



Explorando Multicast en Capa 2: IGMP, IGMP Snooping y Consejos para la Resolución de Problemas

Comunidad de Cisco

Aarón Díaz – Technical Consulting Engineer
Ricardo Bermejo – Technical Consulting Engineer

Jueves 13 de junio de 2024



Conecte, Interactúe, ¡Colabore!

Soluciones

Ayuda a otros usuarios a encontrar las respuestas correctas en el motor de búsqueda de la comunidad indicando que la duda fue resuelta al activar la opción “Aceptar como solución” u otórgales un voto de utilidad.

Aceptar como solución

Votos de utilidad

¡Resalta el esfuerzo de otros miembros!

Los votos útiles motivan a otros miembros que colaboran en la comunidad, a seguir ayudándonos a contestar las preguntas abiertas, y ofreciéndoles la oportunidad de ganar premios. ¡Reconoce su esfuerzo!

👍 0 Útil

Premios Spotlight Awards

¡Destaca por tu esfuerzo y compromiso para mejorar la comunidad y ayudar a otros miembros!

Los premios Spotlight Awards se otorgan trimestralmente para reconocer a los miembros más destacados.

Conoce a los ganadores de [Febrero-Abril 2024](#)

¡Ahora también puedes nominar a un candidato! [Haga clic aquí](#)



Nuestros expertos

Aarón Díaz



Technical Consulting Engineer

Es egresado en Ingeniería Mecatrónica del Instituto Politécnico Nacional (IPN).

Se incorporó a Cisco en 2021 como parte del programa Customer Experience Academy.

Actualmente desempeña el cargo de Technical Consulting Engineer en Cisco TAC en el equipo Enterprise Switching. Se especializa en la gama de switches Catalyst 9000.

Descarga la presentación <https://bit.ly/CL2doc-jun24>

Nuestros expertos

Ricardo Bermejo O.



Technical Consulting Engineer

Es un ingeniero de soporte de TAC para el equipo de LAN Switching. Ha trabajado en Cisco por más de cinco años.

Anteriormente, trabajó en Telmex y Grupo KUO como ingeniero de soporte en proyectos de implementación y soporte en redes de datos, VoIP y seguridad.

Ricardo es ingeniero en Tecnologías de la Información por parte de la Universidad Tecnológica de Nezahualcóyotl y cuenta con diversas certificaciones a nivel CCNA y CCNP de Cisco, con experiencia en la industria por más de diez años.

Descarga la presentación <https://bit.ly/CL2doc-jun24>

slido

Join at
slido.com
#3579 339

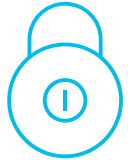
 Passcode: **abgxyi**



Agenda



1. Introducción a Multicast
2. IGMP y Multicast en Capa 2
3. IGMP Snooping
4. Configuración de IGMP Snooping
5. TAC tips para Resolución de problemas



Introducción a Multicast

● Introducción a Multicast

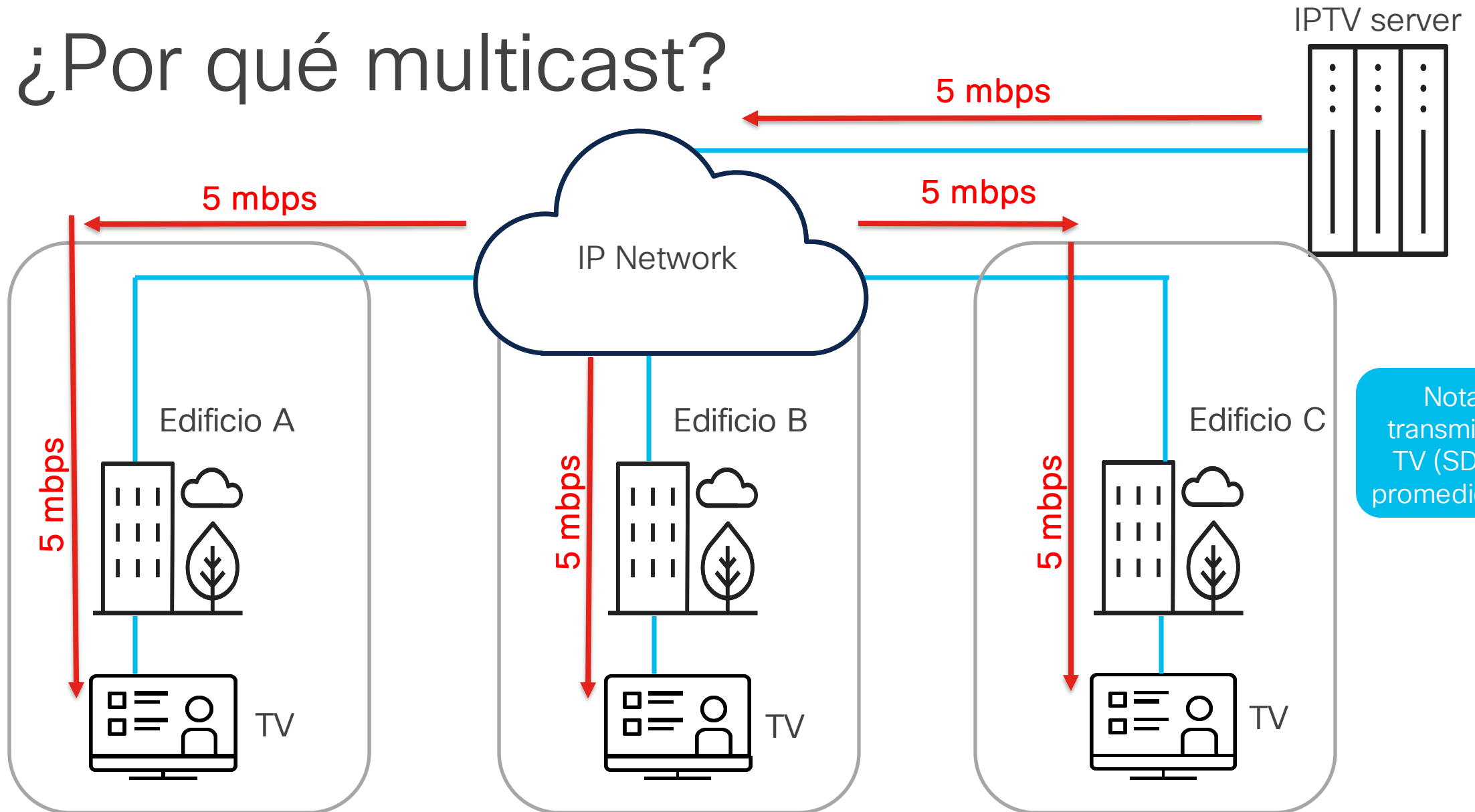
● IGMP y Multicast en
Capa 2

● IGMP Snooping

● Configurar IGMP
Snooping

● TAC Tips para
Resolución de
Problemas

¿Por qué multicast?



Nota: Una transmisión de TV (SD) usa un promedio 5 mbps.

¿Por qué multicast?



Principales características de tráfico Multicast

- 1 La información es recibida por múltiples usuarios simultáneamente.
- 2 Sin conexión, no se establece un canal de comunicación en comparación con TCP, si hay pérdida de información, ésta se pierde para siempre.
- 3 Ancho de banda bajo, escala fácilmente a un número ilimitado de clientes finales, con una utilización predecible.
- 4 Todas la IP multicast están mapeadas al prefijo MAC: 0100:5Exx.xxxx.

Multicast a nivel de paquete



Todo el tráfico, ya sea **Unicast** o **Multicast** de igual forma contiene **L2 and L3 headers**, pero ciertos bits en estos headers se encuentran **reservados**, a fin de indicar si un paquete es Unicast o **Multicast**.



Si el último bit del primer octeto está activo, el paquete es Multicast.

Multicast a nivel de paquete



Todo el tráfico, ya sea **Unicast** o **Multicast** de igual forma contiene **L2 and L3 headers**, pero ciertos bits en estos headers se encuentran **reservados**, a fin de indicar si un paquete es Unicast o **Multicast**.



Ejemplos

0011.0022.0033 → 0x00 = b0000 0000

ABAA.BBBB.CCC 0xAB = b1010 1011

1234.5678.9ABC 0x12 = b000 10010

EF98.7654.3210 0xEF = b1110 1111



0x = Representa números hexadecimales
b = Representa números binarios



Si el último bit del primer octeto está activo, el paquete es Multicast.



Multicast a nivel de paquete



Todo el tráfico, ya sea **Unicast** o **Multicast** de igual forma contiene **L2 and L3 headers**, pero ciertos bits en estos headers se encuentran **reservados**, a fin de indicar si un paquete es Unicast o **Multicast**.



Ejemplos

0011.0022.0033 → 0x00 = b0000 0000

ABAA.BBBB.CCC → 0xAB = b1010 1011

1234.5678.9ABC → 0x12 = b000 1001

EF98.7654.3210 → 0xEF = b1110 1111

Unicast

Multicast

Unicast

Multicast

Multicast a nivel de paquete



La IANA (Internet Assigned Numbers Authority) define el siguiente bloque para tráfico multicast: **224.0.0.0/4 (224.0.0.0 – 239.255.255.255)**.



Solo tráfico multicast enviado a los bloques de IANA (IP y MAC) pueden ser monitoreados por la red usando IGMP Snooping.



Multicast a nivel de paquete



La IANA (Internet Assigned Numbers Authority) define el siguiente bloque para tráfico multicast: **224.0.0.0/4 (224.0.0.0 – 239.255.255.255)**.

Subbloques

1	224.0.0.0 /24	Local Network control Block
2	224.0.1.0 /24	Internetwork Control Block
3	232.0.0.0 /8	SSM Block
4	233.0.0.0 /8	GLOP Block
5	239.0.0.0 /8	Administratively Assigned

Multicast a nivel de paquete



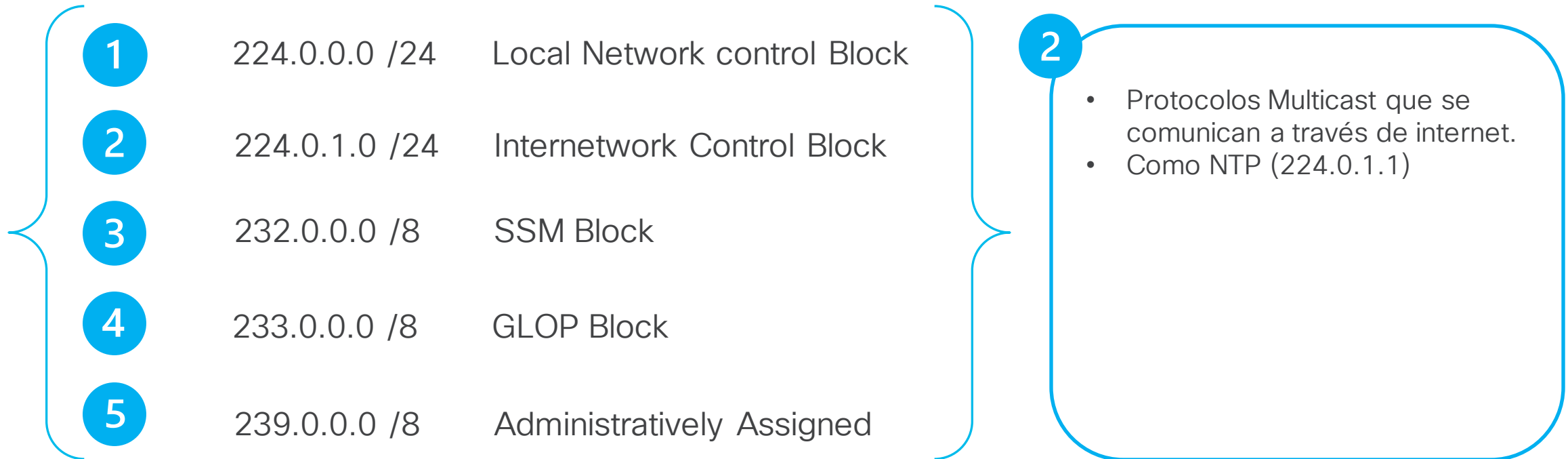
La IANA (Internet Assigned Numbers Authority) define el siguiente bloque para tráfico multicast: **224.0.0.0/4 (224.0.0.0 – 239.255.255.255)**.

1	224.0.0.0 /24	Local Network control Block	<p>1</p> <ul style="list-style-type: none">• Protocolos de ruteo: EIGRP, OSPF, RIP, etc.• TTL (Time to Live) fijado a “1”.• Tráfico no monitoreado por IGMP snooping.• Siempre subirá a CPU del switch/router que reciba el paquete.
2	224.0.1.0 /24	Internetwork Control Block	
3	232.0.0.0 /8	SSM Block	
4	233.0.0.0 /8	GLOP Block	
5	239.0.0.0 /8	Administratively Assigned	

Multicast a nivel de paquete



La IANA (Internet Assigned Numbers Authority) define el siguiente bloque para tráfico multicast: **224.0.0.0/4 (224.0.0.0 – 239.255.255.255)**.



Multicast a nivel de paquete



La IANA (Internet Assigned Numbers Authority) define el siguiente bloque para tráfico multicast: **224.0.0.0/4 (224.0.0.0 – 239.255.255.255)**.

1	224.0.0.0 /24	Local Network control Block
2	224.0.1.0 /24	Internetwork Control Block
3	232.0.0.0 /8	SSM Block
4	233.0.0.0 /8	GLOP Block
5	239.0.0.0 /8	Administratively Assigned

3

- Bloque reservado para SSM (Source Specific Multicast) que es una extensión de IP Multicast.
- Enfocado a aplicaciones one-to-many.

Multicast a nivel de paquete



La IANA (Internet Assigned Numbers Authority) define el siguiente bloque para tráfico multicast: **224.0.0.0/4 (224.0.0.0 – 239.255.255.255)**.

1	224.0.0.0 /24	Local Network control Block
2	224.0.1.0 /24	Internetwork Control Block
3	232.0.0.0 /8	SSM Block
4	233.0.0.0 /8	GLOP Block
5	239.0.0.0 /8	Administratively Assigned

4

- Enfocado a organizaciones con un número AS (Autonomous System).
- A partir del número AS, se obtiene una dirección multicast de este rango.

Multicast a nivel de paquete



La IANA (Internet Assigned Numbers Authority) define el siguiente bloque para tráfico multicast: **224.0.0.0/4 (224.0.0.0 – 239.255.255.255)**.

1	224.0.0.0 /24	Local Network control Block
2	224.0.1.0 /24	Internetwork Control Block
3	232.0.0.0 /8	SSM Block
4	233.0.0.0 /8	GLOP Block
5	239.0.0.0 /8	Organization-Local Scope

5

- Este rango asignado para aplicaciones Multicast dentro de una misma organización.
- Típicamente bloqueadas por Routers mas allá del AS.
- Descritas en el RFC 2365.

Multicast a nivel de paquete



Se recomienda usar el siguiente filtro a nivel de wireshark cuando estemos realizando algun tipo de tshoot con relación a tráfico multicast.

Filtro wireshark:

- `ip.addr==224.0.0.0/4`

The screenshot shows the Wireshark interface with a capture filter `ip.addr==224.0.0.0/4` applied. The 'Conversations' window is open, showing a table of network conversations. The 'UDP · 12' tab is selected, and the table displays two conversations between 10.26.192.72 and 224.0.0.251, and between 10.26.192.72 and 239.255.255.250.

Address A	Address B	Packets	Bytes	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Star
10.26.192.72	224.0.0.251	6	522 bytes	6	100.00%	6	522 bytes	0	0 bytes	5.490486
10.26.192.72	239.255.255.250	46	10 kB	46	100.00%	46	10 kB	0	0 bytes	5.758371



¿Cuál es el rango de direcciones IP multicast reservado para direcciones privadas?

a) 224.0.0.0 - 224.0.0.255

0%

b) 224.0.0.0 - 239.255.255.255

0%

c) 239.0.0.0 - 239.255.255.255

0%

Join at

slido.com

#3579 339

🔍 Passcode:

abgxyi

IGMP y Multicast en Capa 2

- Introducción a Multicast
- IGMP y Multicast en Capa 2
- IGMP Snooping
- Configurar IGMP Snooping
- TAC Tips para Resolución de Problemas

IGMP y Multicast en Capa 2



IGMP – Internet Group Management Protocol

1

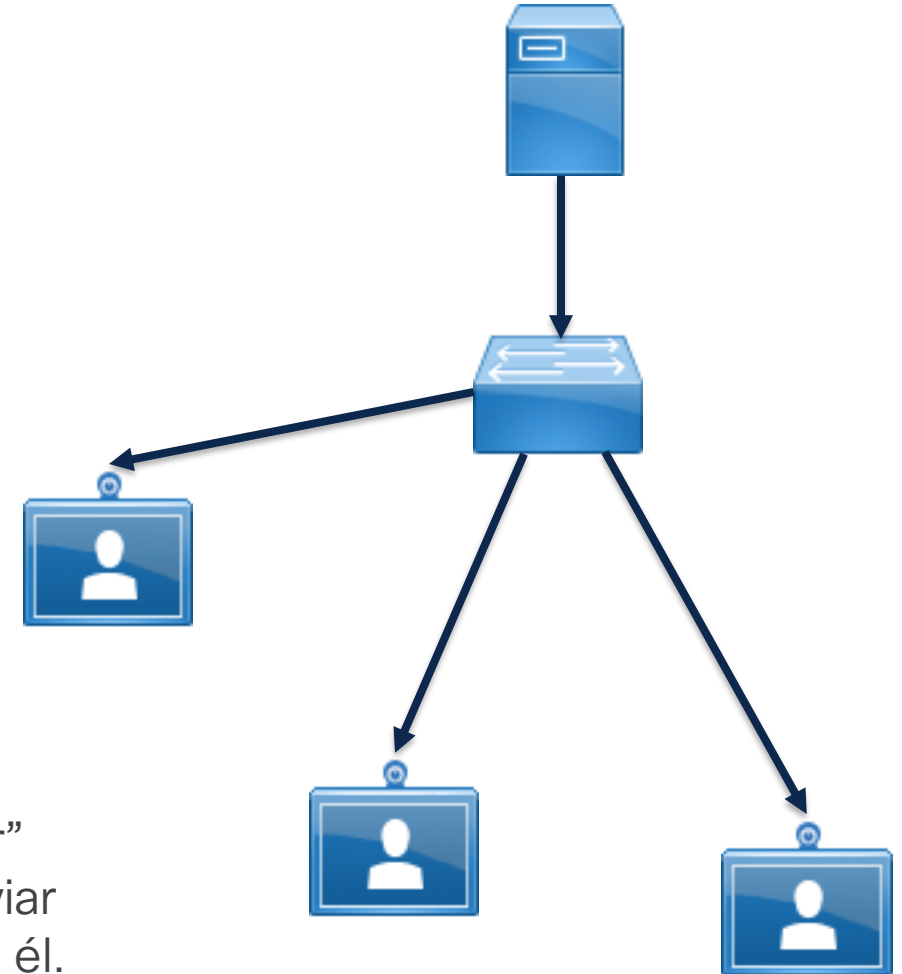
IGMP (Protocolo):

Es el mecanismo usado por un cliente, para solicitar o abandonar un grupo de multicast.

2

IGMP Snooping:

Es la acción del switch de escuchar o “monitorear” estos mensajes enviados por lo clientes, y así enviar tráfico multicast solo a los clientes interesados en él.



IGMP y Multicast en Capa 2

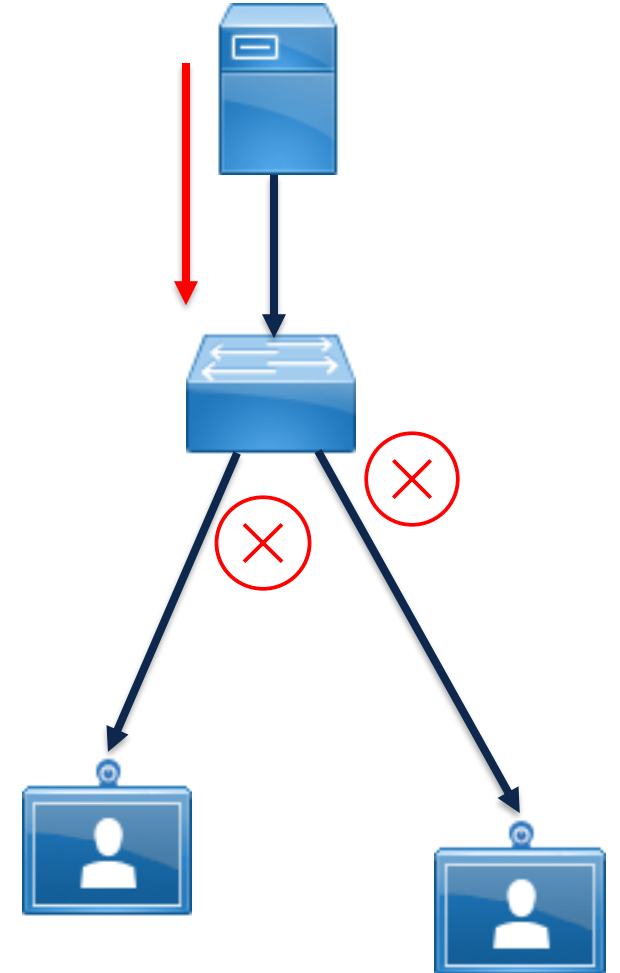


IGMP – Internet Group Management Protocol



IGMP Snooping está habilitado por default en plataformas Catalyst 9000.

