



# Comunidade de Suporte da Cisco - Webcast ao Vivo:

IP Multicast

Ricardo Lourenço  
High Touch Technical Engineer

07/05/2014

# Webcast com Especialistas em Tecnologia da Comunidade Cisco

Especialista de hoje:

**Ricardo Lourenço**, High Touch Technical Engineer



**Ricardo Lourenço**

High Touch Technical  
Engineer

# Webcast com Especialistas em Tecnologia da Comunidade Cisco

Especialista ajudante de hoje:

**Rodrigo Guerra**, High Touch Engineer



Rodrigo Guerra

LatAm FTS - HTE

# Obrigado por estar com a gente hoje!

Durante a apresentação, serão feitas  
algumas perguntas para o público.

Dê suas respostas, participe!





# Obrigado por estar com a gente hoje!

Se você quiser baixar uma cópia da apresentação de hoje, basta clicar no link abaixo ou ir até a Comunidade de Suporte e buscar este webcast na aba “Canto dos especialistas”.

<https://supportforums.cisco.com/pt/document/12195671>





# Comunidade de Suporte Cisco em Português - Webcast:

# Internet Protocol (IP) Multicast: Fundamentos

Ricardo Lourenço  
Customer Support Engineer  
LATAM High-Touch Support Services

07 de Maio de 2014

# Pergunta 1

## Qual o seu nível de experiência com IP Multicast?

- a) Nenhum – possui algumas noções de como funciona.
- b) Básico – possui conhecimentos teóricos.
- c) Intermédio – possui conhecimentos teóricos e implementou em laboratório.
- d) Avançado – Estudou, implementou em laboratório e ou rede de produção. Faz operação de uma rede IP Multicast.

# Agenda

- Porquê IP Multicast?
- Fundamentos IP Multicast
- Multicast em Layer 2
- Multicast Intra-domínio



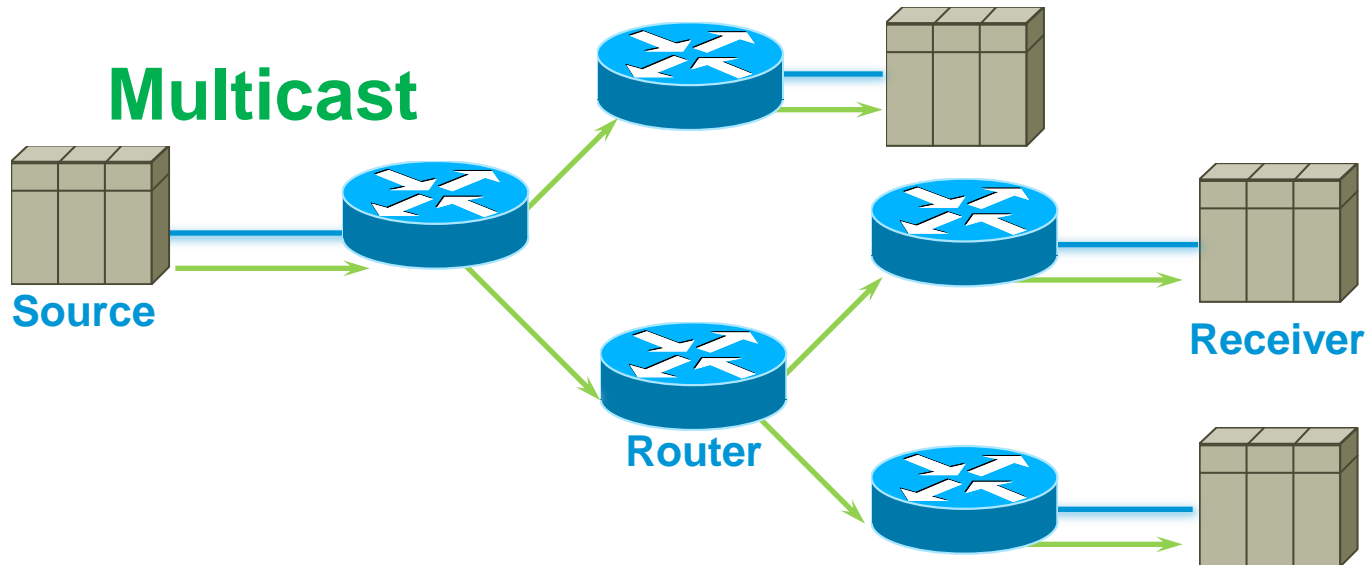
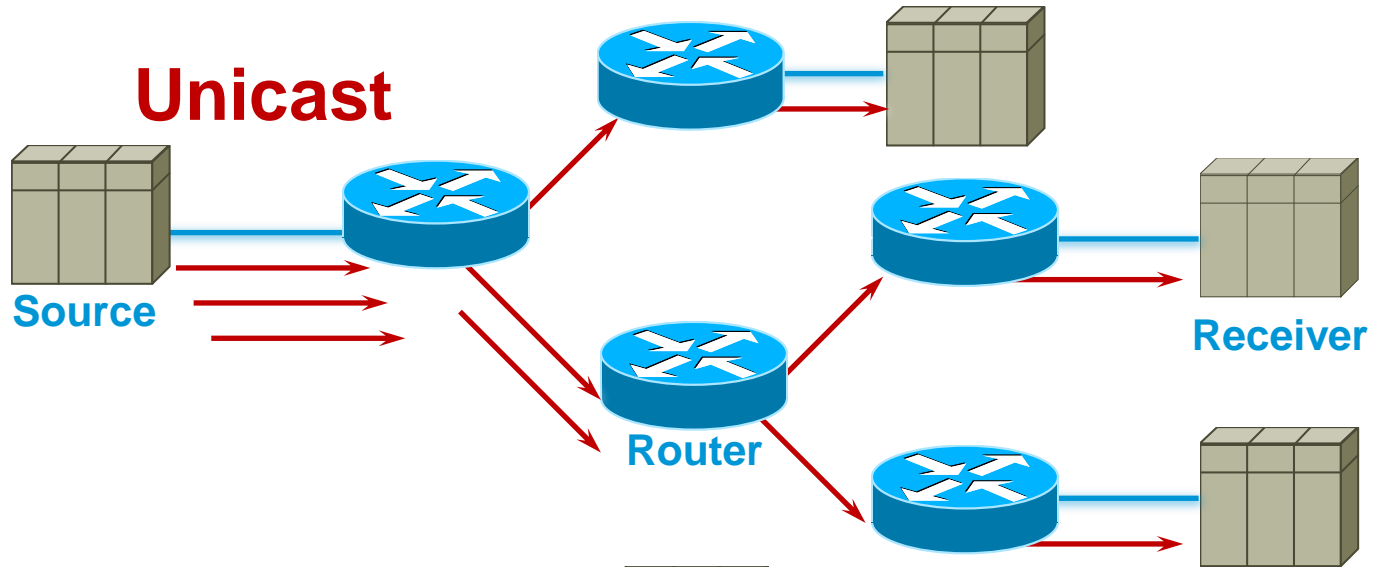


# Agenda

- **Porquê IP Multicast?**
- Fundamentos IP Multicast
- Multicast em Layer 2
- Multicast Intra-domínio

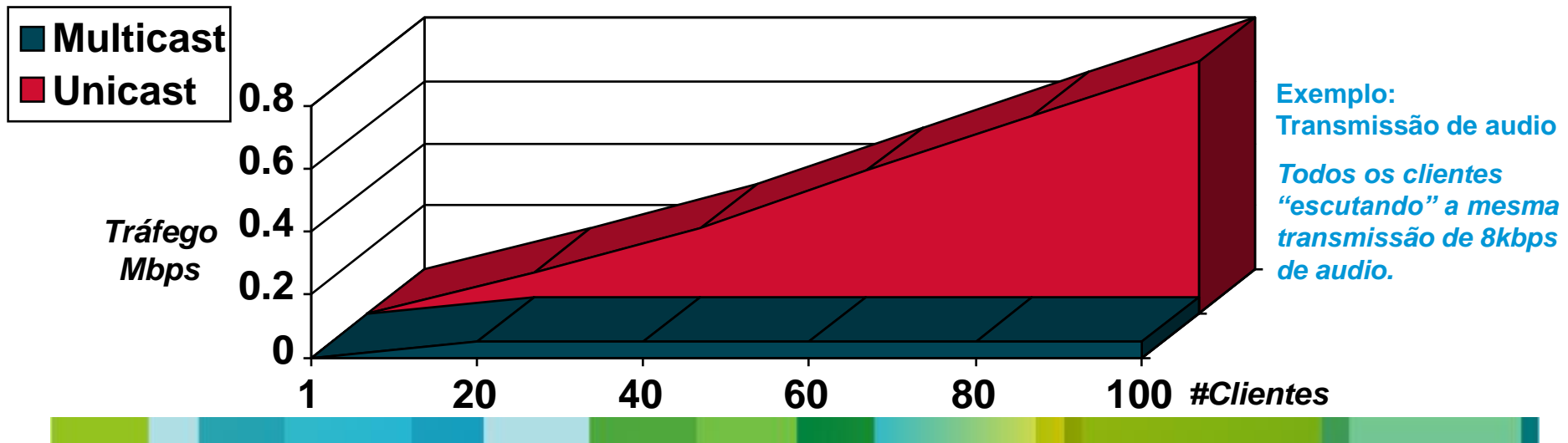


# Unicast vs. Multicast



# Vantagens de Multicast

- **Melhor Eficiência**
  - ✓ Largura de banda utilizada de modo mais eficiente.
  - ✓ Menor esforço computacional (*source*).
- **Melhor Desempenho**
  - ✓ Eliminação de tráfego redundante.
- **Aplicações Distribuídas**
  - ✓ Maior escalabilidade em ambientes aplicativos multiponto.



# Características de Multicast

## ***Multicast é baseado em UDP!***

- **Transmissão em “Best-Effort”**
  - ✓ Perdas de pacotes são esperadas. As aplicações que usam Multicast devem considerar este comportamento no seu desenho.
- **Inexistência de mecanismos de gestão de congestão**
  - ✓ Não existem mecanismos de gestão de congestão como os que podemos encontrar no protocolo TCP (*congestion window, slow-start*). No seu desenho as aplicações devem considerar este aspecto e possuírem mecanismos próprios de gestão de congestão – detectar e/ou evitar – na rede.
- **Pacotes duplicados ou fora de ordem**
  - ✓ Em algumas topologias redundantes, cenários de alteração de topologia de rede, ou mesmo por força de alguns mecanismos de multicast (*Asserts, Registers*) podem momentaneamente ocorrer pacotes duplicados. As aplicações devem ser desenhadas considerando esta possibilidade.

# Exemplos de Aplicações de Multicast

- **Audio/Video**

Palestras, apresentações, concertos, televisão, rádio, ensino à distância.

- **Push Media**

Notícias, meteorologia, desporto.

- **Distribuição de Informação/Dados**

Conteúdos de *sites*, actualização de código ou aplicações.

- **Aplicações Financeiras**

Transacções em bolsa, cotações.

***Qualquer aplicação baseada num modelo de comunicação de um para muitos ou muitos para muitos (one-to-many, many-to-many)***

Referências adicionais: [RFC3170](#)

# Pergunta 2

**Quantos anos de experiência possui?**

- a) 1 a 3 anos**
- b) 3 a 6 anos**
- c) 6 a 9 anos**
- d) 9 a 12 anos**
- e) Mais de 12 anos**

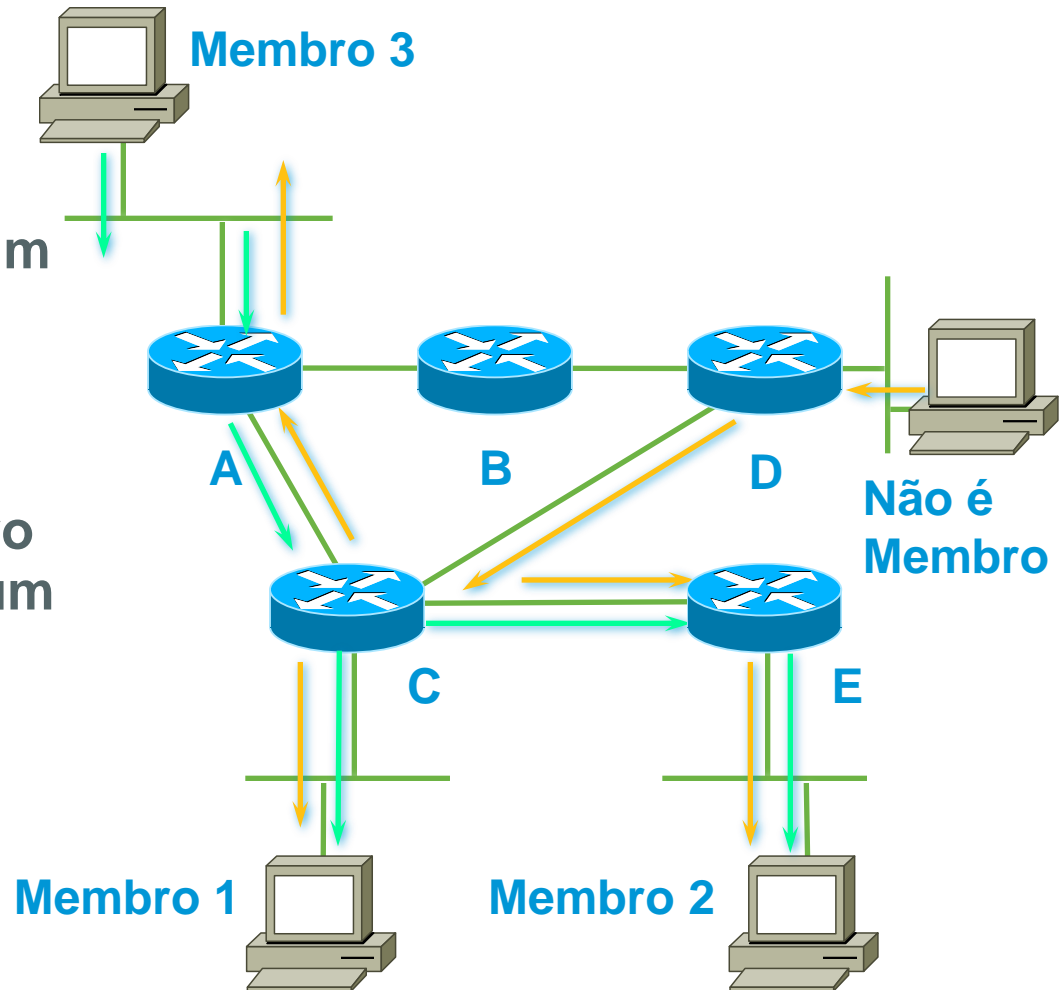
# Agenda

- Porquê IP Multicast?
- **Fundamentos IP Multicast**
- Multicast em Layer 2
- Multicast Intra-domínio



# Conceito de Grupo de Multicast

1. O tráfego enviado para um grupo de Multicast é recebido por todos os membros desse grupo.
2. Para receber tráfego de um determinado grupo de Multicast é preciso ser membro desse grupo.
3. Não tem de se ser membro para enviar tráfego para um grupo de Multicast.
4. Grupo de Multicast / Endereço IP Multicast.





# Endereço IP de Multicast

- **Endereços IP Multicast**

- ✓ Espaço de Endereçamento Classe “D”: 224.0.0.0 – 239.255.255.255
- ✓ Os bits mais significativos do primeiro octeto = “1110” – “1110XXXX”

- **Endereços IP Multicast reservados (endereços “Link-Local”)**

- ✓ 224.0.0.0 – 224.0.0.255
- ✓ Enviados com TTL = 1

**Exemplos:**

224.0.0.1	All Systems on this Subnet
224.0.0.2	All Routers on this Subnet
224.0.0.5	OSPF All Routers
224.0.0.9	RIPv2 Routers
224.0.0.13	All PIM Routers
224.0.0.18	VRRP
224.0.0.22	IGMPv3-capable multicast routers
224.0.0.102	HSRPv2

Referências adicionais: [RFC5771](#), [IPv4 Multicast Address Space Registry](#)

# Endereço IP de Multicast

- ***Administratively scoped IPv4 multicast space***

- ✓ de 239.0.0.0 a 239.255.255.255 (239/8).
- ✓ Similar à definição RFC1918 para endereços privados IP Unicast.
- ✓ Não podem ser roteados na Internet.
- ✓ Permitem restringir o alcance do tráfego de multicast.
- ✓ O mesmo endereço pode ser utilizado em zonas distintas da rede.
- ✓ Exemplos:

Site-local: 239.255.0.0/16

Organization-local: 239.192.0.0/14



# Endereço IP de Multicast

## *Mapeamento endereço IP Multicast / MAC (Ethernet)*

### Sobreposição de mapeamento IP:MAC 32:1

32 – Endereços 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 – Endereço MAC Multicast

0x0100.5E01.0101

# Endereço IP de Multicast

## *Mapeamento endereço IP Multicast / MAC (Ethernet)*

Evitar endereços que sejam tratados como broadcast

32 – Endereços IP Multicast

224.0.0.X  
224.128.0.X  
225.0.0.0  
225.128.0.X  
⋮  
⋮  
238.0.0.X  
238.128.0.X  
239.0.0.X  
239.128.0.X

1 – Endereço MAC Multicast

0x0100.5E00.00XX

✓ Tráfego com destino a endereços IP Multicast “Link-Local” será tratado como broadcast.

# Agenda

- Porquê IP Multicast?
- Fundamentos IP Multicast
- **Multicast em Layer 2**
- Multicast Intra-domínio



# Sinalização entre Hosts e Routers: IGMP

- **I**nternet **G**roup **M**anagement **P**rotocol

- ✓ Protocolo utilizado pelos receivers para sinalizar aos routers que pretendem receber tráfego de um determinado grupo de multicast.
- ✓ Routers interrogam os receivers directamente conectados se pretendem receber tráfego de multicast (*General, Specific*).
- ✓ Existem três versões: IGMPv1, IGMPv2, e IGMPv3.

*“(...) Version 1, specified in [RFC-1112], was the first widely-deployed version and the first version to become an Internet Standard. Version 2, specified in [RFC-2236], added support for "low leave latency", that is, a reduction in the time it takes for a multicast router to learn that there are no longer any members of a particular group present on an attached network. Version 3 adds support for "source filtering", that is, the ability for a system to report interest in receiving packets \*only\* from specific source addresses (...)” - Texto incluído na RFC4604*

Referências adicionais:

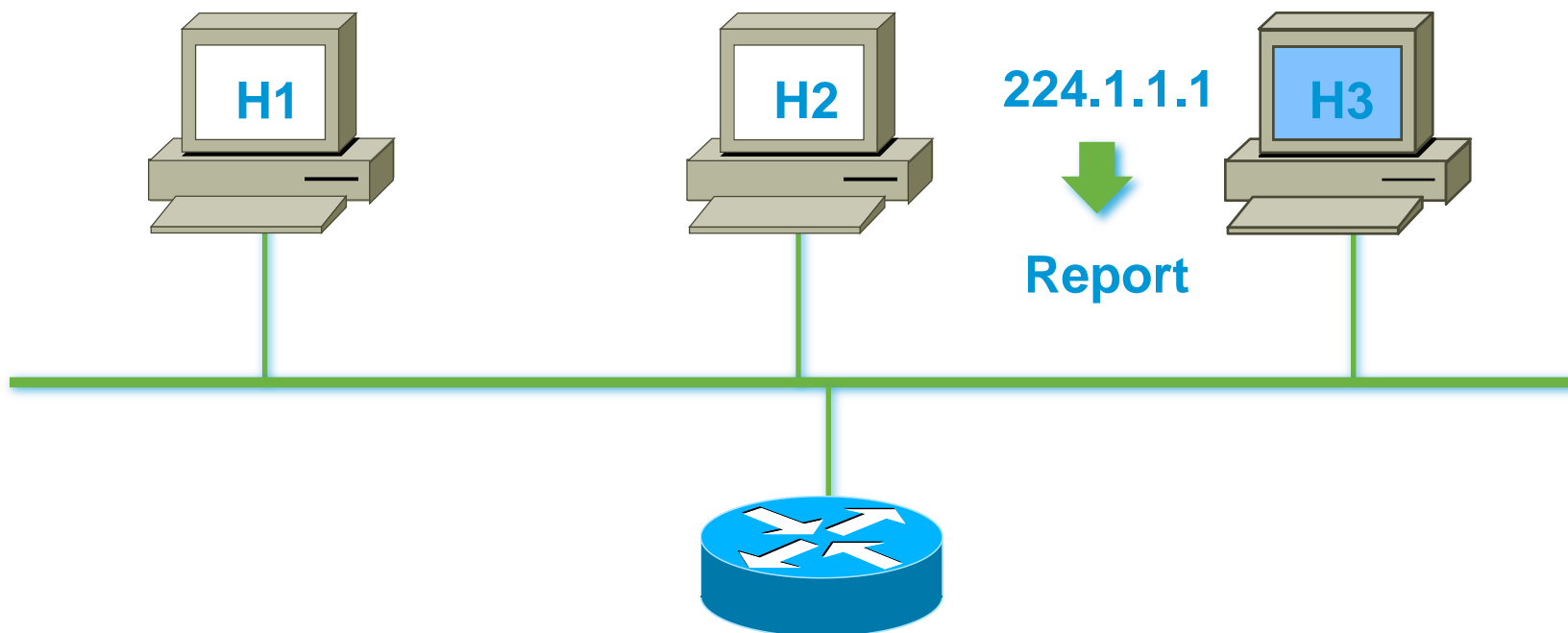
IGMPv1 – [RFC1112](#)

IGMPv2 – [RFC2236](#)

IGMPv3 – [RFC4604](#)

# Sinalização entre Hosts e Routers: IGMP<sub>v1/v2</sub>

Como sinalizar que se pretende receber tráfego de um determinado grupo?

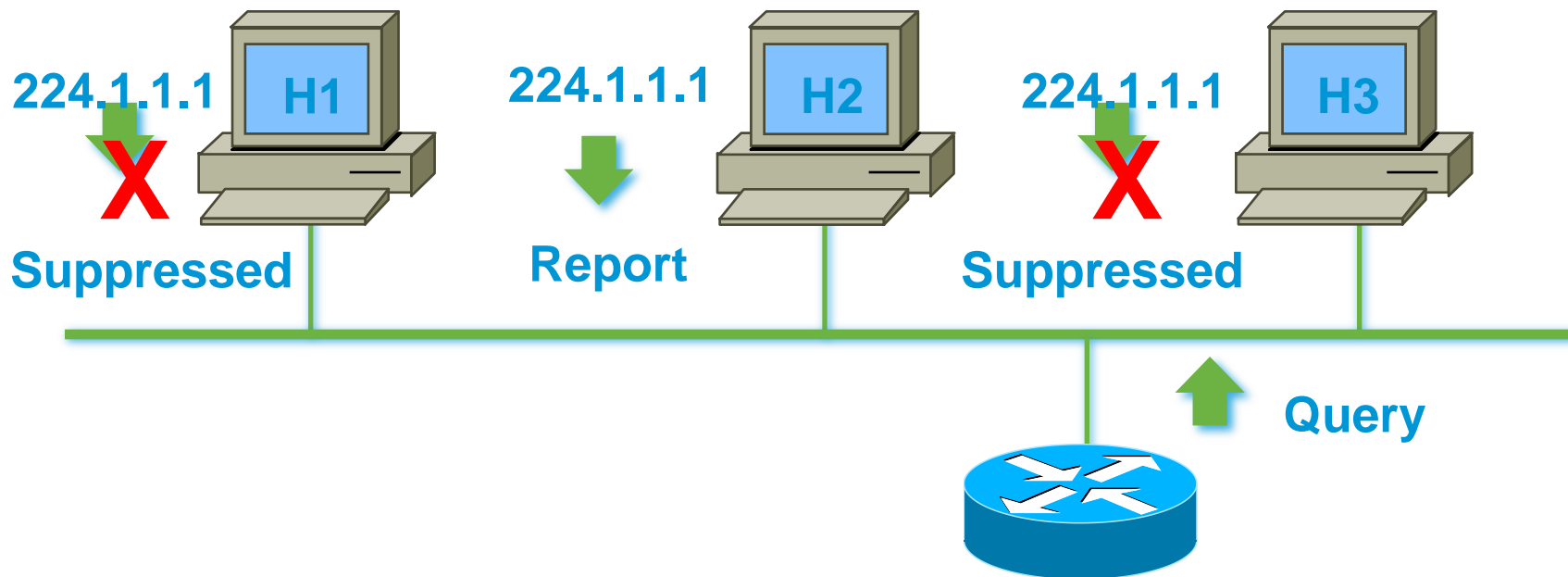


- Receiver envia um “IGMP Report” para sinalizar que pretende receber tráfego de um determinado grupo (*unsolicited*).



