Multicast em uma rede do campus: Espionagem de CGMP e IGMP

Contents

Introduction

A finalidade da espionagem do Cisco Group Management Protocol (CGMP) e do Internet Group Management Protocol (IGMP) é restringir o tráfego multicast em uma rede comutada. Por padrão,

um switch LAN inunda tráfego multicast no domínio de broadcast, e isso poderá consumir muita largura de banda se muitos servidores de multicast enviarem fluxos para o segmento.

Antes de Começar

Conventions

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Prerequisites

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

Informações de Apoio

O tráfego multicast é inundado porque um switch geralmente aprende endereços MAC ao olhar o campo de endereço de origem de todos os quadros que recebe. Um endereço MAC de multicast nunca é usado como o endereço de origem de um pacote. Tais endereços não aparecem na tabela de endereços MAC, e o switch não tem nenhum método para aprendê-los.

A primeira solução para esse problema é configurar os endereços MAC estáticos de cada grupo e cliente. Essa solução funciona bem, mas não é escalável nem dinâmica. Você pode usas essa solução em um Catalyst 4000, 5000 ou 6000 Switch ao executar um dos seguintes comandos:

- **set cam static**
- **set cam permanent**

Esses dois comandos têm o mesmo efeito, exceto que as entradas estáticas desaparecem na reinicialização e as entradas permanentes não.

A segunda solução é utilizar CGMP, que é um protocolo proprietário da Cisco executado entre o roteador de transmissão múltipla e o Switch. O CGMP permite que o roteador multicast da Cisco compreenda as mensagens de IGMP enviadas pelos hosts e notifique o switch sobre as informações contidas no pacote de IGMP.

A última (e mais eficiente) solução é usar a espionagem de IGMP. Com a espionagem de IGMP, o switch intercepta mensagens de IGMP do host em si e atualiza sua tabela de MAC de acordo. Para dar suporte a espionagem do IGMP é necessário hardware avançado.

As configurações de CGMP mostradas neste documento destinam-se aos Catalyst 4000 e 5000 Switches com CatOS (o CGMP não é aceito em Catalyst 6000 Switches). As configurações de espionagem de IGMP aplicam-se aos Catalyst 5000 e 6000 Switches com CatOS.

A seção a seguir descreve brevemente um endereço de multicast, explica a funcionalidade do IGMP e fornece detalhes adicionais sobre a espionagem de CGMP e de IGMP.

Endereço de Multicast

1. Os endereços IP de multicast são endereços IP da Classe D. Portanto, todos os endereço de IP de 224.0.0.0 até 239.255.255.255 são de multicast. Eles também são conhecidos como Endereços de Destino de Grupo (GDA).
2. Há um endereço MAC associado a cada GDA. Esse endereço MAC é formado por 01-00-5e, seguido pelos últimos 23 bits do GDA convertidos em hexadecimal, como mostrado a seguir.239.20.20.20 corresponde ao MAC 01-00-5e-14-14-14.239.10.10.10 corresponde ao MAC 01-00-5e-0a-0a-0a.Consequentemente, esse é um não mapeamento um a um, mas um mapeamento de um para muitos. Desses dois endereços, você pode ver que o primeiro octeto (239) não é usado no endereço MAC. Assim, os endereços de multicast com os mesmos três últimos octetos, mas com o primeiro octeto diferente, possuem endereços MAC sobrepostos.
3. Alguns endereços IP multicast são reservados para uso especial, como mostrado abaixo.224.0.0.1 – Todos os hosts habilitados para multicast.224.0.0.2 - Todos os roteadores habilitados para multicast.O 224.0.0.5 e o 224.0.0.6 são usados pelo OSPF (Open Shortest Path First).

Geralmente, os endereços de 224.0.0.1 a 224.0.0.255 são reservados e usados por vários protocolos (padrão ou de proprietário, como o protocolo de Hot Standby Router Protocol [HSRP]). A Cisco recomenda usá-los para GDA em uma rede de multicast. A espionagem de CGMP e IGMP não funciona com essa faixa de endereços reservados.

Internet Group Management Protocol

O IGMP é um padrão definido em RFC1112 para IGMPv1, em RFC2236 para IGMPv2 e em RFC3376 para IGMPv3. O IGMP especifica como um host pode se registrar em um roteador a fim de receber tráfego multicast específico. A próxima seção fornece uma visão geral resumida do IGMP.

IGMPv1

As mensagens do IGMP Versão 1 (IGMPv1) são transmitidas em datagramas IP e contêm os seguintes campos:

- Versão: 1
- Digite: Há dois tipos de mensagens de IGMP: Consulta de Associação e Relatório de Associação.
- Checksum
- GDA

Os relatórios de associação são emitidos pelos hosts que desejam receber um grupo de multicast específico (GDA). As consultas de associação são emitidas pelos roteadores em intervalos regulares para verificar se ainda há um host interessado no GDA daquele segmento.

Os relatórios de associação de hosts são emitidos de forma não solicitada (quando o host deseja receber o tráfego GDA primeiro) ou em resposta a uma consulta de associação. Eles são enviados com os seguintes campos:

- MAC de origem: Endereço MAC do host
- MAC de destino: MAC de destino para o GDA

Informações de L3

- IP de origem: Endereço IP do host
- IP de destino: GDA

Pacote de IGMP

- Os dados de IGMP contêm, além disso, os campos do GDA e alguns outros campos.

As consultas de associação do host são enviadas pelo roteador para o endereço somente multicast: 224.0.0.1. Essas consultas usam 0.0.0.0 no campo IGMP GDA. Um host para cada grupo deverá responder a essa consulta. Caso contrário, o roteador irá para de enviar o tráfego desse GDA para esse segmento (após três tentativas). O roteador mantém a entrada do roteamento de multicast para cada fonte e a vincula a uma lista de interfaces de saída (a interface de origem do relatório IGMP). Após três tentativas de consulta de IGMP sem resposta, essa interface é apagada da lista de interfaces de saída para todas as entradas vinculadas a esse GDA.

> **Note**: O IGMPv1 não possui nenhum mecanismo de saída. Se um host não deseja mais receber o tráfego, ele simplesmente sai. Se esse for o último host na sub-rede, o roteador não receberá qualquer tipo de resposta para a consulta e eliminará o GDA dessa sub-rede.

IGMPv2

No IGMP Versão 2 (IGMPv2), o campo de versão foi removido e o campo de tipo pode agora aceitar diferentes valores. Os tipos são mostrados abaixo.

- Consulta de associação
- Relatório de associação do IGMPv1
- Relatório de Associação da Versão 2
- Saída de Grupo

As descrições dos novos recursos mais importantes adicionados ao IGMPv2 estão listadas a seguir.

- Mensagem de IGMP Leave: quando um host quer sair de um grupo, ele deve enviar uma mensagem de saída de grupo do IGMP para o destino 224.0.0.2 (em vez de sair silenciosamente como no IGMPv1).
- Um roteador pode agora enviar uma consulta específica de grupo enviando uma Consulta de Associação ao grupo GDA em vez de enviá-la a 0.0.0.0.

IGMPv3

No IGMP Versão 3 (ICMPv3), há um tipo campo que pode ter os seguintes valores:

- Consulta de associação
- Relatório de Associação da Versão 3

Uma implementação do IGMPv3 *deve também oferecer suporte aos seguintes três tipos de mensagem para a interoperação com versões anteriores do IGMP:*

- Relatório de Associação da Versão 1 [RFC1112]
- Relatório de Associação da Versão 2 [RFC2236]
- Saída de Grupo da Versão 2 [RFC2236]

O IGMPv3 adiciona suporte à filtragem de origem, ou seja, a capacidade de um sistema relatar o interesse em receber pacotes de endereços de origem específicos ou de **todos, com exceção dos endereços de origem específicos enviados para um endereço de multicast específico.** Este recurso também é chamado Source Specific Multicast (SSM).