Si no hay clientes interesados en la transmisión, el switch lo restringirá.



IGMP y Multicast en Capa 2



IGMP – Internet Group Management Protocol

IGMP Snooping cuenta con 3 versiones.

IGMPv1:

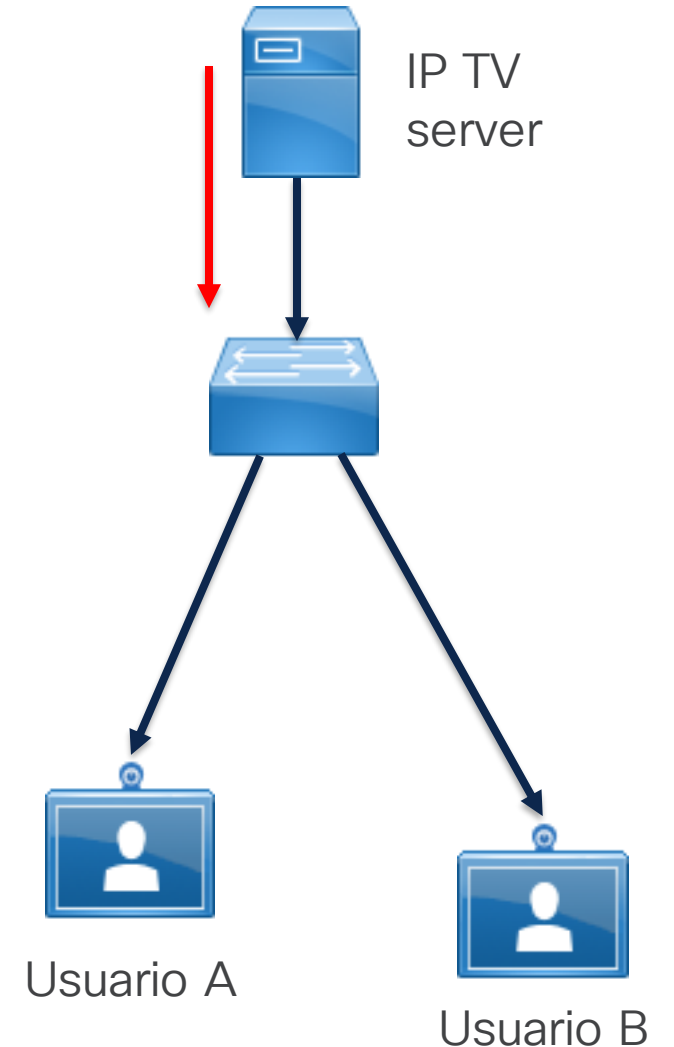
- Membership Report
- Membership Query

1

El tráfico es enviado por el servidor



El servidor no participa en el proceso de IGMP, solo envía el tráfico al grupo multicast deseado.



IGMP y Multicast en Capa 2



IGMP – Internet Group Management Protocol

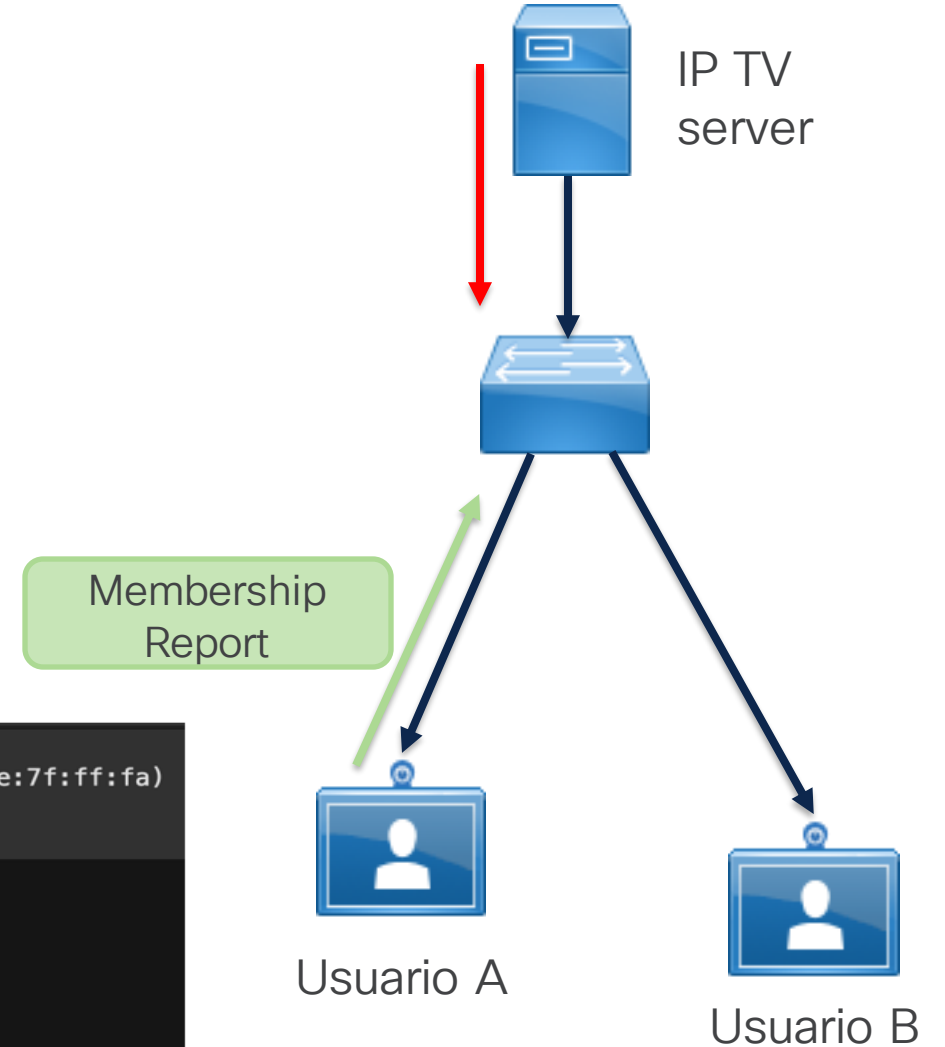
IGMPv1: **2** Un usuario envía un “Membership report”, la cual contiene la dirección multicast.



Filtro wireshark Membership Report:

- `igmp.type == 0x16`

```
> Frame 10111: 46 bytes on wire (368 bits), 46 bytes captured (368 bits) on interface en0, id 0
> Ethernet II, Src: WistronNeweb_7d:f2:86 (38:b8:00:7d:f2:86), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
> Internet Protocol Version 4, Src: 192.168.100.5, Dst: 239.255.255.250
< Internet Group Management Protocol
  [IGMP Version: 2]
  Type: Membership Report (0x16)
  Max Resp Time: 0.0 sec (0x00)
  Checksum: 0xfa04 [correct]
  [Checksum Status: Good]
  Multicast Address: 239.255.255.250
```



IGMP y Multicast en Capa 2

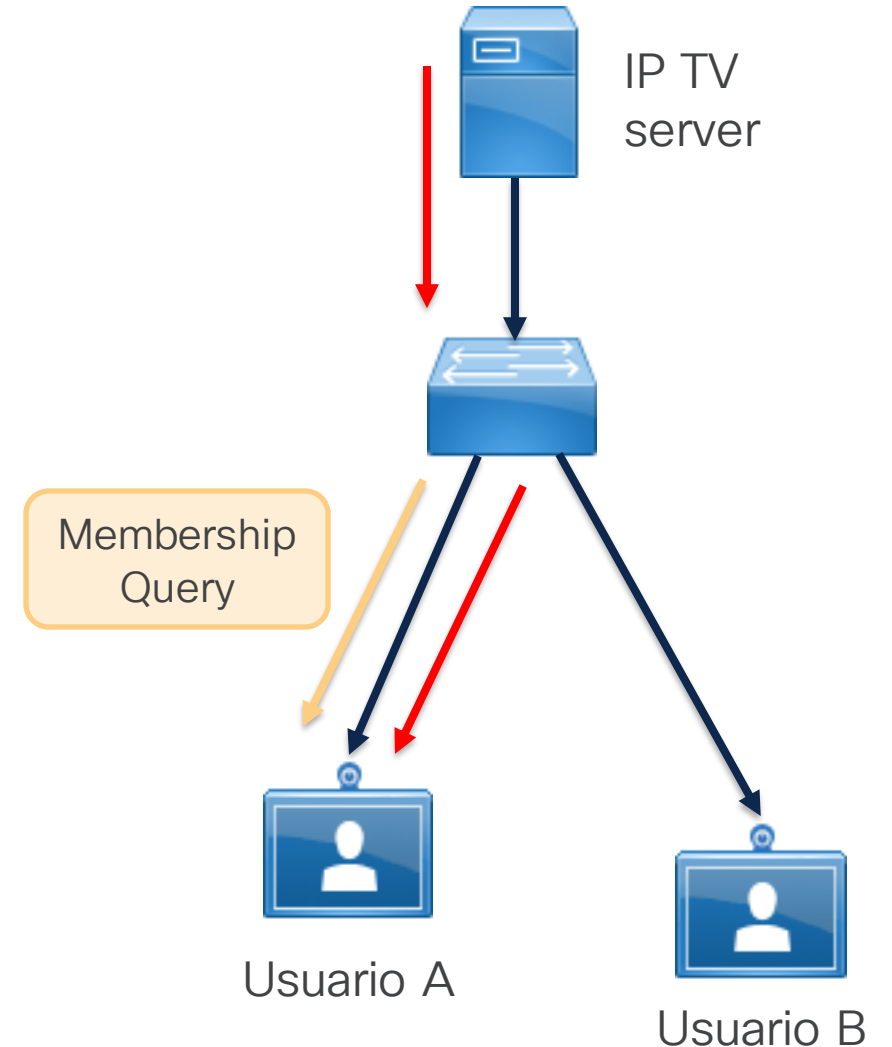


IGMP – Internet Group Management Protocol

IGMPv1:

- 3 El switch transmite el tráfico hacia el Usuario.
- 4 El switch manda un paquete “Membership query” cada 60 segundos.

Después de 3 membership queries, el switch deja de transmitir tráfico hacia este puerto.



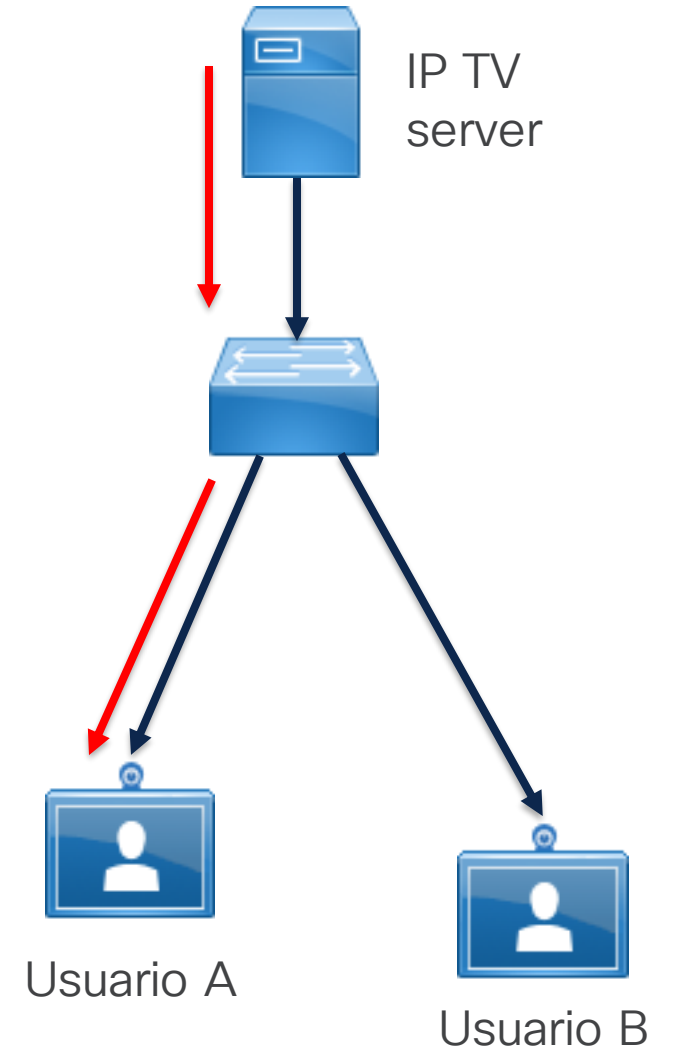
IGMP y Multicast en Capa 2



IGMP – Internet Group Management Protocol

IGMPv1:

5. 1. Si el usuario desea permanecer en el grupo, este enviará un nuevo “Membership Report”
2. De lo contrario el switch restringirá la transmisión de tráfico Multicast en este puerto.



IGMP y Multicast en Capa 2



IGMP – Internet Group Management Protocol

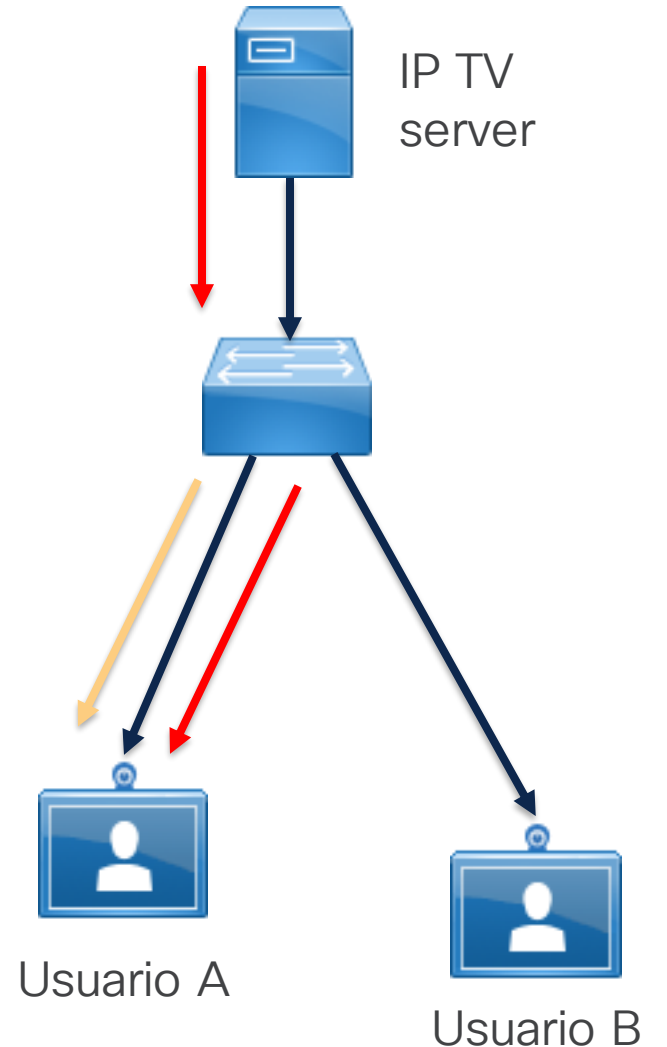
IGMPv1:



Filtro wireshark Membership Query:

- `Igmp.type == 0x11`

```
> Frame 9806: 46 bytes on wire (368 bits), 46 bytes captured (368 bits) on interface en0, id 0
> Ethernet II, Src: TPLink_01:4e:1c (5c:e9:31:01:4e:1c), Dst: IPv4mcast_01 (01:00:5e:00:00:01)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 224.0.0.1
< Internet Group Management Protocol
  [IGMP Version: 2]
  Type: Membership Query (0x11)
  Max Resp Time: 10.0 sec (0x04)
  Checksum: 0xee9b [correct]
  [Checksum Status: Good]
  Multicast Address: 0.0.0.0
```



IGMP y Multicast en Capa 2



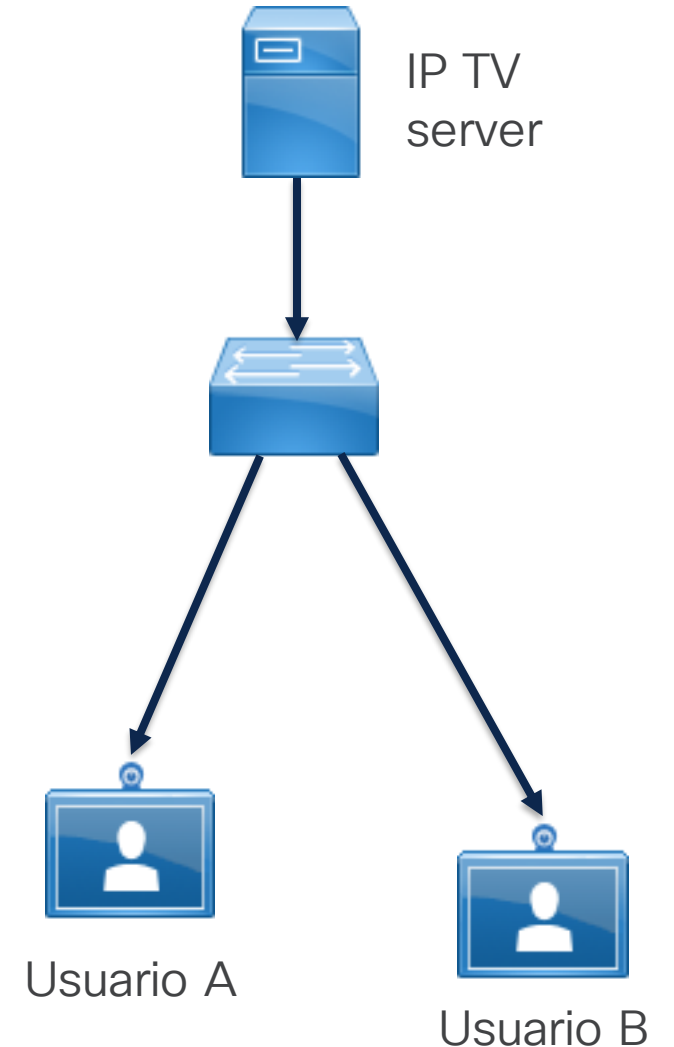
IGMP – Internet Group Management Protocol

IGMPv2:

- Leave Group
- Group Specific Queries (GSQ)



Lo switches Catalyst 9000 corren IGMPv2 por default



IGMP y Multicast en Capa 2



IGMP – Internet Group Management Protocol

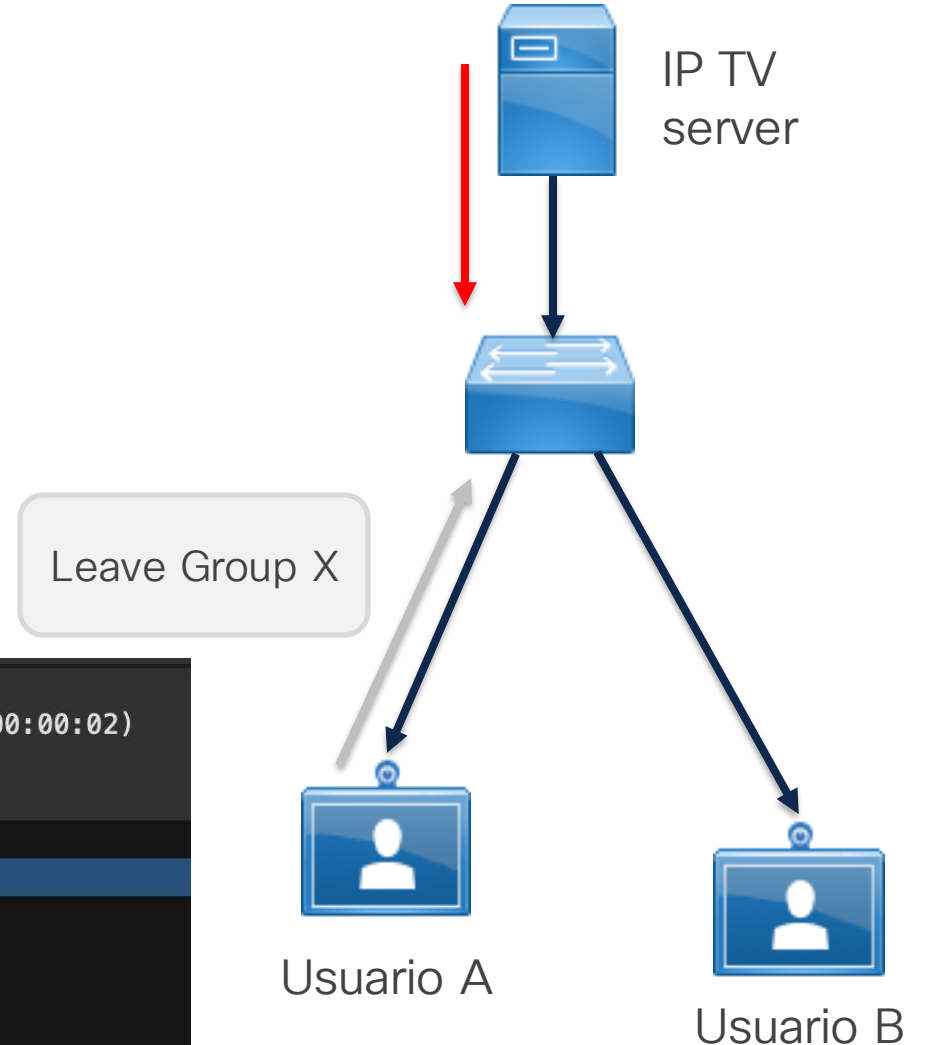
IGMPv2:



