

Reconstruindo as entradas multicast com CGMP e alterações na topologia de árvore de abrangência

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Alterações de CGMP e de topologia](#)

[Estado estável](#)

[Durante e após a mudança de topologia](#)

[Duas consultas gerais de IGMP após a notificação de alteração de topologia](#)

[Melhorias de CGMP](#)

[Comunicação entre o Switch e o roteador](#)

[Comportamento do roteador](#)

[Comportamento do Switch Catalyst](#)

[Informações Relacionadas](#)

[Introduction](#)

Este documento discute como o Cisco Group Management Protocol (CGMP) trabalha nos switches Cisco Catalyst e nos roteadores Cisco IOS® em relação à reconstrução das entradas multicast para CGMP depois de uma alteração na topologia da spanning tree.

[Prerequisites](#)

[Requirements](#)

A Cisco recomenda que você conheça estes tópicos:

- basic operation of switches, routers, and multicasting
- operação básica do spanning tree, CGMP e Internet Group Management Protocol (IGMP)

[Componentes Utilizados](#)

As informações neste documento são baseadas nestas versões de software e hardware:

- Catalyst 3550 versão 12.1(9)EA1c
- Catalyst 2900/3500XL versão 12.0(5)WC3b
- Catalyst 4000 Supervisor Engine III versão 12.1(11b)EW
- Catalyst 4000 Supervisor Engine I/II versão 7.2(2)
- Catalyst 6500 Supervisor Engine Cisco IOS Software Release 12.1(11b)EX
- Catalyst 6500 Catalyst OS (CatOS) versão 7.2(2)
- Catalyst 5500 CatOS versão 4.5(13a)

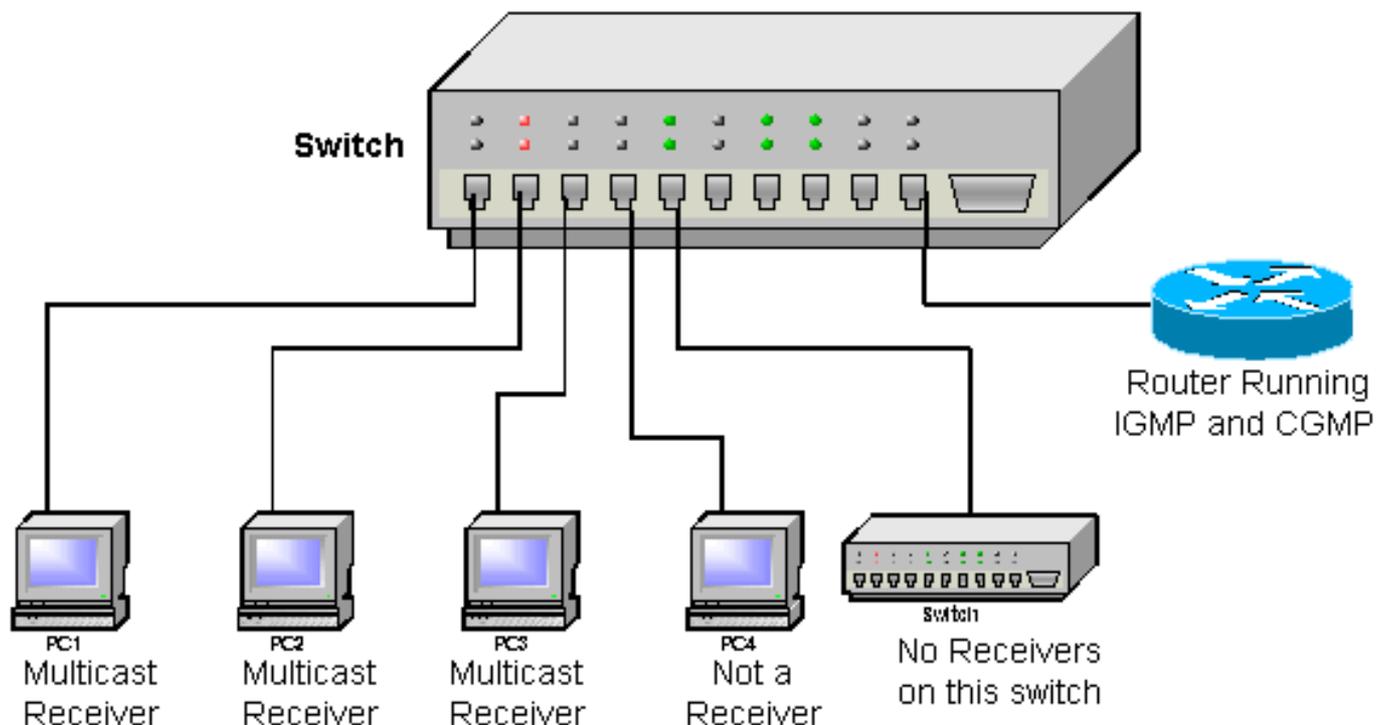
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Consulte as [Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.](#)

