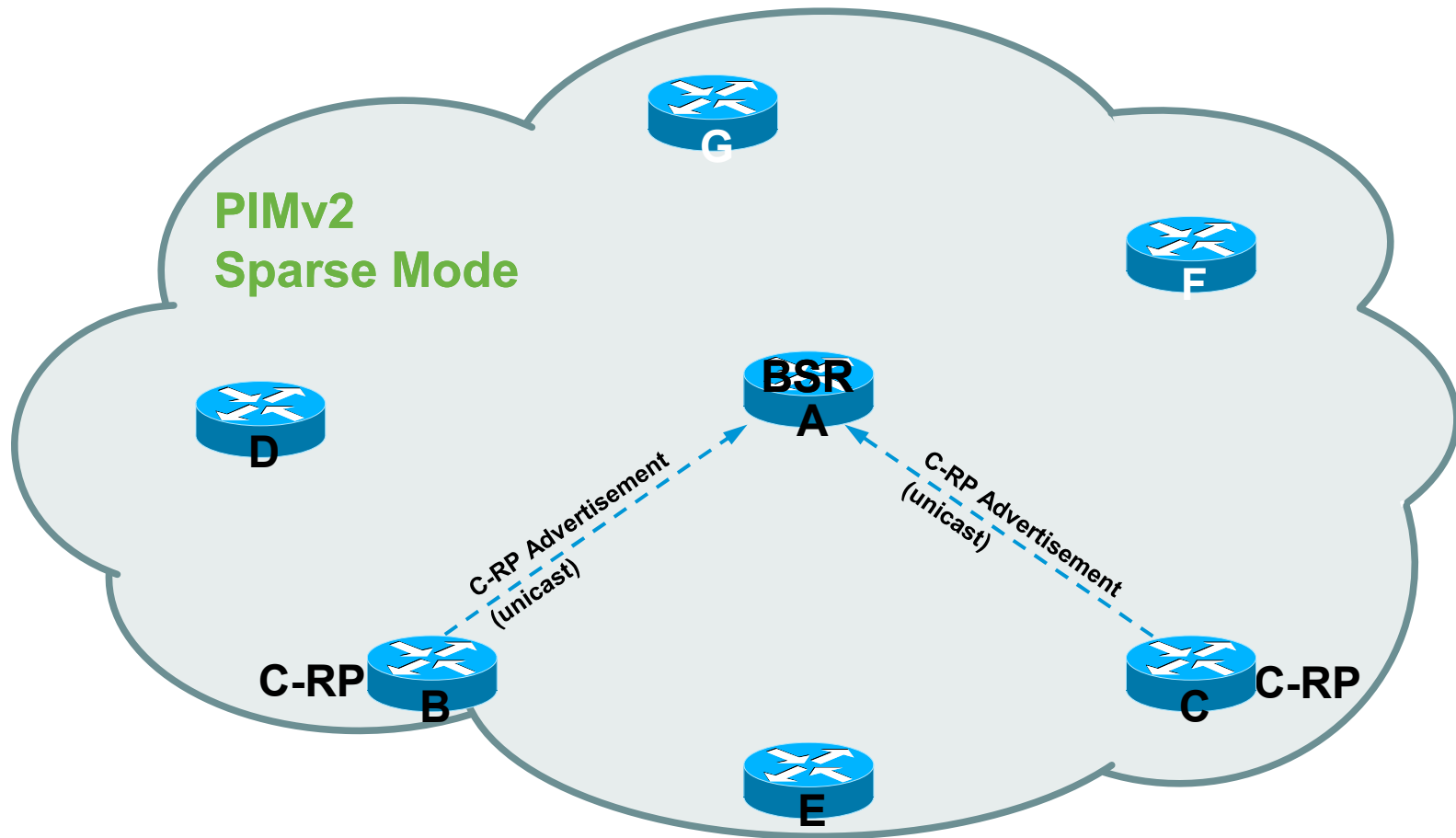
Los mensajes son inundados en la red, salto por salto, del BSR hacia afuera.