# Sinalização entre Hosts e Routers: IGMP<sub>v1/v2</sub>

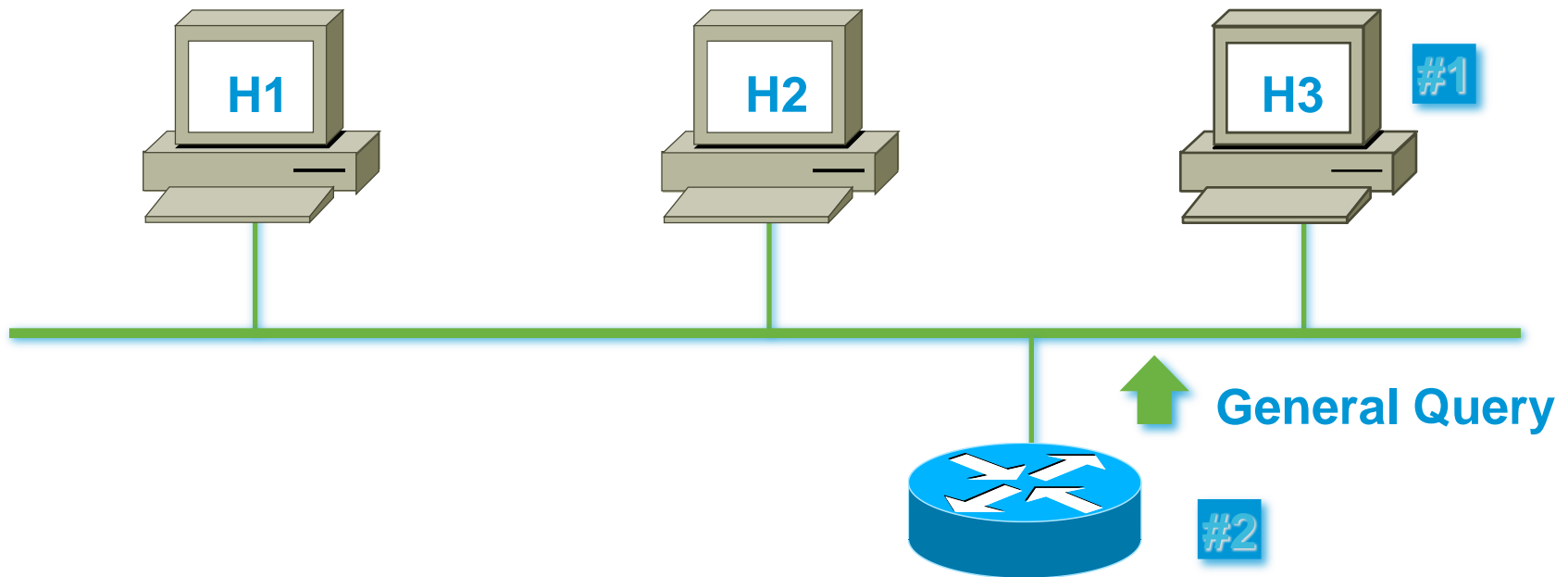
Como manter a associação a um determinado grupo?



- Router envia “IGMP Query” para o endereço 224.0.0.1 (*General*).
- Um membro por grupo e por segmento envia um “IGMP Report” (*random count-down timer*).
- Restantes membros suprimem o envio dos seus “IGMP Reports”.

# Sinalização entre Hosts e Routers: IGMP<sub>v1/v2</sub>

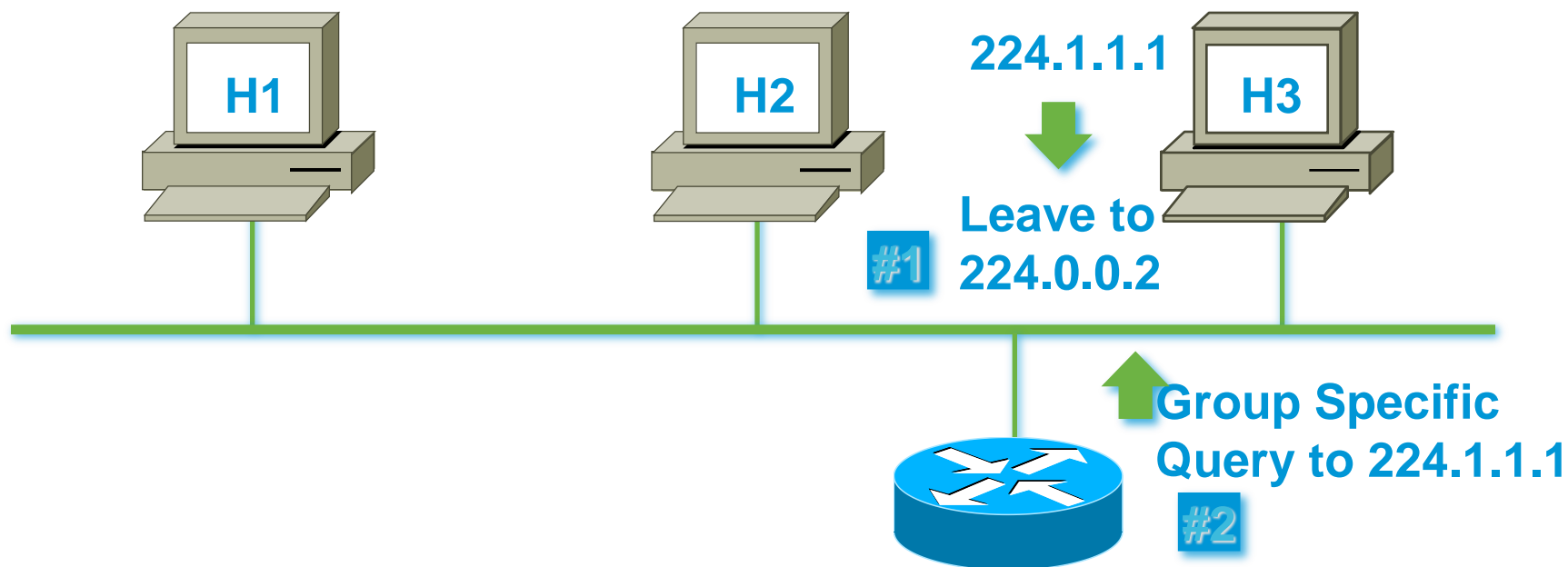
## Como deixar de escutar um grupo em IGMPv1?



- Receivers deixam silenciosamente os grupos.
- Routers enviam 3 “General Queries” (intervalo 60 segundos).
- Nenhum “IGMP Report” é recebido para o grupo.
- Informação de estado do grupo expira (pior cenário 3 minutos).

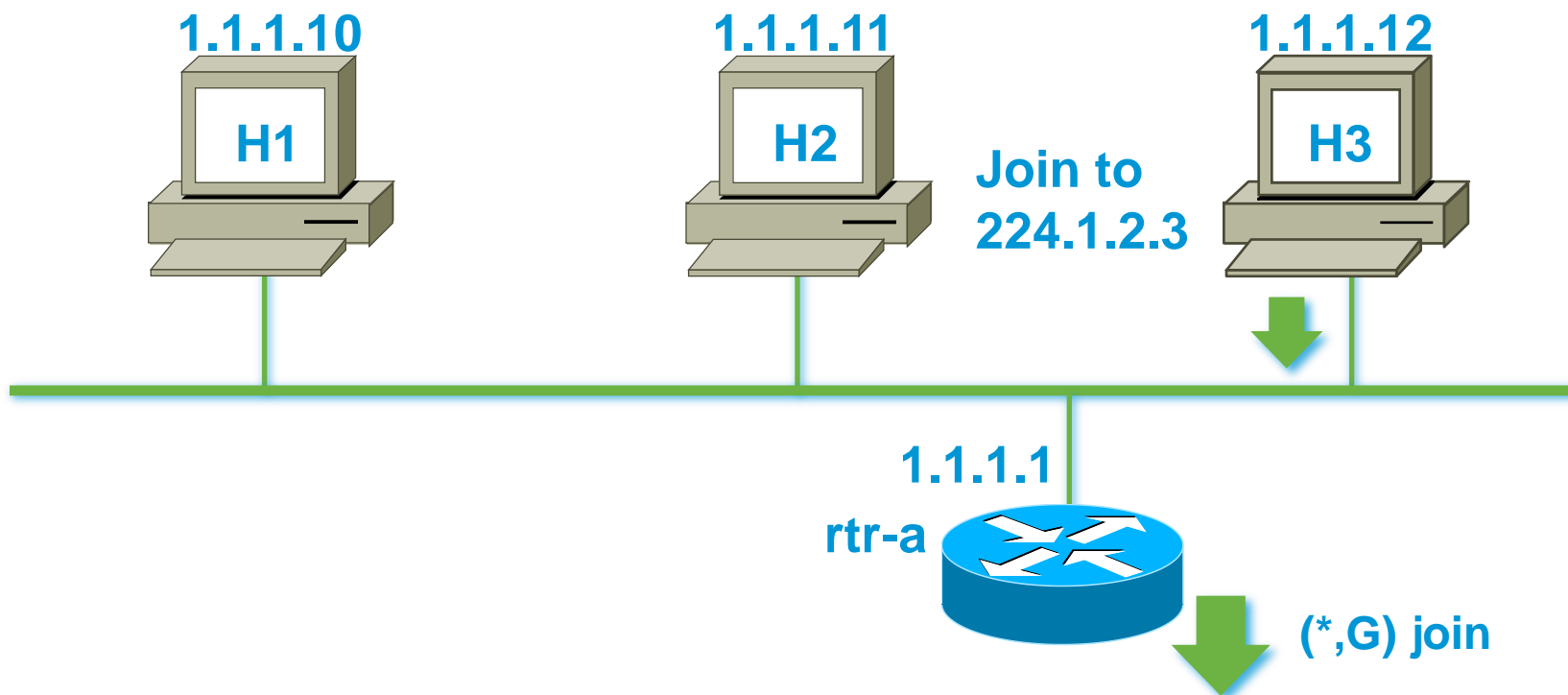
# Sinalização entre Hosts e Routers: IGMP<sub>v1/v2</sub>

## Como deixar de escutar um grupo em IGMPv2?



- Receiver envia “IGMP Leave” para endereço 224.0.0.2 (*All Routers*).
- Router envia “Group Specific Query” para 224.1.1.1 (Grupo).
- Espera “IGMP Report” em 1 segundo (*Last Member Query Interval*).
- Informação de estado expira em menos de 3 segundos.

# Sinalização entre Hosts e Routers: IGMP<sub>v1/v2</sub>



- O receiver envia “IGMP Report” com destino ao grupo.
- O router cria uma entrada de estado de acordo com a informação de *membership*.
- O router envia um “(\*,G) join” – A *source* do grupo não é conhecida.

# Sinalização entre Hosts e Routers: IGMP<sub>v3</sub>

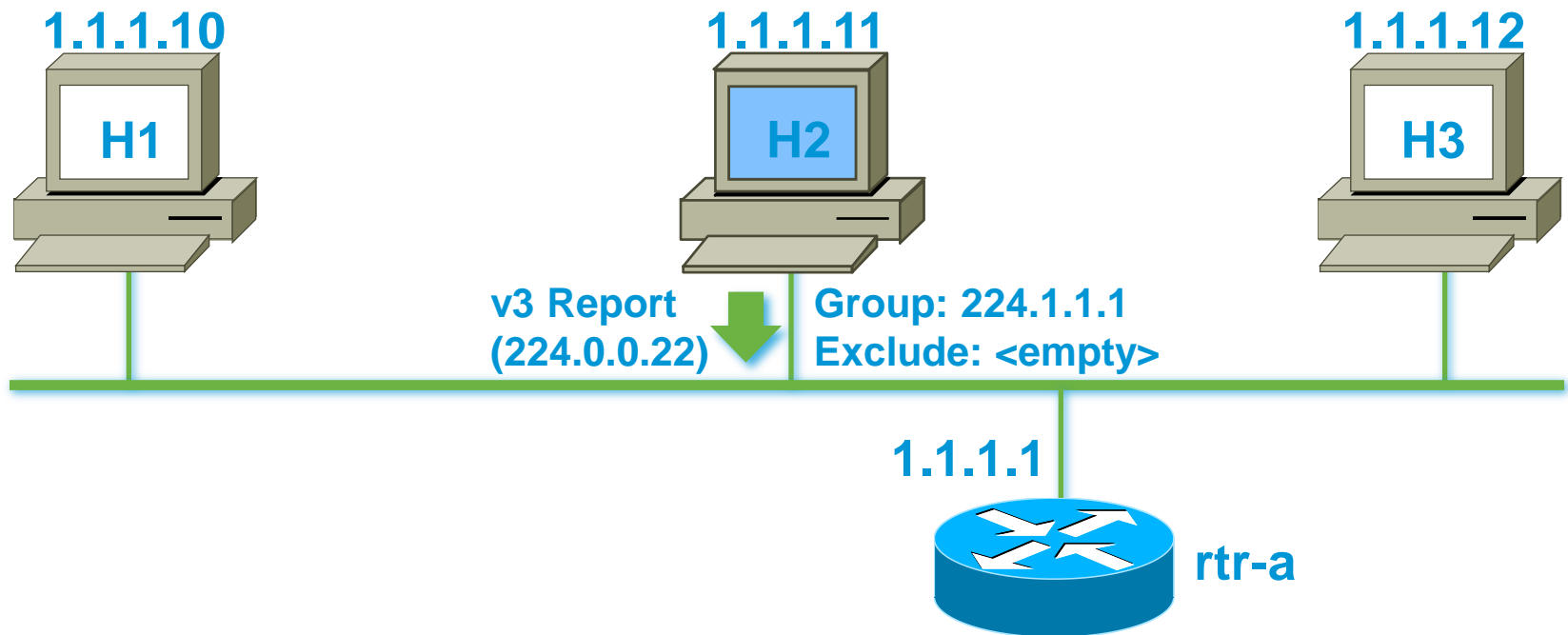
- **Permite especificar que *sources* Incluir/Excluir**
  - ✓ O receiver pode escutar um determinado grupo de uma ou mais *sources* específicas.
  - ✓ As aplicações têm de suportar a implementação da funcionalidade de *include/exclude source list*.

# Sinalização entre Hosts e Routers: IGMP<sub>v3</sub>

- **Endereço específico para envio de “Membership Reports”**
  - ✓ 224.0.0.22 (IGMPv3 Routers).
  - ✓ Todos os receivers que usam IGMPv3 utilizam este endereço para os Memberships Reports.
  - ✓ Todos os routers que suportam IGMPv3 escutam o tráfego deste grupo.
  - ✓ Os receivers não escutam nem respondem a tráfego com destino a este grupo de multicast.
- **Não implementa “Report Suppression”**
  - ✓ Todos os receivers no segmento respondem “IGMP Queries”.
  - ✓ O intervalo de resposta pode ser configurado.
    - ✓ Útil quando existem muitos receivers no segmento.

# Sinalização entre Hosts e Routers: IGMP<sub>v3</sub>

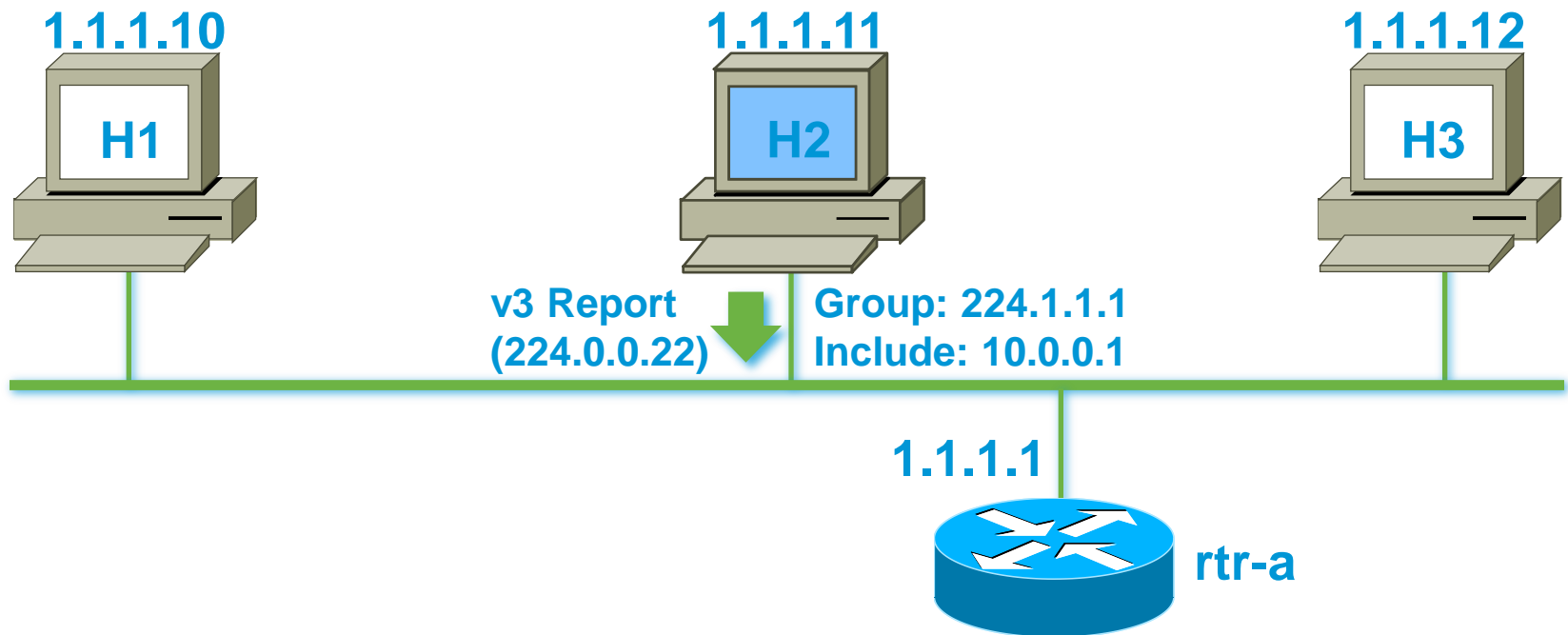
Como sinalizar que se pretende receber tráfego de um determinado grupo?



- Receiver envia “IGMPv3 Report” para o endereço 224.0.0.22 sem esperar “query” do router (*unsolicited*).

# Sinalização entre Hosts e Routers: IGMP<sub>v3</sub>

Como sinalizar que se pretende receber tráfego de um determinado grupo e de uma determinada source?

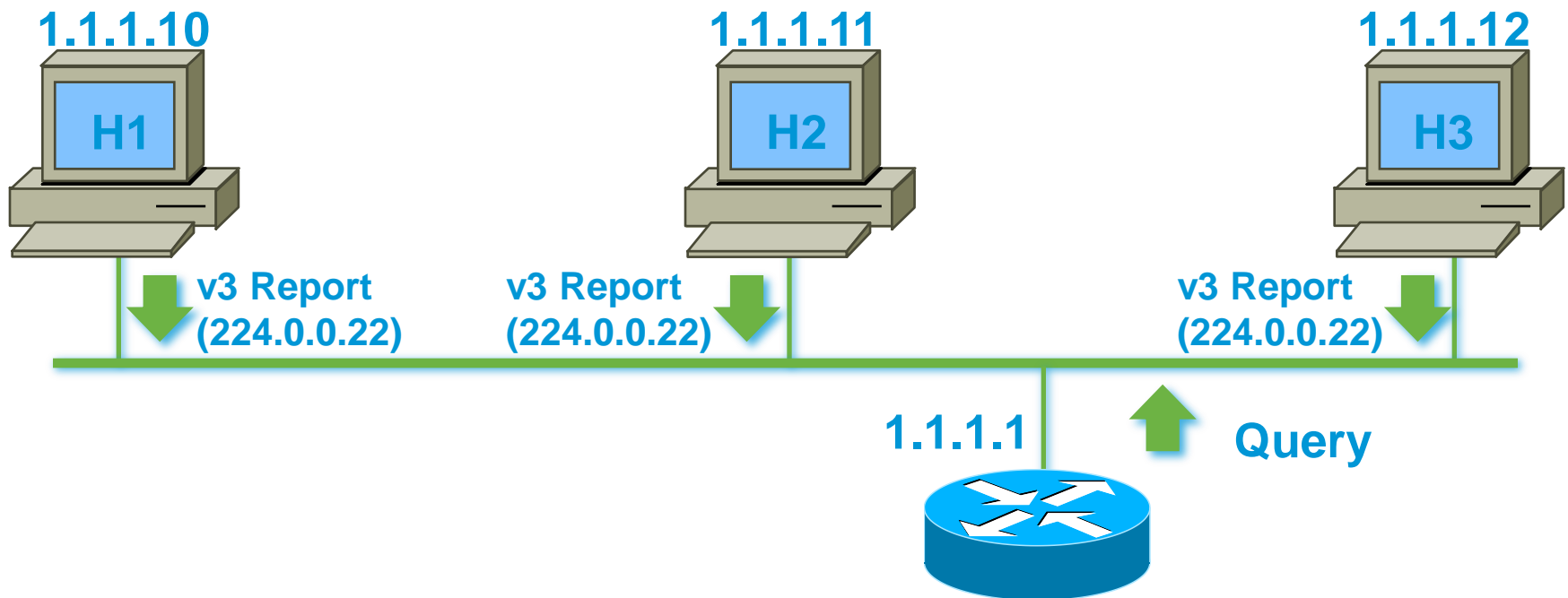


- “IGMPv3 Report” inclui a source pretendida.
- Apenas se pretende receber tráfego das sources especificadas na “include list”.



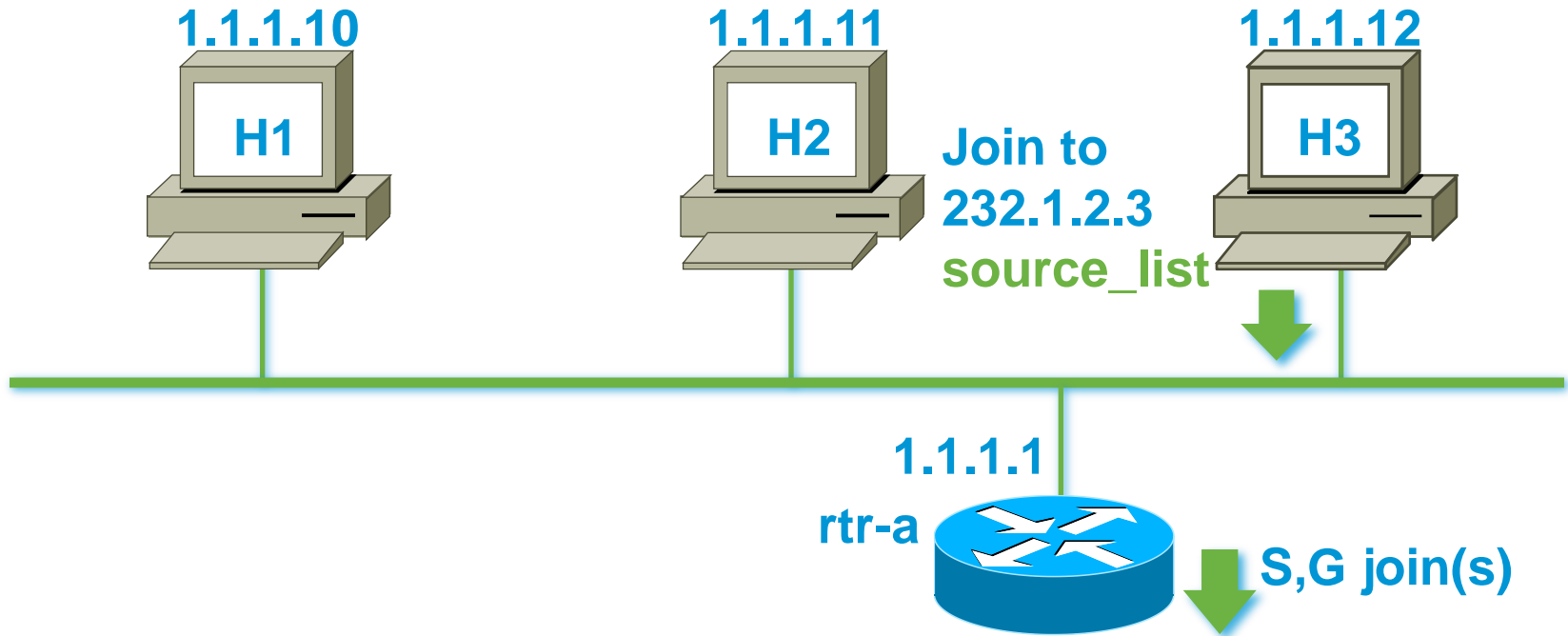
# Sinalização entre Hosts e Routers: IGMP<sub>v3</sub>

Como manter a associação a um determinado grupo?