Alterações de CGMP e de topologia

Esta seção descreve passo a passo o que ocorre e quais problemas podem surgir quando uma alteração na topologia de spanning tree é detectada em uma VLAN onde o CGMP é usado para conter o tráfego multicast de inundação em todas as portas. Como mostra este exemplo, a rede discutida neste documento consiste em um roteador, um switch e quatro PCs:



- porta 1—receptor PC 1
- porta 2—receptor PC 2
- porta 3—receptor PC 3
- porta 4—não um receptor PC 4
- porta 5 — outro switch (sem receptores ou roteadores neste switch)
- port 48 — Cisco IOS Router executando IGMP e CGMP

Para o propósito deste documento, supõe-se que os PCs receptores usem IGMP e que o switch

execute CGMP. O roteador Cisco IOS executa IGMP e CGMP, que recebe um fluxo multicast de um servidor de vídeo em uma interface diferente. Essa interface envia ao grupo multicast IP 239.100.100.100.

Estado estável

Quando todos os dispositivos são inicializados e os PCs receptores enviam suas mensagens de junção IGMP para o grupo 239.100.100.100, todos eles são adicionados pelo CGMP ao grupo correspondente da camada 2 representado pelo endereço MAC 01-00-5e-64-64-64.

Essa lista mostra quais portas, destacadas em negrito, no switch recebem o fluxo multicast que passa pelo roteador Cisco IOS.

- **porta 1**—receptor PC 1
- **porta 2**—receptor PC 2
- **porta 3**—receptor PC 3
- porta 4—não um receptor PC 4
- porta 5 — outro switch (sem receptores ou roteadores neste switch)
- porta 48—roteador Cisco IOS que executa IGMP e CGMP

Observação: o roteador Cisco IOS também é adicionado ao grupo multicast, mas como é a origem, ele não recebe seus próprios pacotes.

Em cada intervalo de consulta, o roteador Cisco IOS envia uma consulta geral de IGMP (que é enviada para o grupo de multicast 224.0.0.1 e, portanto, inundada para todos os outros componentes). Quando isso acontece, todos os receptores começam a criar um relatório IGMP para o grupo 239.100.100.100. Os receptores enviam esse relatório de volta para o grupo multicast IP 239.100.100.100, com um endereço MAC de Camada 2 de 01-00-5E-64-64-64. Como isso é enviado para o endereço do grupo, todos os receptores recebem os relatórios enviados por outros receptores, bem como o relatório enviado de volta pelo primeiro receptor. Isso ativa os outros PCs receptores para cancelarem seu relatório para esse grupo. Isso significa que apenas uma mensagem de junção CGMP é enviada para esse grupo como o endereço MAC de origem do PC que foi o primeiro a responder. Isso continua por um longo período, e todos os PCs receptores recebem a transmissão de vídeo.

Durante e após a mudança de topologia

Neste ponto, o outro switch aciona uma alteração de topologia na rede. De acordo com a especificação CGMP ao receber a alteração de topologia, o switch limpa todas as entradas de multicast que aprendeu através do CGMP. O tráfego multicast do roteador é inundado para todas as portas no switch.

Esta lista mostra quais portas, destacadas em negrito, no switch recebem o fluxo multicast que passa pelo roteador Cisco IOS:

- **porta 1**—receptor PC 1
- **porta 2**—receptor PC 2
- **porta 3**—receptor PC 3
- porta 4—não um receptor PC 4
- porta 5 — outro switch (sem receptores ou roteadores neste switch)
- porta 48—roteador Cisco IOS que executa IGMP e CGMP

À medida que o tráfego é inundado para todas as portas, os PCs receptores não notam nenhuma diferença e continuam a receber o broadcast de vídeo. No entanto, como o tráfego é inundado para todas as portas, o PC 4, que não é um receptor, e o outro switch agora também recebe o fluxo multicast, embora não o tenha solicitado. Isso continua até que o Cisco IOS Router envie sua consulta geral de IGMP periódica novamente. O valor padrão para isto é 60 segundos nos roteadores Cisco IOS (configurados com um intervalo de consulta IGMP IP).