Todos los routers eligen al RP del "RP-SET"

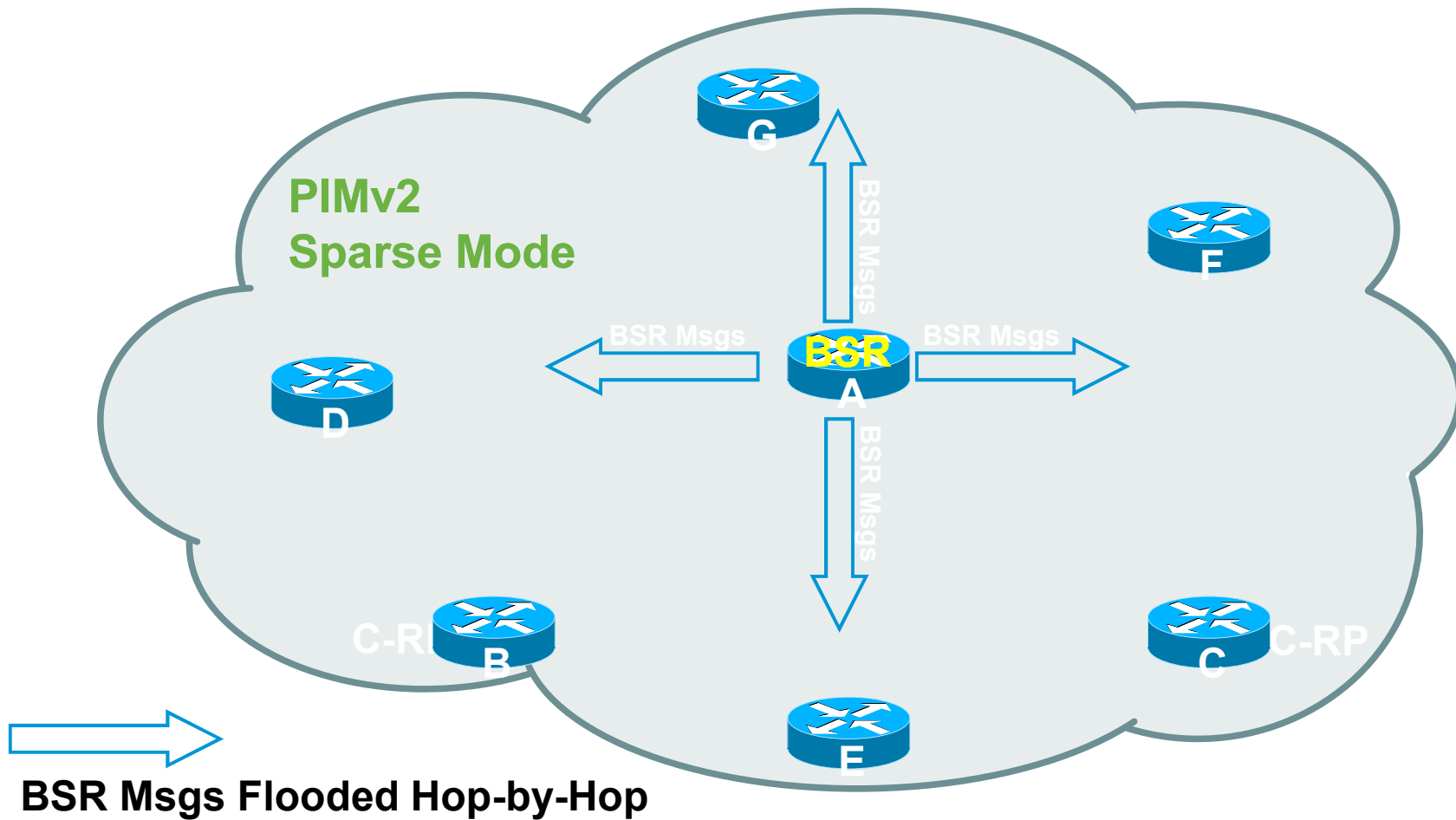
Todos los ruteadores utilizan el mismo algoritmo, por lo tanto eligen el mismo RP.