Filtro wireshark Leave Group:

- *Igmp.type == 0x17*

```
> Frame 5: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: AminoCommuni_19:51:28 (00:02:02:19:51:28), Dst: IPv4mcast_02 (01:00:5e:00:00:02)
> Internet Protocol Version 4, Src: 192.168.11.201, Dst: 224.0.0.2
> Internet Group Management Protocol
  [IGMP Version: 2]
  Type: Leave Group (0x17)
  Max Resp Time: 0.0 sec (0x00)
  Checksum: 0x06fb [correct]
  [Checksum Status: Good]
  Multicast Address: 225.1.1.3
```



IGMP y Multicast en Capa 2



IGMP – Internet Group Management Protocol

IGMPv2:

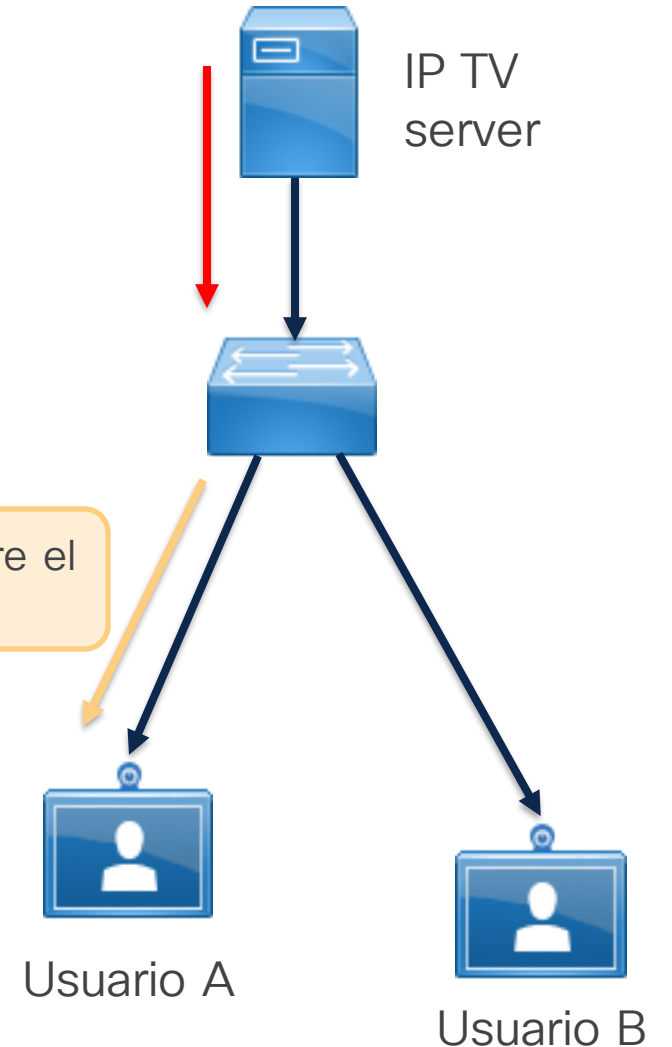


Filtro wireshark GSQ:

- *igmp.type == 0x11*

```
> Frame 6: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: DLink_10:26:11 (00:1b:11:10:26:11), Dst: IPv4mcast_01:01:03 (01:00:5e:01:01:03)
> Internet Protocol Version 4, Src: 192.168.1.2, Dst: 225.1.1.3
> Internet Group Management Protocol
  [IGMP Version: 2]
  Type: Membership Query (0x11)
  max resp time: 1.0 sec (0x0a)
  Checksum: 0x0cf1 [correct]
  [Checksum Status: Good]
  Multicast Address: 225.1.1.3
```

GSQ – Quién quiere el grupo X



IGMP y Multicast en Capa 2



IGMP – Internet Group Management Protocol

IGMPv3:

- Source Specific group



Filtro wireshark Membership Report v3:

- `igmp.type == 0x22`

```
▶ Frame 13: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▶ Ethernet II, Src: CiscoSPV_51:c3:81 (00:25:2e:51:c3:81), Dst: IPv4mcast_16 (01:00:5e:00:00:16)
▶ Internet Protocol Version 4, Src: 192.168.1.66, Dst: 224.0.0.22
▼ Internet Group Management Protocol
  [IGMP Version: 3]
  Type: Membership Report (0x22)
  Reserved: 00
  Checksum: 0xea03 [correct]
  [Checksum Status: Good]
  Reserved: 0000
  Num Group Records: 1
  ▼ Group Record : 239.255.255.250 Change To Exclude Mode
    Record Type: Change To Exclude Mode (4)
    Aux Data Len: 0
    Num Src: 0
    Multicast Address: 239.255.255.250
```

Server A (HD)

Server B (SD)



Membership Report
Solo de Server A



Usuario A



Usuario B



Join at
slido.com
#3579 339

🔍 Passcode:
abgxyi

¿Cuál es la versión predeterminada de IGMP que ejecutan los switches Catalyst 9000?

a) IGMPv1

0%

b) IGMPv2

0%

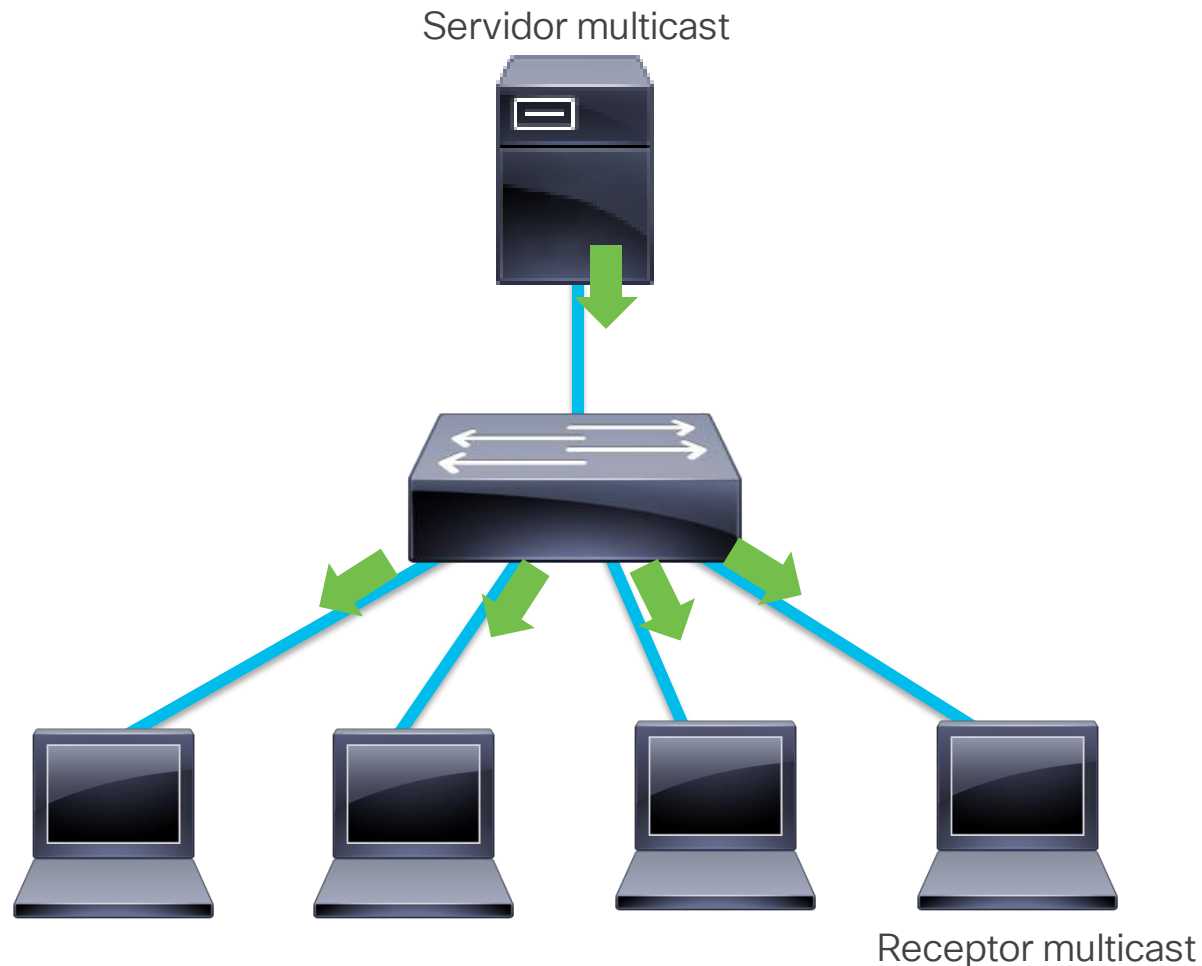
c) IGMPv3

0%

IGMP Snooping

- Introducción a Multicast
- IGMP y Multicast en Capa 2
- **IGMP Snooping**
- Configurar IGMP Snooping
- TAC Tips para Resolución de Problemas

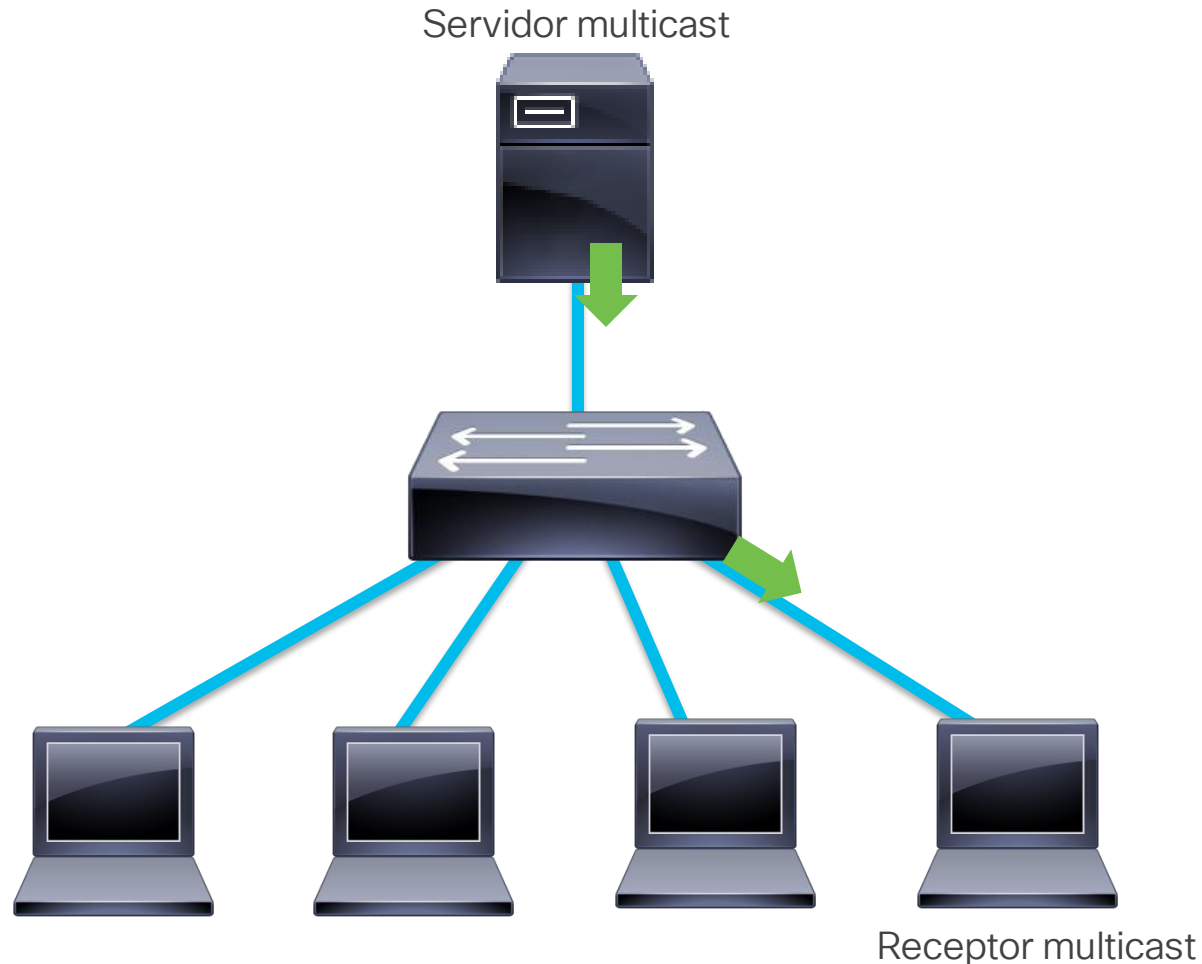
Manejo de tráfico multicast sin IGMP Snooping



- El tráfico es "inundado" por el switch.
- ¿Qué pasa en un ambiente con múltiples switches?
 - Ineficiencia
 - Seguridad
 - Inestabilidad

IGMP Snooping resuelve estos temas

Manejo de tráfico multicast con IGMP Snooping



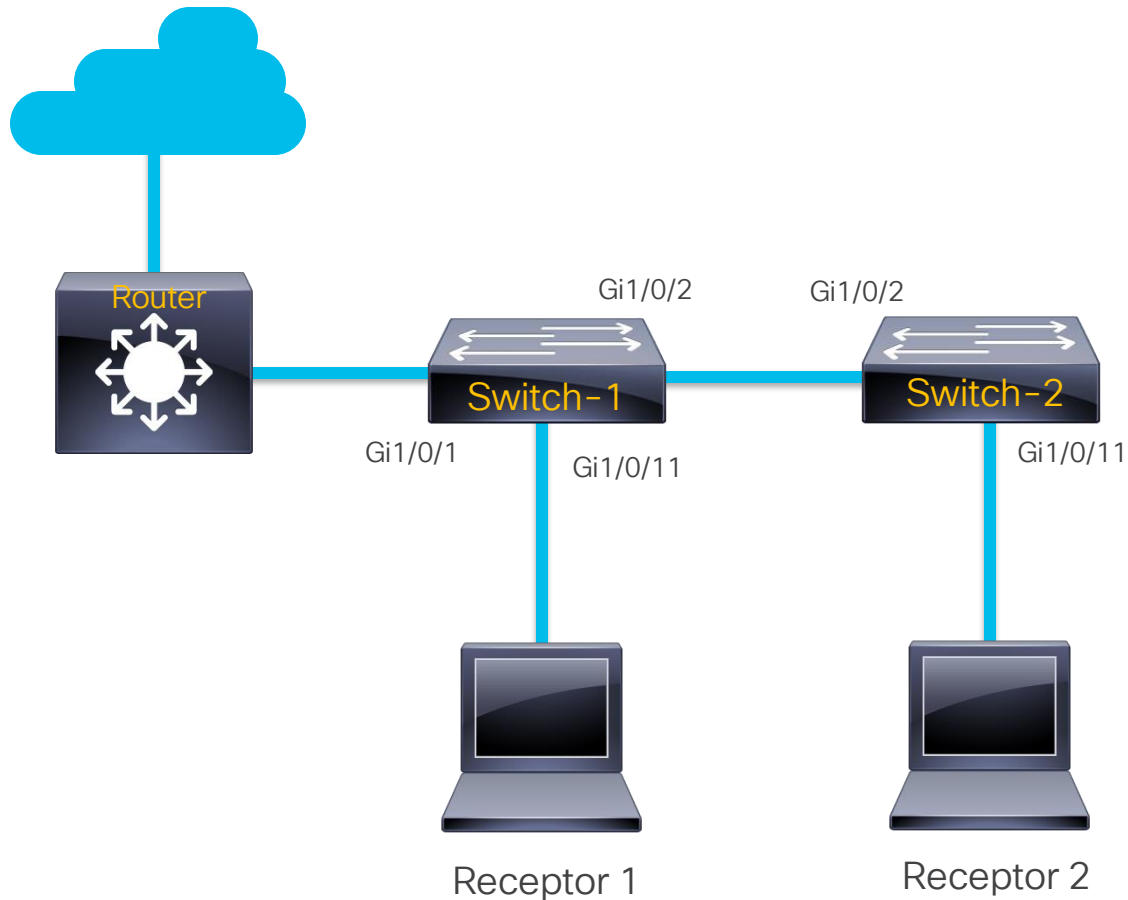
- El switch escucha y monitorea mensajes de IGMP.
- El tráfico multicast solo es enviado a puertos con dispositivos interesados.
- Optimiza el rendimiento de la red, la seguridad y escalabilidad de aplicaciones multicast.



Tráfico inmune a IGMP snooping:

- Rango local 224.0.0.0/24
- Cisco auto-rp 224.0.1.39-40

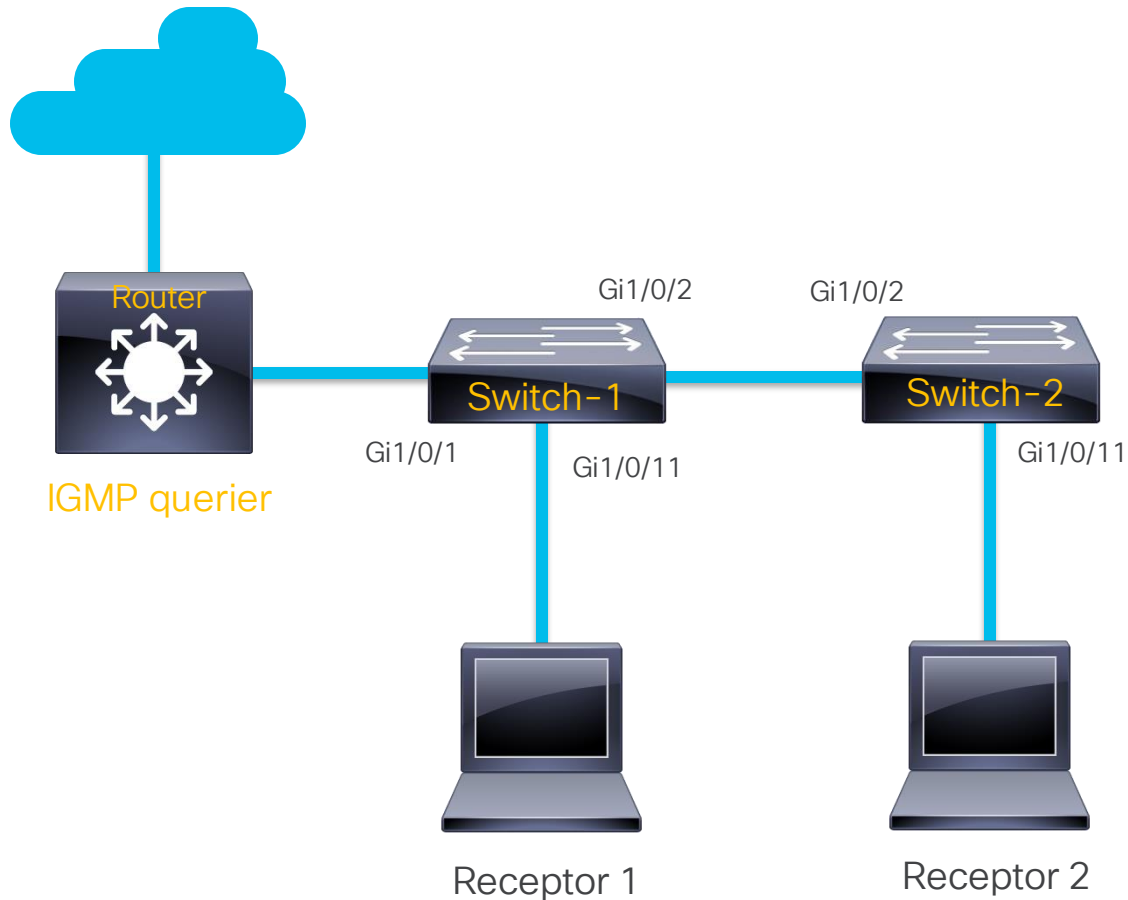
Funcionamiento de IGMP Snooping



- Para que IGMP Snooping de forma dinámica funcione se necesita:

- ✓ IGMP querier
- ✓ Puerto mrouter
- ✓ Receptor IGMP

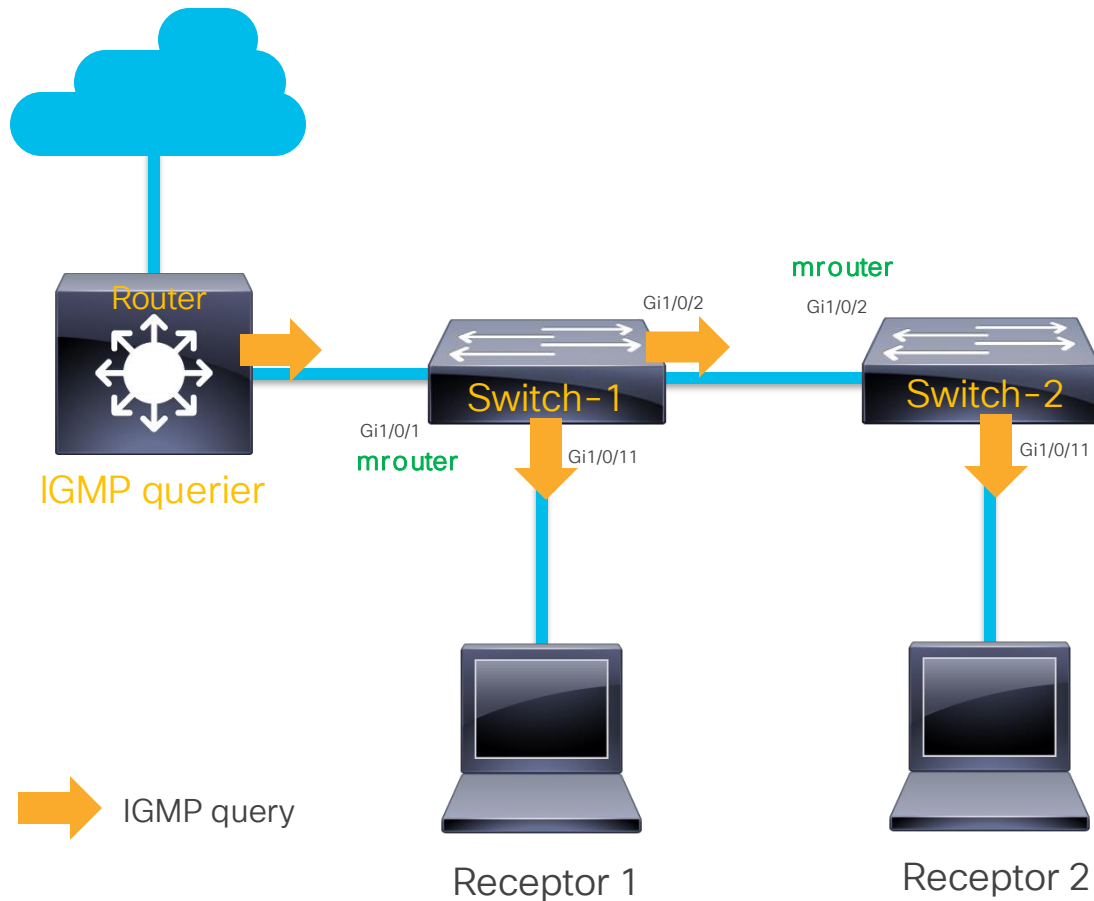
Funcionamiento de IGMP Snooping



✓ IGMP querier

- Generalmente es el multicast router en la VLAN. Habilitar PIM en una interfaz capa 3 también habilita IGMP.
- Si no hay un multicast router en la VLAN, se puede configurar un switch como IGMP snooping querier.