Duas consultas gerais de IGMP após a notificação de alteração de topologia

Quando o roteador Cisco IOS envia sua primeira consulta geral de IGMP, todos os PCs receptores começam a criar seu relatório de IGMP para o grupo 239.100.100.100. Uma delas (neste documento, é PC 3) é a primeira a retornar seu relatório IGMP. Since there is no multicast entry built on the Switch yet, it is received by all PCs, and the other receiver PCs cancel their IGMP report. O roteador Cisco IOS recebe o relatório e envia a mensagem de junção CGMP subsequente com o endereço de origem do PC 3 receptor.

O Switch constrói novamente uma entrada multicast para o grupo 01-00-5e-64-64-64 e adiciona a porta 3, pois este é o endereço de origem no pacote de conexão CGMP. Como a porta 5 é a porta do roteador de transmissão múltipla, isso também é adicionado ao grupo de transmissão múltipla. Por isso, somente o receptor PC 3 recebe o fluxo de vídeo, enquanto o fluxo de vídeo em PC1 e PC2 permanece sem alterações.

Esta lista mostra quais portas, destacadas em negrito, no switch recebem o fluxo multicast que passa pelo roteador Cisco IOS:

- porta 1—receptor PC 1
- porta 2—receptor PC 2
- **porta 3—receptor PC 3**
- porta 4—não um receptor PC 4
- porta 5 — outro switch (sem receptores ou roteadores neste switch)
- port 48 — Cisco IOS Router executando IGMP e CGMP

No final de um intervalo de consulta IGMP, o roteador Cisco IOS envia outra consulta geral IGMP. Ao receberem a consulta, todos os PCs receptores criam um relatório para o grupo 239.100.100.100. Desta vez, no entanto, os relatórios dos outros PCs são recebidos somente pelo receptor PC 3 e pelo roteador Cisco IOS. (A porta do roteador é adicionada automaticamente a cada grupo de multicast.)

Como os receptores PC 1 e PC 2 não vêm um relatório de nenhum outro receptor, ambos enviam seus relatórios. Subseqüentemente, o Cisco IOS Router envia uma mensagem de ligação CGMP com o MAC Address de origem dos respectivos computadores e, portanto, eles são adicionados e começam a receber novamente o fluxo pelo Cisco IOS Router.

Esta lista mostra quais portas, destacadas em negrito, no switch recebem o fluxo multicast que passa pelo roteador Cisco IOS:

- **porta 1—receptor PC 1**
- **porta 2—receptor PC 2**
- **porta 3—receptor PC 3**
- porta 4—não um receptor PC 4
- porta 5 — outro switch (sem receptores ou roteadores neste switch)
- port 48 — Cisco IOS Router executando IGMP e CGMP

A configuração está de volta ao estado estável original e tudo funciona corretamente novamente. Esta é uma discriminação do que ocorreu:

1. Ocorre uma alteração na topologia. **Dica:** quando o portfast não está habilitado em uma porta de host, toda vez que um host é reinicializado ou conectado/desconectado da porta/da porta, uma alteração no status dos links aciona uma notificação de alteração de topologia na VLAN. Se a depuração do CGMP estiver ativada no momento da alteração de topologia, esta mensagem de depuração será exibida:
`CGMP SHIM: got short age timer`
2. A inundação começa em todas as portas.
3. A primeira consulta geral de IGMP é enviada.
4. A inundação para.
5. Nem todos os receptores recebem o fluxo multicast.
6. A segunda consulta geral do IGMP é enviada.
7. Todos os receptores são adicionados e recebem o fluxo multicast novamente.

Melhorias de CGMP

Como não é sempre aceitável ter uma perda de um minuto (o intervalo de consulta IGMP padrão) de um fluxo de multicast para um PC, houve algumas melhorias feitas para os roteadores e switches que executam o CGMP.

Comunicação entre o Switch e o roteador

Como os roteadores são dispositivos da Camada 3 e, portanto, geralmente não sabem sobre alterações de spanning tree e topologia que ocorrem, há uma necessidade de os switches na rede alertarem o roteador sobre essa alteração de topologia. Uma mensagem de licença global IGMP é definida para lidar com isso.

Essa mensagem de licença do IGMP pode ser transmitida por um Switch e contém uma solicitação para deixar o grupo 0.0.0.0.

Para garantir que o roteador não esteja sobrecarregado com mensagens de saída global IGMP, somente o switch raiz em um domínio spanning tree é responsável por enviar essa mensagem de licença global IGMP quando a alteração de topologia terminar.

Comportamento do roteador

Quando o roteador recebe essa mensagem de licença global de IGMP em uma interface que executa o Cisco IOS Software, ele reconhece que ocorreu uma alteração na topologia de spanning tree nessa interface e toma estas ações para tentar limitar a perda de tráfego multicast para os receptores multicast:

1. Envia mensagens CGMP de junção em lote após receber a mensagem IGMP de licença global. O roteador envia uma mensagem de junção CGMP com seu próprio endereço MAC como o endereço de origem do usuário para cada grupo de multicast que tem em seu cache IGMP para essa interface. Ao enviar essas mensagens de autoingresso CGMP, os switches CGMP criam automaticamente uma entrada para cada grupo com apenas a porta do roteador. Esta lista mostra a rede usada neste documento, após a união de lote CGMP.