Para que um computador ofereça suporte ao SSM, ele deverá oferecer suporte ao IGMPv3. Relativamente poucos SO, no entanto, oferecem suporte ao IGMPv3. O Windows XP oferece suporte ao IGMPv3 e há patches de suporte ao IGMPv3 disponíveis para FreeBSD e Linux.

Os administradores devem distinguir entre o suporte ao IGMPv3 em nível de roteador e à espionagem de IGMPv3 em nível de switch. Eles são dois recursos diferentes.

Suporte ao IGMPv3 em Catalyst Switches (L2)

- O Catalyst 6000 que executa software de modo híbrido (CatOS no Supervisor e Cisco IOS® Software no MSFC) oferecem suporte oficialmente à espionagem de IGMPv3 a partir da versão 7.5(1).
- Nas versões anteriores à 7.5(1), o Catalyst 6000 Switch não possuía suporte oficial ao IGMPv3, mas deve ser capaz de lidar normalmente com os pacotes IGMPv3.
- Os Catalyst 6000 que executam IOS Software integrado oferecem suporte ao IGMPv3 em nível de roteador (interface L3) a partir da versão versão 12.1(8a)E.
- O Catalyst 4000 apenas oferece suporte ao IGMPv3 em nível de roteador no Supervisor III e IV. Ele não oferece suporte à espionagem de IGMPv3.

Suporte ao IGMPv3 em Cisco Routers (L3)

O IGMPv3 é aceito em todas as plataformas que executam o Cisco IOS® Software Release 12.1(5)T ou posterior.

Caveats

Quando um switch executa a espionagem de IGMP, ele intercepta os pacotes de IGMP e preenche a tabela de encaminhamento estática da camada 2 (L2) com base no conteúdo dos pacotes interceptados. Quando há hosts IGMPv1 ou v2 na rede, o switch lê as uniões e saídas do IGMP para determinar quais hosts querem receber qual fluxo de multicast ou parar de receber o fluxo de multicast.

O IGMPv3 é mais complicado, porque usa não somente o endereço de grupo (endereço de multicast), mas também as origens das quais o tráfego é esperado. Independentemente de o switch Catalyst 6000 executar o CatOS 7.5, ou versões posteriores, e a versão 12.1(8a)E nativa do IOS, ou versões posteriores, nenhum outro switch está habilitado a rastrear esses pacotes e criar uma tabela de encaminhamento com base nessas informações. Consequentemente, a espionagem de IGMP deve ser desligada quando há um host IGMPv3 no switch. Quando a espionagem de IGMP é desativada, o switch não pode construir dinamicamente uma tabela de

encaminhamento L2 para os fluxos de multicast. Ou seja, o switch inunda os fluxos de multicast.

Quando a espionagem de IGMP está desabilitada, uma solução é configurar manualmente as entradas CAM dinâmicas de multicast para evitar inundação da sub-rede com tráfego multicast. Esta é uma tarefa administrativa, porém não é uma solução dinâmica. Quando um cliente não quer mais receber o tráfego, a entrada de CAM não é removida do switch (a menos que por intervenção manual). Assim, o tráfego de rede ainda é endereçado para o host.

Além disso, quando o IGMPv3 é usado na rede, os switches que usam o CGMP funcionam normalmente, independentemente do fato do CGMP Fastleave não funcionar. Se o CGMP Fastleave for necessário, é melhor reverter para o IGMPv2.

As advertências pendentes específicas de plataforma podem ser encontradas nas notas de versão dos respectivos Switches.

Interoperabilidade entre IGMPv1 e IGMPv2

Com o IGMPv1 e o IGMPv2, apenas um roteador por sub-rede de IP envia consultas. Este roteador é denominado roteador de consulta. No IGMPv1, o roteador de consulta é escolhido com a ajuda do Multicast Routing Protocol. No IGMPv2, ele é escolhido pelo menor endereço IP entre os roteadores. Há várias possibilidades abaixo:

Cenário 1: Roteador IGMPv1 com uma Mistura de Hosts IGMPv1 e IGMPv2

O roteador não compreende o relatório de IGMPv2 e, portanto, todos os hosts devem usar apenas o relatório de IGMPv1.

Cenário 2: Roteador IGMPv2 com uma Mistura de Hosts IGMPv2 e IGMPv3

Os hosts IGMPv1 não compreendem a consulta IGMPv2 ou a pergunta de associação de grupo IGMPv2. O roteador deve usar somente o IGMPv1 e suspender a operação de saída.

Cenário 3: Roteador IGMPv1 e Roteador IGMPv2 Localizados no Mesmo Segmento

O roteador IGMPv1 não tem como detectar o roteador IGMPv2. Assim, o roteador IGMPv2 deve ser configurado pelo administrador como um roteador IGMPv1. Em todo caso, ele possível que eles não concordem sobre o roteador de consulta.

Interoperabilidade entre IGMPv1/IGMPv2 e IGMPv3

Com todas as versões do IGMP, somente um roteador por sub-rede de IP envia consultas. Este roteador é denominado roteador de consulta. No IGMPv1, o roteador de consulta é escolhido com a ajuda do Multicast Routing Protocol. No IGMPv2 e no IGMPv3, ele é escolhido pelo endereço IP mais baixo entre os roteadores. A seguir são mostradas várias opções de interoperabilidade.

Cenário 1: Roteador IGMPv1/IGMPv2 com uma Mistura de Hosts IGMPv1/IGMPv2 e IGMPv3

Como o roteador não compreende os relatórios IGMPv3, todos os hosts usam relatórios IGMPv1/IGMPv2.

Cenário 2: Roteador IGMPv3 com uma Mistura de Hosts IGMPv1/IGMPv2 e IGMPv3

Os hosts IGMPv1/IGMPv2 não compreendem a consulta IGMPv3 ou a consulta de associação IGMPv3. O roteador deverá usar apenas a versão do IGMP correspondente à versão mais baixa de cliente IGMP presente. Se houver clientes IGMPv3 e IGMPv2, o roteador usará o IGMPv2. Se houver clientes IGMPv1, IGMPv2 e IGMPv3, o roteador usará o IGMPv1.

Cenário 3: Roteadores de Versões Diferentes no Mesmo Segmento

Quando há roteadores de versões diferentes no mesmo segmento, os roteadores da versão menor não têm nenhum meio de detectar os roteadores de versão mais alta. Portanto, os roteadores diferentes devem ser configurados pelo administrador como a mesma versão. Essa versão deve corresponder à versão mais baixa presente em qualquer roteador de consulta.

IGMP em um roteador

Se, por padrão, não houver nenhum usuário registrado em um grupo específico em uma sub-rede, o roteador não enviará o tráfego multicast para esse grupo nessa sub-rede. Isso significa que um roteador precisa receber um relatório de IGMP para um GDA para adicioná-lo à tabela de roteamento de multicast e para iniciar o tráfego de encaminhamento para esse grupo.

Em um roteador, você precisa executar as seguintes ações:

1. Habilite o Multicast Routing no modo global, conforme mostrado abaixo.

   ```
   ip multicast-routing
   ```

2. Configure um protocolo de roteamento multicast na interface envolvida, conforme mostrado abaixo.

   ```
   ip pim dense-mode
   ```

3. Monitore o IGMP, como mostrado abaixo.

   ```
   show ip igmp interface
   show ip igmp group
   show ip mroute
   ```

4. Configure um roteador para enviar o relatório IGMP (na interface), conforme mostrado abaixo.

   ```
   ip igmp join-group [GDA_ip_address]
   ip igmp version [1 | 2 | 3]
   ```

Exemplo Prático em um Roteador

Um roteador é configurado para rotear entre duas subinterfaces, Fast-Ethernet 0.2 e Fast-Ethernet 0.3. Ambas as interfaces também são configuradas para executar IGMP. Na saída abaixo, você pode ver a versão do IGMP, o grupo unido, e assim por diante.