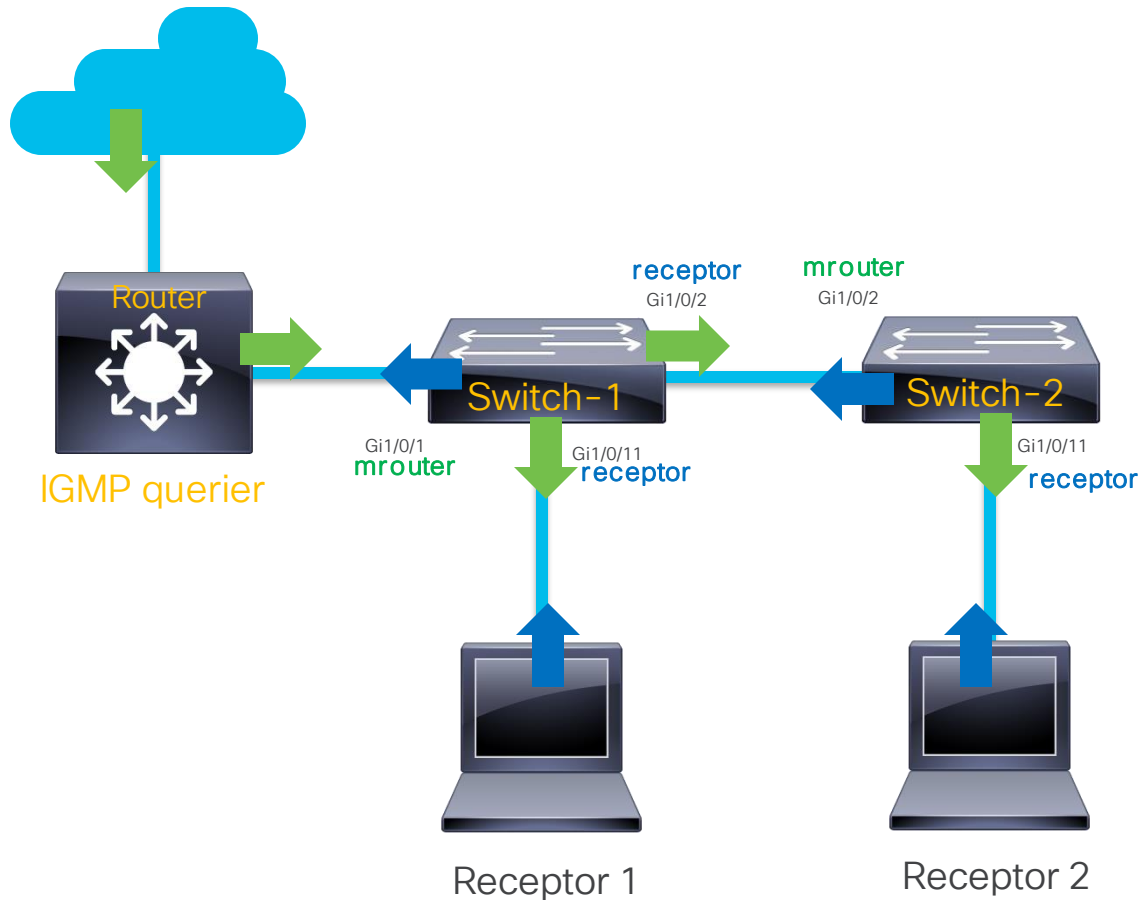
Funcionamiento de IGMP Snooping



✓ Puerto mrouter

- Puerto(s) conectado(s) hacia el multicast router o IGMP querier
- Se aprenden de forma dinámica al recibir IGMP queries o PIM hellos
- Todo el tráfico multicast se envía por el puerto mrouter (incluyendo membership reports)

Funcionamiento de IGMP Snooping

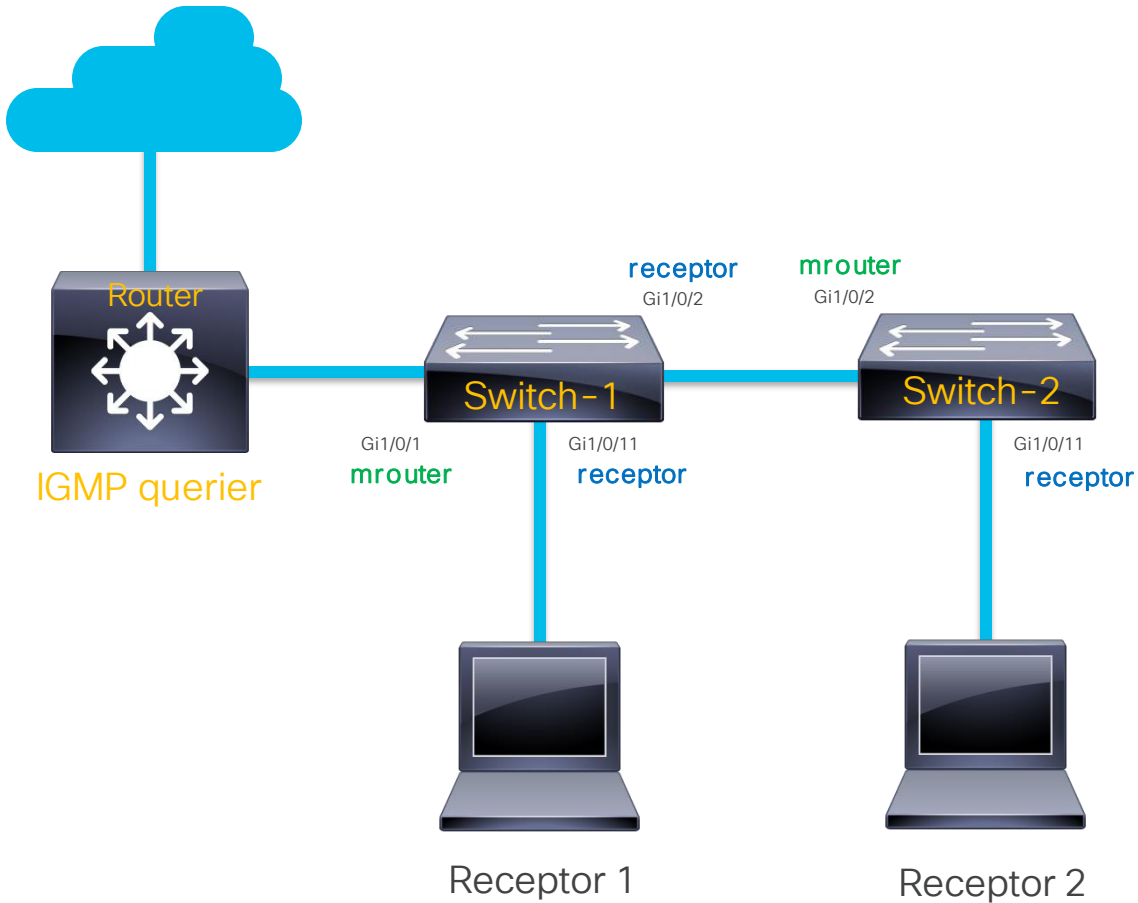


✓ Receptor IGMP

- Al recibir un IGMP membership report, el switch añade la interfaz a la forwarding-table para ese grupo multicast.

- ➡ IGMP membership report grupo 239.1.1.1
- ➡ Tráfico multicast grupo 239.1.1.1

Verificando IGMP Snooping



Switch-1

```
Switch-1#show ip igmp snooping mrouter
```

```
Vlan  ports
----  ----
    10  Gi1/0/1(dynamic)
```

```
Switch-1#show ip igmp snooping groups
```

Vlan	Group	Type	Version	Port List
10	239.1.1.1	igmp	v2	Gi1/0/2, Gi1/0/11

```
Switch-1#show ip igmp snooping querier
```

Vlan	IP Address	IGMP Version	Port
10	192.168.10.1	v2	Gi1/0/1

Switch-2

```
Switch-2#show ip igmp snooping mrouter
```

```
Vlan  ports
----  ----
    10  Gi1/0/2(dynamic)
```

```
Switch-2#show ip igmp snooping groups
```

Vlan	Group	Type	Version	Port List
10	239.1.1.1	igmp	v2	Gi1/0/11

```
Switch-2#show ip igmp snooping querier
```

Vlan	IP Address	IGMP Version	Port
10	192.168.10.1	v2	Gi1/0/2



¿Qué comando es útil para validar la lista de puertos en los que hay clientes interesados en tráfico multicast?

a) show ip igmp snooping groups

0%

b) show ip igmp snooping clients

0%

c) show ip igmp snooping mrouter

0%

Join at
slido.com
#3579 339

🔒 Passcode:

abgxyi

Configurar IGMP Snooping

- Introducción a Multicast
- IGMP y Multicast en Capa 2
- IGMP Snoping
- **Configurar IGMP Snooping**
- TAC Tips para Resolución de Problemas

IGMP Snooping con multicast router presente

- IGMP snooping está habilitado por defecto en todas las VLANs.
- Si hay un IGMP querier en la VLAN, IGMP snooping programará los puertos mrouter de manera dinámica y no se necesita configuración adicional.
- Al habilitar PIM en una interfaz del router, también se habilita IGMP, y enviará queries.

```
ip multicast-routing  
!  
interface Vlan10  
  ip address 192.168.10.1 255.255.255.0  
  ip pim sparse-mode  
end
```

IGMP Snooping sin multicast router presente

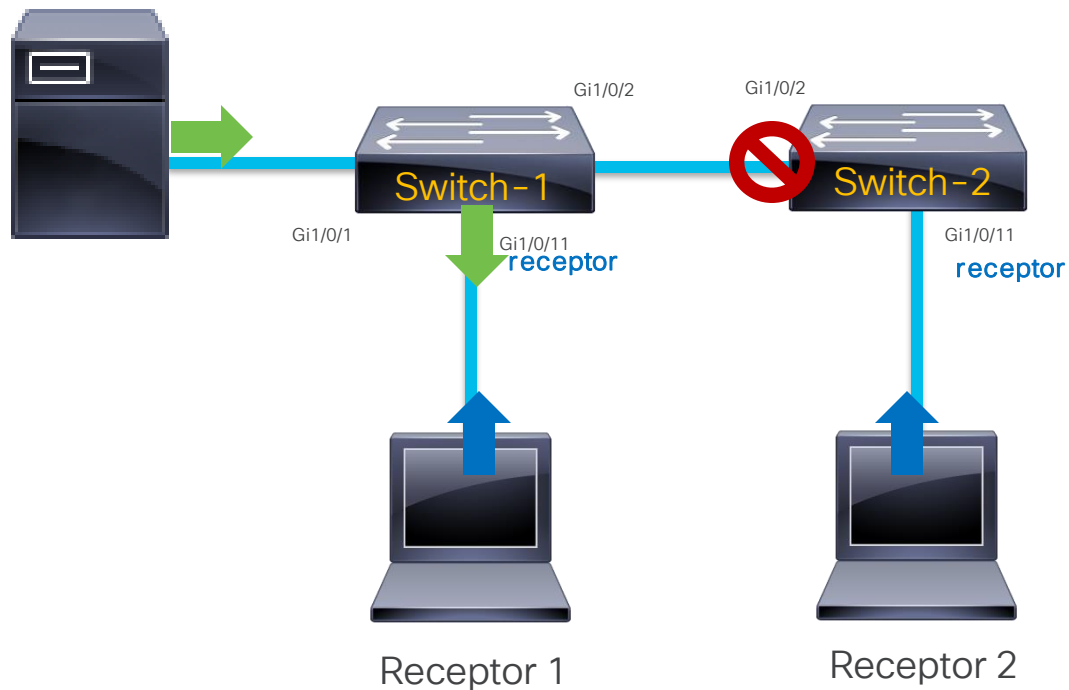
- Si no hay un multicast router en la VLAN, se necesita configurar un IGMP snooping querier para permitir el envío de tráfico multicast en la misma VLAN.

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



- El switch envía IGMP queries, los cuales programa los puertos mrouter de los otros switches en la VLAN.
- El switch debe tener al menos una interfaz capa 3 para ser la dirección IP origen de los IGMP queries.

IGMP Snooping sin IGMP querier

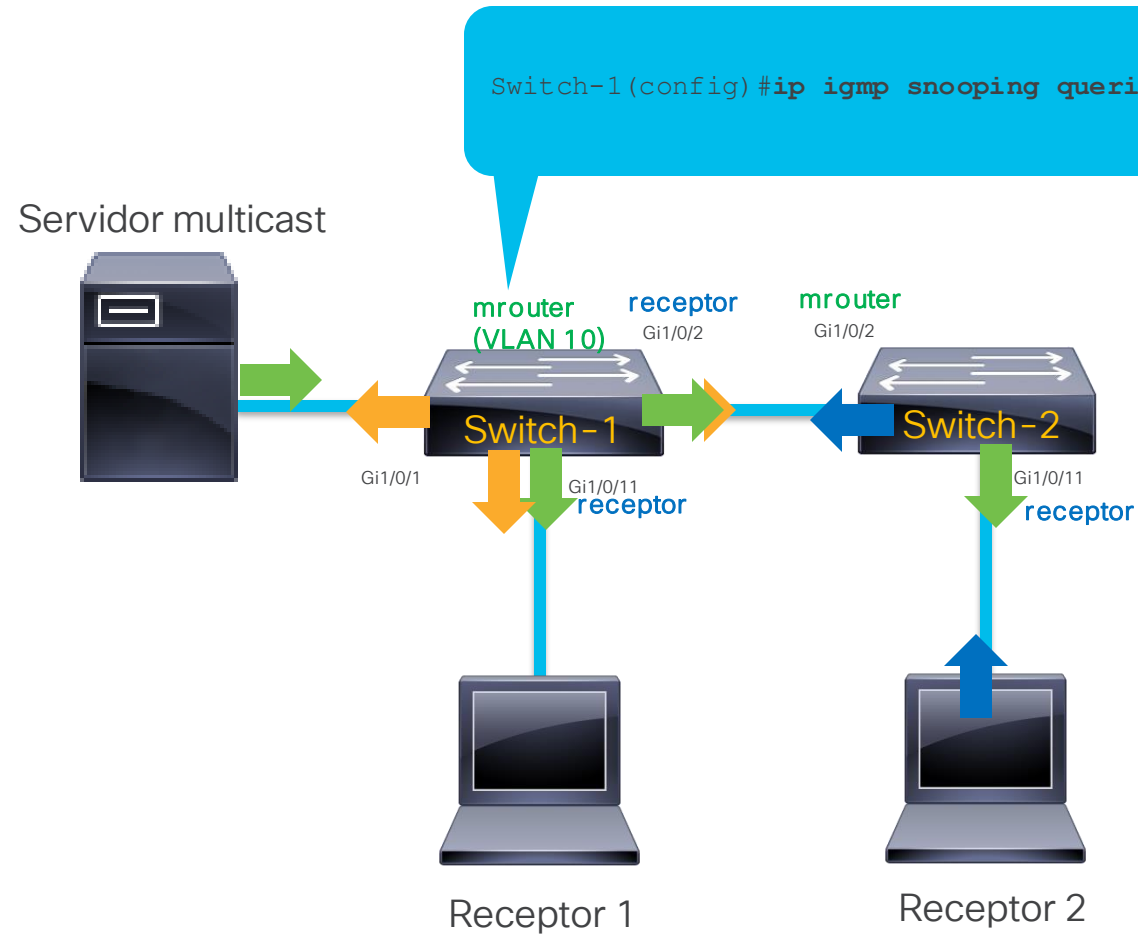
Servidor multicast



¿Cómo lo solucionamos?

-  IGMP membership report grupo 239.1.1.1
-  Tráfico multicast grupo 239.1.1.1

IGMP Snooping con IGMP querier



Switch-1 tiene una SVI en la VLAN 10, sin configuración de PIM.

```
Switch-1#sh run int vlan 10
!
interface Vlan10
 ip address 192.168.10.11 255.255.255.0
end
```

- IGMP membership report grupo 239.1.1.1
- Tráfico multicast grupo 239.1.1.1
- IGMP query

Configuración estática de IGMP Snooping

- No hay un IGMP querier en la red

```
Switch(config)# ip igmp snooping vlan 10 mrouter interface Gi1/0/1
```

- El receptor multicast no soporta IGMP

```
Switch(config)# ip igmp snooping vlan 10 static 239.1.1.1 interface Gi1/0/3
```



¿Con qué comando se habilita IGMP Snooping querier en un switch?

a) Switch(config)# ip igmp snooping enable querier

0%

b) Switch(config)# ip pim querier

0%

c) Switch(config)# ip igmp snooping querier

0%

Join at
slido.com
#3579 339

🔒 Passcode:
abgxyi

TAC Tips para Resolución de Problemas

- Introducción a Multicast
- IGMP y Multicast en Capa 2
- IGMP Snooping
- Configurar IGMP Snooping
- TAC Tips para Resolución de Problemas

Problemas comunes en multicast para Catalyst 9000

Problemas en CPU por tráfico multicast

Pérdida total del tráfico multicast

¿Cómo los manejamos?