- Routers enviam “Queries” periódicos para 224.0.0.1 (*All Hosts*).
- Todos os receivers de IGMPv3 respondem.
  - Os “reports” possuem múltiplos “Group state records”

# Sinalização entre Hosts e Routers: IGMP<sub>v3</sub>

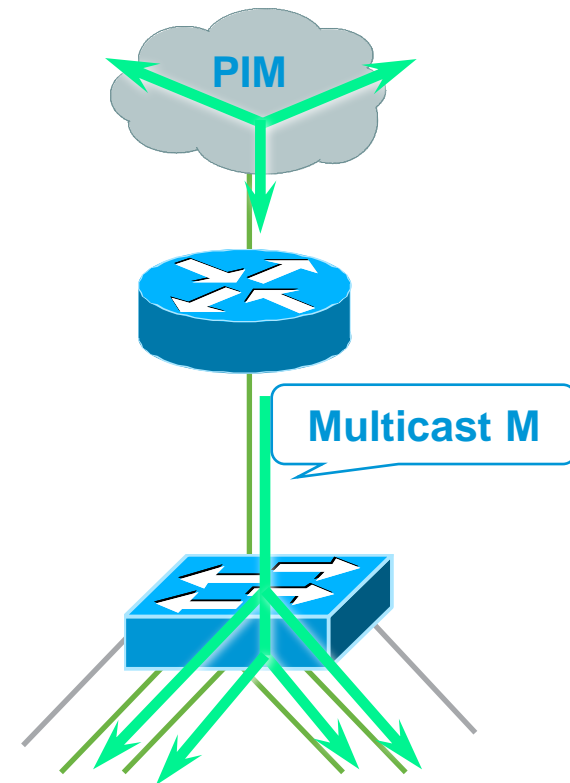


- O receiver envia um “IGMPv3 Report” para o grupo e pode especificar a(s) Sources pretendidas.
- Os routers mantêm a informação de estado entre sources e grupos solicitados.
- O router envia um “(S,G) join” especificando as sources pretendidas – A *source* do grupo é conhecida.

# Multicast Frame Switching em Layer 2

## Problema: Flood de multicast frames em Layer 2

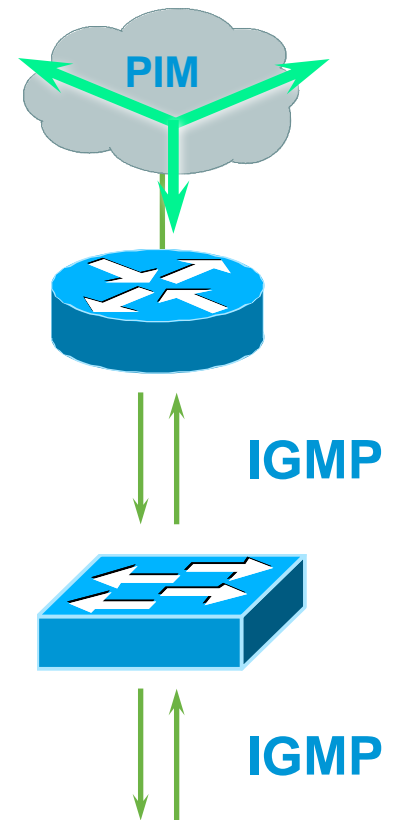
- Tráfego de Multicast é tratado como desconhecido ou broadcast e enviado para todos os interfaces.
- Configuração de entradas estáticas pode ser usada para especificar quais as interfaces que devem receber o tráfego de Multicast.
- A configuração dinâmica destas entradas permitiria diminuir o esforço administrativo/operacional da sua configuração e manutenção.



# Multicast Frame Switching em Layer 2

## Solução: IGMPv1-v2 Snooping

- Os switches têm de suportar IGMP.
- Os pacotes de IGMP são interceptados pelo NMP ou por ASICs específicos.
  - ✓ Hw dedicado é necessário para garantir a capacidade de processamento e *throughput*.
- O switch tem de examinar o conteúdo das mensagens de IGMP para determinar os interfaces que devem receber o tráfego de multicast.
  - ✓ IGMP membership reports ; IGMP leave messages.
- Terá impacto significativo no desempenho de switches *low-end* ou gama baixa.



# Multicast Frame Switching em Layer 2

- **Impacto de IGMPv3 em IGMP Snooping**
  - As mensagens de “IGMPv3 Reports” são enviados com destino a um endereço específico (224.0.0.22).
    - ✓ Switches apenas “escutam” este grupo.  
Apenas tráfego de IGMP – não a multicast stream
    - ✓ Reduz substancialmente o esforço de processamento do CPU do switch.  
Permite IGMPv3 snooping em switches de baixa capacidade
  - **Não há “Report Suppression” em IGMPv3**
    - ✓ Permite a gestão individual de cada membro.
  - **IGMPv3 suporta “Includes/Excludes” de sources específicas.**
    - ✓ Permite que o estado (S,G) possa ser mantido no switch.  
Puderá implicar a implementação de todas as funcionalidades de IGMPv3  
Actualmente não implementado em switches

# Pergunta 3

**Quais as áreas de IP Multicast que gostaria de aprofundar?**

- a) Multicast VPN**
- b) Multicast LDP**
- c) Protocolos de Routing de Multicast**
- d) IP Multicast Inter-domínio**
- e) Troubleshooting de Multicast**
- f) IPv6 Multicast**

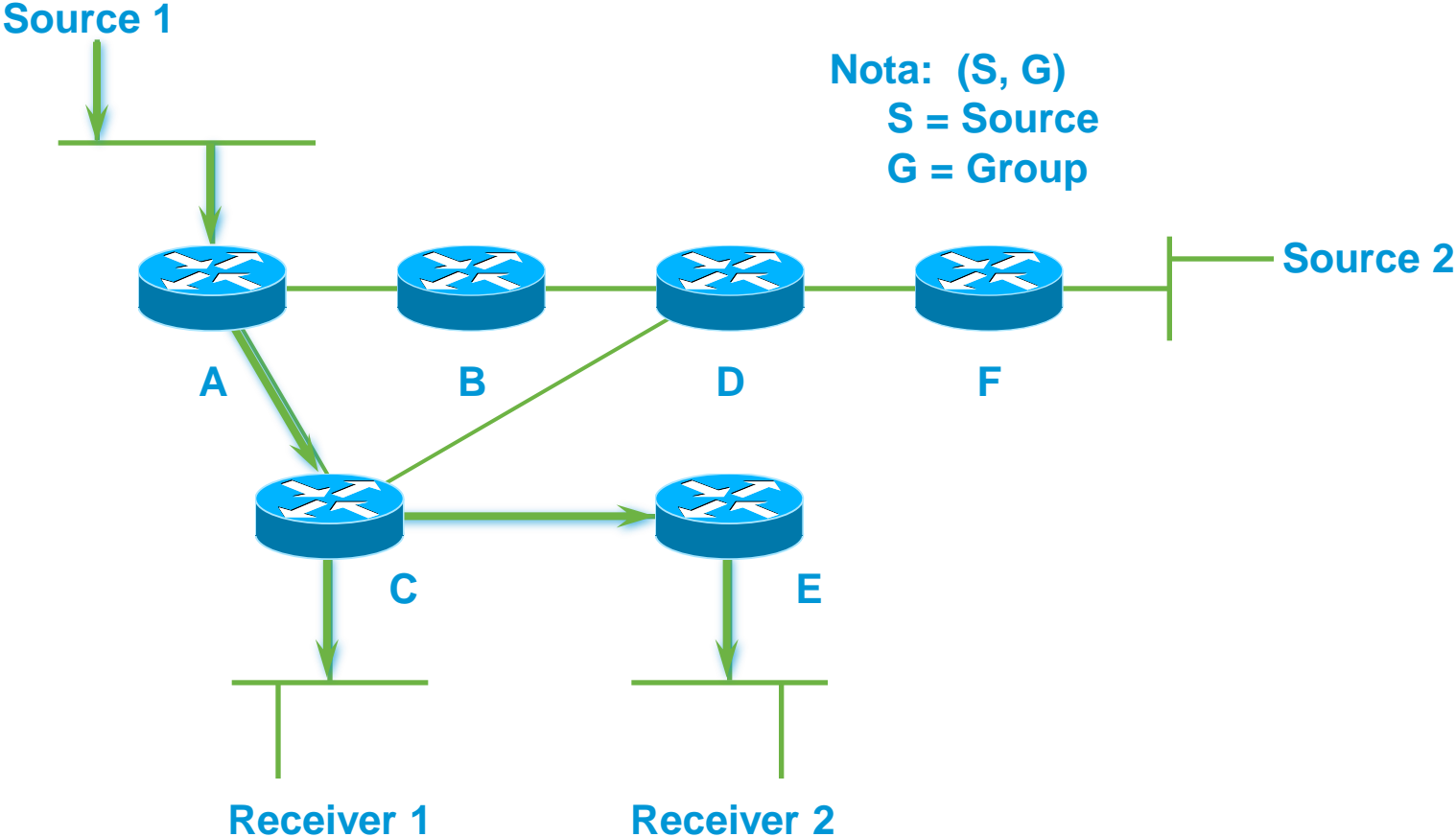
# Agenda

- Porquê IP Multicast?
- Fundamentos IP Multicast
- Multicast em Layer 2
- **Multicast Intra-domínio**



# Multicast Distribution Trees

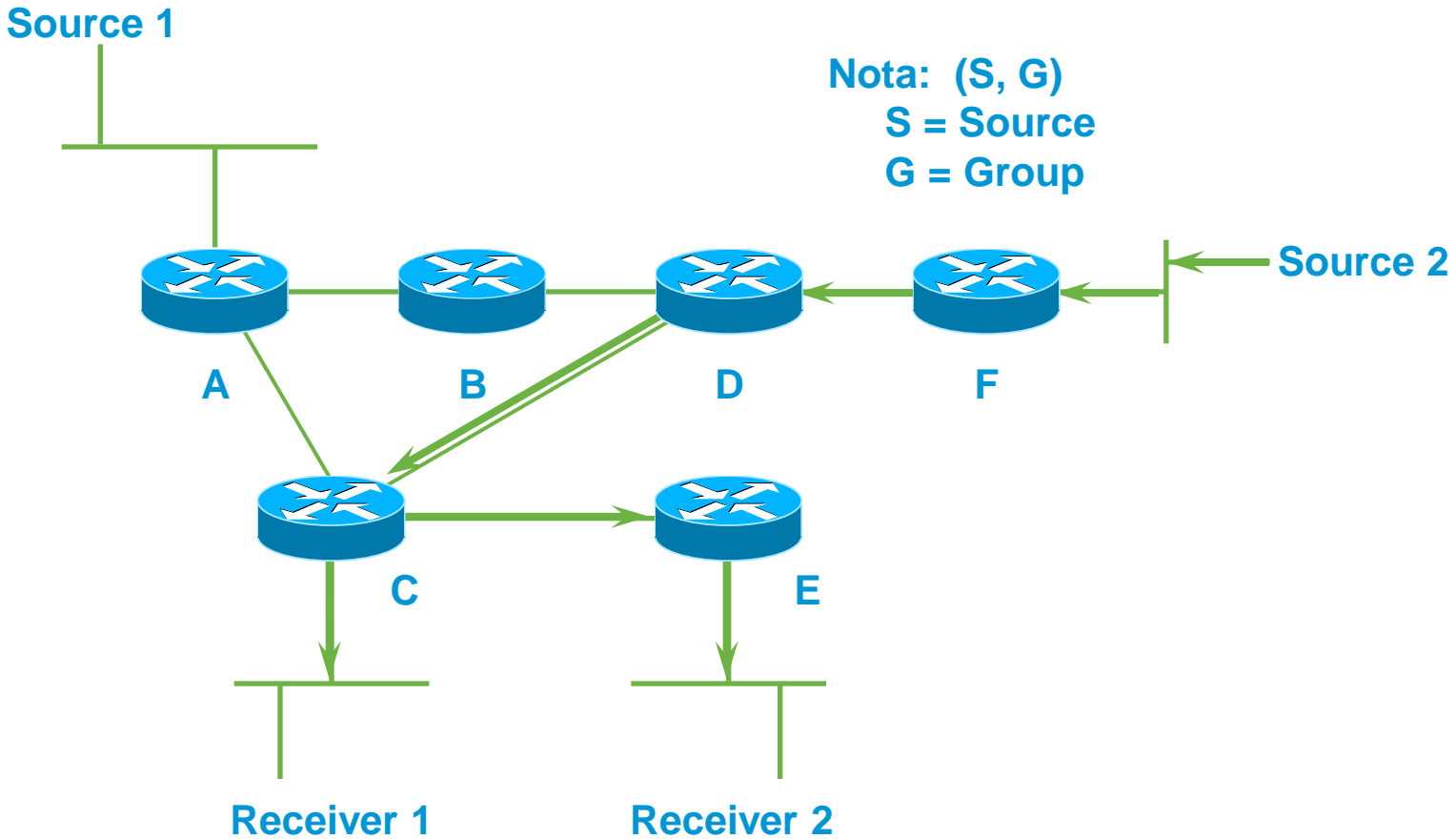
“Shortest Path Tree” ou “Source Distribution Tree”





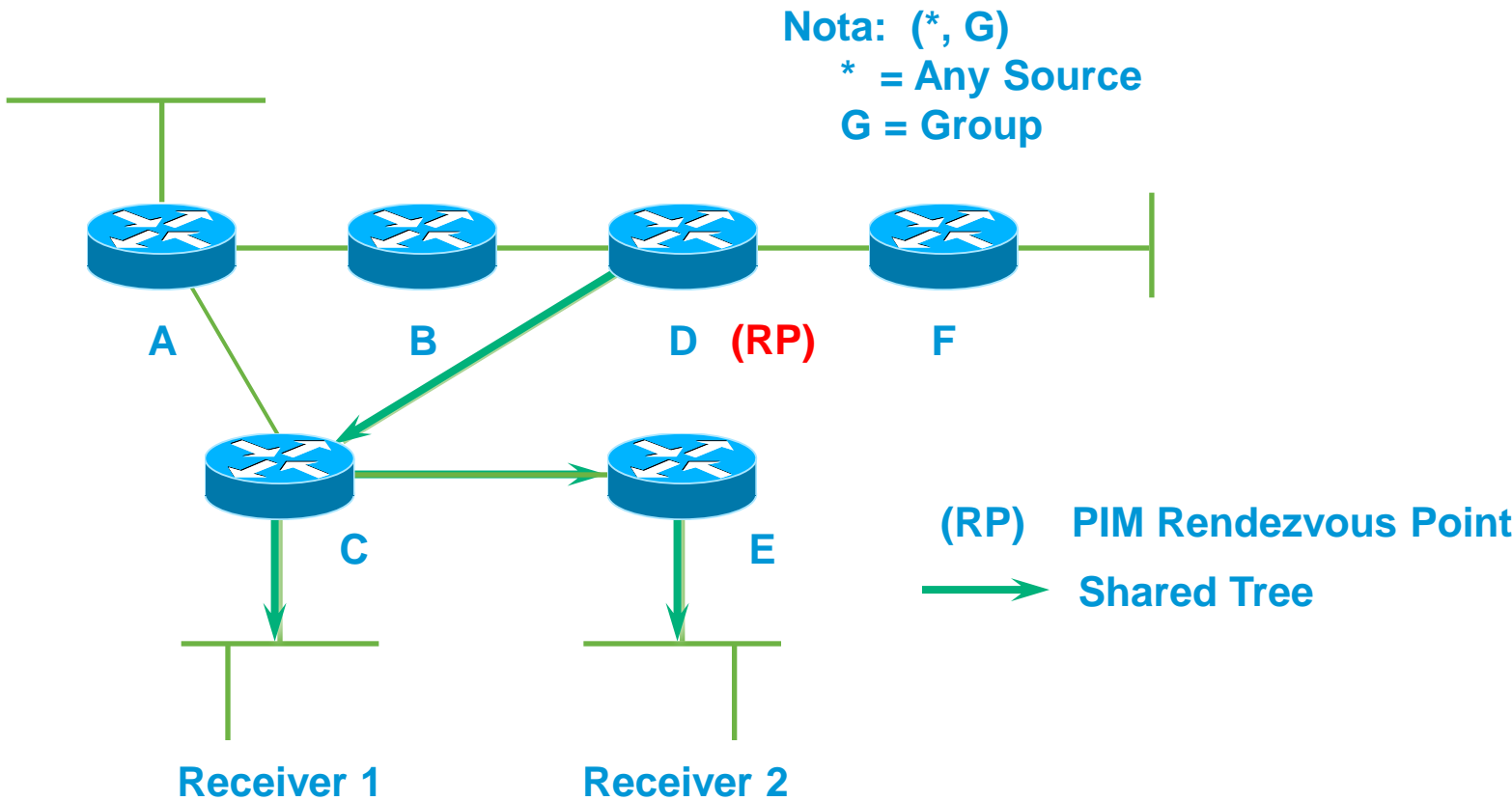
# Multicast Distribution Trees

“Shortest Path Tree” ou “Source Distribution Tree”



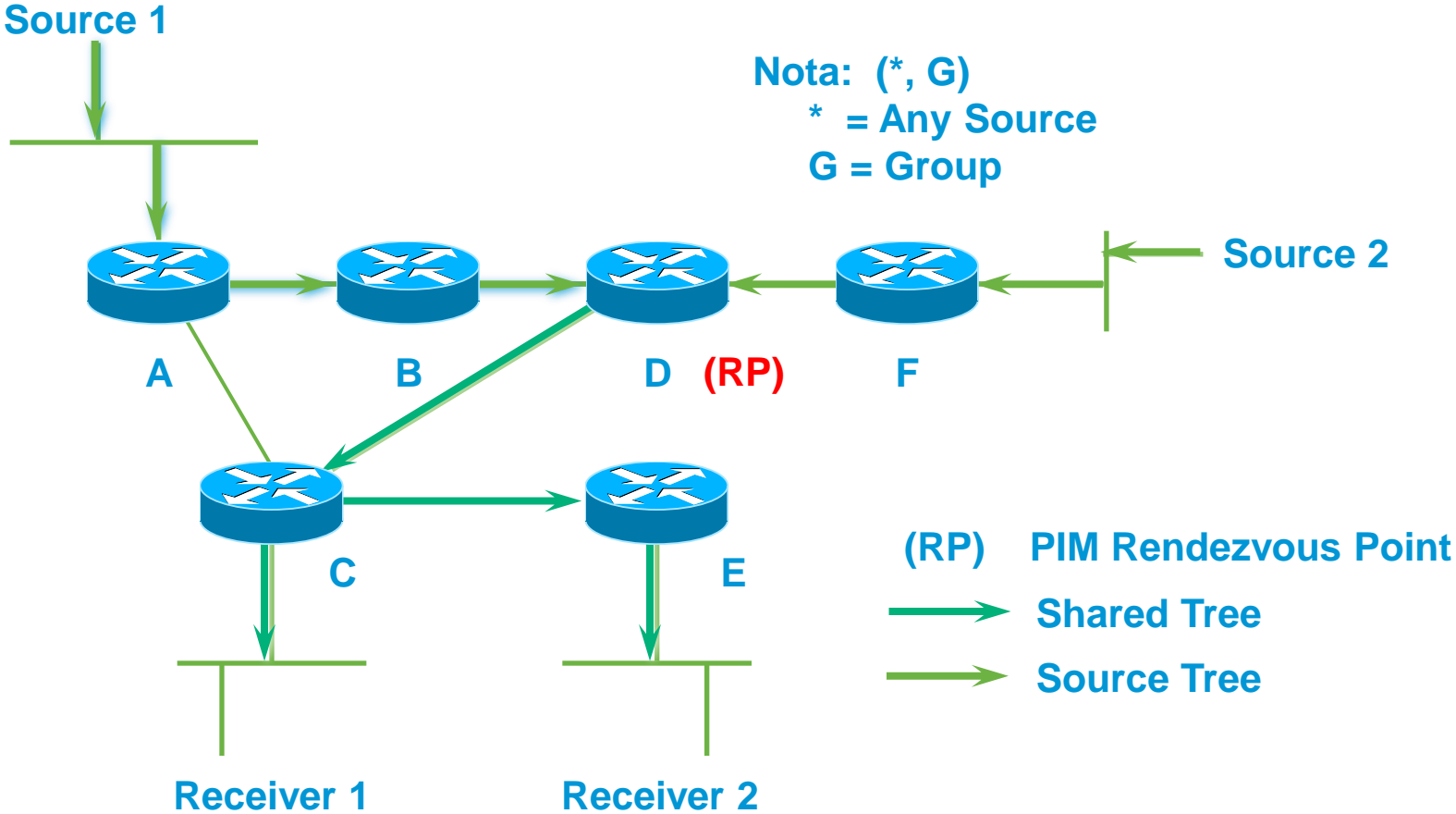
# Multicast Distribution Trees

## “Shared Distribution Tree”



# Multicast Distribution Trees

## “Shared Distribution Tree”



# Multicast Distribution Trees

## Características das “Distributions Trees”

- **Source ou Shortest Path trees**

- ✓ Maior consumo de memória – estados (S,G).
- ✓ Utilizam o melhor caminho entre a source e os receivers (melhor métrica) minimizando o tempo de transmissão.

- **Shared trees**

- ✓ Menor consumo de memória – estados (\*,G).
- ✓ Utilizam caminhos sub-óptimos entre a source e os receivers podendo introduzir atrasos na transmissão.