Configuração

```
ip multicast-routing


interface FastEthernet0
 no ip address
 no ip directed-broadcast
!
interface FastEthernet0.2
 encapsulation isl 2
 ip address 10.2.2.1 255.255.255.0
 no ip redirects
 no ip directed-broadcast
 ip pim dense-mode
!
interface FastEthernet0.3
 encapsulation isl 3
 ip address 10.3.3.1 255.255.255.0
 no ip redirects
 no ip directed-broadcast
 ip pim dense-mode
!
```

show ip igmp interface

```
 Fa0.2 is up, line protocol is up
 Internet address is 10.2.2.1/24
 IGMP is enabled on interface
 Current IGMP version is 2
 CGMP is disabled on interface
 IGMP query interval is 60 seconds
 IGMP querier timeout is 120 seconds
 IGMP max query response time is 10 seconds
 Inbound IGMP access group is not set
 IGMP activity: 3 joins, 2 leaves
 Multicast routing is enabled on interface
 Multicast TTL threshold is 0
 Multicast designated router (DR) is 10.2.2.1 (this system)
 IGMP querying router is 10.2.2.1 (this system)
 Multicast groups joined: 224.0.1.40

 Fa0.3 is up, line protocol is up
 Internet address is 10.3.3.1/24
 IGMP is enabled on interface
 Current IGMP version is 2
 CGMP is disabled on interface
 IGMP query interval is 60 seconds
 IGMP querier timeout is 120 seconds
 IGMP max query response time is 10 seconds
 Inbound IGMP access group is not set
 IGMP activity: 1 joins, 1 leaves
 Multicast routing is enabled on interface
 Multicast TTL threshold is 0
 Multicast designated router (DR) is 10.3.3.1 (this system)
 IGMP querying router is 10.3.3.1 (this system)
 No multicast groups joined
```

show ip mroute and show ip igmp group

```
Router_A#show ip mroute
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned
       R - RP-bit set, F - Register flag, T - SPT-bit set, J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode


(*, 239.10.10.10), 00:01:15/00:02:59, RP 0.0.0.0, flags: DJC
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    FastEthernet0.3, Forward/Dense, 00:01:16/00:00:00

(10.2.2.2, 239.10.10.10), 00:00:39/00:02:20, flags: CT
  Incoming interface: FastEthernet0.2, RPF nbr 0.0.0.0
  Outgoing interface list:
    FastEthernet0.3, Forward/Dense, 00:00:39/00:00:00

Router_A#show ip igmp groups
IGMP Connected Group Membership
Group Address    Interface            Uptime    Expires   Last Reporter
239.10.10.10     Fa0.3                00:02:48  00:02:04  10.3.3.2
Router_A#
```

Protocolo de gerenciamento de grupo Cisco

Para o suporte ao CGMP em Catalyst Switches, consulte a Matriz de Suporte dos Catalyst Switches Multicast.

Tipos de quadros e mensagens CGMP

O CGMP foi implementado pela primeira vez pela Cisco para restringir o tráfego de multicast em uma rede L2. Como o Switch, por natureza, não é capaz de buscar os pacotes L3, ele não consegue distinguir um pacote IGMP. Com o CGMP, o roteador fornece a interface entre os hosts. Os roteadores “falam” IGMP e os switches “falam” CGMP.

Os quadros CGMP são quadros Ethernet com o endereço MAC de destino 01-00-0c-dd-dd-dd e com um cabeçalho Subnetwork Access Protocol (SNAP) igual as0x2001. Os quadros CGMP contêm os seguintes campos:

- Versão: 1 ou 2.
- Tipo de mensagem: União ou Saída.
- Contagem: O número de pares de endereços multicast/unicast na mensagem.
- GDA: O endereço MAC de 48 bits do grupo de multicast.
- Endereço de origem unicast (EUA): O endereço unicast MAC de 48 bits dos dispositivos que querem se unir ao GDA.

  Note: O valor do campo do contador determina quantas vezes os dois últimos campos são exibidos.

Por padrão, os processadores de um switch (chamado de NMP no Catalyst) ouvem somente endereços multicast quando o **show cam system** é emitido. Quando você ativa o CGMP em um switch, o endereço 01-00-0c-dd-dd-dd é adicionado ao **show cam system** Saída do comando.

A tabela abaixo lista todos as possíveis mensagens de CGMP.

GDA	USA	Juntar/Separar	Significado
Mcast MAC	Cliente MAC	União	Adicione porta ao grupo.
Mcast MAC	Cliente MAC	Sair	Exclua a porta do grupo.
00-00-00-00-00-00	MAC de roteador	União	Atribuir a porta do roteador.
00-00-00-00-00-00	MAC de roteador	Sair	Cancele a atribuição da porta do roteador.
Mcast MAC	00-00-00-00-00-00	Sair	Eliminar grupo.
00-00-00-00-00-00	00-00-00-00-00-00	Sair	Exclua todos os grupos.

Conhecendo as Portas do Roteador

O switch precisa estar ciente de todas as portas de roteador para que elas sejam adicionadas automaticamente qualquer entrada de multicast recém-criada. O Switch identifica as portas do roteador quando recebe uma Junção CGMP para GDA 00-00-00-00-00-00 com Roteador MAC USA (terceiro tipo de mensagem na tabela). Essas mensagens são geradas pelo roteador em todas as interfaces configuradas para executar o CGMP. Há também um método estático para configurar portas de roteador no switch.

União a Grupos com o CGMP

- Um cliente novo solicita o recebimento do tráfego para um GDA e, portanto, envia uma mensagem de relatório de associação IGMP.
- O roteador recebe o relatório IGMP, processa-o e envia uma mensagem CGMP ao Switch. O roteador copia o endereço MAC de destino no campo GDA da união de CGMP e copia o endereço MAC de origem no USA da união de CGMP. Ele então o envia de volta para o switch.
- Um switch com CGMP habilitado precisa escutar os endereços CGMP 01-00-0c-dd-dd-dd. O processador do switch procura na tabela CAM o USA. Quando o USA é encontrado na tabela CAM, o switch sabe em qual porta o USA se encontra e executa uma das seguintes ações:Cria uma entrada estática nova para o GDA e vincular a porta USA a ela junto com todas as portas de roteador.Adiciona a porta USA à lista de portas deste GDA (se a entrada estática já existir).

Saída de Grupos com CGMP

As entradas estáticas aprendidas com o CGMP são permanentes, a não ser que ocorra uma alteração na topologia da árvore de abrangência na VLAN ou o roteador envie uma das últimas mensagens de CGMP Leave na tabela anterior.

Quando o IGMPv1 é o host, não envie mensagens de IGMP Leave. O roteador envia somente mensagens de saída se não recebe uma resposta a três consultas do IGMP consecutivas. Isso significa que nenhuma porta será eliminada de um grupo se houver usuários ainda interessados nesse grupo.

Com a introdução de IGMPv2 e a presença de IGMP Leave, a Cisco fez um acréscimo à especificação CGMP original (CGMPv2). Essa adição é denominada CGMP Fast-Leave.

O processamento CGMP Fast-Leave permite que o switch detecte as mensagens de saída do IGMPv2 enviadas para o endereço de multicast somente de roteador (224.0.0.2) por hosts em qualquer uma das portas do Supervisor Engine Module. Quando o Supervisor Engine Module receber uma mensagem de saída, um temporizador de consulta-resposta é iniciado e uma mensagem é enviada à porta na qual a saída foi recebida para determinar se ainda há um host aguardando o recebimento do grupo de multicast naquela porta. Se esse temporizador expirar antes que uma mensagem de união do CGMP seja recebida, a porta será removida da árvore de multicast do grupo de multicast especificado na mensagem de saída original. Se essa for a última porta no grupo de multicast, ela encaminhará a mensagem de IGMP Leave para todas as portas do roteador. O roteador então inicia o processo normal de exclusão ao enviar uma consulta específica de grupo. Como nenhuma resposta é recebida, o roteador remova esse grupo da tabela de Multicast Routing dessa interface. Ele também envia uma mensagem de CGMP Leave para o switch que apaga o grupo da tabela estática. O processamento de licença rápida garante um melhor gerenciamento da largura de banda para todos os hosts em uma rede comutada, mesmo que vários grupos de multicast estejam em uso simultaneamente.