Herramientas para diagnosticar problemas

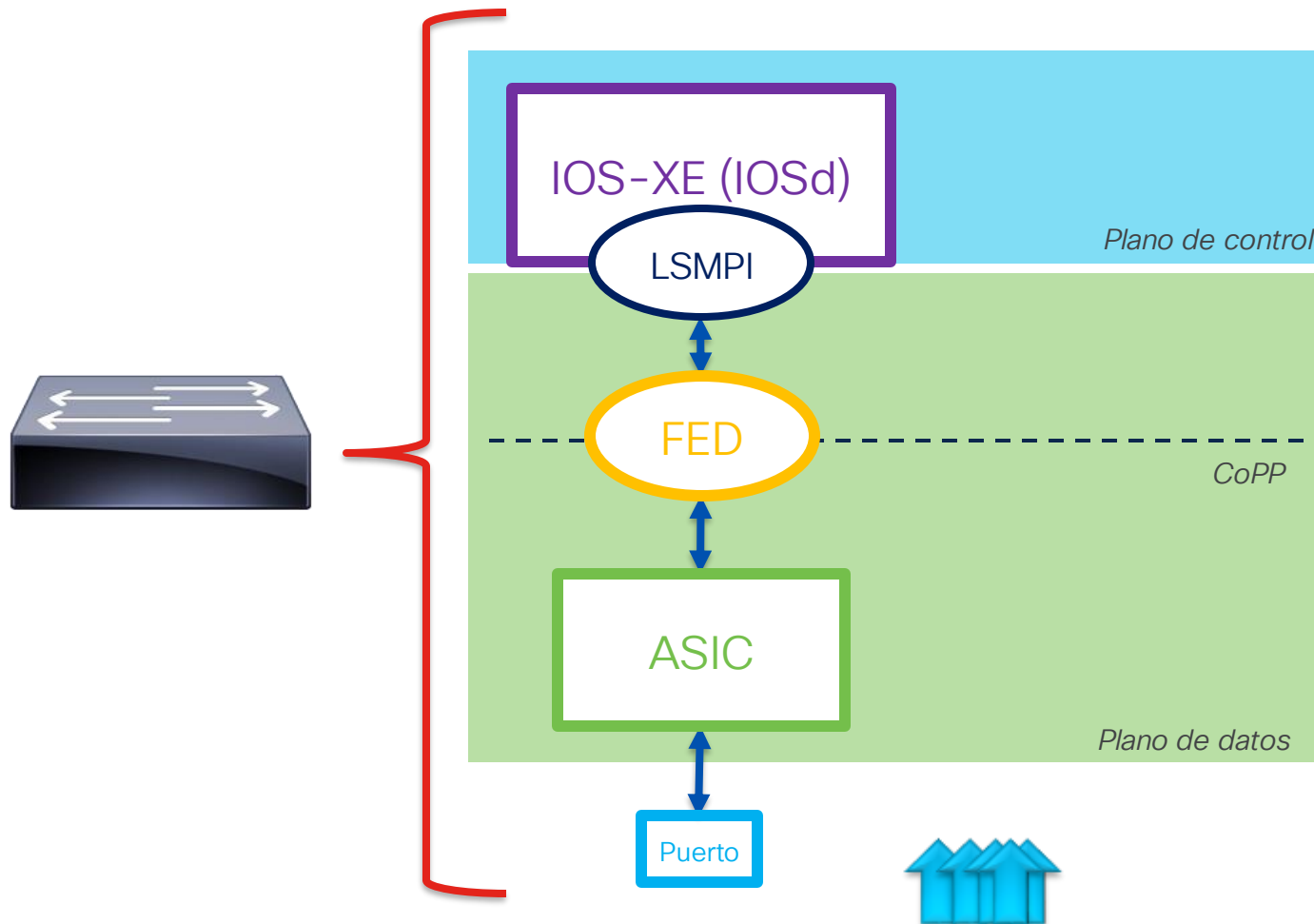
- Información del problema {
- Topología
 - Dirección IP del grupo multicast
 - Dirección IP del servidor multicast
 - Dirección IP del cliente multicast

- Tablas y debugs de IGMP Snooping {
- `show ip igmp snooping groups`
 - `show ip igmp snooping mrouter`
 - `show ip igmp snooping querier`
 - `debug ip igmp snooping`

- Herramientas de captura de paquetes {
- Embedded Packet Capture (EPC) {
 - `monitor capture TAC interface GiX/Y/Z in access-list IGMP start`
 - `monitor capture TAC stop`
 - `show monitor capture TAC buffer { brief | detailed }`
 - FED CPU Debug {
 - `debug platform software fed switch active punt packet-capture start`
 - `debug platform software fed switch active punt packet-capture stop`
 - `show platform software fed switch active punt packet-capture brief`

- Estado de CoPP y CPU {
- `show platform hardware fed switch active qos queue stats internal cpu policer`
 - `show process cpu sorted | exclude 0.00`

Recordatorio de CoPP y tráfico hacia el CPU en Cat9k




Control Plane Policing (CoPP)
Es una serie de políticas que protegen al CPU de tráfico excesivo hacia el Plano de Control

Causas comunes de problemas en CoPP y CPU

Causa de tráfico subiendo a CPU	Fila de CoPP	Tasa de aceptación
Tormenta de tráfico IGMP	MCAST END STATION	2000 pps
Tormenta de tráfico PIM	Routing Control	5400 pps
Proceso PIM Registering / TTL1	MCAST Data	400 pps
Tráfico de datos en grupo reservado (224.0.0.X)		
"ip igmp join-group" en SVI		

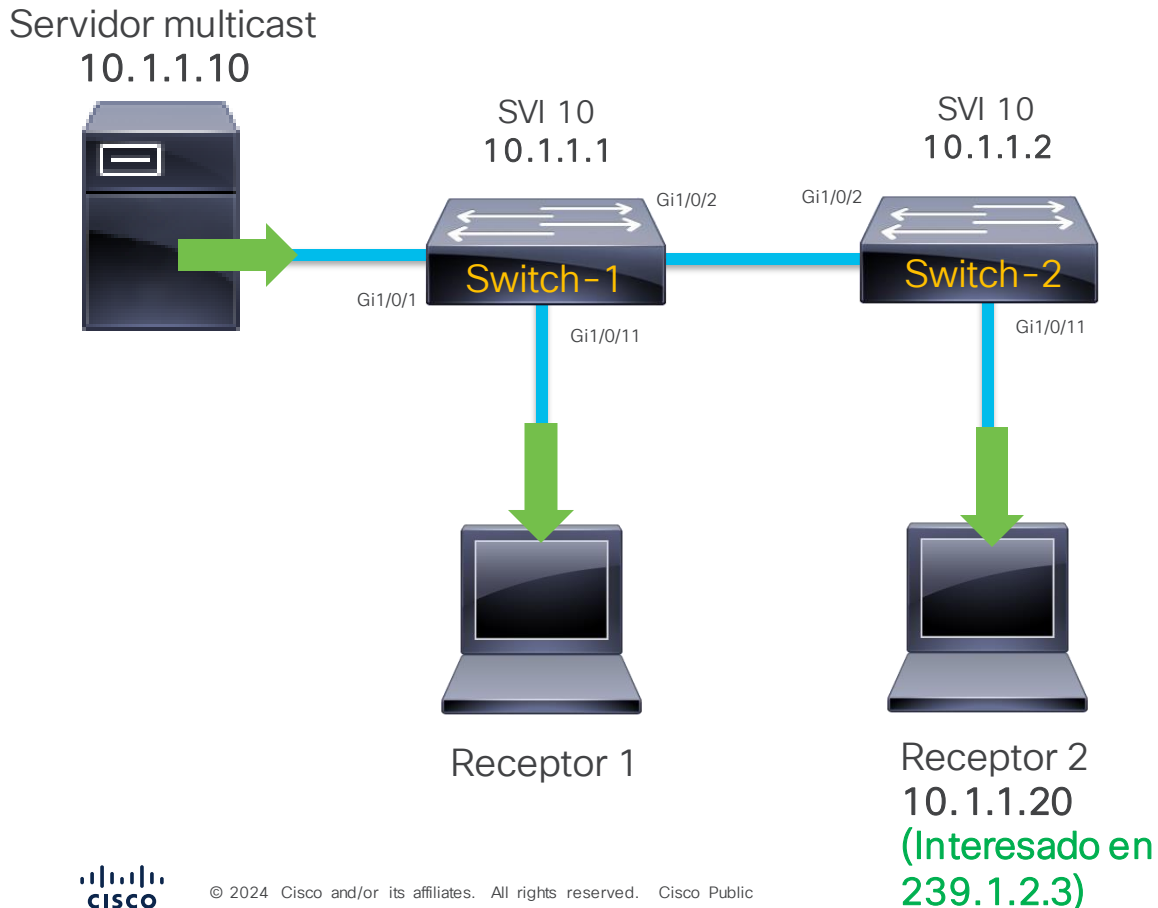
Provocan fallas en el funcionamiento de los protocolos (IGMP o PIM), pues tráfico de control puede ser descartado antes de llegar al CPU. La tasa de aceptación es alta, entonces pueden causar alta utilización de CPU.



Provocan una carga innecesaria al CPU, generalmente tráfico de datos. CoPP usualmente previene que aturdan al CPU.

*Más información sobre PIM Registering [aquí](#).

Escenario 1: Tráfico intermitente



Descripción del Problema

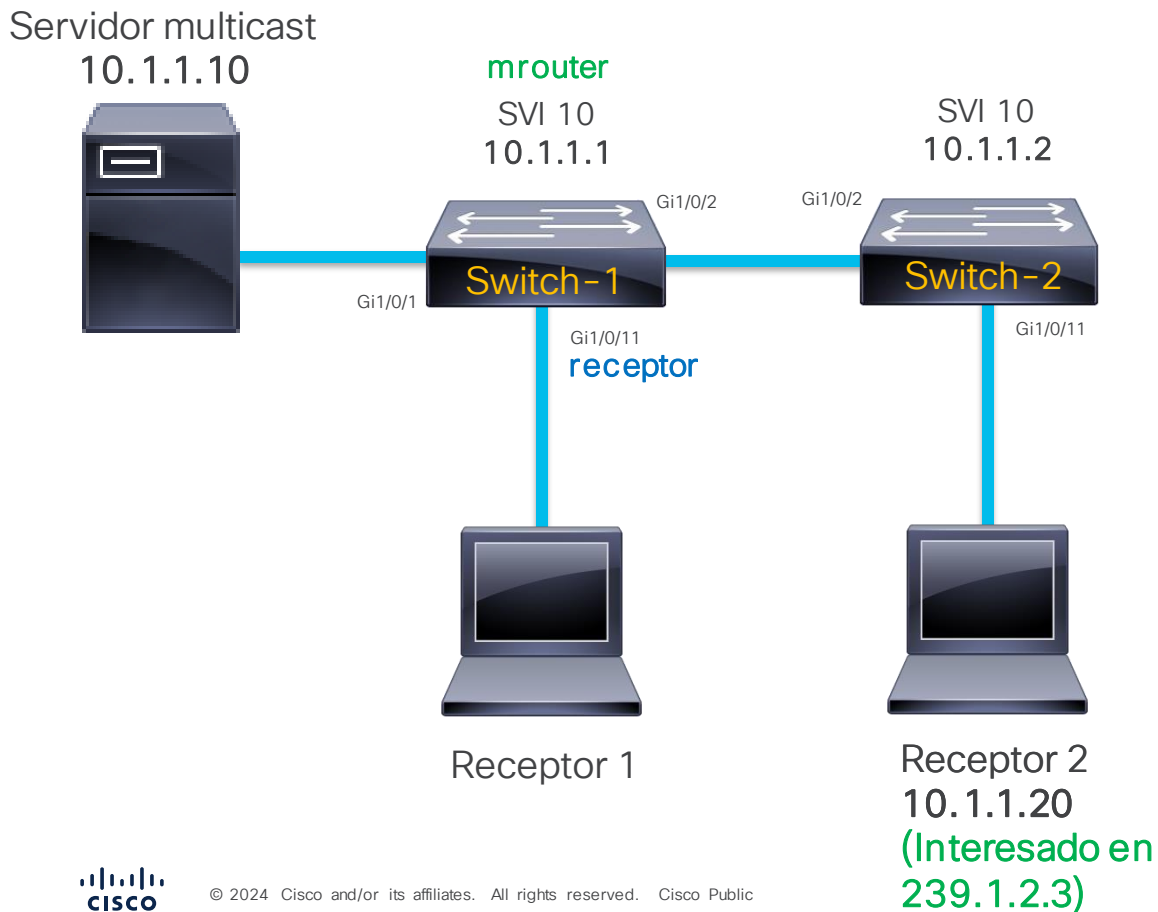
Receptor 2 recibe tráfico del grupo multicast 239.1.2.3 de forma intermitente.
Receptor 1 recibe el mismo tráfico de manera correcta y sin interrupciones.

¿Cada cuánto? Pueden ser cada 5 minutos, 10 o más. La interrupción también puede durar pocos o varios minutos. Parece ser aleatorio.

Hallazgos:

- Servidor envía el tráfico de manera constante.

Escenario 1: Tráfico intermitente



1 Validar IGMP snooping en los switches

Switch-1

```
Switch-1#show ip igmp snooping mrouter
```

```
Vlan ports  
----  
10 Router
```

```
Switch-1#show ip igmp snooping querier
```

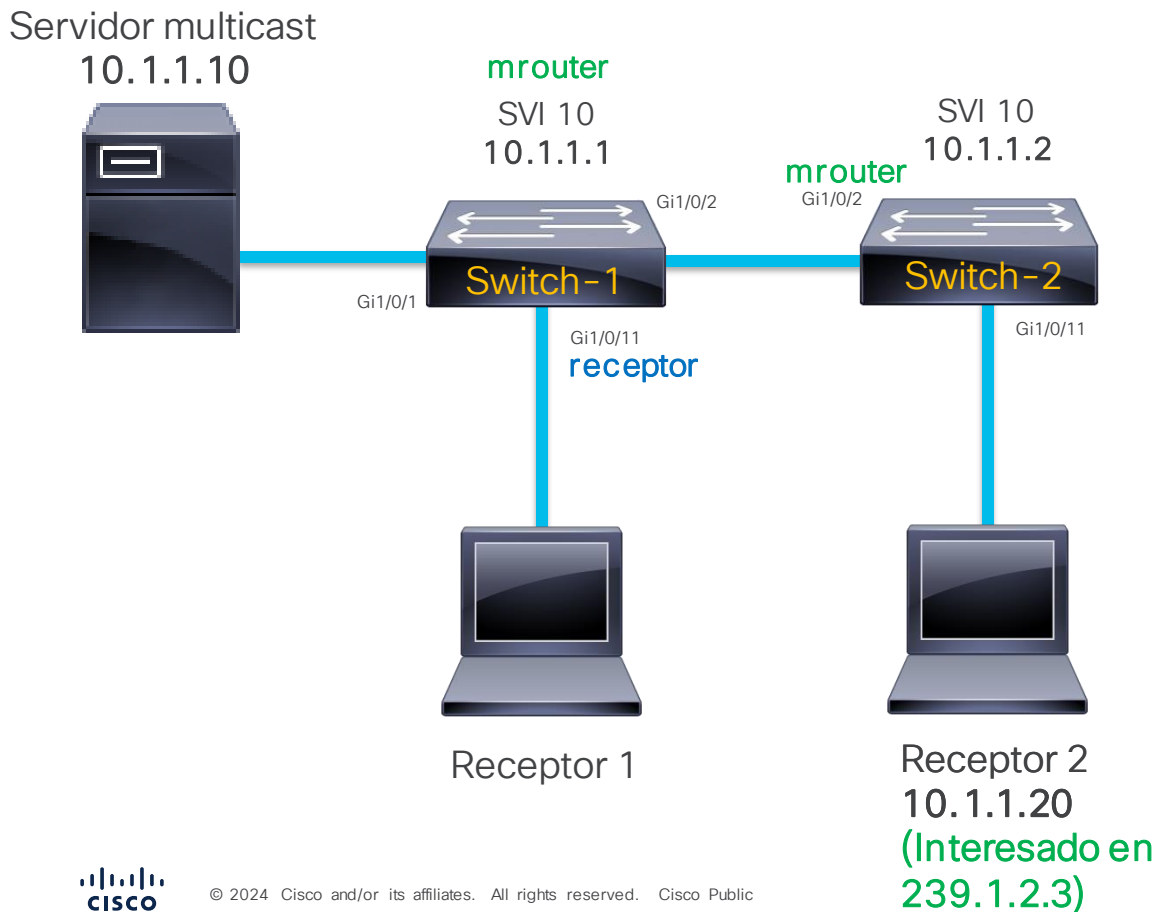
```
Vlan IP Address IGMP Version Port  
-----  
10 10.1.1.1 v2 Router
```

```
Switch-1#show ip igmp snooping groups
```

```
Vlan Group Type Version Port List  
-----  
10 239.1.1.1 igmp v2 Gi1/0/2  
10 239.1.2.3 igmp v2 Gi1/0/11
```

No está Gig1/0/2 para 239.1.2.3

Escenario 1: Tráfico intermitente



1 Validar IGMP snooping en los switches

Switch-2

```
Switch-2#show ip igmp snooping mrouter
Vlan    ports
-----
  10    Gi1/0/2 (dynamic)

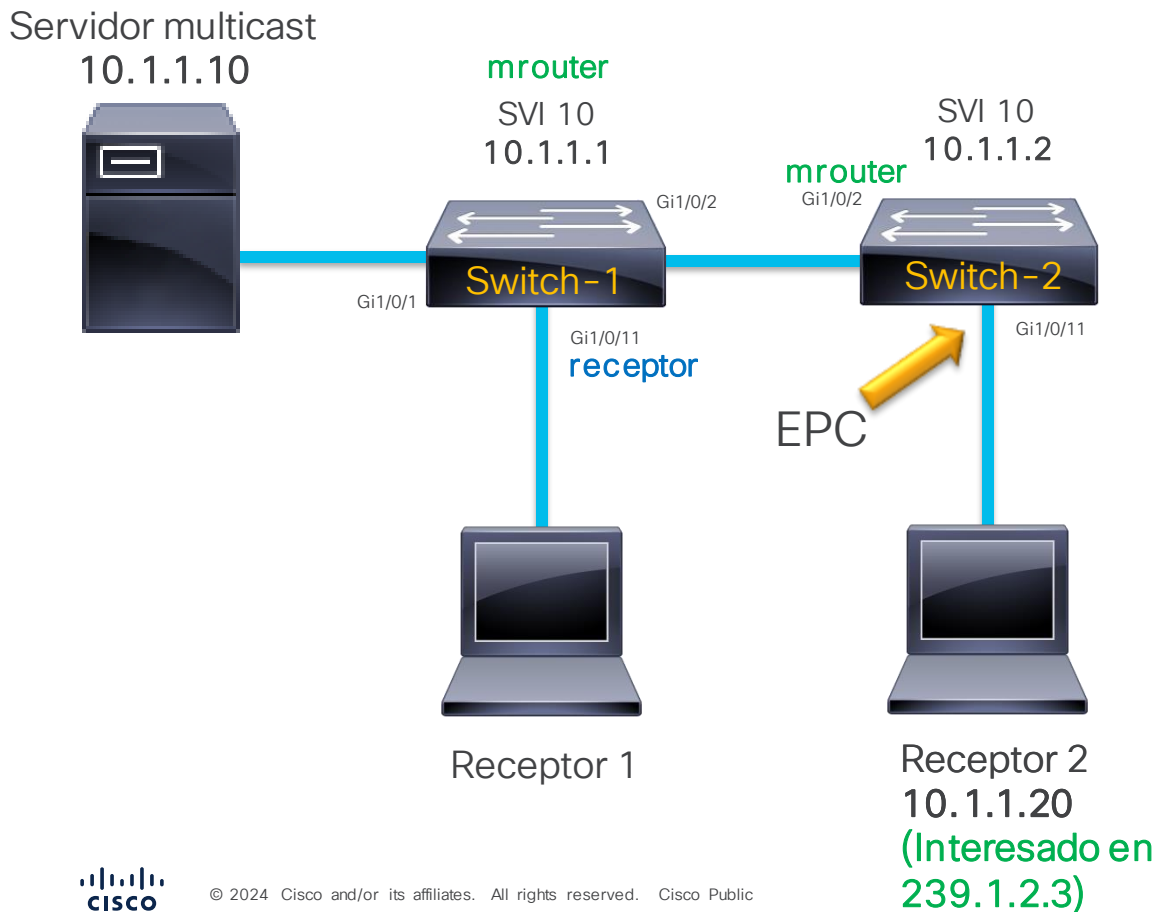
Switch-2#show ip igmp snooping querier
Vlan    IP Address      IGMP Version  Port
-----
  10    10.1.1.1        v2            Gi1/0/2

Switch-2#show ip igmp snooping groups
Vlan    Group           Type          Version  Port List
-----
  10    239.1.1.1      igmp         v2      Gi1/0/1
```

No está Gig1/0/11 para 239.1.2.3

Todo parece indicar que receptor 2 no envía el IGMP membership report...