# Multicast Forwarding

## Reverse Path Forwarding (RPF)

- **O routing do tráfego de Multicast é realizada numa perspectiva inversa do routing de tráfego de Unicast**
  - ✓ O routing do tráfego de Unicast tem em consideração o destino do pacote.
  - ✓ O routing do tráfego de Multicast tem em consideração a origem do pacote.
- **O routing de Multicast utiliza o mecanismo de “Reverse Path Forwarding”**

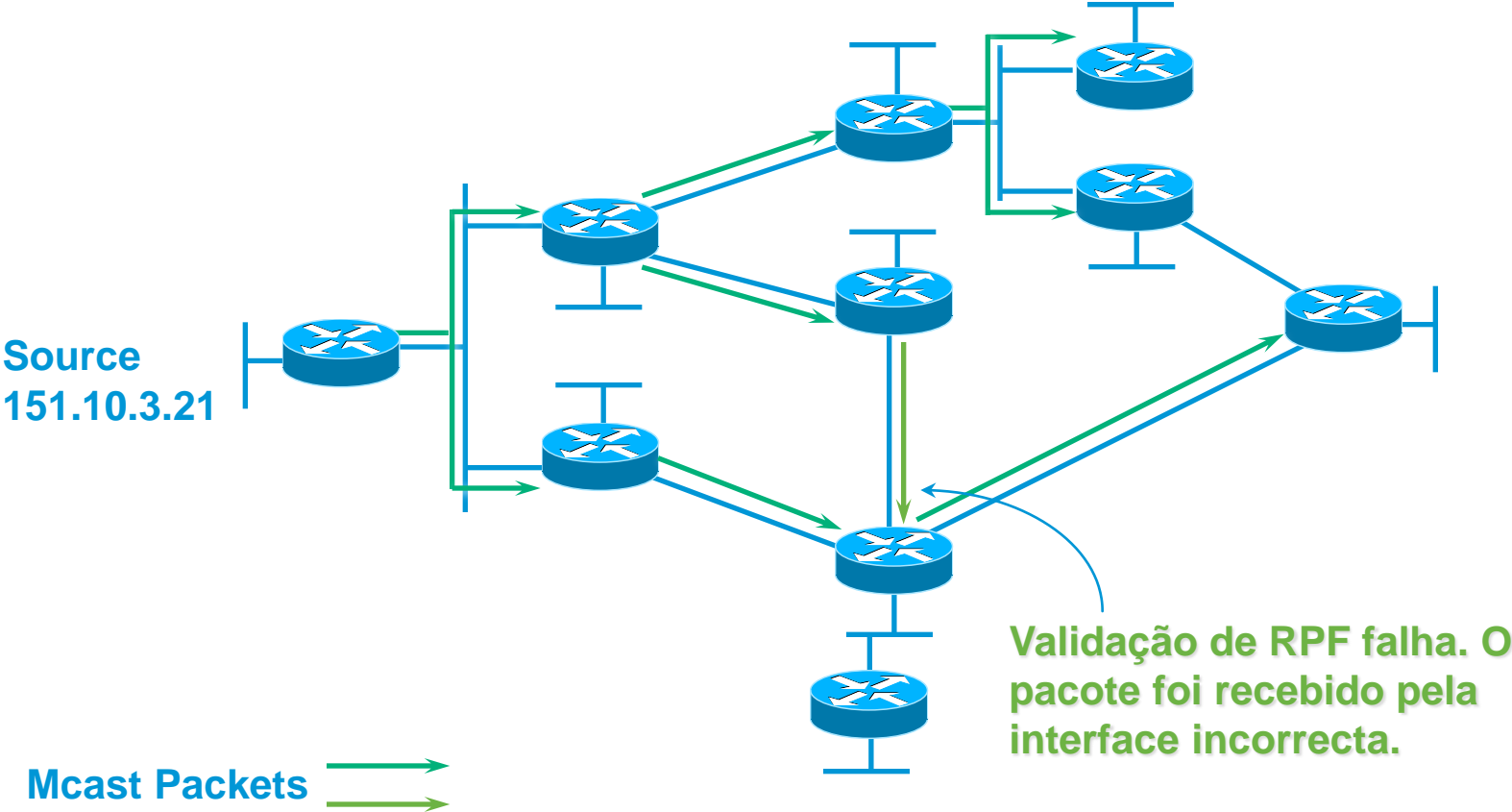
# Multicast Forwarding

## Reverse Path Forwarding (RPF)

- O pacote de Multicast é transmitido apenas se foi recebido pela interface utilizada para chegar à sua origem.
- Validação de RPF
  - ✓ A tabela de routing Unicast é utilizada para validar o caminho em direcção à origem do pacote de Multicast.
  - ✓ Se o pacote de Multicast foi recebido pela interface indicada pela tabela de routing de Unicast para se chegar à source então a validação é bem sucedida. O pacote é enviado para cada uma das interfaces de saída identificadas na *Outgoing Interface List (OIL)* – segue a *Distribution Tree*.
  - ✓ Caso contrário, a validação de RPF falha e pacote é silenciosamente descartado.

# Multicast Forwarding

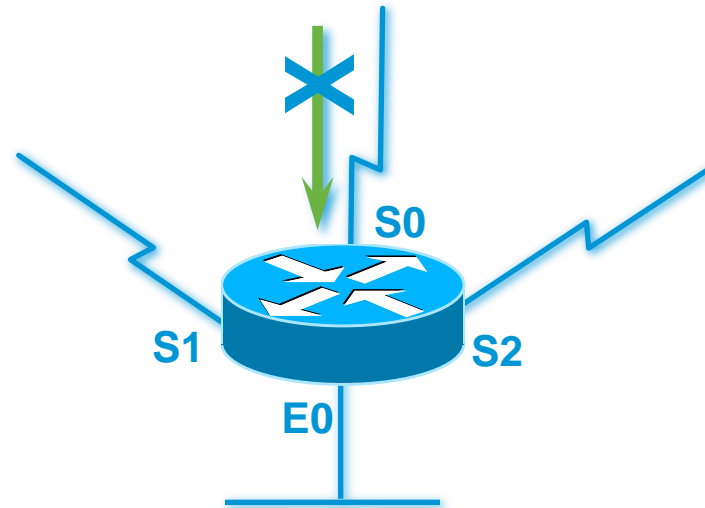
## Exemplo: Validação de RPF



# Multicast Forwarding

## Em detalhe: Validação de RPF mal sucedida

Pacote de Multicast da source  
151.10.3.21



### Validação de RPF NOK

Tabela de Routing Unicast	
Rede	Interface
151.10.0.0/16	<b>S1</b>
198.14.32.0/24	S0
204.1.16.0/24	E0

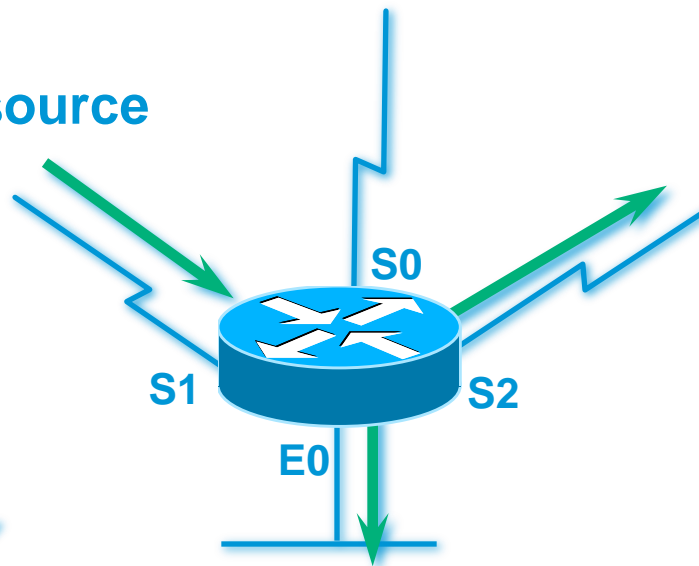
O pacote recebido na interface incorrecta.  
Por essa razão o pacote é descartado.



# Multicast Forwarding

Em detalhe: **Validação de RPF bem sucedida**

Pacote de Multicast da source  
151.10.3.21



Validação de RPF OK

Tabela de Routing Unicast	
Rede	Interface
151.10.0.0/16	<b>S1</b>
198.14.32.0/24	S0
204.1.16.0/24	E0

O Pacote é recebido na interface correcta.  
O Pacote é replicado e enviado a  
todas as interfaces (de acordo com  
“distribution tree”).

# Protocolos de Routing de Multicast

- **Dense mode protocols**
  - ✓ Protocol Independent Multicast – Dense Mode (PIM-DM)
  - ✓ Distance Vector Multicast Routing Protocol (DVMRP)
- **Sparse mode protocols**
  - ✓ Protocol Independent Multicast – Sparse Mode (PIM-SM)  
*Any-Source Multicast (ASM) e Source-Specific Multicast (SSM)*
  - ✓ Bidirectional Protocol Independent Multicast (BiDir-PIM)
  - ✓ Core-Based Trees (CBT)
- **Link-state protocols**
  - ✓ Multicast Open Shortest Path First (MOSPF)

Referências adicionais:  
PIM-DM – [RFC3973](#)  
PIM-SM – [RFC4601](#)  
BIDIR-PIM – [RFC5015](#)

# Protocolos de Routing de Multicast

- **Dense mode protocols**

- ✓ Modelo “Push”.
- ✓ Tráfego é enviado para toda a rede (*flooded*).
- ✓ Tráfego é eliminado (*pruned*) nos troços onde não existem receivers interessados.
- ✓ Comportamento “Flood & Prune” (a cada 3 minutos).

- **Sparse mode protocols**

- ✓ Modelo “Pull”.
- ✓ Tráfego é enviado apenas se explicitamente solicitado.
- ✓ Comportamento de “Joins” explícitos.

# Protocolos de Routing de Multicast: PIM-DM

- **Protocol Independent**

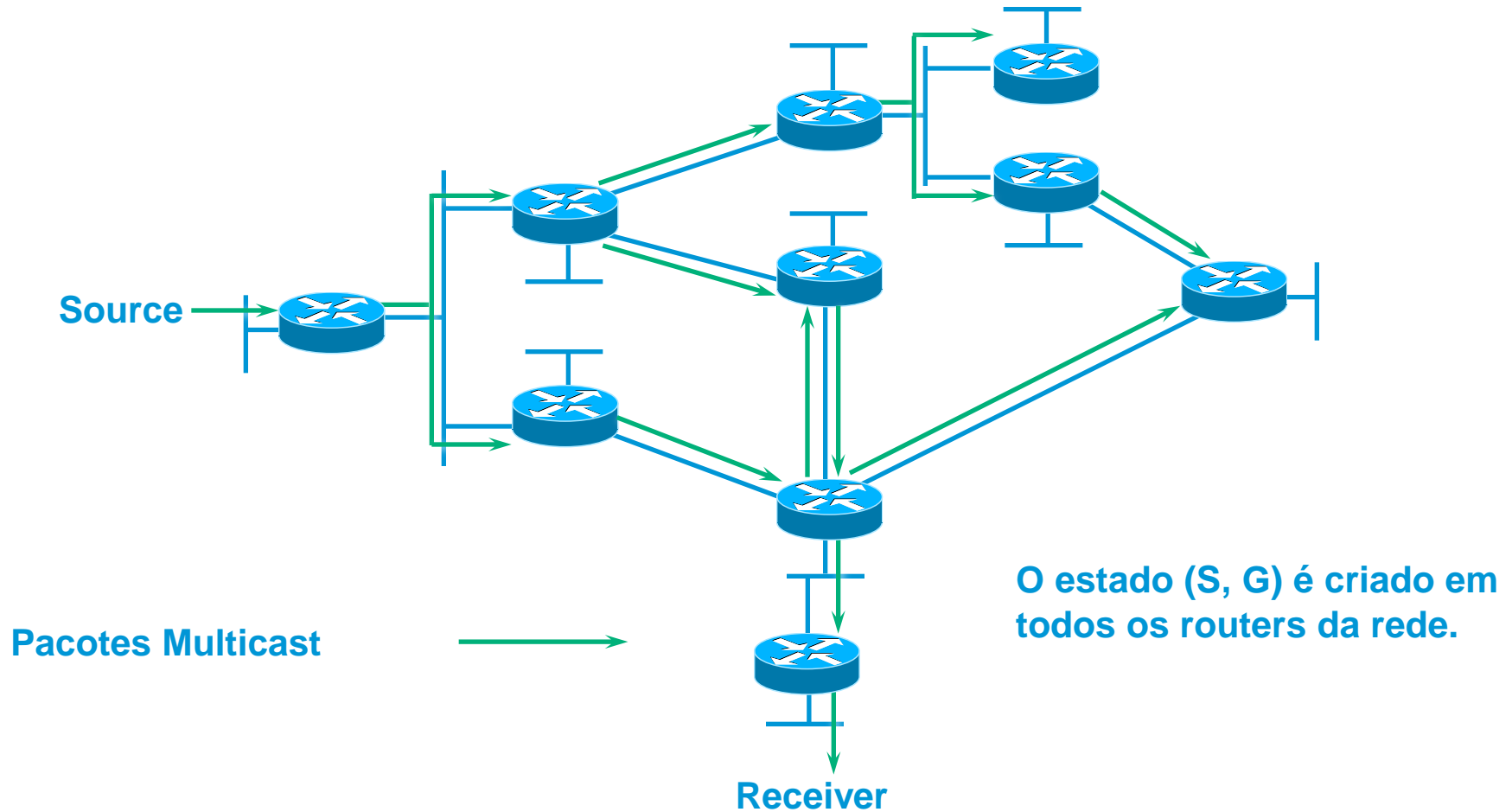
- ✓ Suporta todos os protocolos de routing de Unicast incluindo: rotas estáticas, RIP, IGRP, EIGRP, ISIS, BGP e OSPF.
- ✓ Inunda a rede (flood) e elimina o tráfego (prune) de Multicast baseado na inexistência de receivers.
- ✓ Utiliza o mecanismo de “Assert” para eliminar (prune) fluxos redundantes.

- **Apropriado para:**

- ✓ Pequenas implementações e soluções piloto/experimentais.

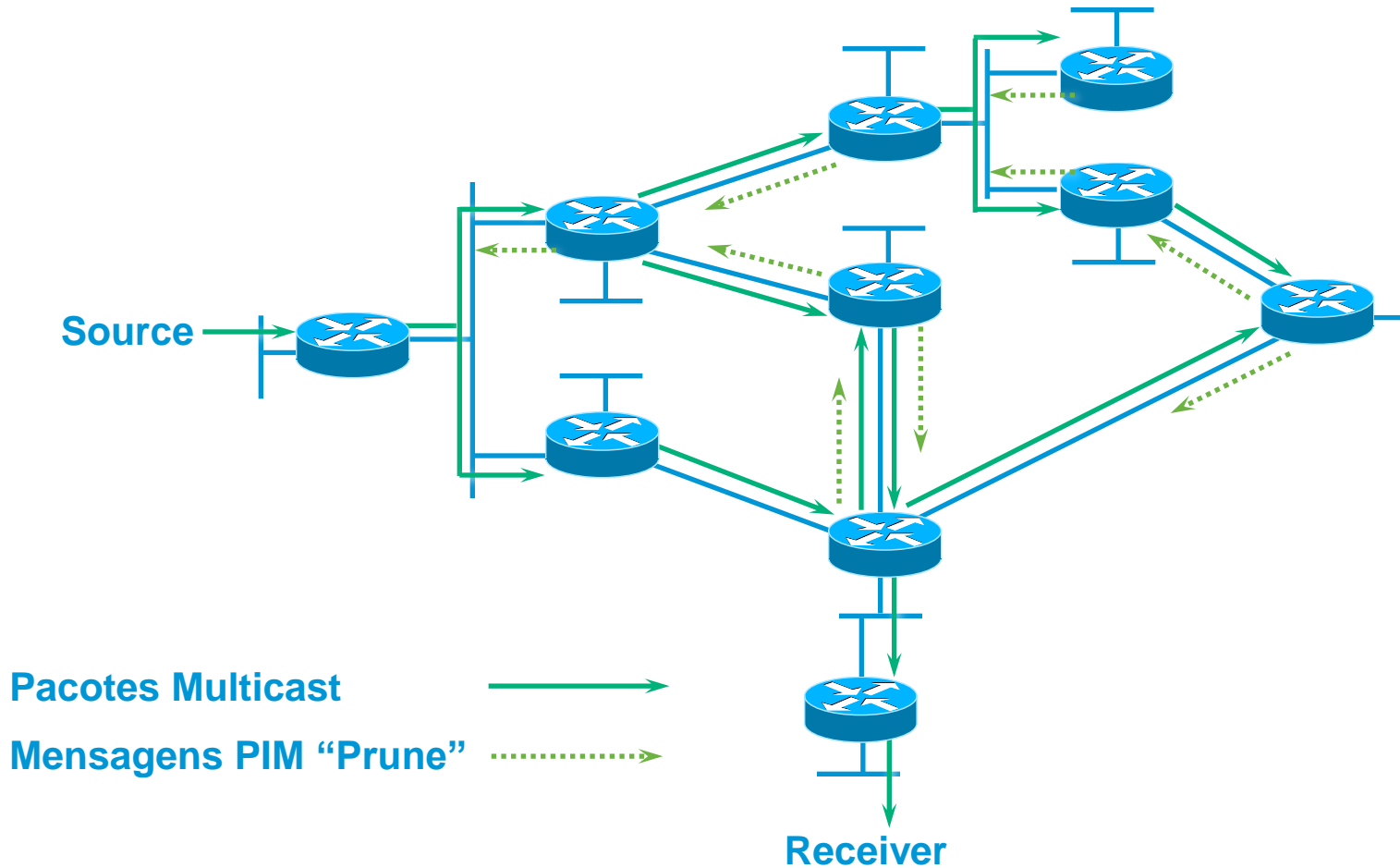
# Protocolos de Routing de Multicast: PIM-DM

## Flood e Prune: *Flooding* inicial



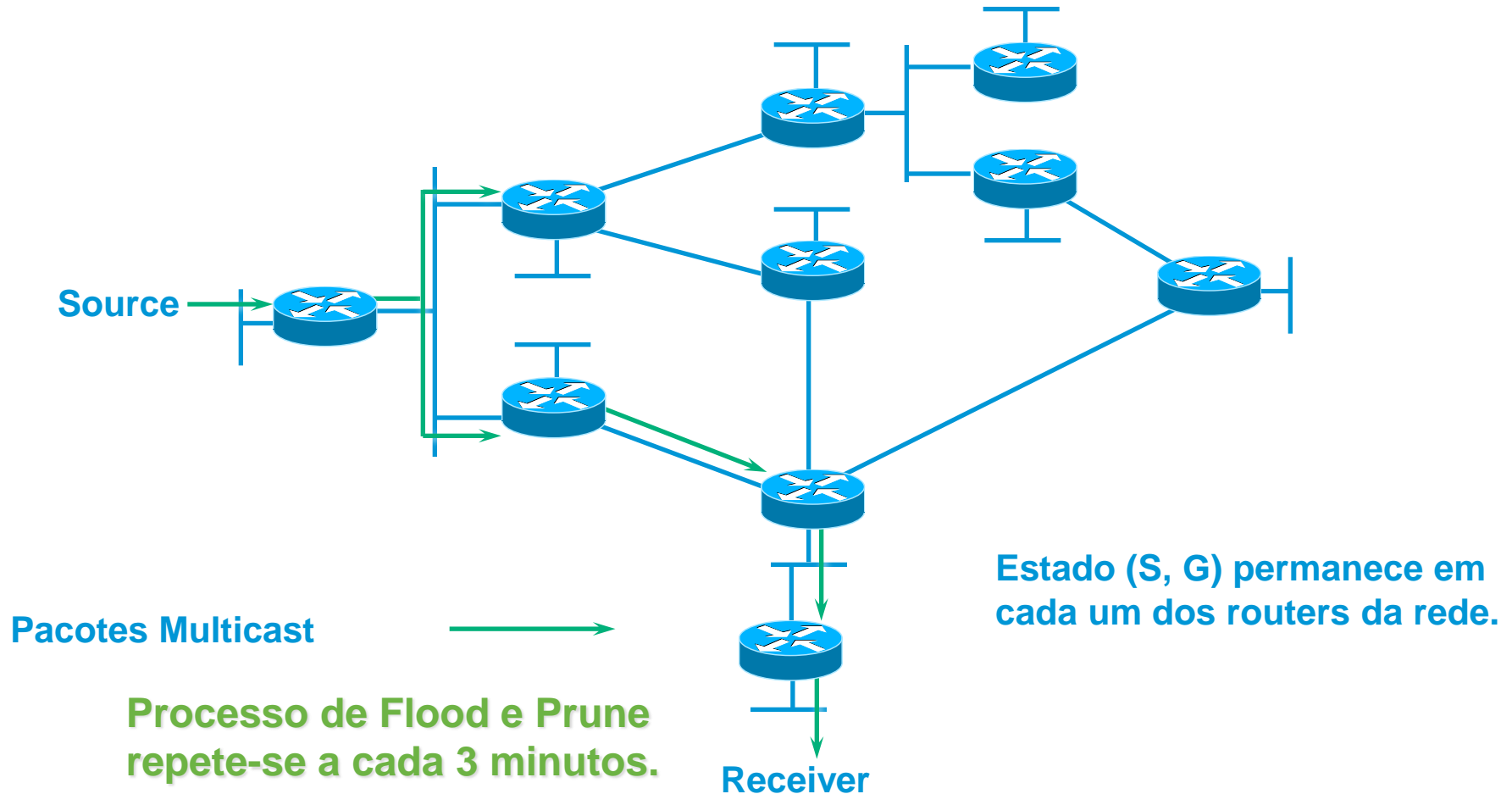
# Protocolos de Routing de Multicast: PIM-DM

## Flood e Prune: Eliminando o tráfego não desejado



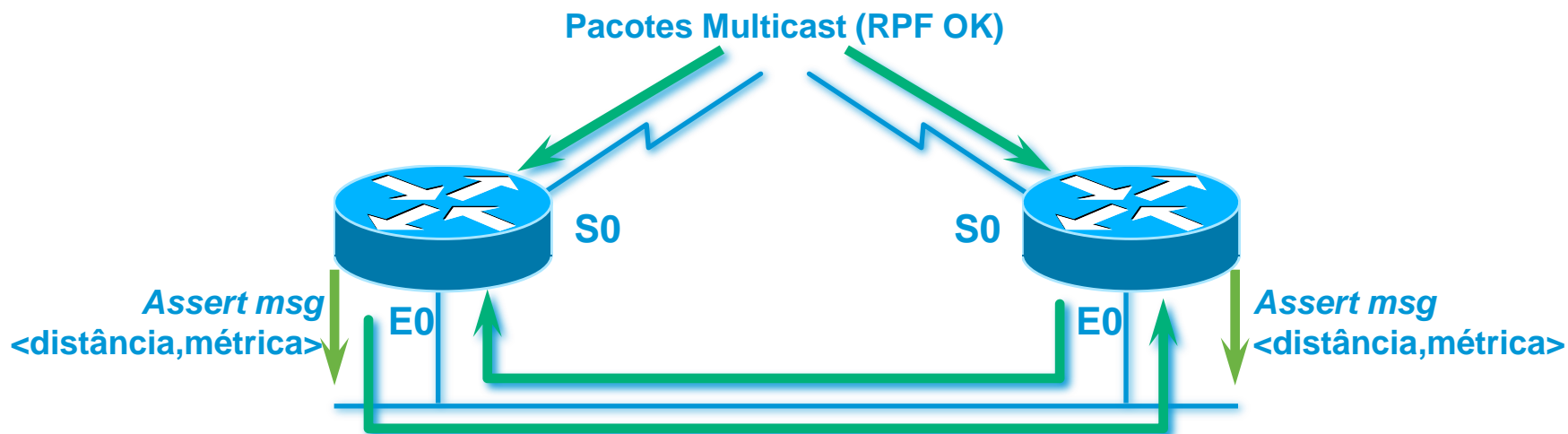
# Protocolos de Routing de Multicast: PIM-DM

## Flood e Prune: Após o *prunning*



# Protocolos de Routing de Multicast: PIM-DM

## Mecanismo de “Assert”



- Se os routers recebem pacotes de Multicast numa interface incluída na OIL list: Apenas um router deverá enviar pacotes de forma a evitar a sua duplicação.
- Os routers enviam mensagens “PIM Assert”.
  - ✓ São comparados os valores de distância e os valores de métrica.
  - ✓ É eleito o router com a melhor rota (métrica) para a source do grupo de Multicast.
  - ✓ Se a métrica e a distância são iguais, é eleito o router com o maior endereço IP.
  - ✓ O router que perde a eleição deixará de enviar tráfego (interface prune).