Quando CGMP Leave está habilitado, duas entradas são adicionadas ao **show cam system** saída do comando, conforme mostrado abaixo.

```
01-00-5e-00-00-01
01-00-5e-00-00-02
```

A mensagem de IGMP Leave utiliza 224.0.0.2 e a consulta de IGMP utiliza 224.0.0.1.

Use as etapas a seguir para fazer Troubleshooting de CGMP:

1. Devido a um conflito com o HSRP, o processamento do CGMP Leave é desabilitado por padrão. O HSRP usa o endereço MAC 01-00-5e-00-00-02, o qual é o mesmo do IGMP Leave no IGMP Versão 2. Com o CGMP Fast-Leave, todos os pacotes HSRP vão para a CPU do switch. Porque uma mensagem HSRP não é um pacote de IGMP, o switch regenera todas as mensagens desse tipo e as envia para todas as portas de roteador. Os roteadores que recebem saudação hsrp ou peers hsrp perdem conectividade. Portanto, ao depurar problemas de HSRP, tente desabilitar CGMP Fast-Leave.Para habilitar o processamento CGMP Leave, emita o comando **set cgmp leave enable** comando.
2. Quando o processamento do CGMP Leave está habilitado, o Catalyst 5000 Family Switch aprende as portas de roteador através de mensagens do PIM-v1, do HSRP e de auto-união do CGMP. Quando o processamento de licença do CGMP está desabilitado, o Switch da

família Catalyst 5000 identifica as portas do roteador somente por meio de mensagens de junção automática do CGMP.

3. O CGMP não elimina o tráfego multicast para nenhum endereço IP de multicast mapeado no intervalo de endereços MAC de 01-00-5E-00-00-00 a 01-00-5E-00-00-FF. Os endereços IP de multicast reservados, no intervalo de 224.0.0.0 a 224.0.0.255, são utilizados para encaminhar o tráfego IP de multicast local em um único salto L3.

CGMP e rede de somente origem

Uma rede somente de origem é um segmento com apenas um multicast de origem e nenhum cliente real. Por isso, existe a possibilidade de que nenhum relatório IGMP seja gerado nesse segmento. No entanto, o CGMP ainda precisa restringir a inundação dessa origem (apenas para o uso do roteador). Se um roteador detectar tráfego multicast em uma interface sem relatório de IGMP, ela é identificada como uma rede multicast somente de origem. O roteador gera uma mensagem de união do CGMP para si, e o switch simplesmente adiciona esse grupo (com a porta de roteador apenas).

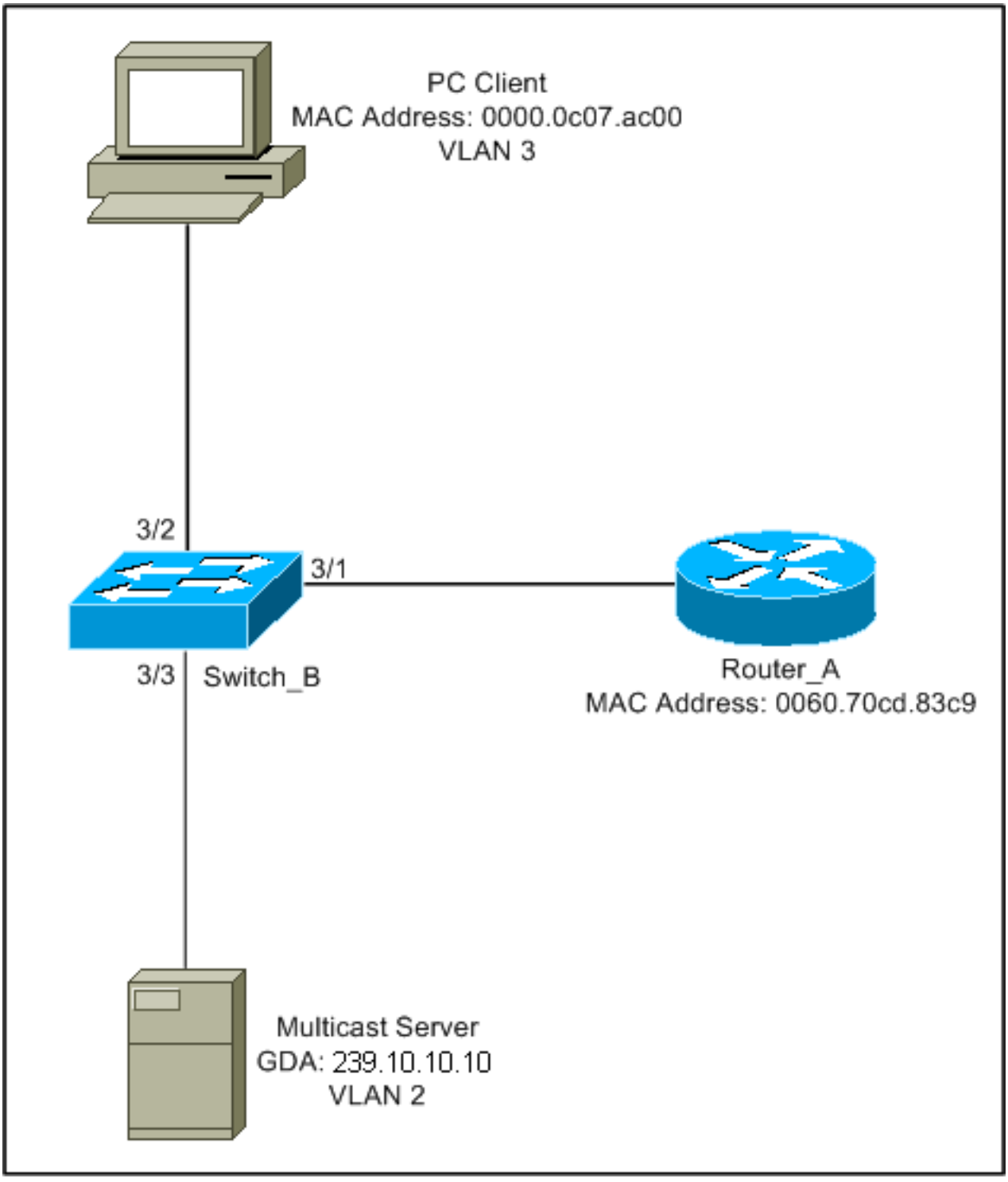
Configuração de Cisco Routers e Switches para Habilitar o CGMP

Os comandos abaixo são válidos somente para o Catalyst 4000 e 5000 Series (mais 2901, 2902, 2926, 2948G e 4912).

- Roteador MulticastHabilitar o multicasting de IP (comando global):**ip multicast-routing**Habilite cada interface que executa o CGMP (modo de interface) com os seguintes comandos:**ip pimip igmpip cgmp**Depure o problema de multicast de L2 com os seguintes comandos:**debug ip igmpdebug ip cgmp**
- Catalyst 4000 ou 5000 SeriesHabilitar/desabilitar CGMP com os seguintes comandos:**set cgmp**Habilite/desabilite o CGMP Fast-Leave com os seguintes comandos:**set cgmp leave**Configure o roteador de multicast (estático) com os seguintes comandos:**set multicast router**Limpe o roteador multicast com os seguintes comandos:**clear multicast router**A seguir, uma lista dos vários comandos para verificar a operação do CGMP é apresentada.**show cam staticshow cgmp statisticshow cgmp leaveshow multicast routershow multicast groupshow multicast group cgmpshow multicast group count**

Exemplo prático de uso de CGMP e comando e saída debug

Este é um exemplo de configuração prático de um roteador Cisco e de Catalyst Switches.