- BSR *no puede ser utilizado* con el rango "Admin-Scoping"

# BSR—Visto en un alto nivel

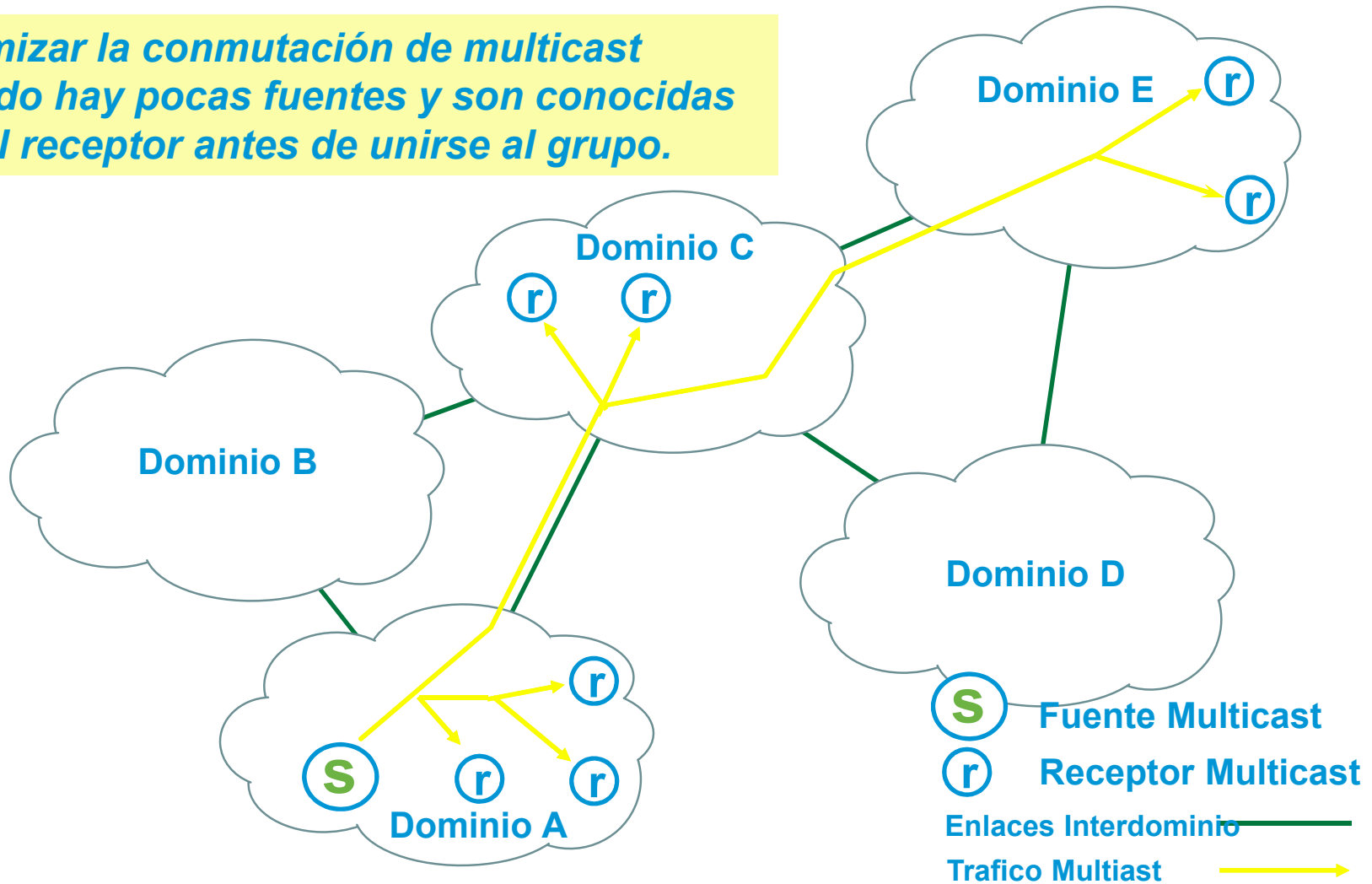


# BSR—Visto en un alto nivel



# Objetivo de Multicast SSM

*Optimizar la conmutación de multicast cuando hay pocas fuentes y son conocidas por el receptor antes de unirse al grupo.*