Escenario 1: Tráfico intermitente



2

Validar que el receptor está interesado

Switch-2

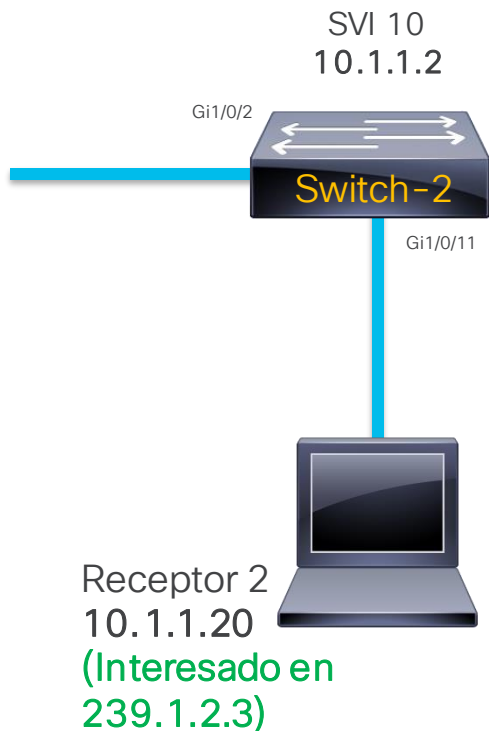
```
Switch-2#monitor capture TAC interface Gi1/0/11 in access-list IGMP start  
  
Switch-2#monitor capture TAC stop  
  
Switch-2#show monitor capture TAC buffer brief  
Starting the packet display ..... Press Ctrl + Shift + 6 to exit  
  
1  0.000000  10.1.1.20 -> 239.1.2.3  IGMPv2 64 Membership Report group 239.1.2.3  
2  8.112090  10.1.1.20 -> 239.1.2.3  IGMPv2 64 Membership Report group 239.1.2.3  
3  15.564242  10.1.1.20 -> 239.1.2.3  IGMPv2 64 Membership Report group 239.1.2.3
```

Receptor 2 sí envía el report

¿Switch 2 no está procesando el IGMP memberhsip report?

Escenario 1: Tráfico intermitente

Debugs (IOSd)



3

Validar por qué Switch-2 no procesa el report

Switch-2

```
Switch-2#debug ip igmp snooping
```

```
Switch-2#show logging
```

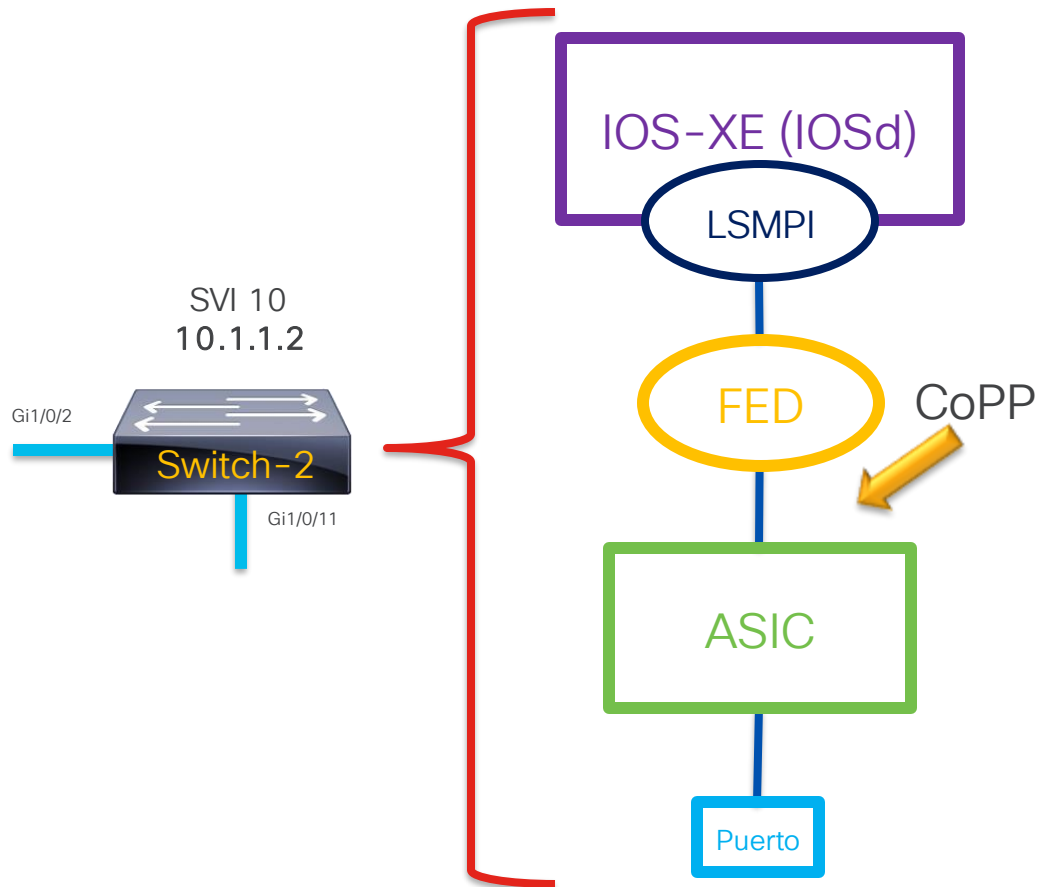
```
*May 27 21:04:14.850: IGMP SN: Received IGMPv2 Report for group 239.1.1.1 received on Vlan 10, port Gi1/0/1
*May 27 21:04:14.850: IGMP SN: Group: Received IGMPv2 report for mcast group 239.1.1.1 from Client 10.1.1.100.
Received on Vlan 10, port Gi1/0/1.
*May 27 21:04:14.851: IGMP SN: Received IGMPv2 Report for group 239.1.1.1 received on Vlan 10, port Gi1/0/1
*May 27 21:04:14.851: IGMP SN: Group: Received IGMPv2 report for mcast group 239.1.1.1 from Client 10.1.1.100.
Received on Vlan 10, port Gi1/0/1.
*May 27 21:04:14.851: IGMP SN: Received IGMPv2 Report for group 239.1.1.1 received on Vlan 10, port Gi1/0/1
*May 27 21:04:14.851: IGMP SN: Group: Received IGMPv2 report for mcast group 239.1.1.1 from Client 10.1.1.100.
Received on Vlan 10, port Gi1/0/1.
*May 27 21:04:14.852: IGMP SN: Received IGMPv2 Report for group 239.1.1.1 received on Vlan 10, port Gi1/0/1
*May 27 21:04:14.852: IGMP SN: Group: Received IGMPv2 report for mcast group 239.1.1.1 from Client 10.1.1.100.
Received on Vlan 10, port Gi1/0/1.
```

```
Switch-2# show logging | include 239.1.2.3
Switch-2#
```



Los reports no llegan a IOSd

Escenario 1: Tráfico intermitente



3 Validar por qué Switch-2 no procesa el report

Switch-2

```
Switch-2#show platform hardware fed switch active qos queue stats internal cpu policer
```

CPU Queue Statistics							
QId	PlcIdx	Queue Name	Enabled	(default) Rate	(set) Rate	Queue Drop(Bytes)	Queue Drop(Frames)
<snip>							
20	15	MCAST END STATION	Yes	2000	2000	424320	79483
<snip>							

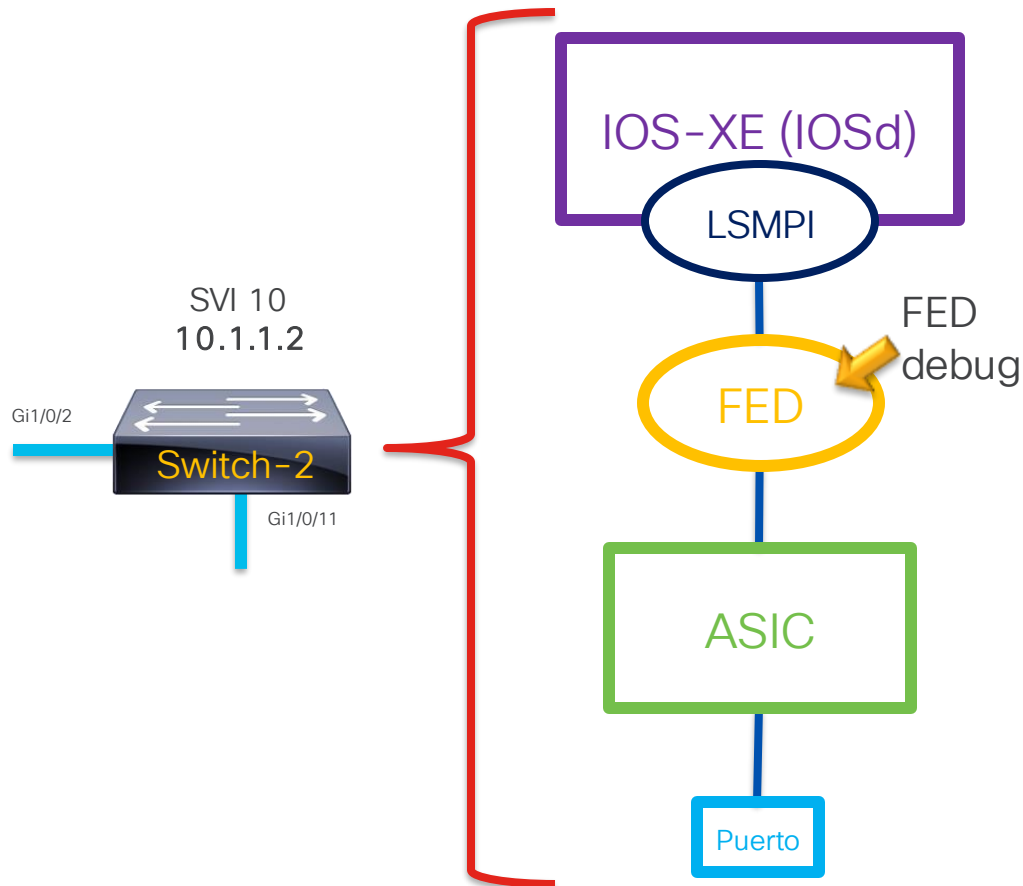
```
Switch-2#show platform hardware fed switch active qos queue stats internal cpu policer
```

CPU Queue Statistics							
QId	PlcIdx	Queue Name	Enabled	(default) Rate	(set) Rate	Queue Drop(Bytes)	Queue Drop(Frames)
<snip>							
20	15	MCAST END STATION	Yes	2000	2000	424320	118291
<snip>							

CoPP tirando tráfico en la fila que maneja IGMP

¿Por qué hay más de 2000 pps de IGMP subiendo a CPU?

Escenario 1: Tráfico intermitente



3 Validar por qué Switch-2 no procesa el report

Switch-2

```
Switch-2#debug platform software fed switch active punt packet-capture start
Punt packet capturing started.


Switch-2#debug platform software fed switch active punt packet-capture stop
Punt packet capturing stopped. Captured 4096 packet(s)

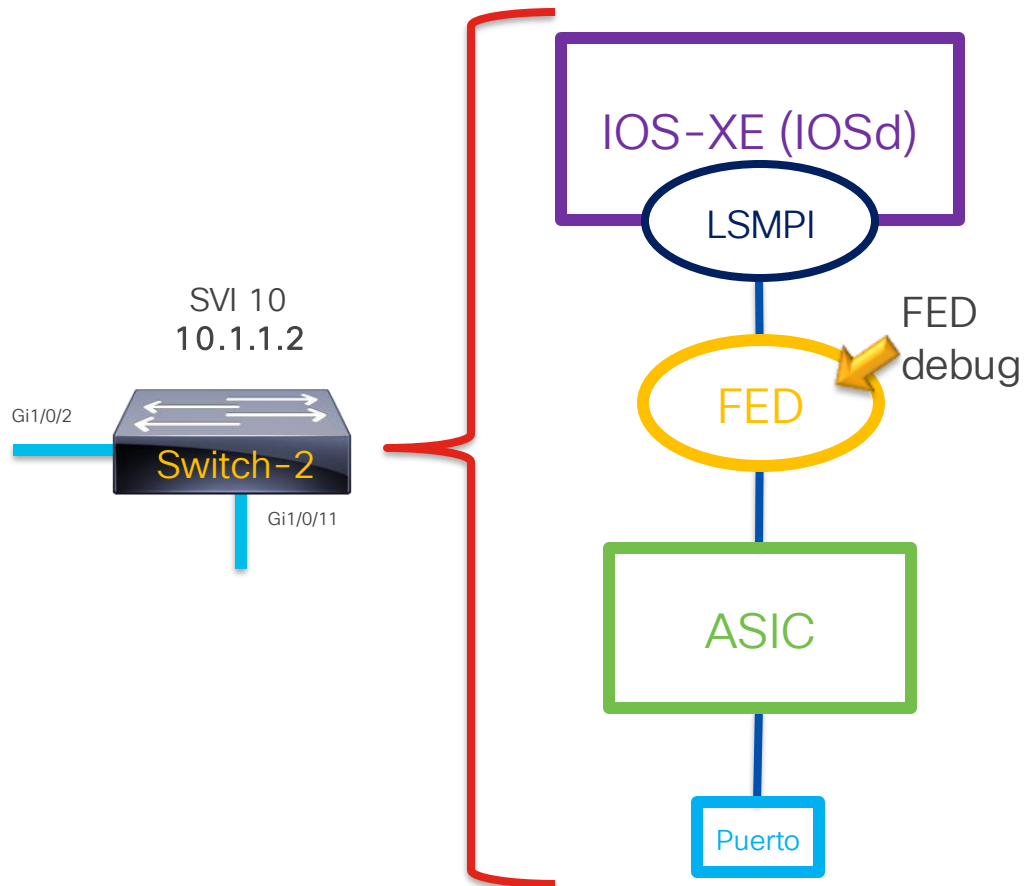
Switch-2#show platform software fed switch active punt packet-capture brief
Punt packet capturing: disabled. Buffer wrapping: disabled
Total captured so far: 4096 packets. Capture capacity : 4096 packets

----- Punt Packet Number: 1, Timestamp: 2024/05/25 04:50:16.698 -----
interface : physical: GigabitEthernet1/0/1[if-id: 0x0000000a], pal: GigabitEthernet1/0/1
[if-id: 0x0000000a]
metadata : cause: 58 [Layer2 bridge domain data packet], sub-cause: 11, q-no: 20, linktype:
MCP_LINK_TYPE_IP [1]
ether hdr : dest mac: 0100.5e01.0101, src mac: 0000.0200.0002
ether hdr : ethertype: 0x0800 (IPv4)
ipv4 hdr : dest ip: 239.1.1.1, src ip: 10.1.1.100
ipv4 hdr : packet len: 28, ttl: 1, protocol: 2
```

Dispositivo agresor enviando tráfico IGMP

Escenario 1: Tráfico intermitente

 **cpu-top-talker** a partir de IOS-XE 17.6.X



3 Validar por qué Switch-2 no procesa el report

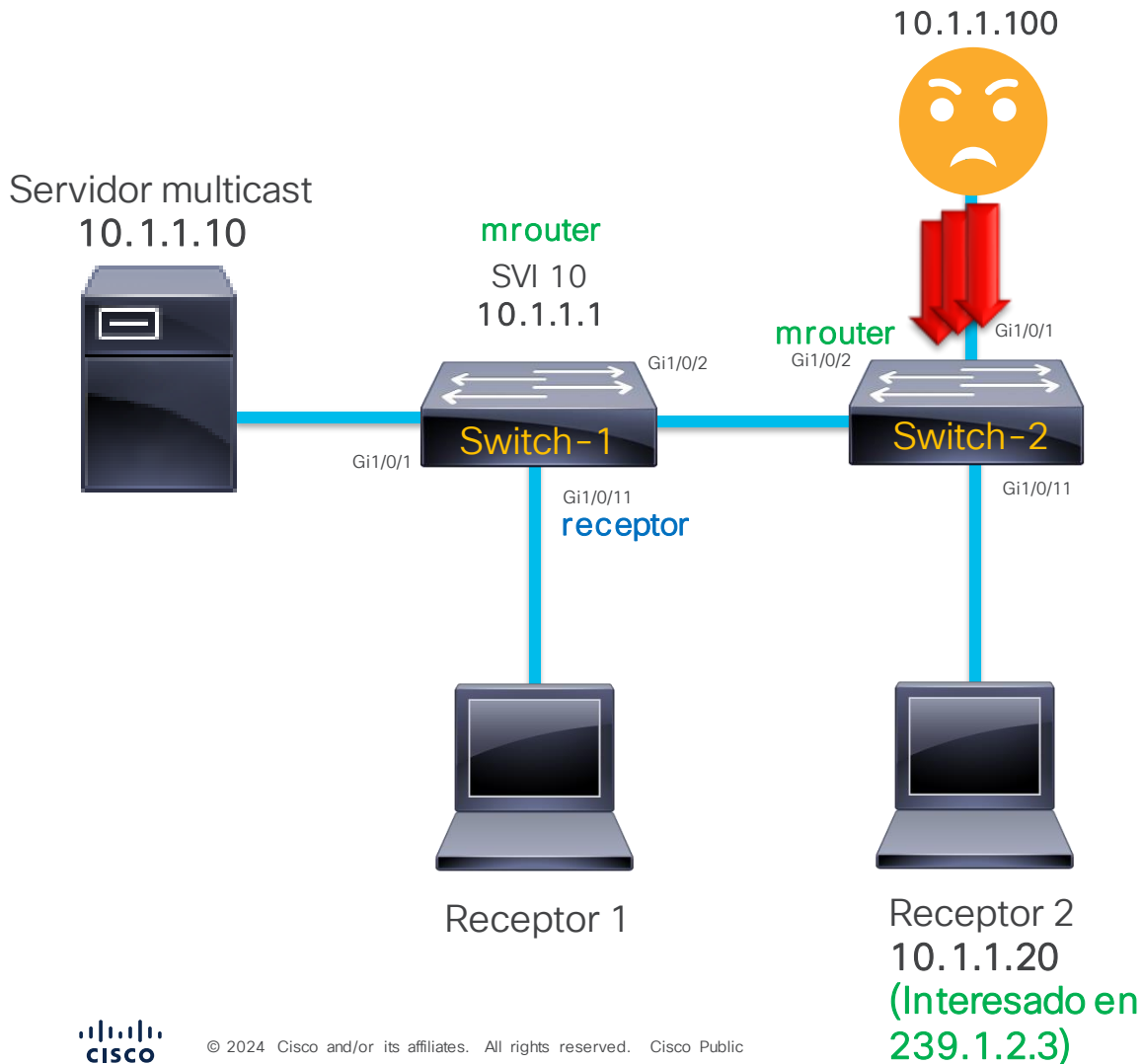
Switch-2

```
Switch-2#show platform software fed switch active punt packet-capture cpu-top-talker dst_ipv4
Punt packet capturing: disabled. Buffer wrapping: disabled
Total captured so far: 4096 packets. Capture capacity : 4096 packets
Sr.no. Value/Key Occurrence
1 239.1.1.1 4043
Not Included : 53

Switch-2#show platform software fed switch active punt packet-capture cpu-top-talker incoming-interface
Punt packet capturing: disabled. Buffer wrapping: disabled
Total captured so far: 4096 packets. Capture capacity : 4096 packets
Sr.no. Value/Key Occurrence
1 GigabitEthernet1/0/1 4043
2 GigabitEthernet1/0/31 53
Not Included : 0
```

Dispositivo agresor enviando tráfico IGMP confirmado

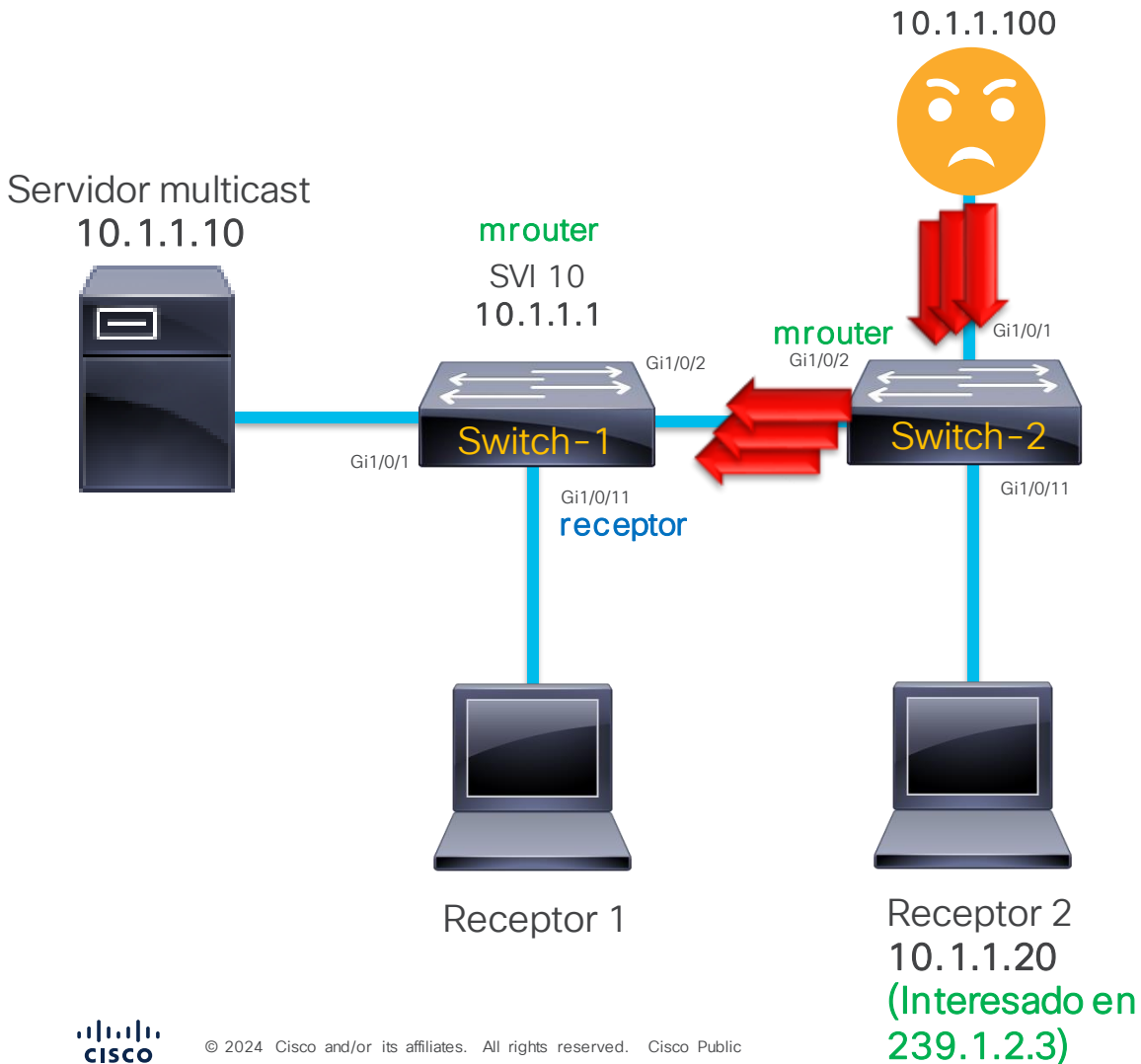
Escenario 1: Tráfico intermitente



4 Tomar acción correctiva

- Identificar el agresor (10.1.1.100) y arreglarlo para que deje de enviar tráfico IGMP.