Essa configuração mostra as operações envolvidas quando um host se une a um grupo. Os alos desta configuração mostram as operações enquanto um host sai de um grupo com o Fast-Leave habilitado. Os rastreamentos do farejador e a configuração do switch e do roteador também são fornecidos.

União a Grupos com o CGMP

Consulte estas etapas ao se unir a um grupo com CGMP.

1. Habilite o CGMP no switch, como mostrado abaixo.

```
Switch_B (enable) set cgmp en
MCAST-CGMP: Set CGMP Sys Entrie
MCAST-CGMP: Set CGMP Sys Entrie
```

```
MCAST-CGMP: Set CGMP Sys Entrie
CGMP support for IP multicast enabled.
Switch_B (enable)
```

Como você pode ver abaixo, a entrada 01-00-0c-dd-dd-dd é incluída para todas as VLANs no **show cam system** Saída do comando. Além disso, como a rede está executando o CGMP Fast-Leave, é possível ver as entradas para 01-00-5e-00-00-01 e 01-00-5e-00-00-02.

```
Switch_B (enable) show cgmp leave

CGMP:       enabled
CGMP leave: enabled
Switch_B (enable) show cam system
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN  Dest MAC/Route Des [CoS]  Destination Ports or VCs / [Protocol Type]
----  ----------------- -----  -------------------------------------------
1     00-10-2f-00-14-00  #          7/1
1     00-e0-fe-4b-f3-ff  #          1/9
1     01-00-0c-cc-cc-cc  #          1/9
1     01-00-0c-cc-cc-cd  #          1/9
1     01-00-0c-dd-dd-dd  #          1/9
1     01-00-0c-ee-ee-ee  #          1/9
1     01-80-c2-00-00-00  #          1/9
1     01-80-c2-00-00-01  #          1/9
2     00-10-2f-00-14-00  #          7/1
2     01-00-0c-cc-cc-cc  #          1/9
2     01-00-0c-cc-cc-cd  #          1/9
2     01-00-0c-dd-dd-dd  #          1/9
2     01-80-c2-00-00-00  #          1/9
2     01-80-c2-00-00-01  #          1/9
3     01-00-0c-cc-cc-cc  #          1/9
3     01-00-0c-cc-cc-cd  #          1/9
3     01-00-0c-dd-dd-dd  #          1/9
3     01-80-c2-00-00-00  #          1/9
3     01-80-c2-00-00-01  #          1/9
Total Matching CAM Entries Displayed = 19
```

2. O roteador envia uma mensagem CGMP Join a GDA 00-00-00-00-00-00 com o MAC USA do roteador. Consequentemente, a porta de roteador é adicionada à lista de portas de roteador (veja o primeiro exemplo abaixo).**No roteador**

```
6d01h: CGMP: Sending self Join on Fa0.3
6d01h:       GDA 0000.0000.0000, USA 0060.70cd.83c9
```

No switch

```
MCAST-CGMP-JOIN: recvd CGMP JOIN msg on port 3/1 vlanNo 2
MCAST-CGMP-JOIN: join GDA 00-00-00-00-00-00 MCAST-CGMP-JOIN:USA
                 00-60-70-cd-83-c9
MCAST-ROUTER: Adding QUERIER port 3/1, vlanNo 2
MCAST-ROUTER: Creating RouterPortTimer for  port 3/1, vlanNo 2

Switch_B (enable) show multi router
CGMP enabled
IGMP disabled

Port       Vlan
---------  ----------------
 3/1       2-3

Total Number of Entries = 1
'*' - Configured
```

3. O PC em 3/1 envia ao IGMP um relatório contendo o GDA: 239.10.10.10 (veja o quadro 2 abaixo). Abaixo é mostrado o comando **show ip igmp group** saída do comando no roteador Router_A.Isso mostra que o roteador agora encaminha o tráfego do endereço 224.10.10.10 para o fa0.3. Esta é uma consequência do recebimento do relatório IGMP de 10.3.3.2, que é o PC cliente.

```
Router_A#show ip igmp groups
IGMP Connected Group Membership
Group Address    Interface            Uptime    Expires   Last Reporter
239.10.10.10     Fa0.3                00:02:48  00:02:04  10.3.3.2
Router_A#
```

4. O roteador recebe o relatório e envia uma mensagem CGMP Join junto com as seguintes informações:MAC de origem: Endereço MAC do roteadorMAC de destino: 01-00-cc-dd-dd-ddÍndice: Endereço MAC do PC cliente (EUA): Endereço MAC 00-00-0c-07-ac-00 do grupo de multicast: 01-00-5e-0a-0a-0a (consulte o quadro 3 a seguir)**No roteador**

```
6d01h: IGMP: Received v2 Report from 10.3.3.2 (Fa0.3) for 239.10.10.10
6d01h: CGMP: Received IGMP Report on Fa0.3
6d01h:       from 10.3.3.2 for 239.10.10.10
6d01h: CGMP: Sending Join on Fa0.3
```

5. O switch com 01-00-cc-dd-dd-dd no **show cam system** a saída do comando tem o CGMP ativado. O switch pode processar o pacote.O switch faz uma consulta na tabela de CAM dinâmica para determinar em que porta o endereço MAC do PC cliente se encontra. O endereço está localizado na porta 3/2 e o switch faz uma entrada estática na tabela CAM para 01-00-5e-0a-0a-0a-0a, vinculada à porta 3/2. O switch também adiciona a porta de roteador 3/1 à entrada estática para esse GDA.**No switch**

```
MCAST-CGMP-JOIN: recvd CGMP JOIN msg on port 3/1 vlanNo 3
MCAST-CGMP-JOIN: join GDA 01-00-5e-0a-0a-0a MCAST-CGMP-JOIN:USA 00-60-5c-f4-bd-e2
MCAST-CGMP-JOIN: 3/2/3: index 81
MCAST-CGMP-JOIN: recvd CGMP JOIN msg on port 3/1 vlanNo 2
MCAST-CGMP-JOIN: join GDA 01-00-5e-00-01-28 MCAST-CGMP-JOIN:USA 00-60-70-cd-83-c9
MCAST-CGMP-JOIN: 3/1/2: index 80
```

6. Todo o tráfego subsequente para o grupo de multicast 239.10.10.10 é enviado somente para essa porta nesta VLAN. Abaixo é mostrada a entrada estática no Catalyst Switch onde 3/1 é a porta de roteador e 3/2 é a porta do cliente.

```
Switch_B (enable) show cam static
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN  Dest MAC/Route Des    [CoS]  Destination Ports or VCs / [Protocol Type]
----  ------------------    -----  ------------------------------------------
3     01-00-5e-0a-0a-0a             3/1-2
Total Matching CAM Entries Displayed = 3
Switch_B (enable)
```

Deixando um grupo com CGMP Fast-Leave Habilitado

O exemplo abaixo exige que o cliente seja um IGMP Versão 2 e que o Fast-Leave seja habilitado no Switch.