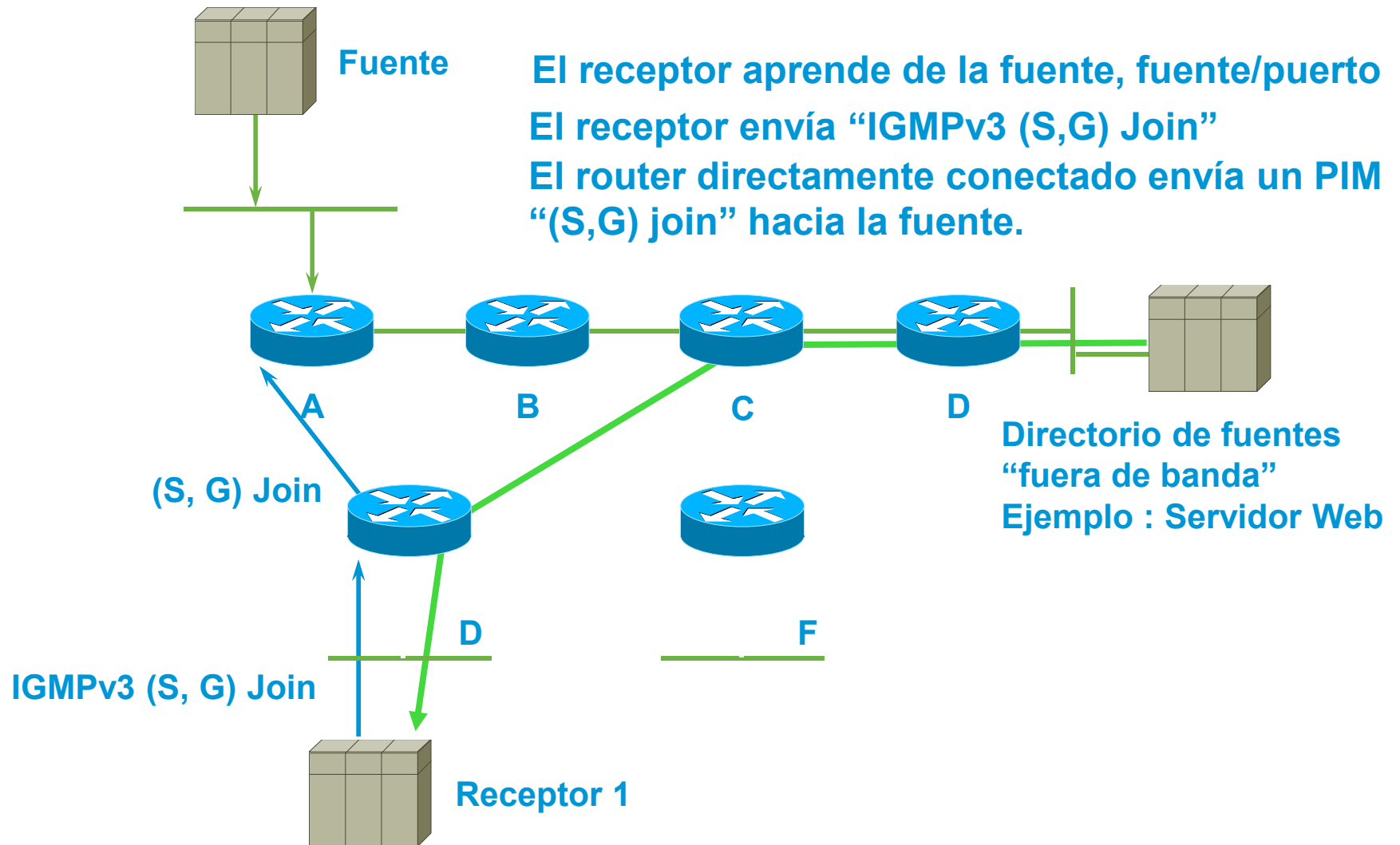
# Source Specific Multicast

- Asume un modelo de multicast “Uno-a-muchos”  
Ejemplo: Video/Audio, Información de la bolsa
- ¿Por qué PIM-SM necesita un “shared-tree”?  
Para que los “hosts” y los routers directamente conectados puedan aprender quien es la fuente activa del grupo.
- ¿Qué pasaría si esto ya lo sabemos?  
“Hosts” pueden utilizar IGMPv3 para señalar exactamente que grupo (S,G) SPT quieren unirse.  
El “shared tree” y el RP ya no serían necesarios.  
Fuentes distintas podrían utilizar el mismo grupo sin interferir una con otra.
- Resultado : Source Specific Multicast (SSM)