# Protocolos de Routing de Multicast: PIM-DM

## Sumário

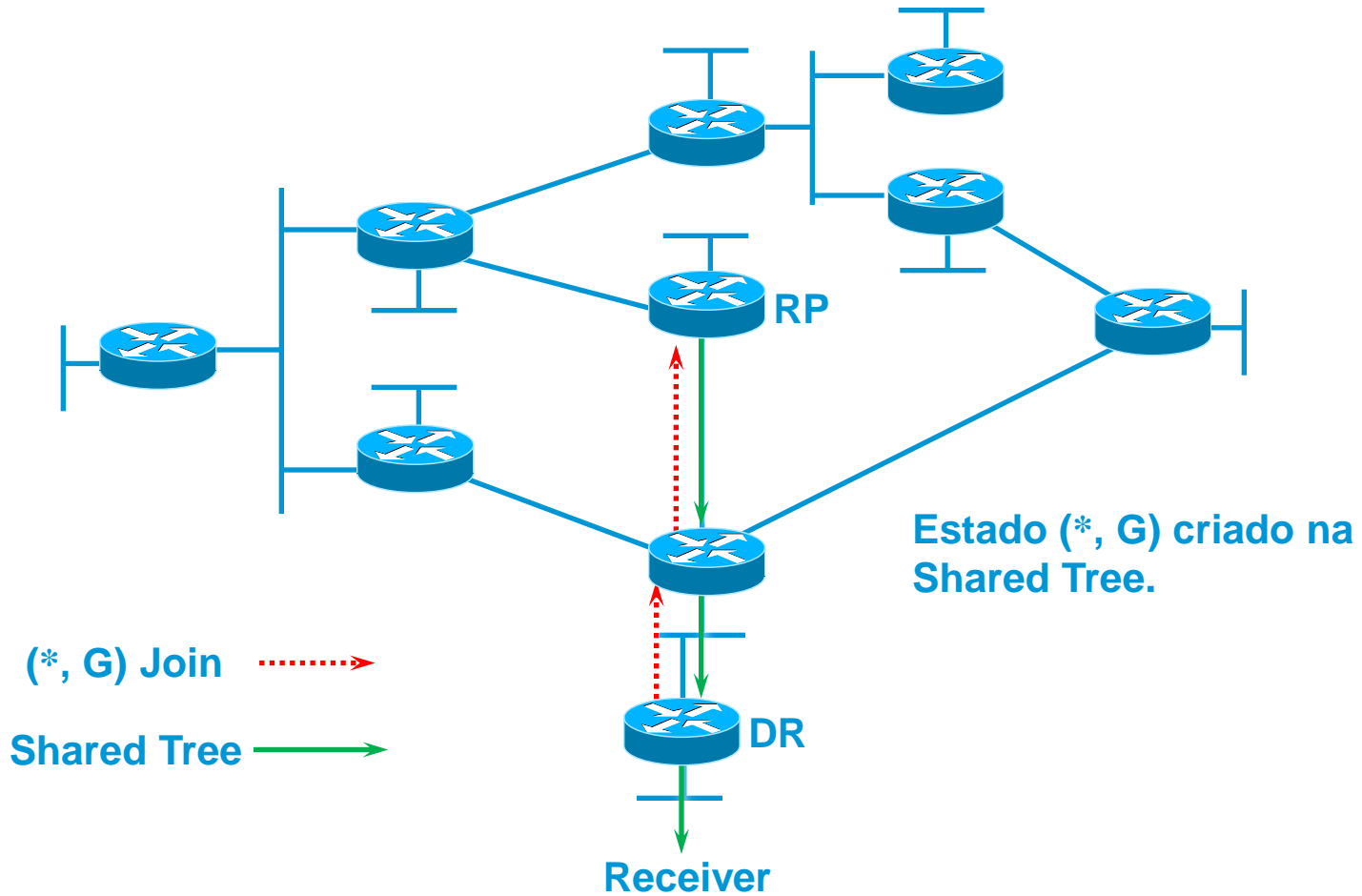
- **Eficaz em pequenas redes piloto/experimentais.**
- **Aspectos positivos:**
  - ✓ Fácil de configurar – dois comandos.
  - ✓ Mecanismo simples de entender e operar (Flood e Prune).
- **Preocupações:**
  - ✓ Mecanismo de “Flood” e “Prune” ineficiente.
  - ✓ Existe dependência entre o plano de controlo e o plano de dados.
    - Resulta na existência de estados (S, G) em cada um dos routers da rede
    - Pode resultar em comportamentos não determinísticos
  - ✓ Não suporta “shared trees”.

# Protocolos de Routing de Multicast: PIM-SM

- **Suporta “Source Trees” e “Shared trees”**
  - ✓ Assume que não existem interessados no tráfego de Multicast salvo se explicitamente sinalizado.
- **Utiliza um Rendezvous Point (RP)**
  - ✓ As sources e os receivers unem-se no RP para saber da existência de um e outro.
  - ✓ As sources registam-se no RP através do router PIM directamente conectado.
  - ✓ Os receivers juntam-se à “Shared Tree” através do Designated PIM router (DR).
- **Apropriado para:**
  - ✓ Redes de larga escala quer em número de receivers quer em número de grupos de multicast dispersos pela rede.

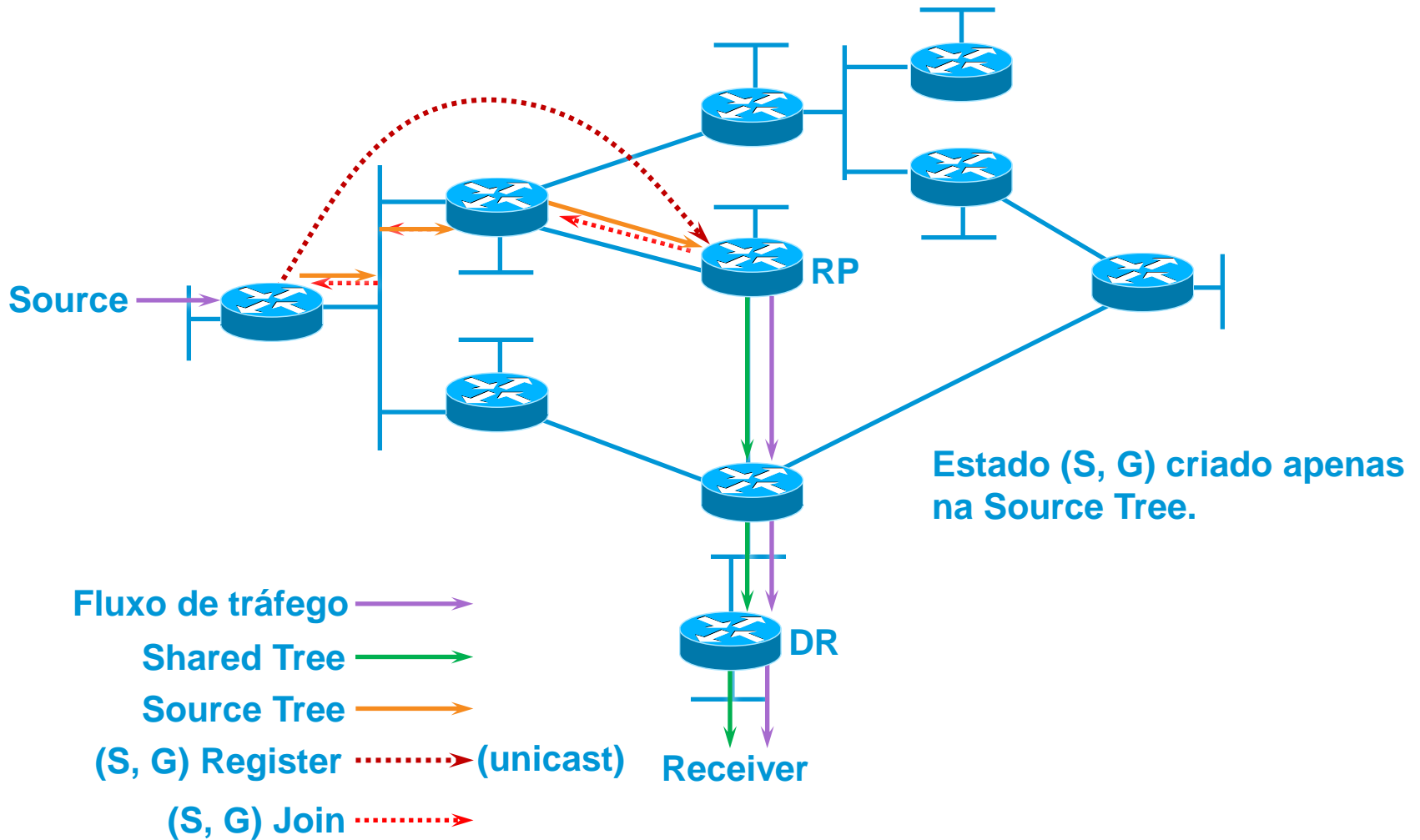
# Protocolos de Routing de Multicast: PIM-SM

## Receiver joins Shared Tree



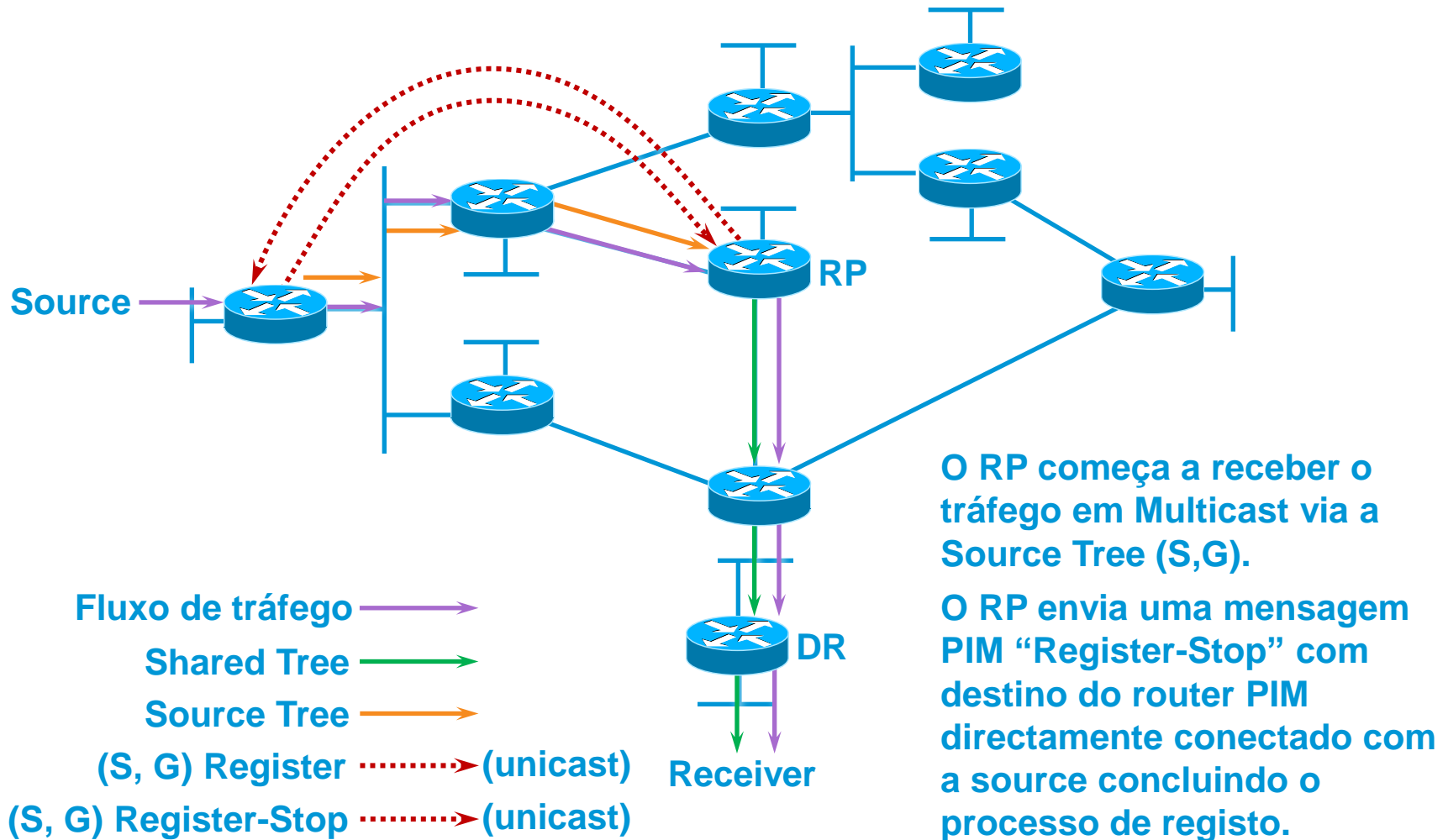
# Protocolos de Routing de Multicast: PIM-SM

## Source joins ("Register" Process)



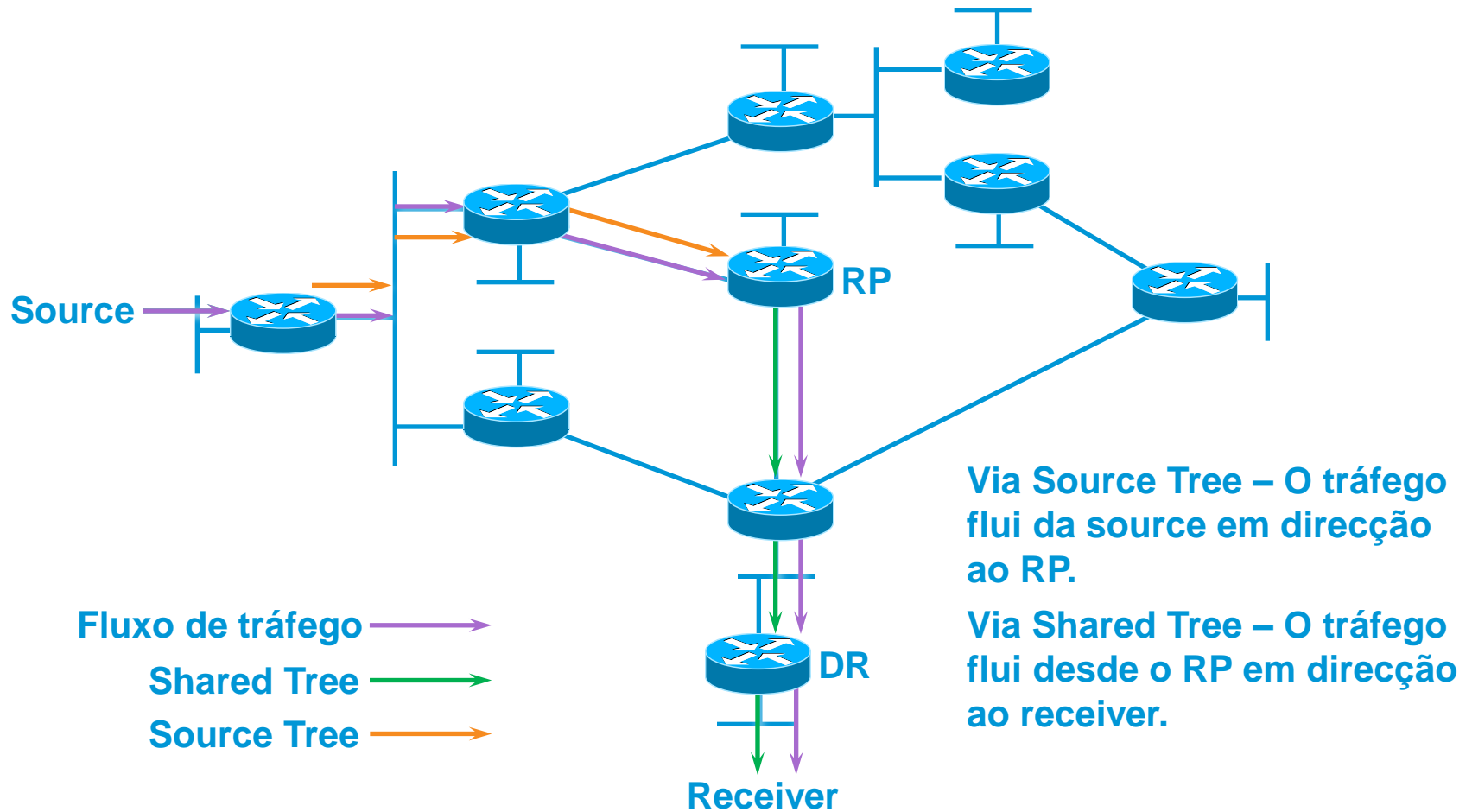
# Protocolos de Routing de Multicast: PIM-SM

## Source joins (“Register” Process)



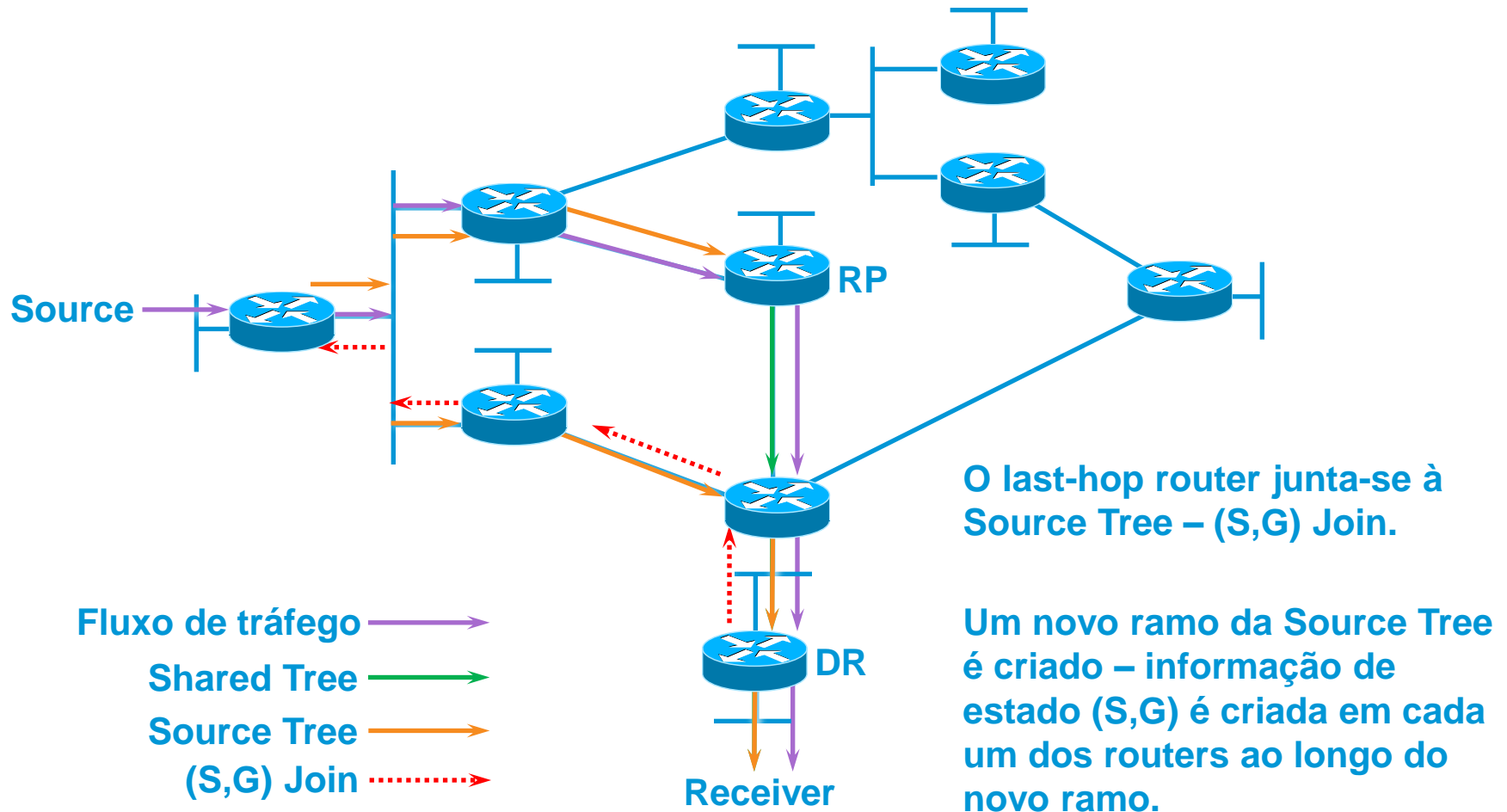
# Protocolos de Routing de Multicast: PIM-SM

## Source joins (“Register” Process)



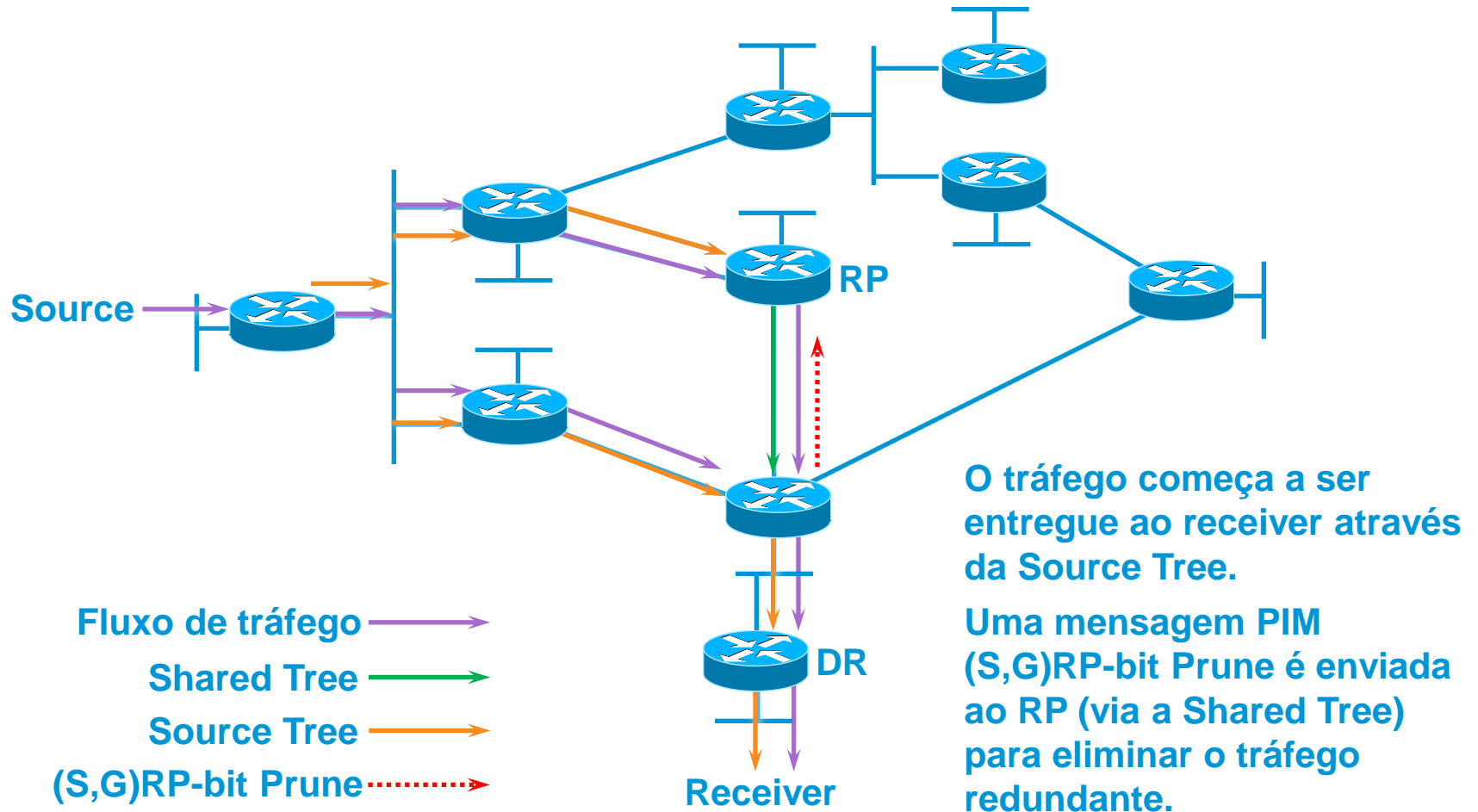
# Protocolos de Routing de Multicast: PIM-SM