1. O seguinte procedimento habilita o CGMP Fast-Leave. Veja o **show cgmp leave** para determinar se está ativado. Além disso, veja o **show cam system** para determinar se o switch está ouvindo 01-00-5e-00-00-01 e 01-00-5e-00-00-02 (endereços usados para a licença).

```
Switch_B (enable) show cgmp leave

CGMP:       enabled
CGMP leave: enabled
Switch_B (enable) show cam sys
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN  Dest MAC/Route Des    [CoS]  Destination Ports or VCs / [Protocol Type]
----  ------------------    -----  -------------------------------------------
1     00-10-2f-00-14-00  #          7/1
1     00-e0-fe-4b-f3-ff  #          1/9
1     01-00-0c-cc-cc-cc  #          1/9
1     01-00-0c-cc-cc-cd  #          1/9
1     01-00-0c-dd-dd-dd  #          1/9
1     01-00-0c-ee-ee-ee  #          1/9
1     01-80-c2-00-00-00  #          1/9
1     01-80-c2-00-00-01  #          1/9
2     00-10-2f-00-14-00  #          7/1
2     01-00-0c-cc-cc-cc  #          1/9
2     01-00-0c-cc-cc-cd  #          1/9
2     01-00-0c-dd-dd-dd  #          1/9
2     01-00-5e-00-00-01  #          1/9
2     01-00-5e-00-00-02  #          1/9
2     01-80-c2-00-00-00  #          1/9
2     01-80-c2-00-00-01  #          1/9
3     01-00-0c-cc-cc-cc  #          1/9
3     01-00-0c-cc-cc-cd  #          1/9
3     01-00-0c-dd-dd-dd  #          1/9
3     01-00-5e-00-00-01  #          1/9
3     01-00-5e-00-00-02  #          1/9
3     01-80-c2-00-00-00  #          1/9
Do you wish to continue y/n [n]?  y
Total Matching CAM Entries Displayed = 22
```

2. O cliente envia uma mensagem de saída do IMPG para 224.0.0.2. O switch a intercepta e envia uma consulta de IGMP na porta em que recebe a saída. O seguinte é **debug** saída no switch:

```
MCAST-IGMP-LEAVE:Recvd leave on port 3/2 vlanNo 3
MCAST-IGMP-LEAVE:router_port_tbl[vlanNo].QueryTime = 0
MCAST-IGMP-LEAVE:deletion_timer = 1
MCAST-SEND:Transmitting IGMP Mac Based GS Query msg on port 3/2 vlanNo 3
MCAST-SEND:  Transmit Succeeded for IGMP Group Specific Query msg on port 3/2 vlanNo 3
```

3. Como nenhuma resposta foi recebida, o Catalyst encaminha a mensagem de IGMP Leave para o roteador, conforme mostrado abaixo.

```
MCAST-TIMER:IGMPLeaveTimer expired on port 3/2 vlanNo 3 GDA 01-00-5e-0a-0a-0a
MCAST-TIMER:IGMPLeaveTimer expiry: Transmit IGMP Leave on port 3/1 vlanNo 3
MCAST-SEND:Transmitting IGMP Leave msg on port 3/1 vlanNo 3
MCAST-SEND: Inband Transmit Succeeded for IGMP Leave Message on port 3/1 vlanNo 3
```

4. O roteador recebe uma mensagem IGMP Leave, portanto, envia uma mensagem CGMP Leave para o Switch e também exclui o grupo de sua lista de grupos IGMP. Abaixo está o

debug saída do comando no roteador.**No roteador**

```
IGMP: Received Leave from 10.200.8.108 (Fa0.3) for 239.10.10.10
IGMP: Send v2 Query on Fa0.3 to 239.10.10.10
IGMP: Send v2 Query on Fa0.3 to 239.10.10.10
CGMP: Sending Leave on Fa0.3
      GDA 0100.5e0a.0a0a, USA 0000.0000.0000
IGMP: Deleting 239.10.10.10 on Fa0.3
```

Rastreamentos e Configuração do CGMP

Quadro 1

O quadro 1 é um quadro de união do CGMP ao GDA 00-00-00-00-00-00. Ele é usado para adicionar a porta de roteador à lista de porta de roteador.

```
ISL: ----- ISL Protocol Packet -----
     ISL:
     ISL: Destination Address               = 01000C0000
     ISL: Type                              = 0 (Ethernet)
     ISL: User                              = 0 (Normal)
     ISL: Source Address                    = 8C958B7B1000
     ISL: Length                            = 76
     ISL: Constant value                    = 0xAAAA03
     ISL: Vendor ID                         = 0x8C958B
     ISL: Virtual LAN ID (VLAN)             = 2
     ISL: Bridge Protocol Data Unit (BPDU)  = 0
     ISL: Port Index                        = 193
     ISL: Reserved
     ISL:
ETHER: ----- Ethernet Header -----
     ETHER:
     ETHER: Destination = Multicast 01000CDDDDDD
!--- Send to the CGMP !--- macaddress present in show cam sys !--- command output.

     ETHER: Source      = Station Cisco11411E1
     ETHER: 802.3 length = 24
     ETHER:
LLC:  ----- LLC Header -----
     LLC:
     LLC:  DSAP Address = AA, DSAP IG Bit = 00 (Individual Address)
     LLC:  SSAP Address = AA, SSAP CR Bit = 00 (Command)
     LLC:  Unnumbered frame: UI
     LLC:
SNAP: ----- SNAP Header -----
     SNAP:
     SNAP: Vendor ID = Cisco1
     SNAP: Type = 2001 (CGMP)
     SNAP:
CGMP: ----- CGMP -----
     CGMP:
     CGMP: Version   = 16
     CGMP: Type      = 0 (Join)
     CGMP: Reserved
     CGMP: Count     = 1
     CGMP:
     CGMP: Group Destination Address and Unicast Source Address
     CGMP:
     CGMP:    GDA    =0000.0000.0000
```

```
     CGMP:    USA    =0000.0C14.11E1
!--- MAC address of the router. CGMP:
```

O resultado do quadro 1 está no switch, onde 3/1 é a porta conectada ao roteador:

Quadro 2

O quadro 2 é um relatório de associação de IGMP enviado pelo host para solicitar (ou confirmar) que os usuários desejam receber tráfego para o grupo 239.10.10.10.

```
ISL: ----- ISL Protocol Packet -----
     ISL:
     ISL: Destination Address              = 01000C0000
     ISL: Type                             = 0 (Ethernet)
     ISL: User                             = 0 (Normal)
     ISL: Source Address                   = 8C958B7B1000
     ISL: Length                           = 76
     ISL: Constant value                   = 0xAAAA03
     ISL: Vendor ID                        = 0x8C958B
     ISL: Virtual LAN ID (VLAN)            = 2
     ISL: Bridge Protocol Data Unit (BPDU)  = 0
     ISL: Port Index                       = 195
     ISL: Reserved
     ISL:
ETHER: ----- Ethernet Header -----
     ETHER:
     ETHER: Destination = Multicast 01005E0A0A0A
!--- Destination is the GDA MAC. ETHER: Source = Station Cisco176DCCA !--- Sourced by the PC
connected in 3/1. ETHER: Ethertype = 0800 (IP) ETHER: IP: ----- IP Header ----- IP: IP: Version
= 4, header length = 20 bytes IP: Type of service = C0 IP: 110. .... = internetwork control IP:
...0 .... = normal delay IP: .... 0... = normal throughput IP: .... .0.. = normal reliability
IP: Total length = 28 bytes IP: Identification = 0 IP: Flags = 0X IP: .0.. .... = may fragment
IP: ..0. .... = last fragment IP: Fragment offset = 0 bytes IP: Time to live = 1 seconds/hops
IP: Protocol = 2 (IGMP) IP: Header checksum = CC09 (correct) IP: Source address = [10.1.1.2] IP:
Destination address = [224.10.10.10] IP: No options IP: IGMP: ----- IGMP header ----- IGMP:
IGMP: Version = 1 IGMP: Type = 6 (Ver2 Membership Report) IGMP: Unused = 0x00 IGMP: Checksum =
FFEA (correct) IGMP: Group Address = [224.10.10.10] IGMP:
```