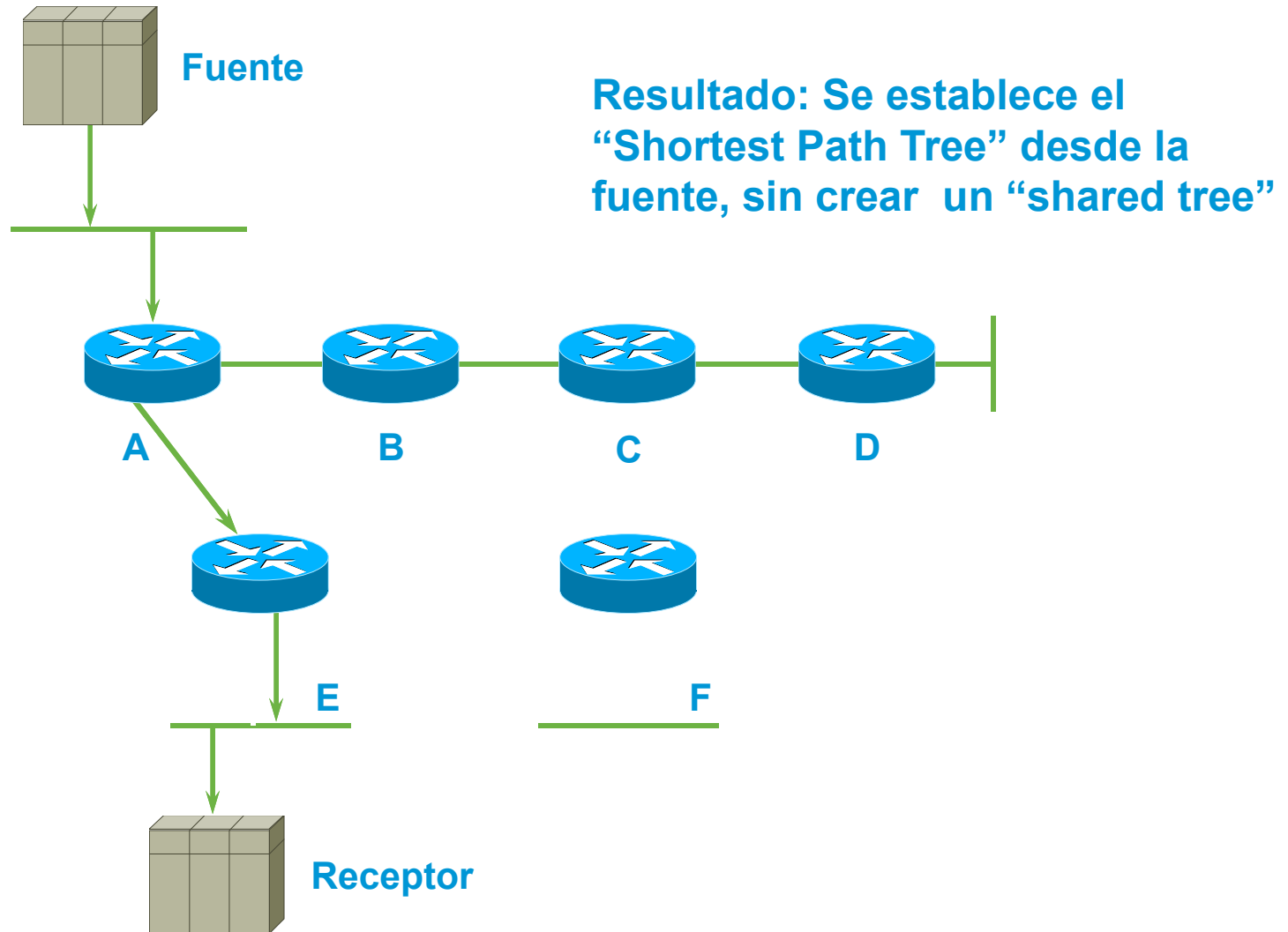
# Ventajas de SSM

- Permite el uso inmediato del camino más corto a la fuente sin la necesidad de primero crear un “shared tree”.
- Simplifica la asignación de direcciones globales donde se tiene fuentes únicas al eliminar los “shared trees”.

# PIM Source Specific Mode



# PIM Source Specific Mode



# Efecto de “shared trees” en SSM

- SSM puede funcionar si la fuente u otras redes utilizan “shared trees”, sin embargo:
  - NO hay control de quien puede transmitir en el ambiente “shared”
  - No hay un mecanismo que evite colisiones de direcciones.
- El rango 232/8 fue asignado para grupos donde los “shared trees” son prohibidos.

# PIM-SSM—Evaluación

- Ideal para aplicaciones con una fuente enviando a muchos receptores.
- Resuelve problemas de asignación de direcciones multicast.

Flujos diferenciados por fuente y grupo

No solamente por grupo

Proveedores de contenido pueden utilizar el mismo grupo de direcciones.

Debido a que cada flujo (S,G) es único.

- Ayuda a prevenir ciertos ataques DoS.

Tráfico “inválido” de fuentes

No puede ocupar ancho de banda en la red.

NO recibido por el host final