Escenario 1: Tráfico intermitente



¿Por qué Switch-1 no se vio afectado?

- Si Switch-2 reenvía todo el tráfico multicast por el puerto mrouter, también debería reenviar todos los IGMP membership reports del agresor y causar el mismo problema en Switch-1.
- Esto no pasó gracias para **IGMP snooping report suppression** (habilitado por defecto).
- IGMP snooping report suppression limita los membership reports que son reenviados al puerto mrouter. Reenvía solamente 1 cada 10 segundos (o lo que indique el Max response time que envía el IGMP querier).



¿En qué fila de CoPP se controla el tráfico de IGMP?

a) MCAST END STATION

0%

b) Routing Control

0%

c) MCAST Data

0%

Join at

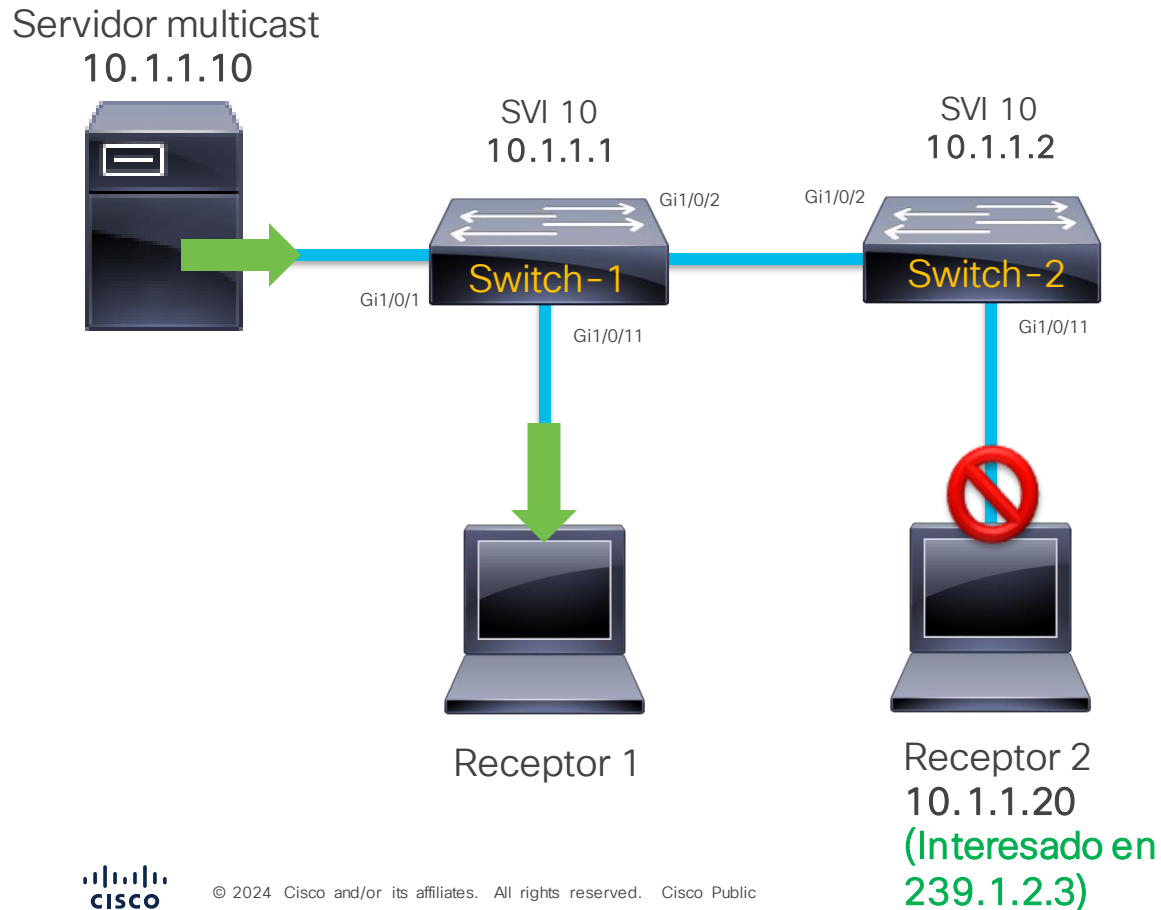
slido.com

#3579 339

🔒 Passcode:

abgxyi

Escenario 2: Pérdida total de tráfico



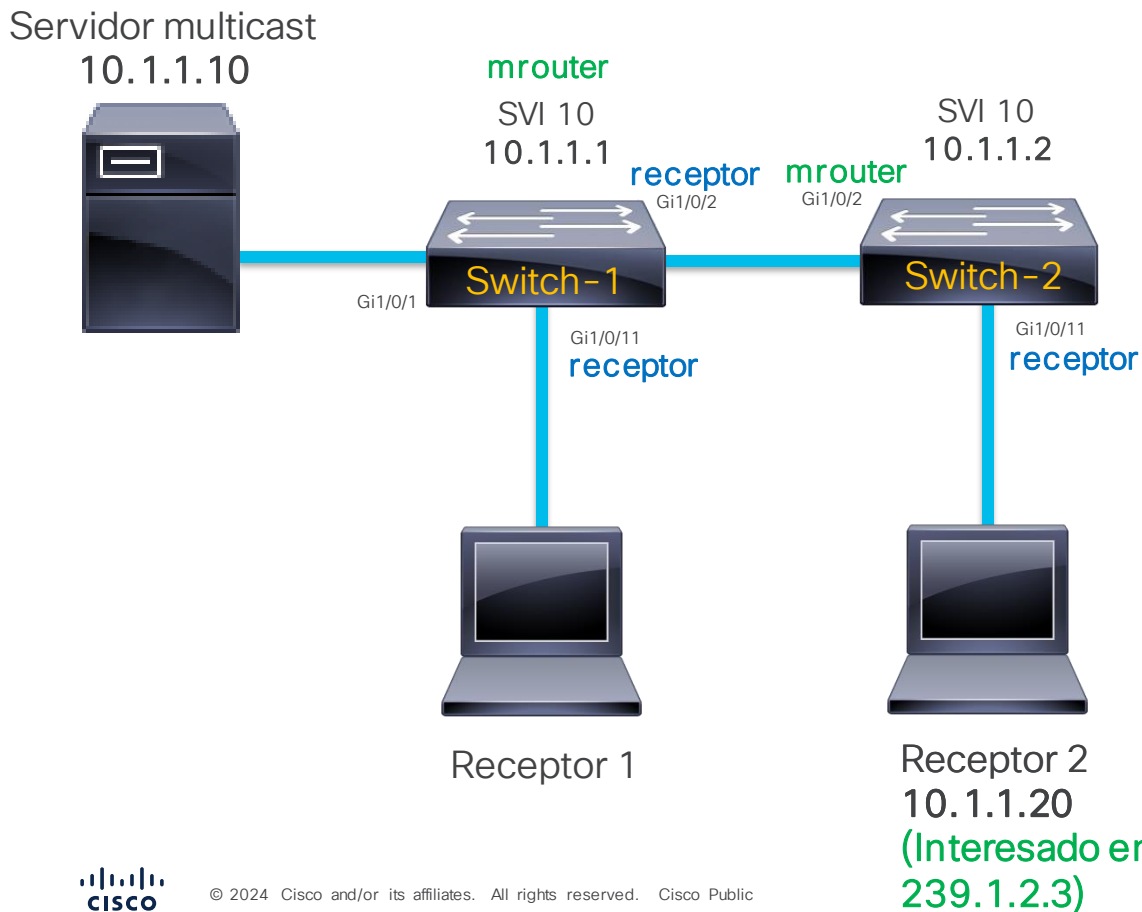
Descripción del Problema

Receptor 2 nunca recibe tráfico del grupo multicast 239.1.2.3.
Receptor 1 recibe el mismo tráfico de manera correcta y sin interrupciones.

Hallazgos:

- Servidor envía el tráfico de manera constante.

Escenario 2: Pérdida total de tráfico



1 Validar IGMP snooping en los switches

Switch-2

```
Switch-2#show ip igmp snooping mrouter
Vlan    ports
-----
  10    Gi1/0/2 (dynamic)

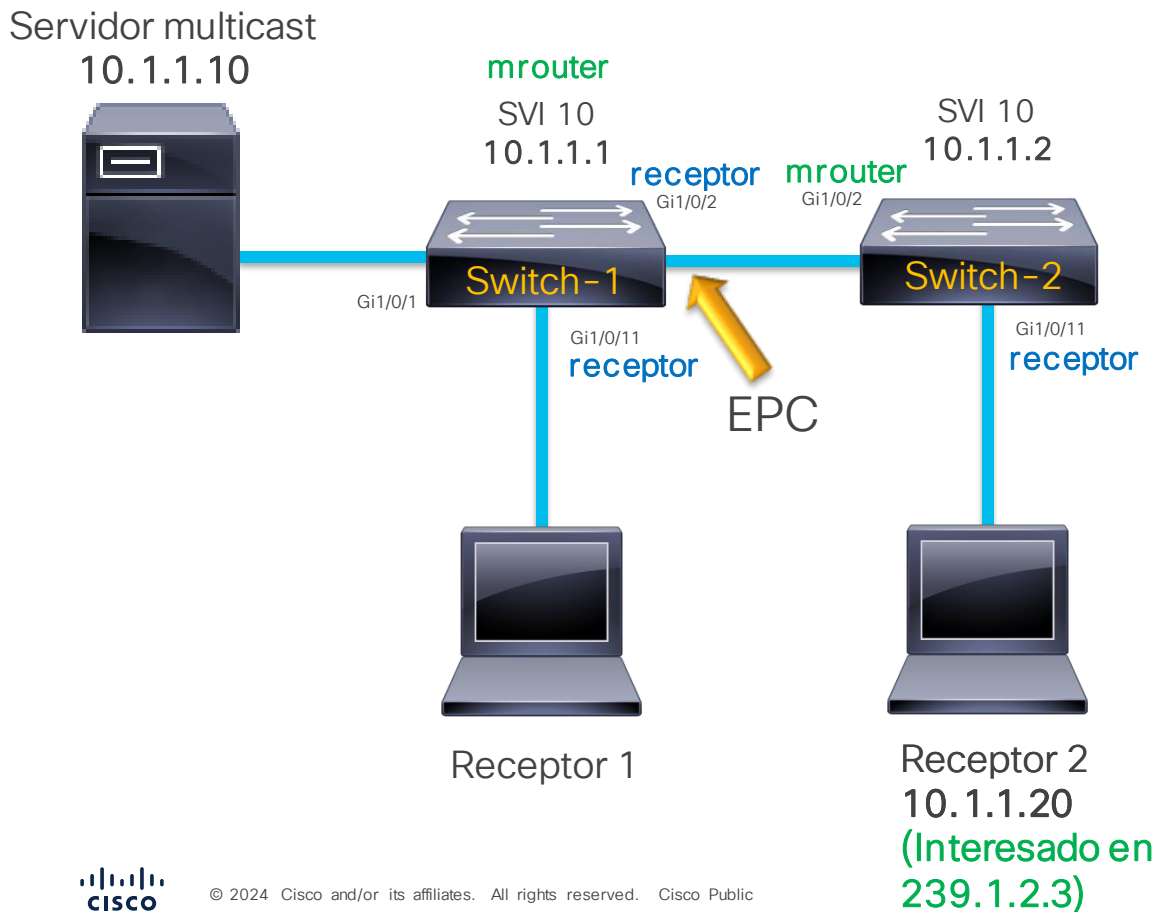
Switch-2#show ip igmp snooping querier
Vlan    IP Address      IGMP Version  Port
-----
  10    10.1.1.1        v2            Gi1/0/2

Switch-2#show ip igmp snooping groups
Vlan    Group           Type          Version  Port List
-----
  10    239.1.2.3      igmp         v2      Gi1/0/11
```

Las tablas de IGMP snooping son correctas en Switch-2.

El servidor multicast está enviando el tráfico, ¿quién no lo está reenviando?

Escenario 2: Pérdida total de tráfico



2

Validar si Switch-1 reenvía el tráfico a Switch-2

Switch-1

```
Switch-1#monitor capture TAC interface Gi1/0/2 out access-list MCAST start
```

```
Switch-1#monitor capture TAC stop
```

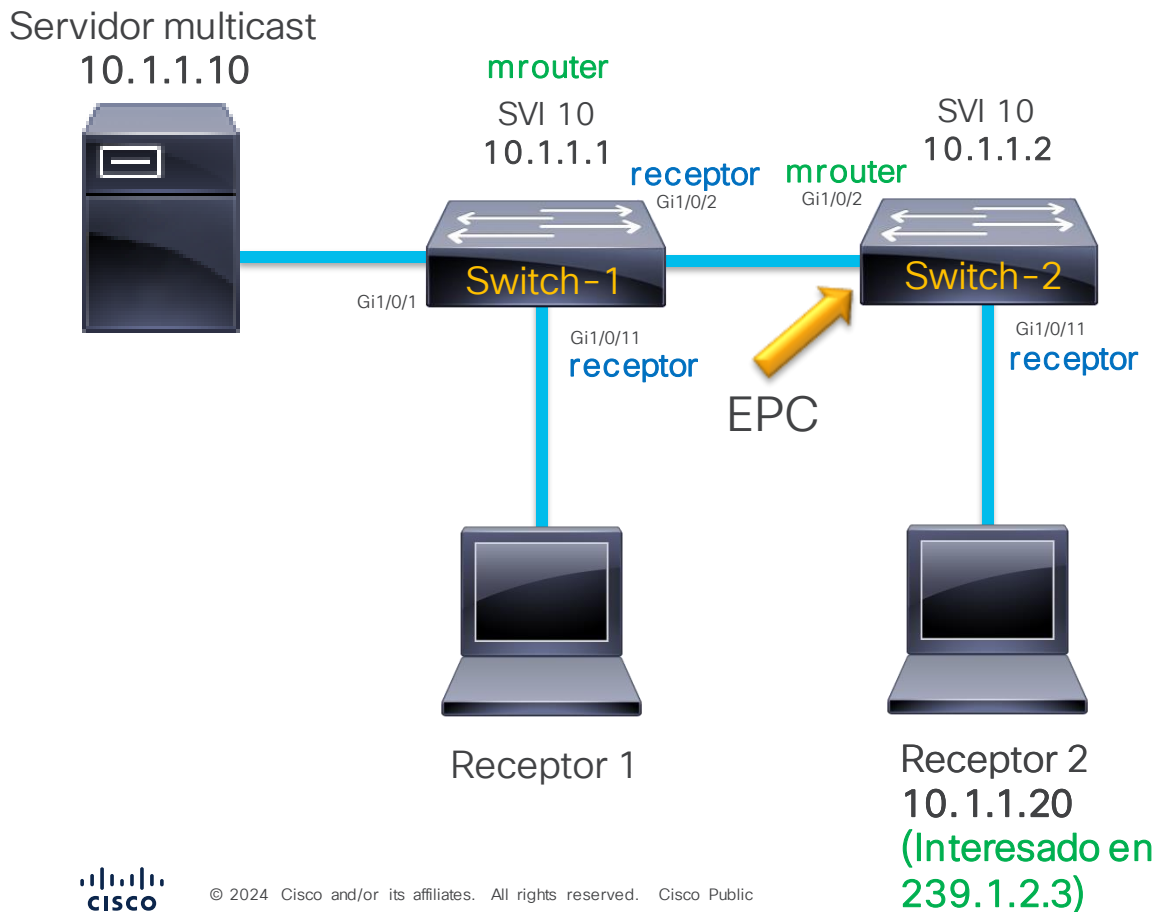
```
Switch-1#show monitor capture TAC buffer brief  
Starting the packet display ..... Press Ctrl + Shift + 6 to exit
```

1	0.000000	10.1.1.10	->	239.1.2.3	UDP	2296	63	->	63	Len=2254
2	0.003669	10.1.1.10	->	239.1.2.3	UDP	2296	63	->	63	Len=2254
3	0.007354	10.1.1.10	->	239.1.2.3	UDP	2296	63	->	63	Len=2254
4	0.011031	10.1.1.10	->	239.1.2.3	UDP	2296	63	->	63	Len=2254
5	0.014711	10.1.1.10	->	239.1.2.3	UDP	2296	63	->	63	Len=2254
6	0.018387	10.1.1.10	->	239.1.2.3	UDP	2296	63	->	63	Len=2254
7	0.022067	10.1.1.10	->	239.1.2.3	UDP	2296	63	->	63	Len=2254
8	0.025747	10.1.1.10	->	239.1.2.3	UDP	2296	63	->	63	Len=2254

Switch-1 sí reenvía el tráfico

¿Switch 2 lo está bloqueando?

Escenario 2: Pérdida total de tráfico



3 Validar si Switch-2 reenvía el tráfico al receptor

Switch-2

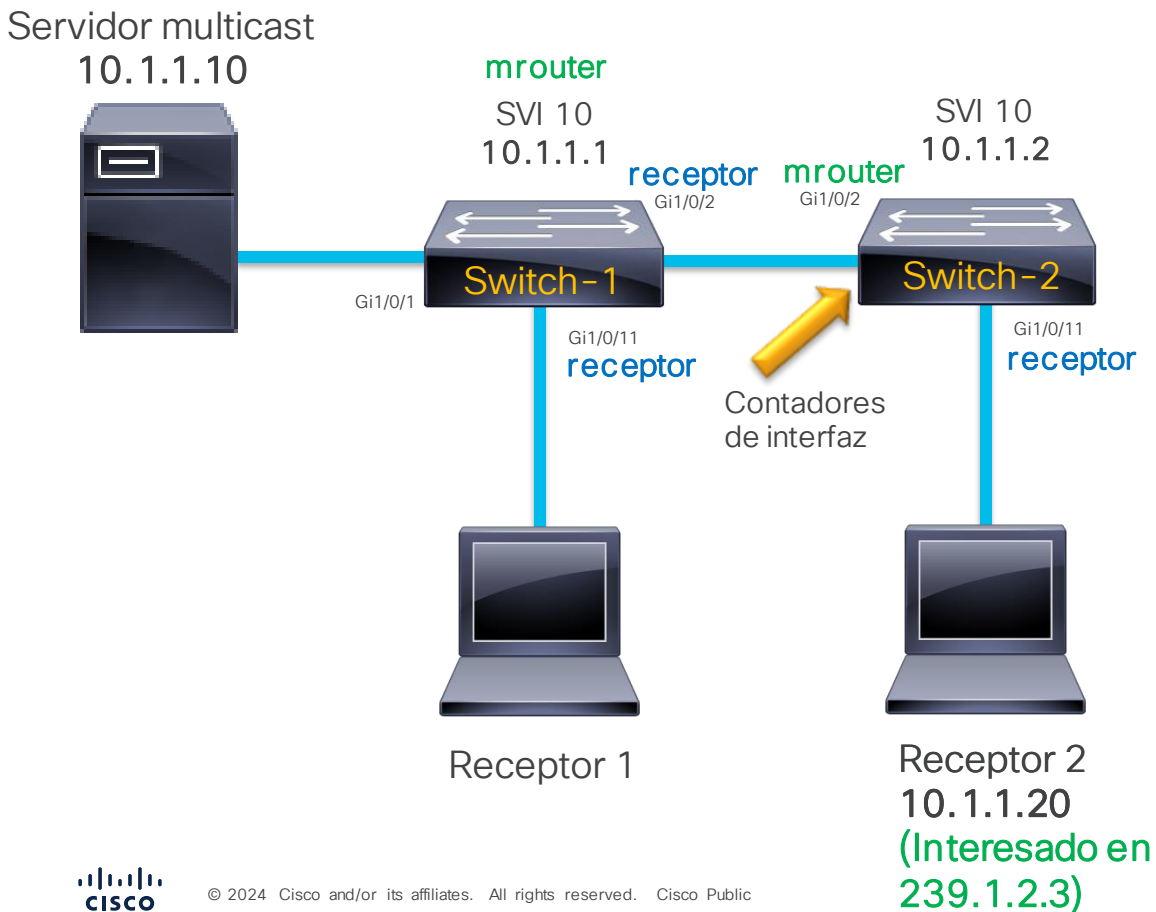
```
Switch-2#monitor capture TAC interface Gi1/0/2 in access-list MCAST start  
Switch-2#monitor capture TAC stop  
Switch-2#show monitor capture TAC buffer brief  
Starting the packet display ..... Press Ctrl + Shift + 6 to exit
```

Switch-2 no recibe los paquetes

¿Existe algún problema en capa física?