Quadro 3

O quadro 3 é o quadro de CGMP enviado pelo roteador ao Switch, para instruí-lo a adicionar uma entrada estática para 01-00-5e-0a-0a-0a.

```
ISL: ----- ISL Protocol Packet -----
     ISL:
     ISL: Destination Address              = 01000C0000
     ISL: Type                             = 0 (Ethernet)
     ISL: User                             = 0 (Normal)
     ISL: Source Address                   = 8C958B7B1000
     ISL: Length                           = 76
     ISL: Constant value                   = 0xAAAA03
     ISL: Vendor ID                        = 0x8C958B
     ISL: Virtual LAN ID (VLAN)            = 2
     ISL: Bridge Protocol Data Unit (BPDU)  = 0
     ISL: Port Index                       = 193
     ISL: Reserved
     ISL:
ETHER: ----- Ethernet Header -----
     ETHER:
     ETHER: Destination = Multicast 01000CDDDDDD
     ETHER: Source      = Station Cisco11411E1
```

```
     ETHER: 802.3 length = 24
     ETHER:
LLC:  ----- LLC Header -----
     LLC:
     LLC:  DSAP Address = AA, DSAP IG Bit = 00 (Individual Address)
     LLC:  SSAP Address = AA, SSAP CR Bit = 00 (Command)
     LLC:  Unnumbered frame: UI
     LLC:
SNAP: ----- SNAP Header -----
     SNAP:
     SNAP: Vendor ID = Cisco1
     SNAP: Type = 2001 (CGMP)
     SNAP:
CGMP: ----- CGMP -----
     CGMP:
     CGMP: Version   = 16
     CGMP: Type      = 0 (Join)
     CGMP: Reserved
     CGMP: Count     = 1
     CGMP:
     CGMP: Group Destination Address and Unicast Source Address
     CGMP:
     CGMP:    GDA    =0100.5E0A.0A0A
!--- GDA MAC added in show cam static !--- command output.

     CGMP:    USA    =0000.0C76.DCCA
!--- MAC of the PC in 3/1. CGMP:
```

Abaixo é mostrada a configuração do roteador e do switch.

```
 Router_A (router) Configuration:

 Router_A#write terminal
 Building configuration...

 Current configuration:
 !
 version 12.0
 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
 !
 hostname Router_A
 !
 !
 ip subnet-zero
 ip multicast-routing
 ip dvmrp route-limit 20000


 interface FastEthernet0
  no ip address
  no ip directed-broadcast
 !
 interface FastEthernet0.1
  encapsulation isl 1
  ip address 10.1.1.1 255.255.255.0
  no ip redirects
  no ip directed-broadcast
 !
 interface FastEthernet0.2
  encapsulation isl 2
  ip address 10.2.2.1 255.255.255.0
```

```
 no ip redirects
 no ip directed-broadcast
 ip pim dense-mode
 ip cgmp
!
interface FastEthernet0.3
 encapsulation isl 3
 ip address 10.3.3.1 255.255.255.0
 no ip redirects
 no ip directed-broadcast
 ip pim dense-mode
 ip cgmp
!

Switch_B configuration for CGMP:

#cgmp
set cgmp enable
set cgmp leave enable
!

CGMP statistics for VLAN 3:

Switch_B (enable) show cgmp sta 3
CGMP enabled

CGMP statistics for vlan 3:
valid rx pkts received           109
invalid rx pkts received         0
valid cgmp joins received        108
valid cgmp leaves received       1
valid igmp leaves received       1
valid igmp queries received      63
igmp gs queries transmitted      1
igmp leaves transmitted          1
failures to add GDA to EARL      0
topology notifications received  0
Switch_B (enable)
```

Espionagem de IGMP

A espionagem de IGMP é uma outra característica que permite capturar diretamente quadros IGMP. Para o suporte à espionagem de IGMP nos Catalyst Switches, consulte Matriz de suporte aos Multicast Catalyst Switches.

Visão geral sobre espionagem de IGMP

A espionagem de IGMP, como implicado pelo nome, é uma característica que permite ao switch “escutar” as conversações IGMP entre hosts e roteadores. Quando um switch ouve um relatório IGMP de um host para um determinado grupo de multicast, o switch adiciona o número da porta do host à lista GDA para esse grupo. E, quando o switch ouve um IGMP Leave, ele remove a porta do host da entrada da tabela CAM.

Conhecimento sobre a porta do roteador

O switch escuta as seguintes mensagens a fim de detectar portas de roteador com aespionagem

de IGMP:

- IGMP Membership query send to 01-00-5e-00-00-01
- PIMv1 hello send to 01-00-5e-00-00-02
- PIMv2 hello send to 01-00-5e-00-00-0d
- Provas DVMRP enviar para 01-00-5e-00-04
- Mensagem MOSPF envia para 01-00-5e-00-05 ou 06.

Ao ativar o rastreamento IGMP em um switch, todas as entradas MAC acima são adicionadas ao **show cam system** saída de comando do switch de espionagem. Quando uma porta de roteador é detectada, ela é adicionada à lista de portas de todos os GDA nessa VLAN.

União a Grupos com o IGMP

A seguir encontram-se dois cenários de associação:

Cenário A: O host A é o primeiro host a se unir a um grupo no segmento.

1. O host A envia um relatório de sociedade de IGMP não solicitado.
2. O switch intercepta os relatórios de associação de IGMP que foram enviados pelo host que queria se unir ao grupo.
3. O switch cria uma entrada de multicast para esse grupo e a vincula à porta em que recebeu o relatório e a todas as portas de roteador.
4. O switch envia o relatório de IGMP a todas as portas de roteador. O roteador também recebe o relatório de IGMP e atualiza sua tabela de roteamento de multicast de acordo.

Cenário B: O host B agora é o segundo host a juntar-se ao mesmo grupo.

1. Host B envia um relatório de associação de IGMP não solicitado.
2. O switch intercepta o relatório de associação de IGMP que foi enviado pelo host que queria se unir ao grupo.
3. O switch não necessariamente envia o relatório de IGMP a todas as portas de roteador. Na realidade, o switch envia relatórios de IGMP às portas de roteador usando o relatório de proxy e encaminha somente um relatório por grupo dentro de 10s.

   Note: A fim de manter a associação ao grupo, o roteador multicast envia a uma consulta IGMP a cada 60 segundos. Essa consulta é interceptada pelo switch e encaminhada para todas as portas no switch. Todos os hosts que são membros do grupo respondem a essa consulta. No entanto, considerando que o switch intercepta o relatório da resposta também, o outro host não vê cada um dos outros relatórios e, assim, todos os hosts enviam um relatório (em vez de um por grupo). O switch usa então o relatório de proxy para enviar somente um relatório por grupo entre todas as respostas recebidas.

Suponha que Host A deseje sair do grupo, mas Host B ainda queira recebê-lo.

- O switch captura a mensagem de IGMP Leave de Host A.
- O switch emite uma consulta IGMP específica do grupo para o grupo nessa porta (e somente nessa porta).
- Se o Switch não receber um relatório, ele descartará essa porta da entrada. Caso ele receba uma resposta dessa porta, nada será feito e a licença será descartada.
- Host B ainda está interessado pelo grupo nesse switch. Esta não seria a última porta sem

roteador na entrada. Consequentemente, o switch não encaminha a mensagem de licença. Agora suponha que o host B deseja sair do grupo e o host B é o último usuário interessado por este grupo neste segmento.

- O switch captura a mensagem de IGMP Leave de Host A.
- O switch emite uma consulta IGMP específica do grupo para o grupo nessa porta.
- Se o switch não receber um relatório, ele descartará esta porta da entrada.
- Esta é a última porta "não roteador" para o GDA. O switch envia a mensagem de IGMP Leave para todas as portas de roteador e remove a entrada da sua tabela.

Interação IGMP/CGMP

Em algumas redes, devido às limitações de hardware, talvez você não consiga usar a espionagem de IGMP em todos os switches. Nesse caso, talvez seja necessário para executar CGMP em alguns Switches em alguma rede.