Somente o roteador Cisco IOS foi adicionado ao grupo multicast, como mostrado em negrito. **Observação:** enquanto em exemplos anteriores neste documento, as portas que recebem tráfego do roteador multicast foram mostradas em negrito, este exemplo mostra todas as portas adicionadas no switch ao grupo multicast. porta 1—receptor PC 1 porta 2—receptor PC 2 porta 3—receptor PC 3 porta 4—não um receptor PC 4 porta 5 — outro switch (sem receptores ou roteadores neste switch) **port 48 — Cisco IOS Router executando IGMP e CGMP**

2. Envia uma consulta geral de IGMP. Todos os receptores recebem essa consulta geral de IGMP e criam um relatório para cada grupo ao qual se juntaram. Como o Switch CGMP já criou uma entrada de multicast para cada um dos grupos com apenas o roteador como receptor, todos os relatórios estão sendo enviados apenas para o roteador. O roteador envia mensagens de união CGMP subsequentes para adicionar todos os receptores aos grupos correspondentes. Depois que todos os receptores enviarem seu relatório de IGMP e o roteador tiver enviado as mensagens de junção de CGMP correspondentes, todos os receptores devem ter sido adicionados de volta ao grupo de multicast.
3. Após 10 segundos (tempo de resposta máxima de IGMP padrão), outra consulta geral de IGMP é enviada para garantir que todos os receptores sejam adicionados. Esta etapa se repete algumas vezes para verificar se todos os receptores voltaram a se juntar no grupo de transmissão múltipla. Todas as portas que deveriam ter sido adicionadas ao grupo multicast foram, como mostrado em negrito neste exemplo: **porta 1—receptor PC 1 porta 2—receptor PC 2 porta 3—receptor PC 3 porta 4—não um receptor PC 4 porta 5 — outro switch (sem receptores ou roteadores neste switch) port 48 — Cisco IOS Router executando IGMP e CGMP**

[Comportamento do Switch Catalyst](#)

Dentro do intervalo de Switches Catalyst, há algumas diferenças em seu comportamento. Cada switch que é compatível com CGMP faz como descrito na seção [Alterações de CGMP e Topologia](#) deste documento. As melhorias para CGMP, entretanto, não são implementadas em todas as plataformas. Esta tabela fornece uma lista de Switches Catalyst e como eles reagem ao CGP:

	Switch CGMP	Rot ead or CGMP	Sends Global Leave When Spanning Tree Protocol (STP) Root
Catalyst 6500 executando o Cisco IOS Software	N	Y	Y
Catalyst 6500 executando CatOS	N	N	N
Catalyst 5500, Catalyst 2926/2926G	Y	N	Y
Catalyst 4000 Supervisor Engine I/II, Catalyst 2948G/2980G, Catalyst 4912G	Y	N	Y

Catalyst 4000/4500 Supervisor Engine III/IV	N	Y	Y
Catalyst 2900XL/3500XL	Y	N	Y
Catalyst 2940	N	N	N
Catalyst 2950	N	N	N
Catalyst 2970	N	N	N
Catalyst 3550	N	Y	Y
Catalyst 3750	N	Y	Y

Observação: no Catalyst 4000/4500 com um Supervisor Engine III/IV, o comportamento em relação às alterações de topologia e CGMP é configurável. Emita este comando para configurar o Catalyst 4000 para enviar ou não uma mensagem de licença global IGMP quando não for a raiz do spanning tree:

- ip igmp snooping tcn query solicit

Observação: emita este formulário "no" do comando para desativá-lo:

- no ip igmp snooping tcn query solicit

[Informações Relacionadas](#)

- [Entendendo as alterações de topologia de protocolo de árvore de abrangência](#)
- [Multicast em uma rede do campus: Espionagem de CGMP e IGMP](#)
- [Restringindo o tráfego de transmissão múltipla com origem e receptores na mesma VLAN nos Switches Catalyst executando o Catalyst OS](#)
- [Guia de configuração para o software Cisco IOS Catalyst 4000: Understanding and Configuring IGMP Snooping \(Compreendendo e configurando a espionagem de EGMP\)](#)
- [Página de suporte técnico de árvore de abrangência](#)
- [Páginas de Suporte de Produtos de LAN](#)
- [Página de suporte da switching de LAN](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)