Escenario 2: Pérdida total de tráfico

3 Validar si Switch-2 reenvía el tráfico al receptor



Switch-2

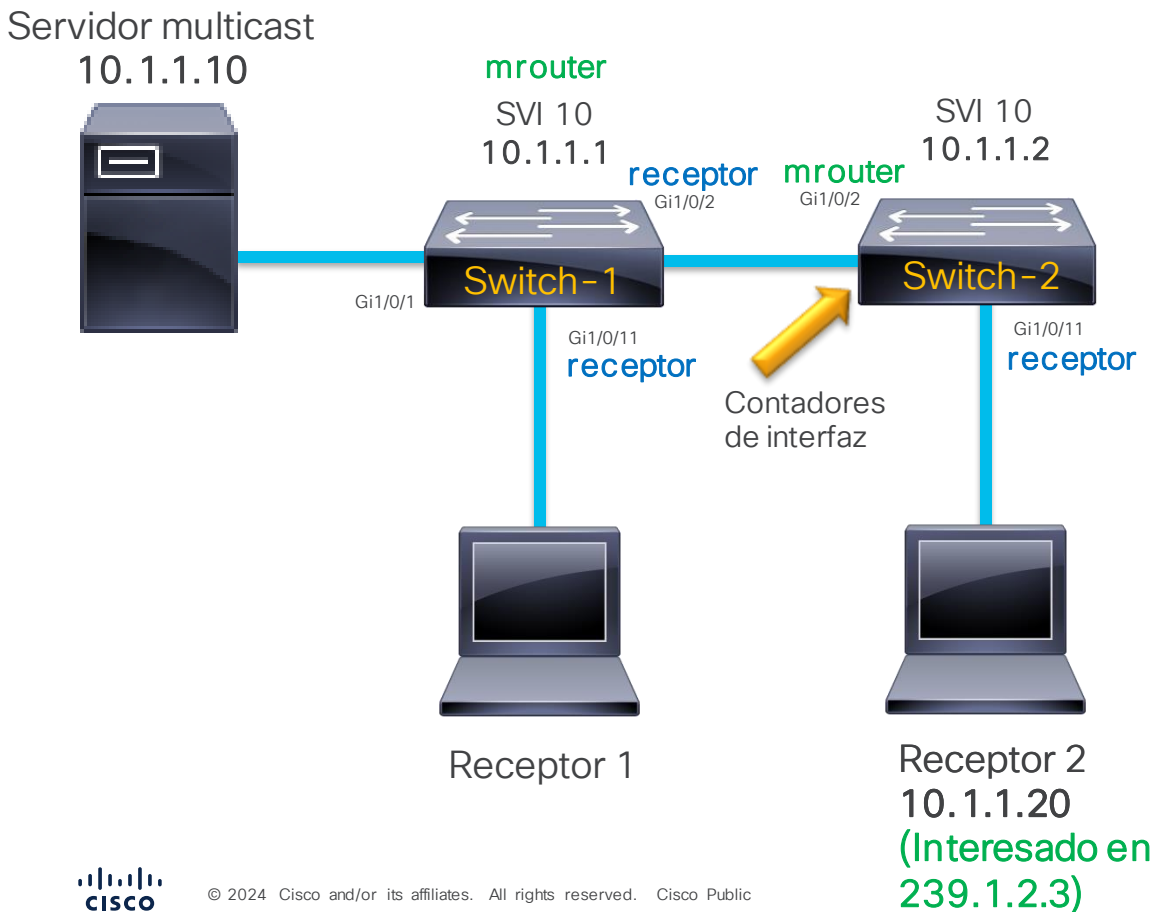
```
Switch-2#show interface Gig1/0/2
GigabitEthernet1/0/2 is up, line protocol is up (connected)
  Hardware is Gigabit Ethernet, address is cc70.ede1.2081 (bia
cc70.ede1.2081)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
    reliability 212/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
<snip>
30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
  6174330314 packets input, 396096394300 bytes, 0 no buffer
  Received 6174330314 broadcasts (6174330314 multicasts)
  0 runts, 78723 giants, 0 throttles
78723 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
  0 watchdog, 1879363018 multicast, 0 pause input
  0 input packets with dribble condition detected
<snip>
```

Input rate es cero

Ha recibido 78,723 Giants

Escenario 2: Pérdida total de tráfico

3 Validar si Switch-2 reenvía el tráfico al receptor



Switch-2

```
Switch-2#show interface Gig1/0/2
GigabitEthernet1/0/2 is up, line protocol is up (connected)
MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10
reliability 156/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive not set
Full-duplex, 1000Mb/s, link type is auto, media type is
10/100/1000BaseTX SFP
<snip>
30 second input rate 0 bits/sec, 0 packets/sec
30 second output rate 0 bits/sec, 0 packets/sec
6174330314 packets input, 396245319300 bytes, 0 no buffer
Received 6174330314 broadcasts (6174330314 multicasts)
0 runts, 143473 giants, 0 throttles
143473 input errors, 0 CRC, 0 frame, 0 over-run, 0 ignored
0 watchdog, 1879363018 multicast, 0 pause input
0 input packets with dribble condition detected
<snip>
```

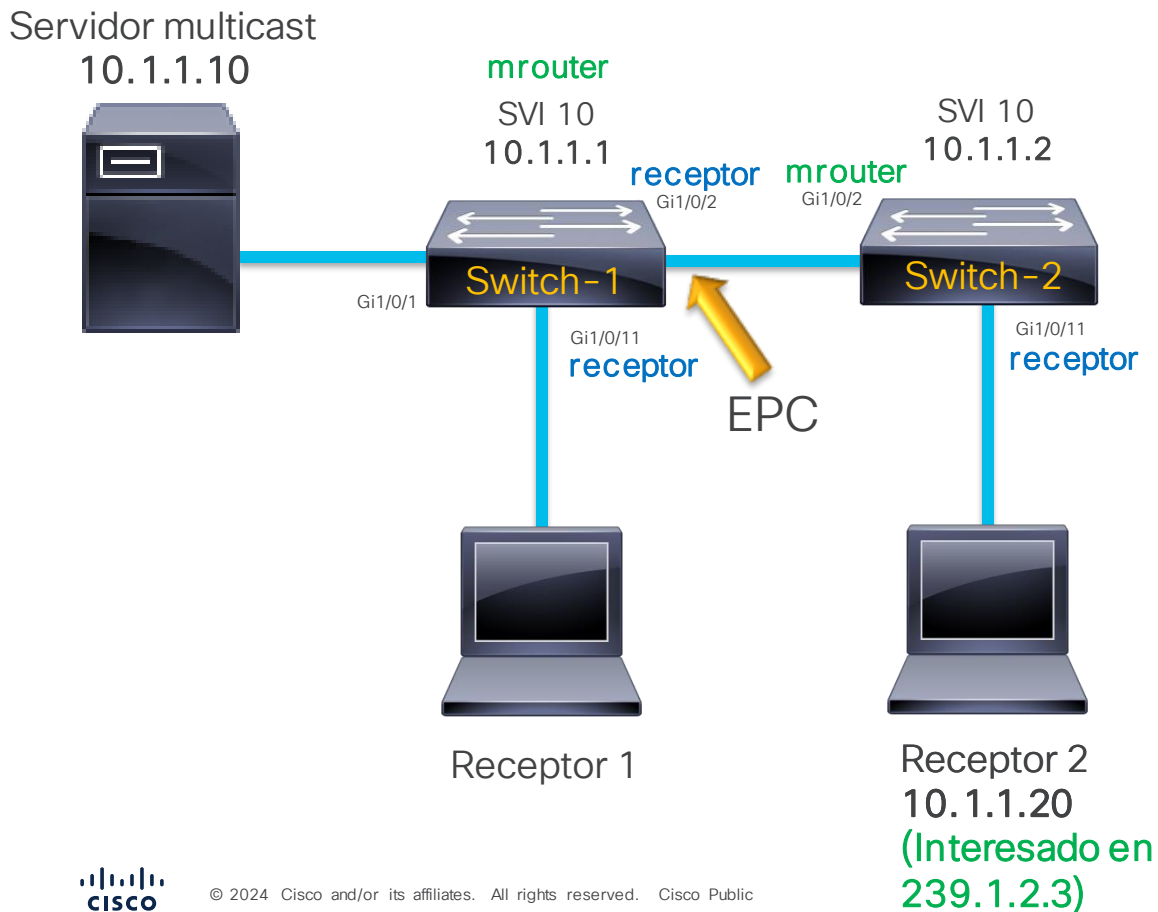
El MTU es 1,500 bytes

Los Giants siguen incrementando

¿Los paquetes de tráfico multicast son mayores de 1500 Bytes?

Escenario 2: Pérdida total de tráfico

3 Validar si Switch-2 reenvía el tráfico al receptor



Switch-1

```
Switch-1#monitor capture TAC interface Gi1/0/2 out access-list MCAST start

Switch-1#monitor capture TAC stop

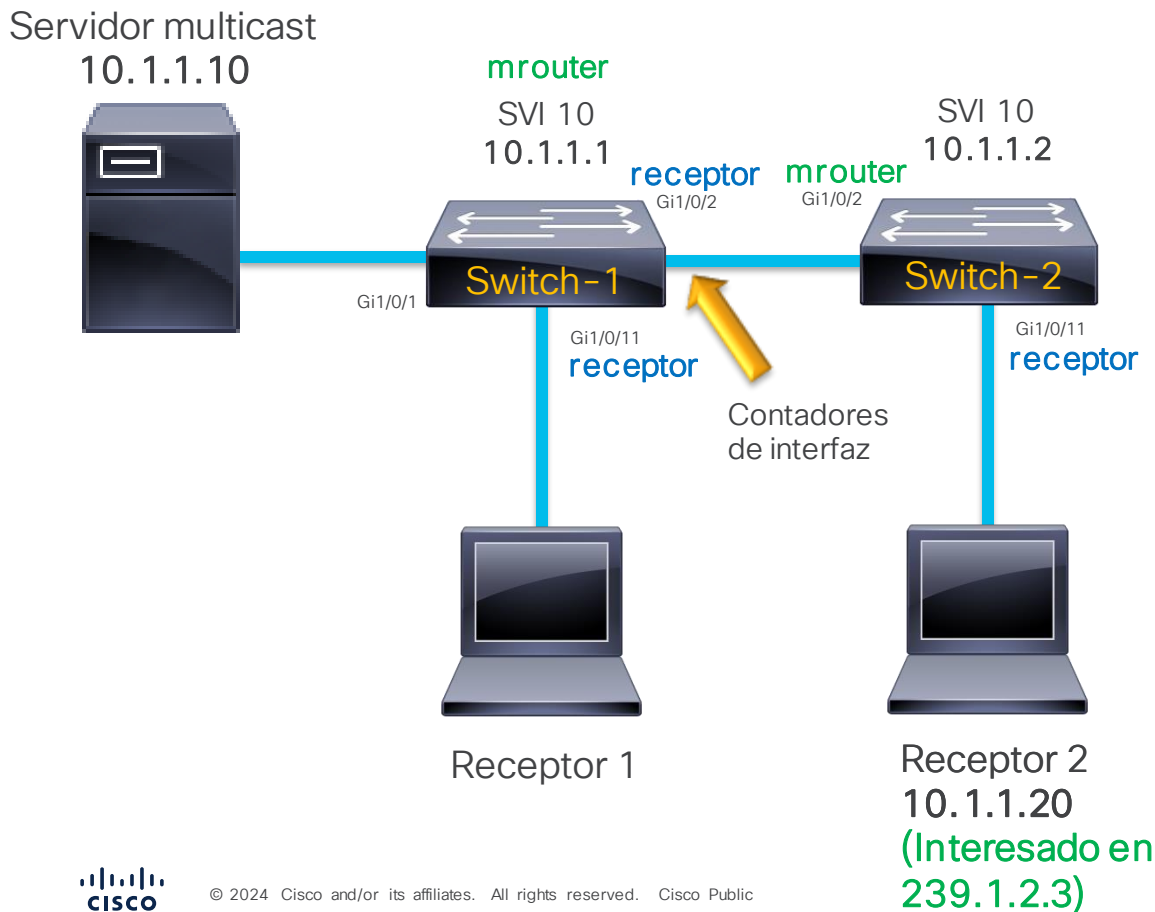
Switch-1#show monitor capture TAC buffer brief
Starting the packet display ..... Press Ctrl + Shift + 6 to exit

  1  0.000000  10.1.1.10 -> 239.1.2.3  UDP 2296 63 -> 63 Len=2254
  2  0.003669  10.1.1.10 -> 239.1.2.3  UDP 2296 63 -> 63 Len=2254
  3  0.007354  10.1.1.10 -> 239.1.2.3  UDP 2296 63 -> 63 Len=2254
  4  0.011031  10.1.1.10 -> 239.1.2.3  UDP 2296 63 -> 63 Len=2254
  5  0.014711  10.1.1.10 -> 239.1.2.3  UDP 2296 63 -> 63 Len=2254
  6  0.018387  10.1.1.10 -> 239.1.2.3  UDP 2296 63 -> 63 Len=2254
  7  0.022067  10.1.1.10 -> 239.1.2.3  UDP 2296 63 -> 63 Len=2254
  8  0.025747  10.1.1.10 -> 239.1.2.3  UDP 2296 63 -> 63 Len=2254
```

El tamaño de las tramas es 2,296 Bytes

El servidor envía tramas jumbo

Escenario 2: Pérdida total de tráfico



4

¿Por qué Switch-1 no tira el tráfico?

Switch-1

```
Switch-1#show interface Gig1/0/2
GigabitEthernet1/0/2 is up, line protocol is up (connected)
MTU 9000 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
reliability 156/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive not set
Full-duplex, 1000Mb/s, link type is auto, media type is 10/100/1000BaseTX
SFP
input flow-control is on, output flow-control is unsupported
ARP type: ARPA, ARP Timeout 04:00:00
<snip>
```

El MTU es 9,000 bytes

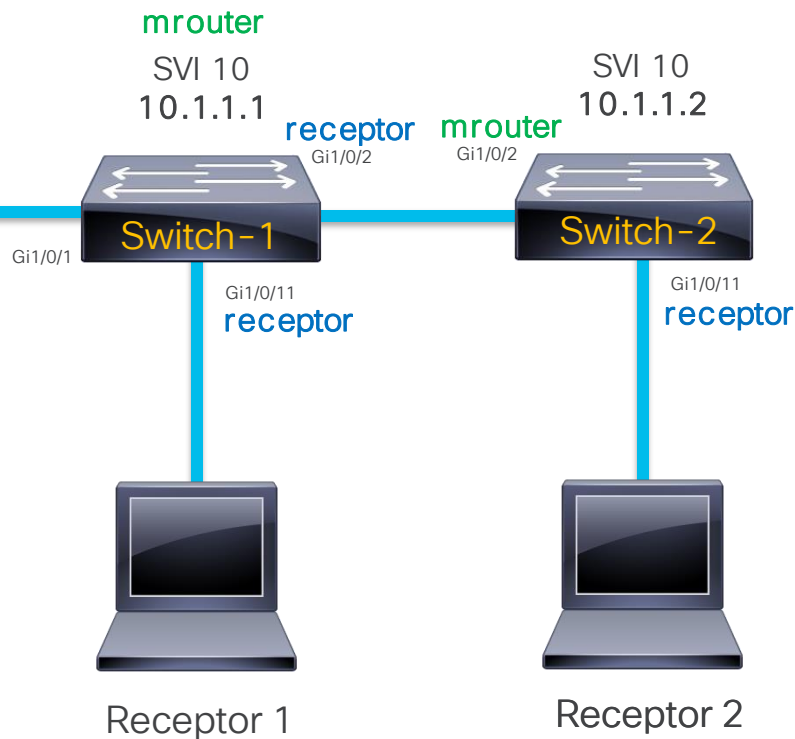
```
Switch-1#show system mtu
Global Ethernet MTU is 9000 bytes.
```

El MTU configurado en el sistema es 9,000 bytes

La discrepancia del MTU entre los switches está causando este problema

Escenario 2: Pérdida total de tráfico

Servidor multicast
10.1.1.10



5

Tomar acción correctiva

Switch-2

```
Switch-2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch-2(config)#system mtu 9000
Global Ethernet MTU is set to 9000 bytes.
Note: this is the Ethernet payload size, not the total
Ethernet frame size, which includes the Ethernet
header/trailer and possibly other tags, such as ISL or
802.1q tags.
```

```
Switch-2#show system mtu
Global Ethernet MTU is 9000 bytes.
```

Q&A



¿Aún tiene dudas?

Si hizo una pregunta en el panel de preguntas y respuestas o regresa a la comunidad en los días posteriores a nuestro webinar ¡Nuestros expertos aún pueden ayudarlo!

Participe en el foro Ask Me Anything (AMA) antes del viernes 21 de junio de 2024

<https://bit.ly/CL2ama-jun24>



Haga valer su opinión

Responda a nuestra encuesta para...

- Sugerir nuevos temas
- Calificar a nuestros expertos y el contenido
- Enviar sus comentarios o sugerencias

¡Ayúdenos respondiendo a 5 preguntas de opción múltiple!

Al término de esta sesión, se abrirá una encuesta en su navegador.



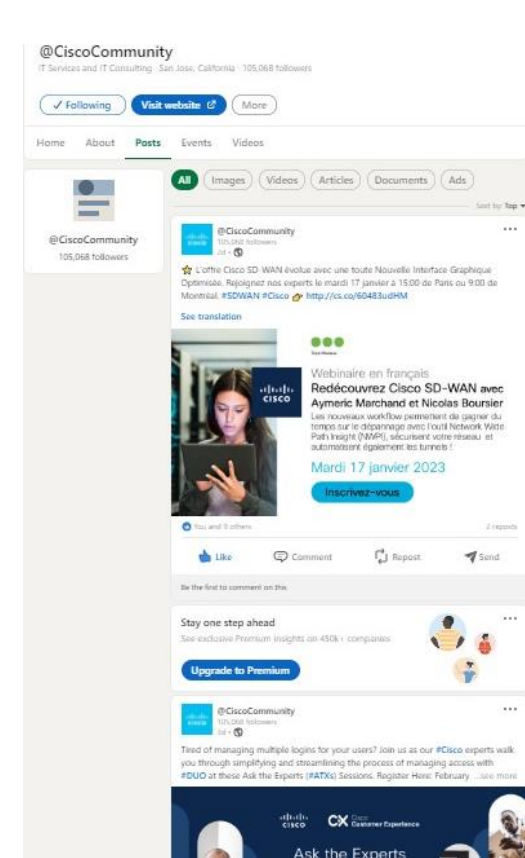
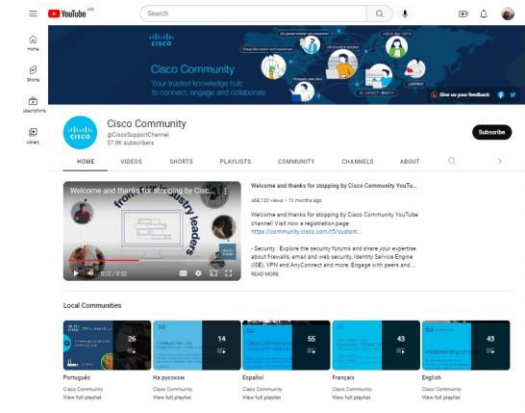
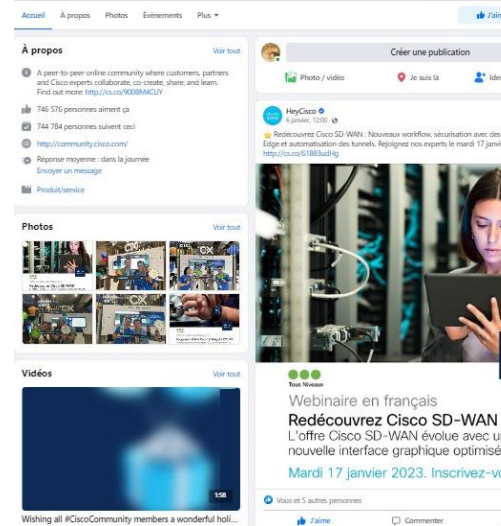
Nuestras Redes Sociales

LinkedIn
[Cisco Community](#)

Twitter
[@CiscoCommunity](#)

YouTube
[CiscoCommunity](#)

Facebook
[CiscoCommunity](#)





The bridge to possible