# Resumen

- Multicast trabaja con el concepto de grupos.
- IGMP es el protocolo que utilizan los hosts para señalar a los routers que quieren escuchar un grupo.
- IGMP snooping da visibilidad a los switches para ver que hosts en una LAN quieren unirse al grupo y así no inundar el segmento.
- Hay dos tipos de árboles “shared trees” y “shortest path tree o source distribution trees”
- PIM nos permite rutear el tráfico de multicast utilizando RPF.
- PIM puede ser utilizado en un modelo “push” conocido como “dense mode” o un modelo “pull” “sparse mode”
- El RP nos permite hacer el mapeo de source trees con shared trees y es utilizado sparse mode.
- SSM no requiere RP ya que se conoce la fuente en un inicio gracias a IGMPv3.

# Referencias

- IP Multicast: PIM configuration

[http://www.cisco.com/en/US/docs/iosxml/ios/ipmulti\\_pim/configuration/15-mt/imc-pim-15-mt-book.html](http://www.cisco.com/en/US/docs/iosxml/ios/ipmulti_pim/configuration/15-mt/imc-pim-15-mt-book.html)

- Customizing IGMP

[http://www.cisco.com/en/US/partner/docs/ios/12\\_4t/ip\\_mcast/configuration/guide/mctigmp.html](http://www.cisco.com/en/US/partner/docs/ios/12_4t/ip_mcast/configuration/guide/mctigmp.html)