## Shortest Path Tree Switchover (SPT-Switchover)



# Protocolos de Routing de Multicast: PIM-SM

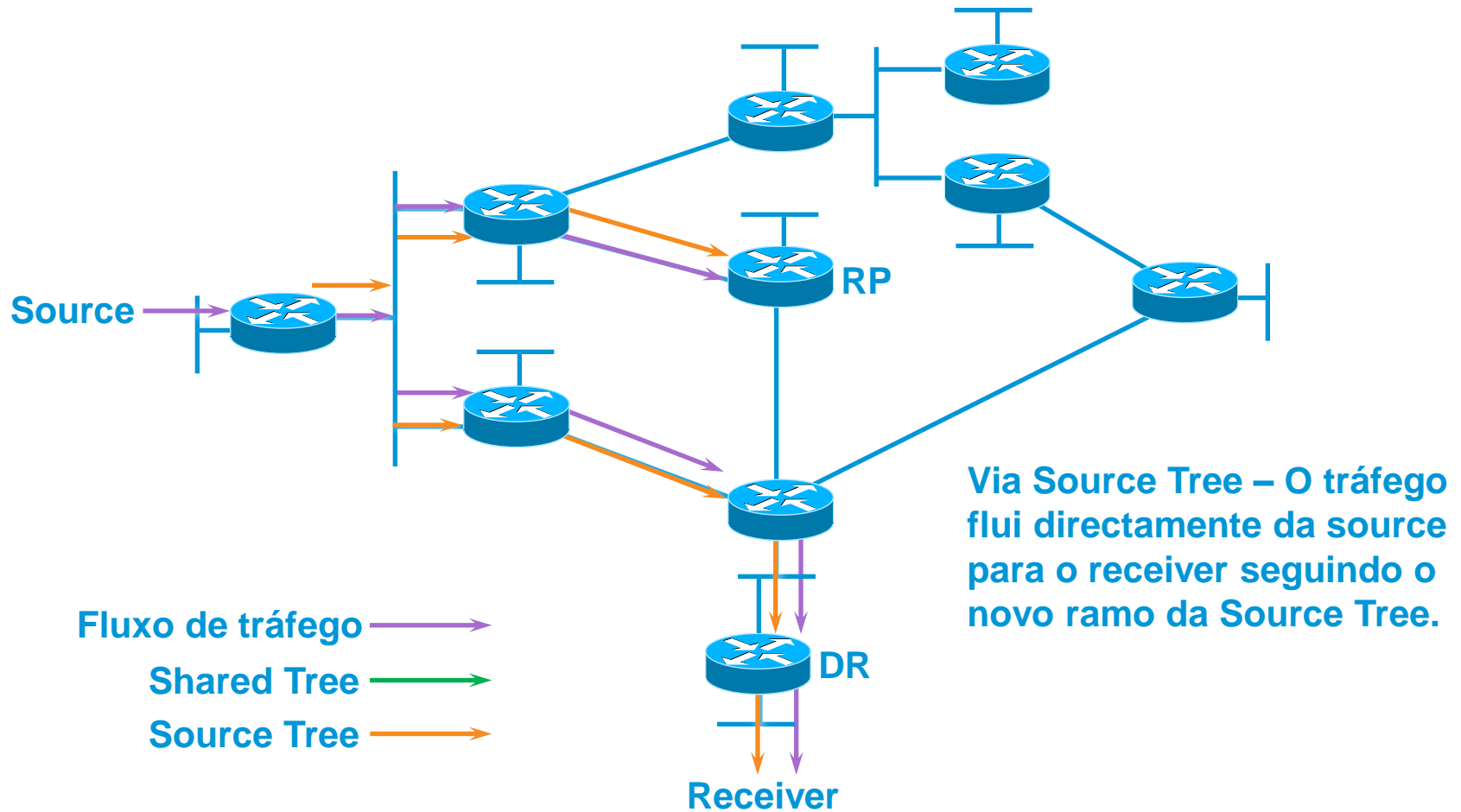
## Shortest Path Tree Switchover (SPT-Switchover)





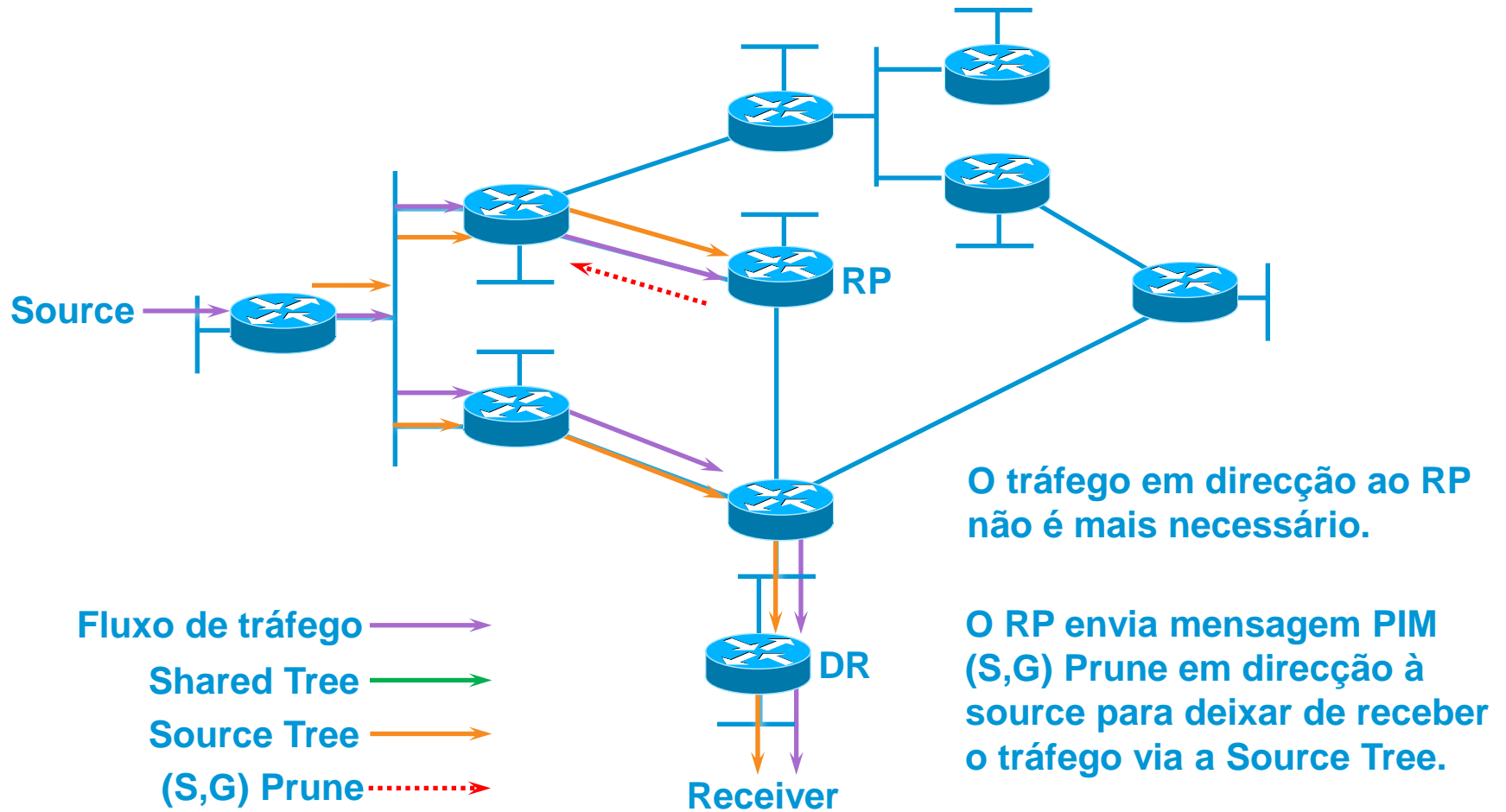
# Protocolos de Routing de Multicast: PIM-SM

## Shortest Path Tree Switchover (SPT-Switchover)



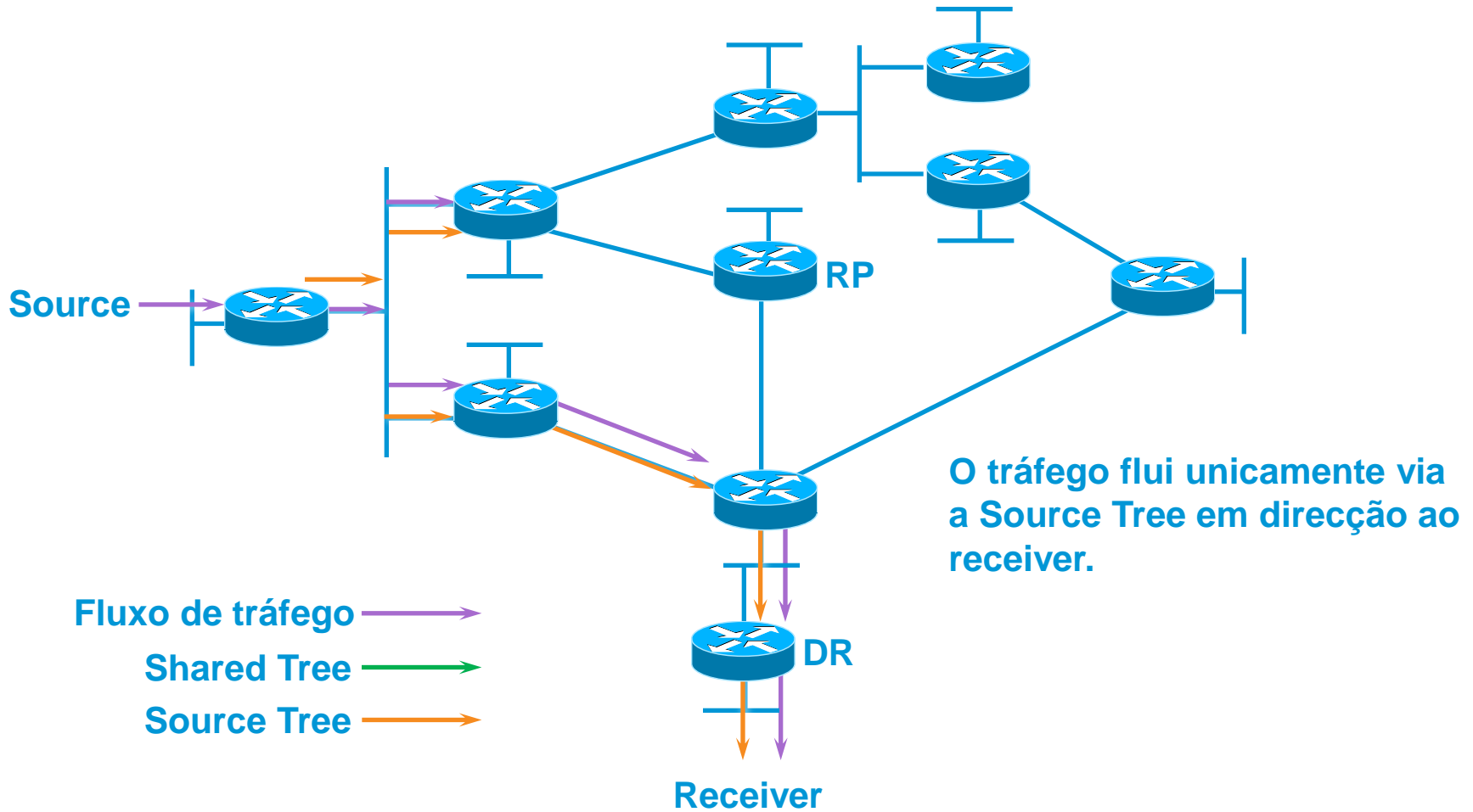
# Protocolos de Routing de Multicast: PIM-SM

## Shortest Path Tree Switchover (SPT-Switchover)



# Protocolos de Routing de Multicast: PIM-SM

## Shortest Path Tree Switchover (*SPT-Switchover*)



# Protocolos de Routing de Multicast: PIM-SM

## Shortest Path Tree Switchover (*SPT-Switchover*)

---

Por omissão o valor de *SPT-Threshold* nos routers Cisco é zero. Um router Cisco (*last-hop router*) irá juntar-se à Source Tree assim que começar a receber tráfego via a Shared Tree.

---

# Protocolos de Routing de Multicast: PIM-SM

## Configuração de RP: RP Estático

- **Endereço IP do RP configurado estaticamente**
  - ✓ Necessário configurar em todos os routers.
  - ✓ Todos os routers devem usar o mesmo endereço IP para o RP.
  - ✓ Não é possível implementar redundância.
    - Exceção: Anycast RPs (necessita MSDP)
  - ✓ Os grupos nunca serão tratados em Dense Mode.

- **Configuração**

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

- ✓ Opcionalmente é possível especificar um conjunto de grupos.

Por omissão é = 224.0.0.0/4 (*Inclui os grupos de Auto-RP!*)

- ✓ “override” sobrepõe-se à informação de Auto-RP.

Por omissão: A informação de Auto-RP é preferida

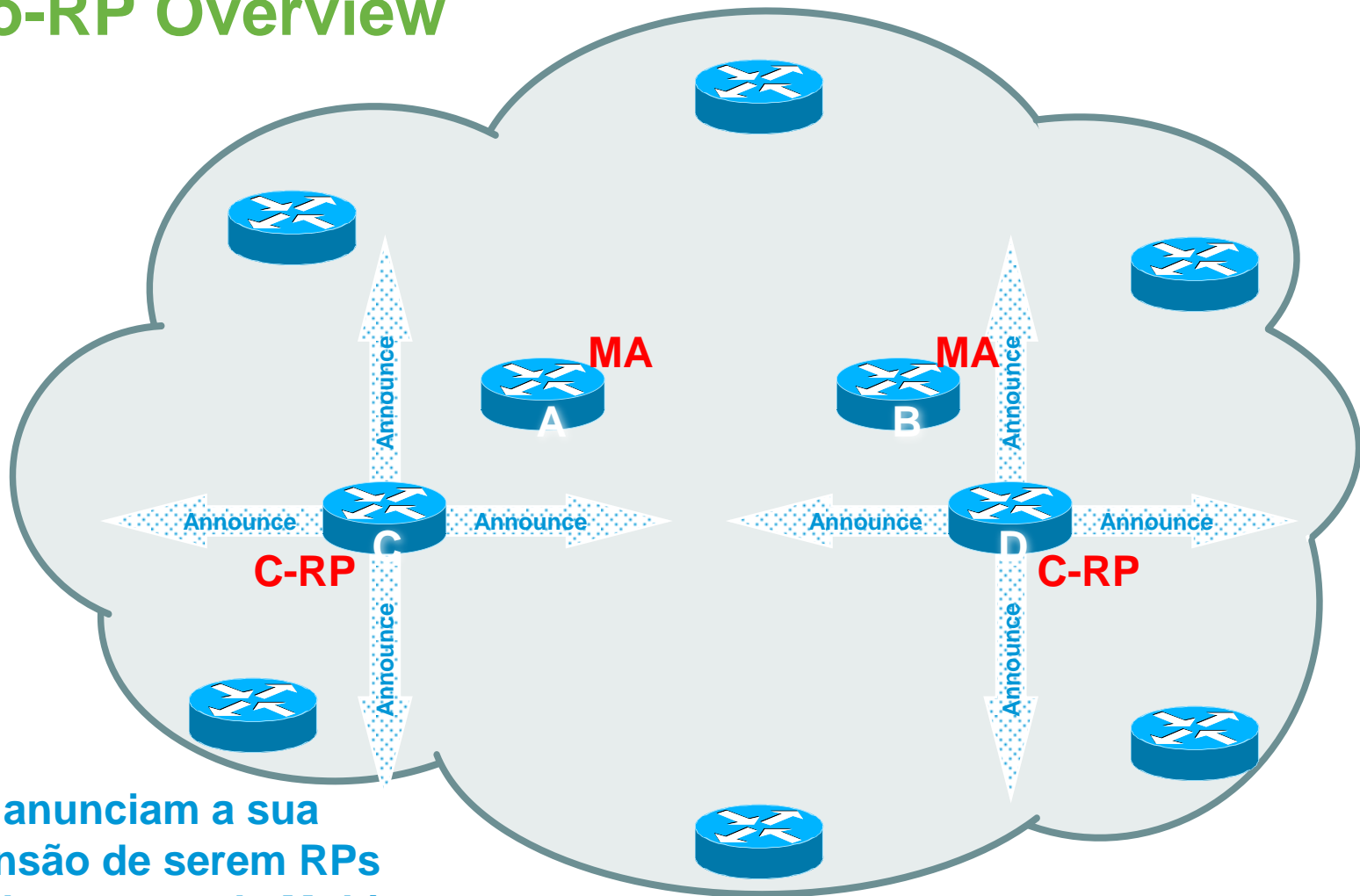
# Protocolos de Routing de Multicast: PIM-SM

## Configuração de RP: Auto-RP

- **Todos os routers aprendem o endereço do RP**
  - ✓ Configuração necessária apenas nos routers que desempenham a função de Candidate RP (C-RP) e Mapping Agent (MA).
- **Utiliza Multicast para distribuir a informação**
  - ✓ Grupos de multicast reservados e assignadas pela IANA.
    - Cisco-Announce – 224.0.1.39
    - Cisco-Discovery – 224.0.1.40Estes grupos funcionam em Dense Mode
- **Permite implementar redundância de RP**
  - ✓ Atenção: Pode resultar em “Dense Mode” fallback se mal configurado.
- **Suporta Administratively Scoped Zones**
- **Proprietário Cisco Systems**

# Protocolos de Routing de Multicast: PIM-SM

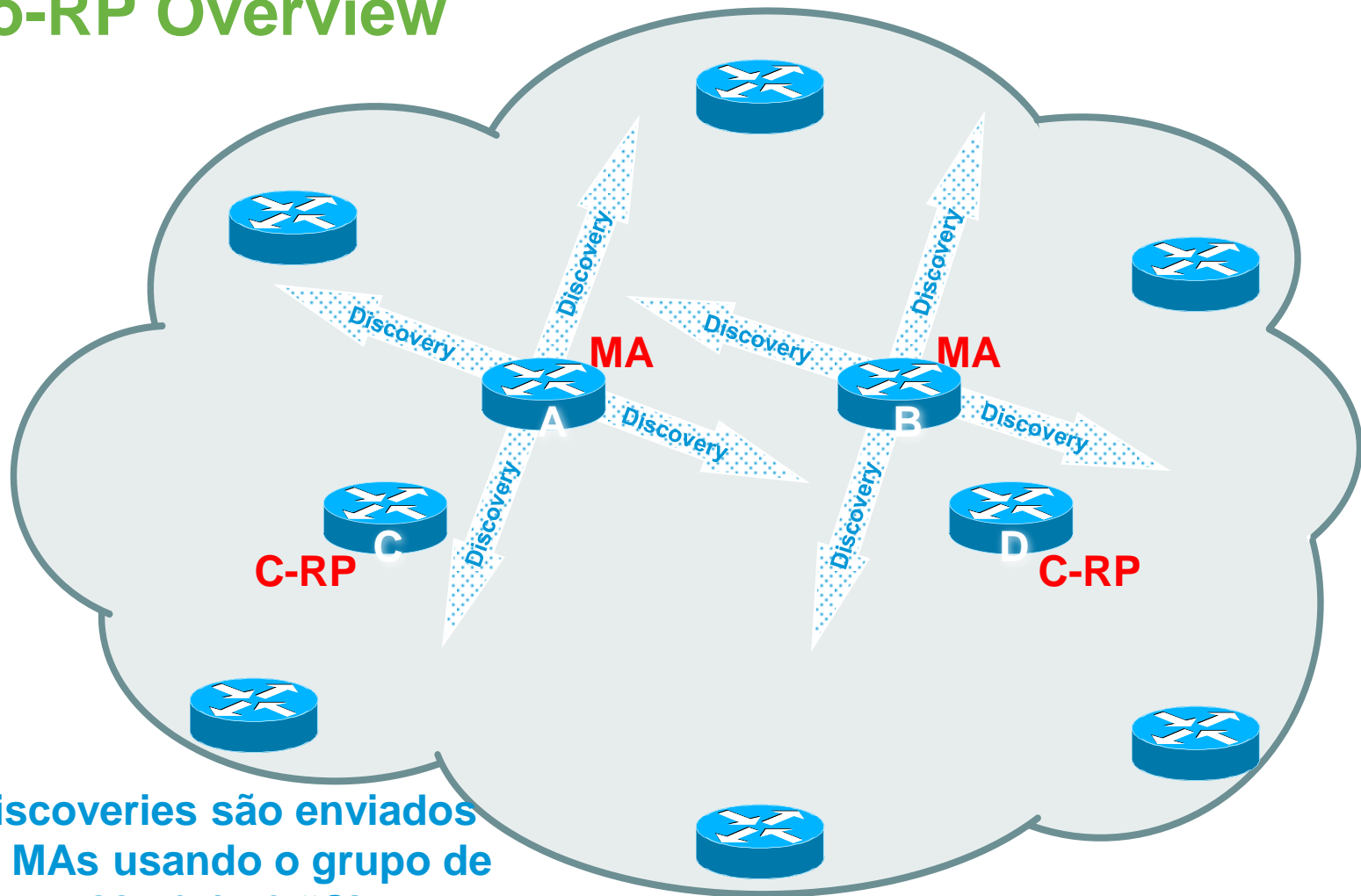
## Auto-RP Overview



C-RP anunciam a sua pretensão de serem RPs usando o grupo de Multicast 224.0.1.39 "Cisco Announce".

# Protocolos de Routing de Multicast: PIM-SM

## Auto-RP Overview



RP-Discoveries são enviados pelos MAs usando o grupo de multicast 224.0.1.40 “Cisco Discovery”.



# Protocolos de Routing de Multicast: PIM-SM

## Configuração de RP: Bootstrap Router (BSR)

- **Eleição do Bootstrap Router (BSR)**

- ✓ Múltiplos candidatos a BSR's (C-BSR) podem ser configurados.

Redundância em caso de falha do BSR eleito

- ✓ C-RPs enviam anúncios (C-RP) ao BSR.

Estes anúncios são enviados em Unicast

O BSR guarda os anúncios C-RP recebidos numa base de dados: RP-Set

- ✓ O BSR envia mensagens periódicas para todos os routers.

As mensagens do BSR contém o seu endereço IP e o RP-Set

As mensagens são enviadas hop-by-hop via Multicast

ALL-PIM Routers 224.0.0.13 ; TTL=1

- ✓ Os routers elegem o RP com base no RP-Set.

Todos os routers usam o mesmo algoritmo na selecção do RP (Hash Algorithm) e desse modo o mesmo RP é seleccionado para um determinado grupo.

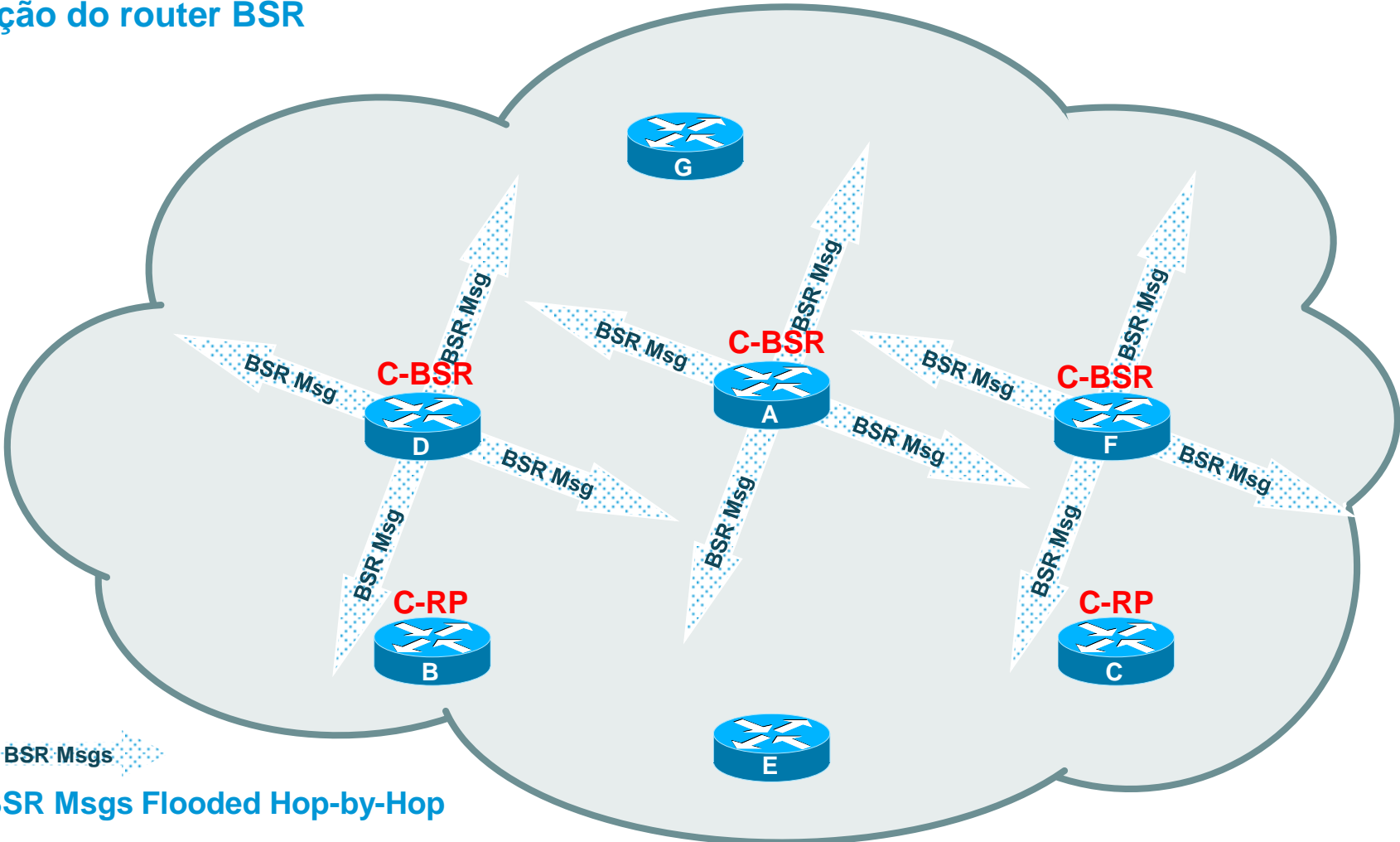
- **Não suporta Administratively Scoped Zones**

Referências adicionais: [RFC5059](#)

# Protocolos de Routing de Multicast: PIM-SM

## BSR Overview

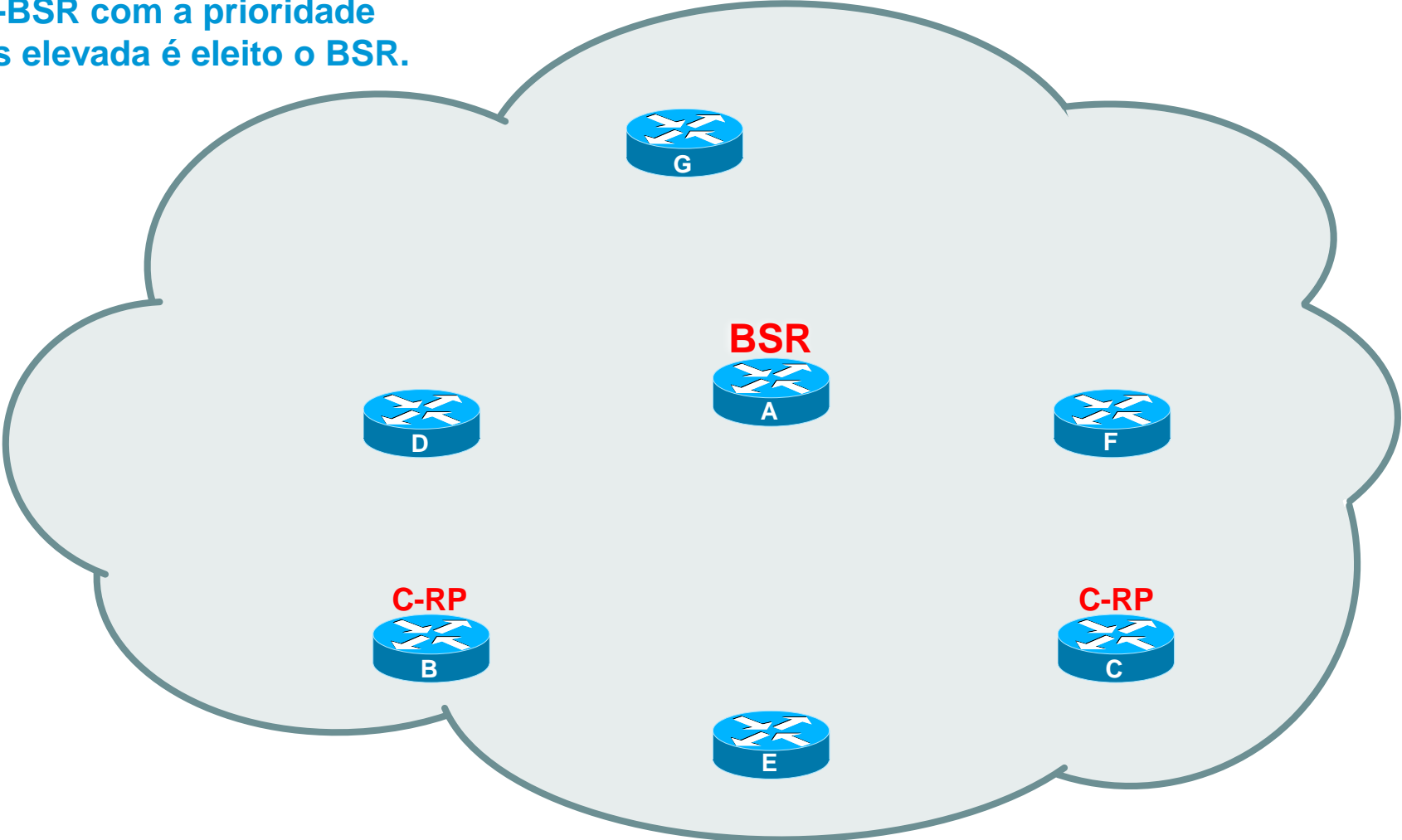
Eleição do router BSR



# Protocolos de Routing de Multicast: PIM-SM

## BSR Overview

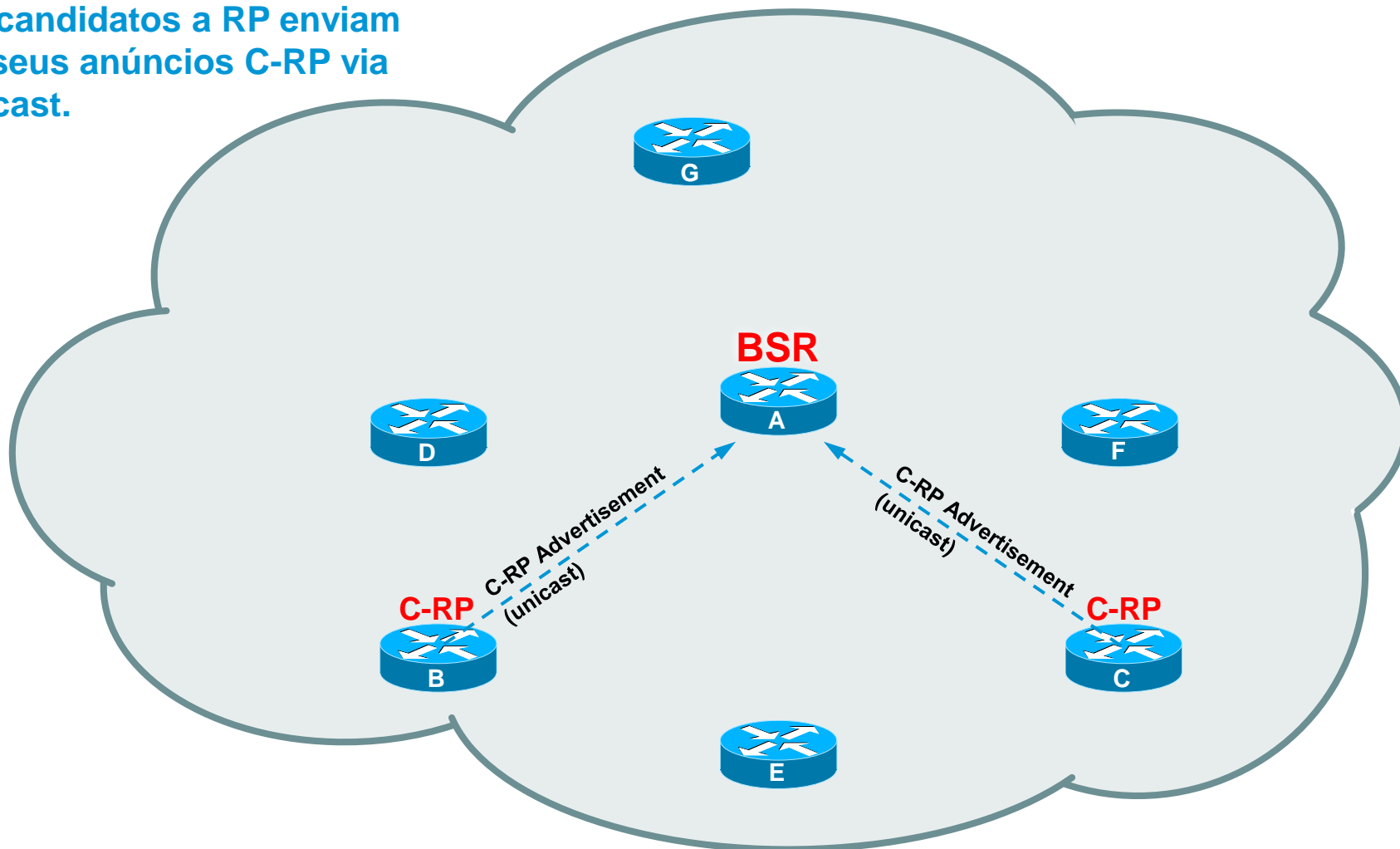
O C-BSR com a prioridade mais elevada é eleito o BSR.



# Protocolos de Routing de Multicast: PIM-SM

## BSR Overview

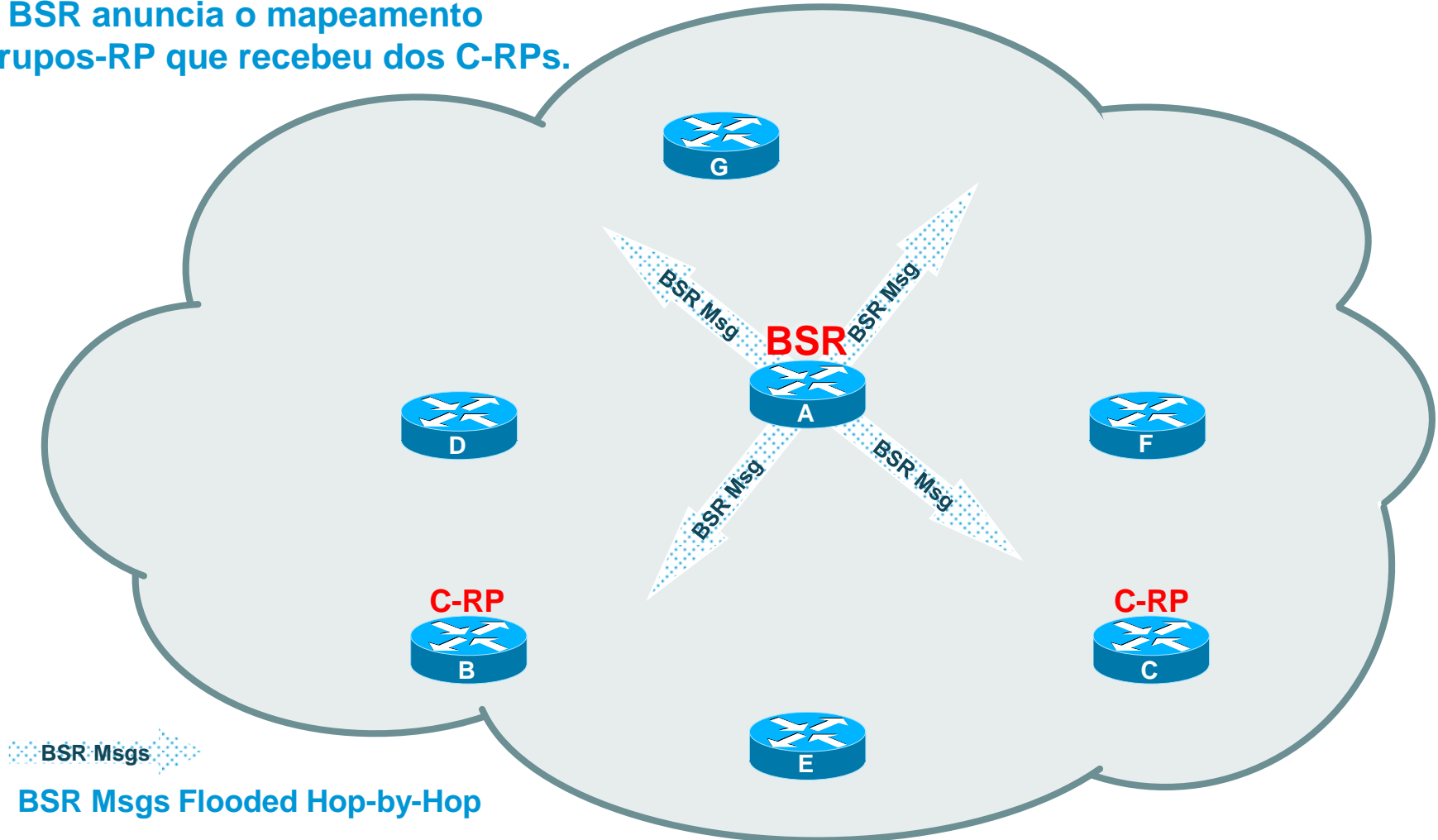
Os candidatos a RP enviam os seus anúncios C-RP via unicast.



# Protocolos de Routing de Multicast: PIM-SM

## BSR Overview

O BSR anuncia o mapeamento Grupos-RP que recebeu dos C-RPs.



# Protocolos de Routing de Multicast: PIM-SM

## Sumário

- **Melhor opção independente da dimensão da rede e do número e/ou distribuição de receivers ou grupos!**
- **Aspectos Positivos:**
  - ✓ Independente do Protocolo de Routing de Unicast.
  - ✓ O tráfego é enviado apenas para os receivers que o tenham explicitamente solicitado (joined).
  - ✓ Comuta de forma dinâmica para a Source Tree.
- **Preocupações:**
  - ✓ **Necessita de um RP**
    - Preocupação adicional no desenho de rede: Localização, Redundância
  - ✓ **Funcionamento e operação complexa.**

# Protocolos de Routing de Multicast: ASM

## Any-Source Multicast (ASM): Desafios

- **Gestão de endereçamento**
  - ✓ Uma única aplicação por endereço de grupo de Multicast.
- **Vulnerabilidade a ataques DoS**
  - ✓ Como impedir sources de tráfego inválidas?
  - ✓ Fará sentido um modelo ASM para a Internet?
- **Crescimento e provisionamento de serviços**
  - ✓ **Shared-Tree**
    - Introduz complexidade acrescida em cenários inter-domínio
    - Sem vantagem em cenários com um pequeno número de sources
  - ✓ **Source-Tree**
    - Gestão de processo de Source discovery complexa (MSDP, não disponível em IPv6)

# Protocolos de Routing de Multicast: SSM

## Source-Specific Multicast (SSM)

- **Porquê Shared Trees?**
  - ✓ Para que os hosts e os routers possam conhecer a source do grupo de multicast.
- **E se a source fosse conhecida à priori?**
  - ✓ Os hosts podem utilizar IGMPv3 para fazer join a um grupo (S,G) específico (alternativa IGMPv2+SSM Mapping).
  - ✓ As árvores de distribuição Shared Trees e os RPs não são mais necessários.
  - ✓ Sources distintas podem utilizar o mesmo grupo sem conflito.



# Protocolos de Routing de Multicast: SSM

## Source-Specific Multicast (SSM)

- **Elimina complexidade na implementação de Multicast**
  - ✓ Possibilita o uso do caminho mais “curto” (melhor métrica) para a source sem a necessidade de criação prévia de Shared Trees.
  - ✓ Não necessita de Shared Trees = Não necessita de RP.
  - ✓ Simplifica a gestão de endereçamento pela eliminação da Shared Trees e utilização de sources únicas.
- **Impossibilita tráfego de sources ilegais/inválidas**
- **Ideal para aplicações “One-to-Many”**
  - ✓ Video/Audio (Palestras, Apresentações, TV, Rádio).
  - ✓ Push Media (Canais de notícias, Informação meteorológica).
  - ✓ Distribuição de informação (Distribuição de conteúdos de sites Web).

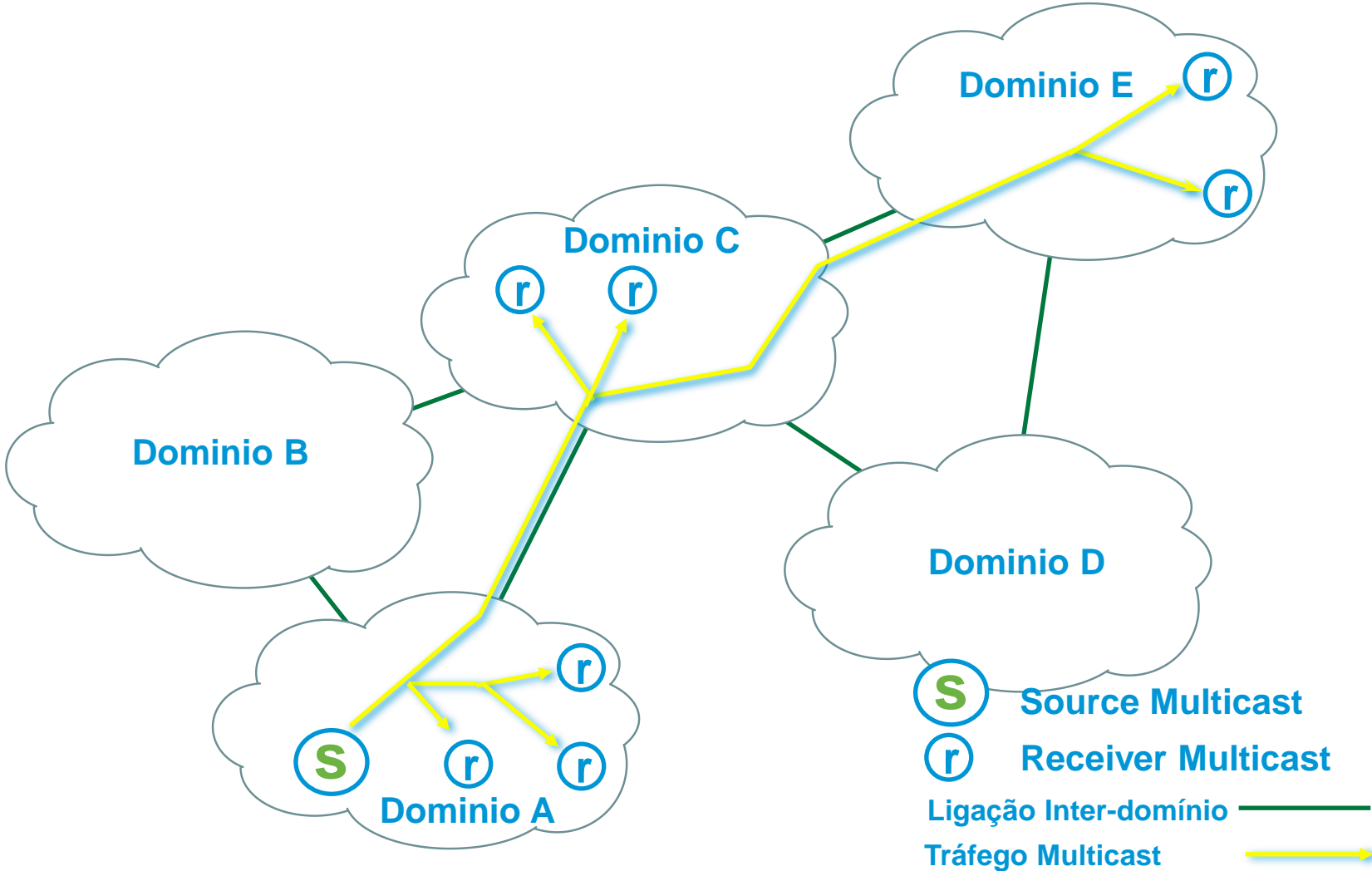
# Protocolos de Routing de Multicast: SSM

## Source-Specific Multicast (SSM)

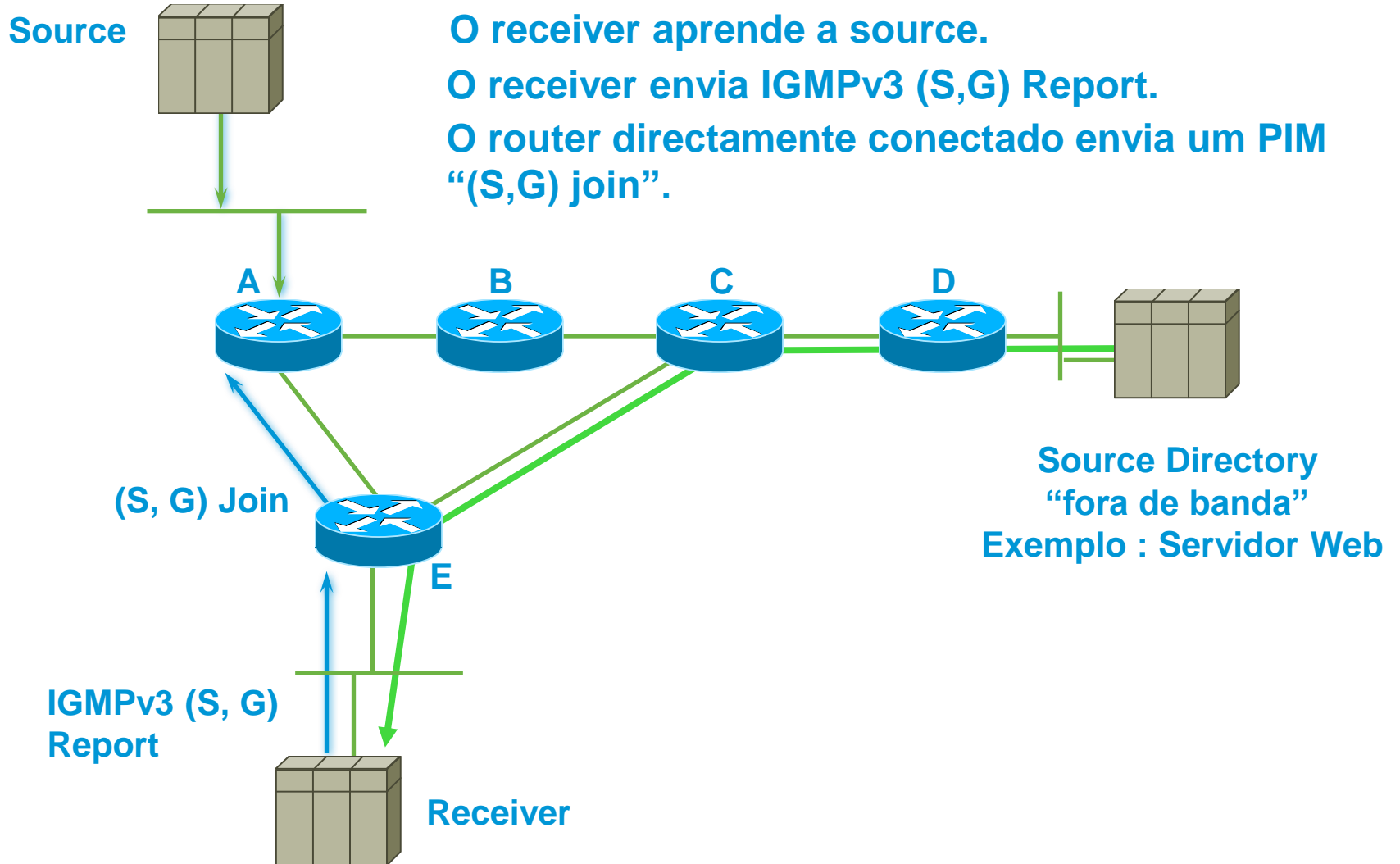
- **SSM pode funcionar na presença de sources/grupos que utilizem shared trees, no entanto:**
  - ✓ Não há controlo de sources no ambiente “shared”.
  - ✓ Não há um mecanismo que evite colisões grupos.
- **O range 232/8 foi reservado para grupos SSM**
  - ✓ Shared Trees não são permitidos neste range.