## Libro

Developing IP Multicast Networks, Volume I Beau Williamson Cisco Press

IP Multicast Troubleshooting guide

[http://www.cisco.com/en/US/tech/tk828/technologies\\_tech\\_note09186a0080094b55.shtml](http://www.cisco.com/en/US/tech/tk828/technologies_tech_note09186a0080094b55.shtml)



# Sesión de Preguntas y Respuestas

El experto responderá verbalmente algunas de las preguntas que hayan realizado. Use el panel de preguntas y respuestas (Q&A) para preguntar a los expertos ahora



# Nos interesa su opinión!!!

Habr  un sorteo con las personas que llenen el cuestionario de evaluaci n.

Tres de los asistentes recibir n un

## **Regalo sorpresa**



Para llenar la evaluaci n haga click en el link que est  en el chat, tambi n aparecer  autom ticamente al cerrar el browser de la sesi n.



# Pregunte al Experto (con Enrique Dávila)



Si tiene preguntas adicionales pregunte aquí

<https://supportforums.cisco.com/thread/2241620>

Enrique responderá del martes 24 de Septiembre al viernes 4 de octubre del 2013.

Puede ver la grabación de este evento, y leer las preguntas y respuestas en 5 días hábiles en:

<https://supportforums.cisco.com/community/spanish/espacio-de-los-expertos/webcasts>



# Sesiones de Webcast (Portugués)

Tema: Fundamentos de Virtualización para Data Center



## Martes 4 de Octubre:

9:00 a.m.	Ciudad de México
9:30 a.m.	Caracas
11:00 a.m.	Buenos Aires
4:00 p.m.	Madrid

Estará presentando el Partner experto de Cisco: **Gustavo Santana**

Durante este evento en vivo, el experto de Cisco dará una introducción a los Fundamentos de Virtualización para Data Center. Participe con nosotros para obtener mayor información sobre este tema y podrá hacer preguntas a los expertos de Cisco.

# Pregunte al Experto

## En español



**Tema: Configuración y Troubleshooting IP Manager Assistance (Jefe/Secretaria) en CallManager.**

Con el experto de Cisco: *Felipe Segnini*

Aprenda y haga preguntas sobre : "Configuración y Troubleshooting IP Manager Assistance (Jefe/Secretaria) en CallManager"

Finaliza el 27 de septiembre del 2013

<https://supportforums.cisco.com/thread/2240865>

# Califique el contenido de la Comunidad de Soporte de Cisco en Español.



**Ahora puede calificar discusiones, documentos, blogs y videos!!...**

Esto es con el fin de que nos ayude a distinguir contenido de calidad y también para reconocer los esfuerzos de los integrantes de la Comunidad de Soporte de Cisco en español.

<https://supportforums.cisco.com/community/spanish/general/blog/2013/06/21/ahora-ratings-en-documentos-blogs-y-videos>

# Soporte Técnico Móvil, anuncia el acceso a las Comunidades de Soporte Globales.



La Comunidad de Soporte de Cisco anuncia su evolución con el lanzamiento del nuevo Acceso Móvil hacia la Comunidades Globales > Español, Portugués, Japonés, Ruso, y Polaco.

<https://supportforums.cisco.com/docs/DOC-34800>



# Lo invitamos a colaborar activamente en CSC en español y en nuestras redes sociales



<https://supportforums.cisco.com/community/spanish>



CiscoLatinoamerica

Cisco Mexico

Cisco España

Cisco Cono Sur

Comunidad Cisco Cansac

CiscoSupportCommunity



@Cisco\_LA

@CiscoMexico

@cisco\_spain

@ciscocansacsm

@ciscoconosur

@cisco\_support



## Más redes sociales:



**CiscoLatam**  
**ciscosupportchannel**



**Cisco Technical Support**



**CSC-Cisco-Support-Community**

Gracias por su  
tiempo

Por favor tomen un momento para llenar su evaluación