# Protocolos de Routing de Multicast: SSM

## Source-Specific Multicast (SSM)

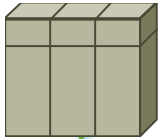


# Protocolos de Routing de Multicast: SSM

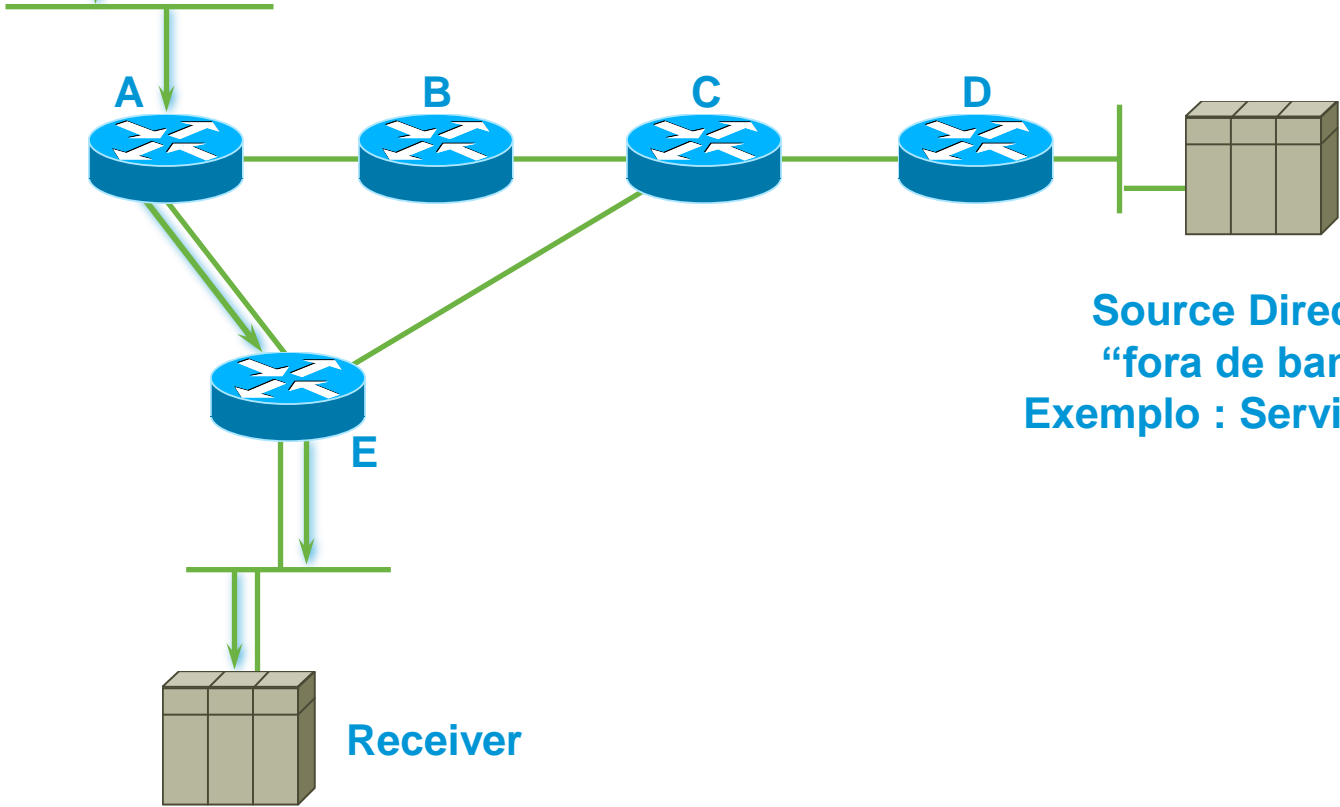


# Protocolos de Routing de Multicast: SSM

Source



Resultado: É construída uma “Shortest Path Tree” sem necessidade de criar uma Shared Tree.



Source Directory  
“fora de banda”  
Exemplo : Servidor Web

Receiver

# Protocolos de Routing de Multicast: SSM

## Sumário

- **Ideal para aplicações com uma source enviando para múltiplos receivers**
- **Resolve problemas de assignação de endereços de multicast**
  - ✓ **Diferenciação por source e grupo.**
  - ✓ **Podem ser reutilizados os endereços de grupo.**

Cada par (S,G) é único, i.e. corresponde a um fluxo único
- **Permite prevenir certos ataques DoS**
  - ✓ **Tráfego “inválido” de sources.**

Não ocupa largura de banda na rede e não é recebido pelo receiver

# Protocolos de Routing de Multicast: BiDir

## Modelos aplicativos “Many-to-Many”

- **Elevado número de estados (S,G)**
  - ✓ O volume da informação de estados (S,G) que é necessário manter aumenta significativamente.
  - ✓ Impacta negativamente o desempenho dos routers e será proporcional ao número de interfaces nas OILs.
- **Usando apenas Shared-Trees (sem *STP-Switchover*)**
  - ✓ Permite diminuir alguns estados (S,G).
  - ✓ Apenas necessária a manutenção dos estados (S,G) via Source Tree em direcção ao RP.
  - ✓ De qualquer modo o número de estados (S,G) pode potencialmente ser muito elevado.

**A solução passa por utilizar apenas estados (\*,G)!**

# Protocolos de Routing de Multicast: BiDir

## Eliminando o estado (S,G)

- **Shared-Trees Bidireccionais**

- ✓ **Permitem que o tráfego seja distribuído utilizando somente Shared Trees.**
  - ✓ O tráfego gerado pela source utiliza uma Shared Tree para chegar ao RP e a todos os receivers.
  - ✓ Utiliza a mesma árvore de distribuição das sources ao RP e do RP aos receivers.
  - ✓ Não é possível de implementar com as actuais regras de RPF para (\*,G).
  - ✓ Tem de haver uma atenção especial para evitar loops de Multicast.
- ✓ **Necessita de um “Designated Forwarder“ (DF).**
  - ✓ Responsável por enviar o tráfego via a Shared Tree.
  - ✓ O DF aceita receber tráfego nas interfaces presents na OIL list.
  - ✓ O tráfego será posteriormente enviado em todas as suas interfaces (incluindo IIF).
- ✓ **Resulta num menor número de estados nos routers – Só (\*,G)!**



# Protocolos de Routing de Multicast: BiDir

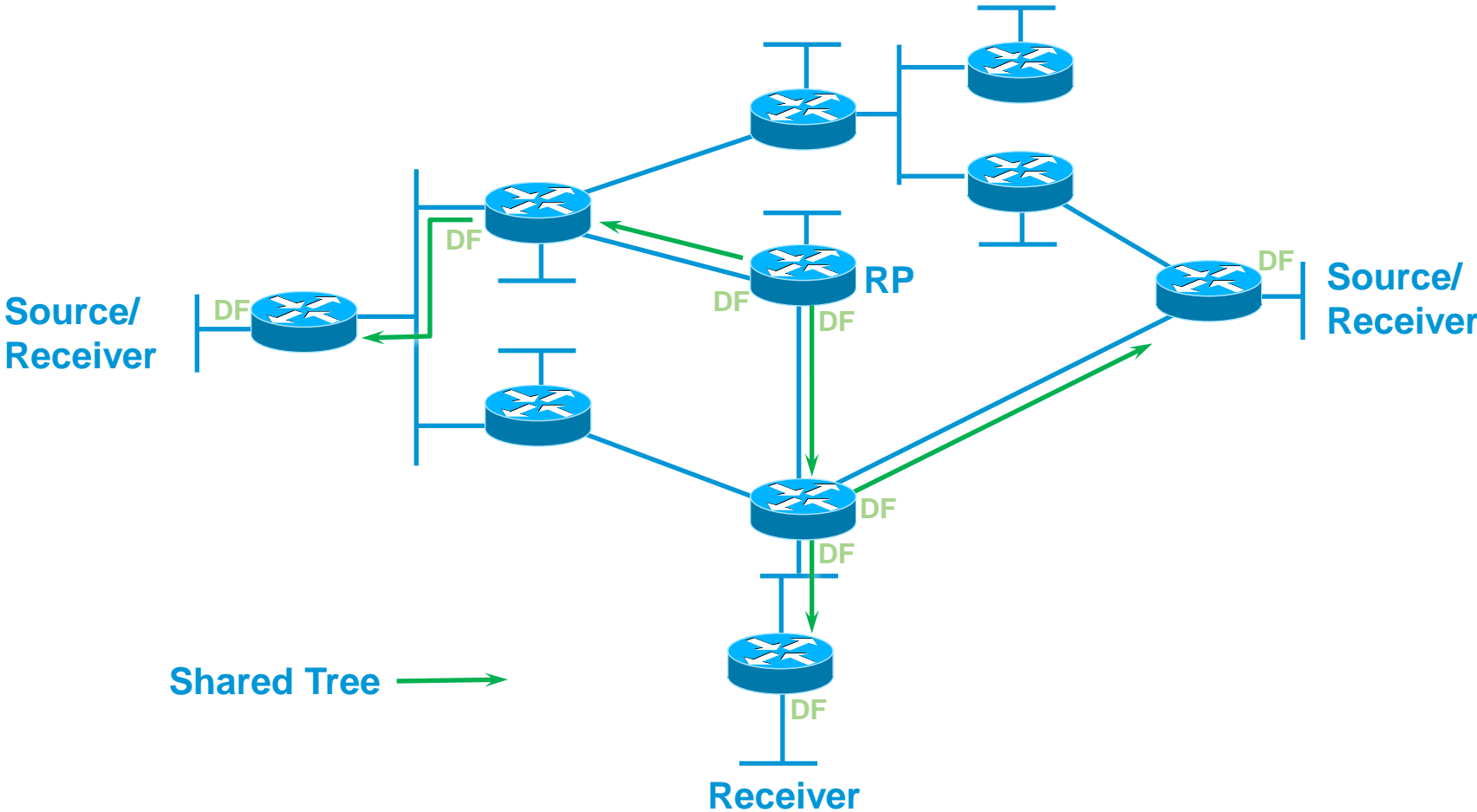
## Alterações de PIM para a implementação de BiDir

- **Designated Forwarders (DF)**

- ✓ Em cada segmento o router com a melhor rota com destino ao RP é eleito como DF.
- ✓ Existe apenas um DF por segmento/LAN.
  - ✓ O DF é o responsável por transmitir o tráfego upstream (com origem nas sources) em direcção ao RP.
  - ✓ O DF é o responsável por transmitir o tráfego downstream (com “destino” aos receivers).
  - ✓ O DF é o responsável por gerar os PIM Joins para os receivers directamente ligados.
    - Para grupos BiDir não existe Designated Router (DR).
- ✓ A existência de um único DF previne a criação de loops.
- ✓ Não existe tratamento especial para as sources locais.

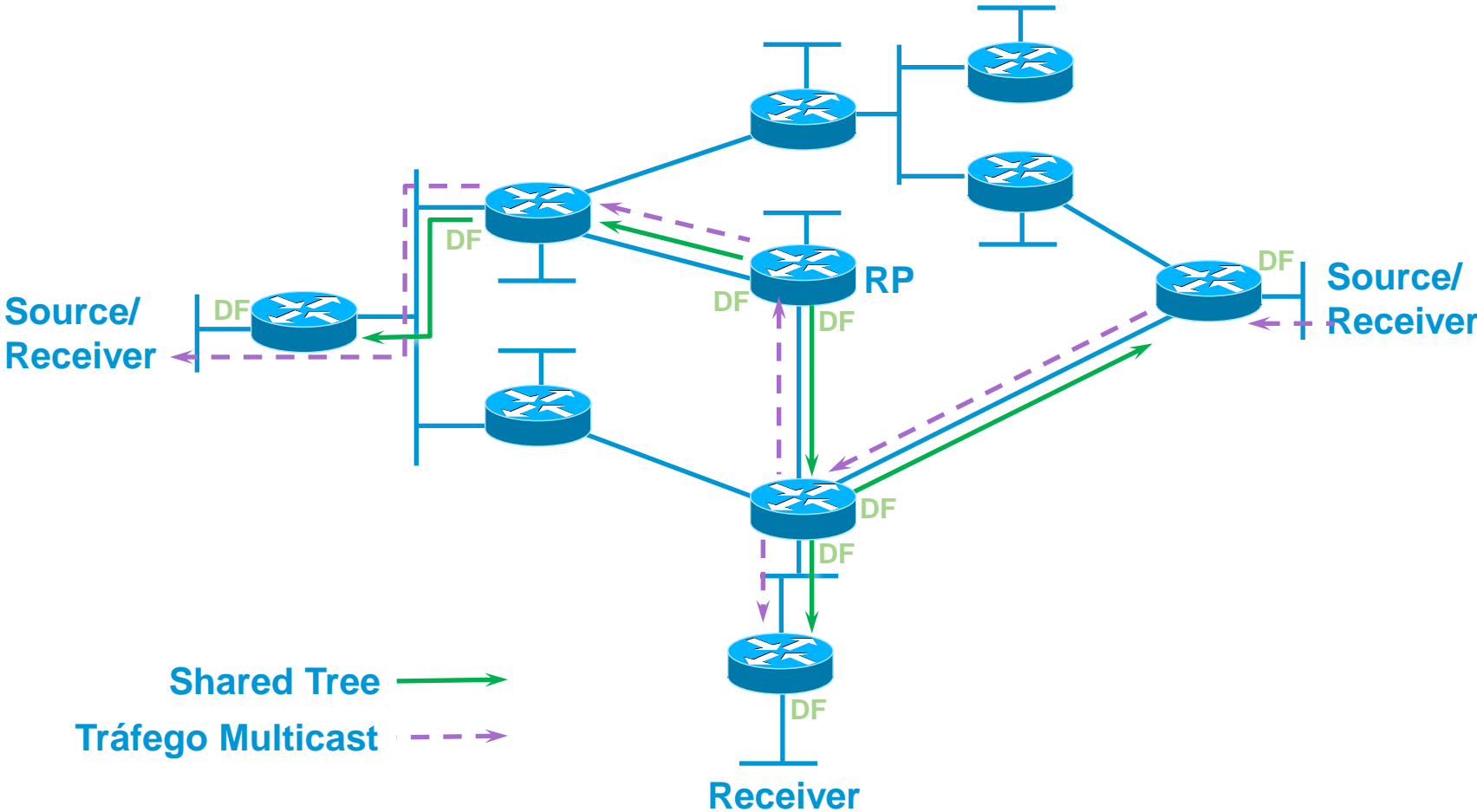
# Protocolos de Routing de Multicast: BiDir

## *BiDirectional PIM Overview*



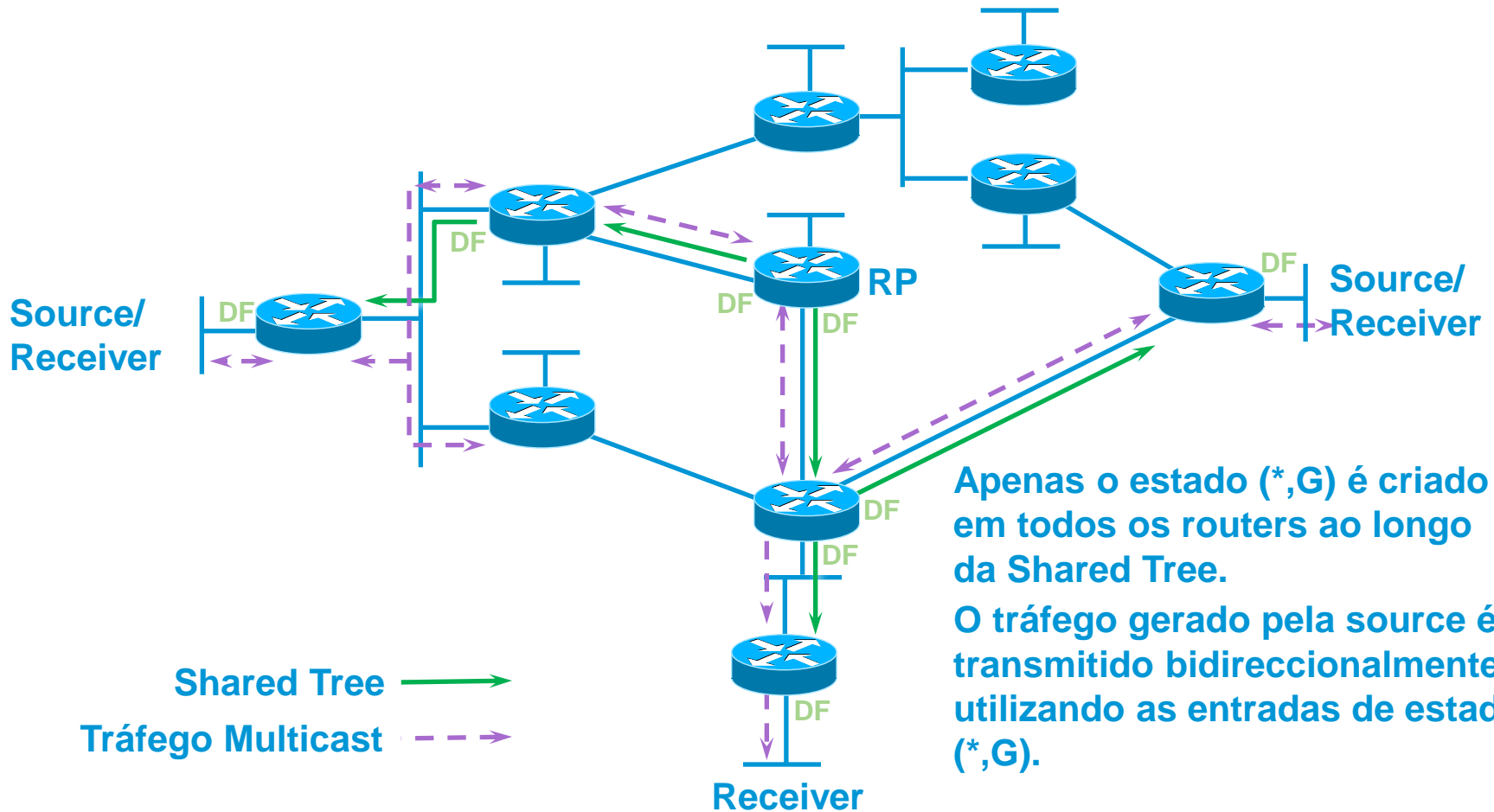
# Protocolos de Routing de Multicast: BiDir

## *BiDirectional PIM Overview*



# Protocolos de Routing de Multicast: BiDir

## *BiDirectional PIM Overview*



Apenas o estado  $(*,G)$  é criado em todos os routers ao longo da Shared Tree.

O tráfego gerado pela source é transmitido bidireccionalmente utilizando as entradas de estado  $(*,G)$ .

# Protocolos de Routing de Multicast: BiDir

## Sumário

- **Ideal para aplicações “Many-to-Many”**
  - ✓ **Permite virtualmente um número ilimitado de sources.**
    - Conferências (Audio/Video, whiteboards)
    - Partilha de recursos (Bases de dados distribuídas e síncronas)
    - Gaming (simuladores multi-player interactivos)
- **Usa apenas Shared Trees**
  - ✓ **Um único estado (\*,G) por grupo**
    - Tráfego flui bidireccionalmente (Up/Down) na Shared Tree
- **Redução drástica do número de estados na mroute**
  - ✓ **Elimina TODOS os estados (S,G) – Não existem SPTs!**

# IP Multicast – Fundamentos: Resumo

- Multicast usa o conceito de grupos.
- O endereçamento IP de Multicast é de 224.0.0.0 a 239.255.255.255 – “Classe D”.
- O MAC Address do tráfego de Multicast tem um início fixo (24 bits): 01-00-5E.
- Existe uma sobreposição de 32:1 no mapeamento entre Endereço IP de Multicast e MAC Address de Multicast.
- IGMP é o protocolo que os receivers utilizam para sinalizar aos routers que querem “escutar” um determinado grupo.
- IGMP snooping permite aos switches terem visibilidade dos receivers vs. grupos na LAN e conter o domínio de flood.
- Árvores de distribuição de Multicast: Source e Shared.

# IP Multicast – Fundamentos: Resumo

- O Forwarding de Multicast tem por base RPF.
- PIM é o protocolo de routing de Multicast e pode ser utilizado num modelo de “Push” – Dense Mode – ou num modelo de “Pull” – Sparse Mode.
- Em PIM-SM o RP permite o mapeamento entre as Source Trees e as Shared Trees.
- A configuração do RP pode ser estática ou dinâmica (Auto-RP e BSR). É possível implementar redundância.
- No modelo SSM não é necessário RP já que a source é conhecida à priori (IGMPv3 ou IGMPv2+SSM Mapping). É a melhor opção para cenários “One-to-Many”. Apenas usa Source Path Trees.
- BiDir-PIM permite escalar em cenários “Many-to-Many”. Apenas usa Shared Trees.

Muito Obrigado!





# Envie sua pergunta agora!

Use o painel Q&A para enviar suas perguntas, os especialistas irão responder ao vivo!

# Evento Pergunte aos Especialistas com Ricardo Lourenço

**Se você quiser tirar mais dúvidas com o nosso especialista, ele estará respondendo a perguntas entre os dias 07 e 16 de Maio, neste link:**

<https://supportforums.cisco.com/pt/community/3746/ask-the-expert>

**O vídeo, a apresentação e as perguntas e respostas serão disponibilizados até a terça-feira da semana que vem no link:**

<https://supportforums.cisco.com/pt/community/2601/webcasts>

# Qualifique o conteúdo da Cisco Support Community em Português

As estrelas dadas aos Documentos, Blogs e Vídeos agora valem pontos!



Incentive os participantes da Comunidade avaliando o conteúdo postado por eles.

[Saiba mais](#)

**Agora é possível qualificar discussões, documentos, blogs e vídeos!!!**

# Spotlight Awards (Prêmio Participantes em Destaque)



- O prêmio “participantes em destaque” foi criado em 2012 na comunidade global da Cisco e é usado para reconhecer àqueles membros que dão um contribuição significativa para a comunidade de suporte da Cisco e que além de tudo exercem um papel de liderança dentro da comunidade em distintas categorias
- Foi lançado na comunidade em português, em 1 de dezembro de 2013 e conta com a categoria “O Novato”.
- Mais detalhes sobre o prêmio, podem ser consultados no link: [https://supportforums.cisco.com/pt/community/11990816/participantes\\_em\\_destaque](https://supportforums.cisco.com/pt/community/11990816/participantes_em_destaque)

# Convidamos você a participar da CSC em português e em nossas redes sociais

<https://supportforums.cisco.com/community/5141/comunidade-de-suporte-cisco-em-portugues>



Portugal: <http://www.facebook.com/ciscoportugal>

Brasil: <http://www.facebook.com/CiscoDoBrasil>



Portugal: <https://twitter.com/CiscoPortugal>

Brasil: <http://twitter.com/CiscoDoBrasil>



Portugal: <http://www.youtube.com/user/ciscoportugal>

Brasil: <http://www.youtube.com/user/ciscoDoBrasilTV>



Portugal: <http://ciscoportugalblog.wordpress.com/>

**Muito Obrigado  
por assistir.**

Por favor complete o formulário de avaliação e dê sugestões de temas para os próximos webcasts!