Observe que este é um caso especial. O switch que executa a espionagem de IGMP detecta mensagens de CGMP e também que alguns switches na rede estão executando o CGMP. Portanto, ele entra em um modo IGMP-CGMP especial e desabilita a geração de relatórios de proxy. Isso é absolutamente necessário para a operação apropriada do CGMP porque os roteadores usam o endereço MAC de origem do relatório de IGMP para criar uma união de CGMP. Roteadores que executam o CGMP precisam ver todos os relatórios de IGMP para que a geração de relatórios de proxy seja desabilitada. Os relatórios enviados para o roteador devem ser somente aqueles estritamente necessários para a espionagem do IGMP.

Rede Multicast Somente de Origem

Se o segmento contiver somente um servidor multicast (origem de multicast) e nenhum cliente, você poderá se ver frente a uma situação em que não terá nenhum pacote IGMP nesse segmento, mas terá muito tráfego multicast. Nesse caso, o switch simplesmente envia o tráfego desse grupo para todos no segmento. Felizmente, um switch que executa a espionagem de IGMP pode detectar estes fluxos de multicast e adicionar uma entrada de multicast para esse grupo com somente a porta de roteador. Essas entradas são sinalizadas internamente como mcast_source_only e expiram a cada 5 minutos, ou quando a porta do roteador sai. Observe que, mesmo depois de tal envelhecimento, o endereço será reaprendido em alguns segundos se o tráfego continuar. Dentro do período de retransmissão, pode ocorrer inundação momentânea na VLAN. Para evitar isso e manter as entradas, use o comando **set igmp flooding enable | disable** comando. Depois que a inundação é desativada, o switch não envelhece as entradas somente de origem.

Limitações

Assim como no CGMP, os GDAs mapeados em um MAC do intervalo 01-00-5e-00-00-xx nunca são removidos pela espionagem de IGMP.

Configuração da espionagem IGMP nos Cisco Switches

Para habilitar/desabilitar a espionagem de IGMP, emita o seguinte comando:

- **set igmp**

Para configurar o roteador de multicast (estático), execute o seguinte comando:

- **set multicast router**
- **clear multicast router *port* | *all>***

Para monitorar e verificar as estatísticas IGMP, acione os seguintes comandos:

- **show igmp statistics**
- **show multicast router**

Exemplo prático de espionagem de IGMP

A configuração para este exemplo é similar à do teste de CGMP utilizado anteriormente neste documento. A única diferença é que as portas 3/2 e 3/3 estão ambas conectadas à mesma VLAN e ambas estão configuradas para clientes e para se juntarem ao grupo 224.10.10.10.

O exemplo a seguir explica várias manipulações, examina o que o Switch faz e a saída resultante. No exemplo a seguir, *Switch_B é um Catalyst 5500 que executa a espionagem de IGMP e Router_A é o roteador multicast conectado à porta 3/1.*

1. Ative o rastreamento IGMP no switch e veja o resultado emitindo o comando **debug** comando. Observe que cada conjunto de entradas foi adicionado ao **show cam sys** saída do comando, permitindo a detecção da porta do roteador através de PIM, MOSPF e assim por diante.

```
Switch_B (enable)  set igmp en

MCAST-IGMP: Set Sys Entries
MCAST-SYS-ENTRIES: Add system Entries in vlan 1
MCAST-IGMP: Set Sys Entries
MCAST-SYS-ENTRIES: Add system Entries in vlan 2
MCAST-IGMP: Set Sys Entries
MCAST-SYS-ENTRIES: Add system Entries in vlan 3

IGMP feature for IP multicast enabled

Switch_B (enable) show cam sys
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN  Dest MAC/Route Des [CoS]  Destination Ports or VCs / [Protocol Type]
----  ----------------- -----  -------------------------------------------
1     00-10-2f-00-14-00  #          7/1
1     00-e0-fe-4b-f3-ff  #          1/9
1     01-00-0c-cc-cc-cc  #          1/9
1     01-00-0c-cc-cc-cd  #          1/9
1     01-00-0c-dd-dd-dd  #          1/9
1     01-00-0c-ee-ee-ee  #          1/9
1     01-00-5e-00-00-01  #          1/9
1     01-00-5e-00-00-04  #          1/9
1     01-00-5e-00-00-05  #          1/9
1     01-00-5e-00-00-06  #          1/9
1     01-00-5e-00-00-0d  #          1/9
1     01-80-c2-00-00-00  #          1/9
1     01-80-c2-00-00-01  #          1/9
2     00-10-2f-00-14-00  #          7/1
2     01-00-0c-cc-cc-cc  #          1/9
2     01-00-0c-cc-cc-cd  #          1/9
2     01-00-0c-dd-dd-dd  #          1/9
2     01-00-5e-00-00-01  #          1/9
2     01-00-5e-00-00-04  #          1/9
2     01-00-5e-00-00-05  #          1/9
```

```
2     01-00-5e-00-00-06  #          1/9
2     01-00-5e-00-00-0d  #          1/9
```

2. O switch recebe um pacote PIMv2 do roteador Router_A e adiciona a porta de roteador.

```
MCAST-IGMPQ:recvd a PIM V2 packet of type HELLO on the port 3/1 vlanNo 2
MCAST-ROUTER: Adding port 3/1, vlanNo 2
MCAST-ROUTER: Creating RouterPortTimer for  port 3/1, vlanNo 2
MCAST-IGMPQ:recvd a PIM V2 packet of type HELLO on the port 3/1 vlanNo 3
MCAST-ROUTER: Adding port 3/1, vlanNo 3
MCAST-ROUTER: Creating RouterPortTimer for  port 3/1, vlanNo 3

Switch_B (enable) show multi router
CGMP disabled
IGMP enabled

Port       Vlan
---------  ----------------
 3/1       2-3

Total Number of Entries = 1
'*' - Configured
Switch_B (enable)
```

3. Conecte um novo host no grupo 224.10.10.10 (na porta 3/2). Esse host envia um relatórios de associação de IGMP. O relatório é recebido e espionado pelo switch, a entrada é adicionada e o relatório de IGMP é enviado para o roteador.Em Switch_B

```
MCAST-IGMPQ:recvd an IGMP V2 Report on the port 3/2 vlanNo 3
      GDA 224.10.10.10
MCAST-RELAY:Relaying packet on port 3/1 vlanNo 3
MCAST-SEND: Inband Transmit Succeeded for IGMP RELAY msg on port 3/1
      vlanNo 3

Switch_B (enable) show cam static
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN  Dest MAC/Route Des [CoS] Destination Ports or VCs / [Protocol Type]
----  ------------------ ----- -------------------------------------------
3     01-00-5e-0a-0a-0a         3/1-2
```

4. Adicione mais um usuário na VLAN 3 na porta 3/3, conforme mostrado abaixo.

```
Switch_B (enable) show cam static

  * = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.

  X = Port Security Entry

  VLAN Dest MAC/Route Des [CoS] Destination Ports or VCs / [Protocol Type]
  ---- ------------------ ----- -------------------------------------------
  3    01-00-5e-0a-0a-0a         3/1-3
```

5. Remova a porta 3/2. A porta 3/2 envia uma mensagem de IGMP Leave; o switch envia de volta uma consulta específica de grupo IGMP na porta 3/2 e inicia um temporizador. Quando o temporizador expira sem receber uma resposta, ele exclui a porta do grupo.

```
MCAST-IGMPQ:recvd an IGMP Leave on the port 3/2 vlanNo 3 GDA 224.10.10.10
MCAST-IGMPQ-LEAVE:router_port_tbl[vlanNo].QueryTime = 0
```

```
MCAST-DEL-TIMER: Deletion Timer Value set to Random Value  1
MCAST-SEND:Transmitting IGMP Mac Based GS Query msg on port 3/2 vlanNo 3
MCAST-SEND:  Transmit Succeeded for IGMP Group Specific Query msg on port 3/2 vlanNo 3
MCAST-TIMER:IGMPLeaveTimer expired on port 3/2 vlanNo 3 GDA 01-00-5e-0a-0a-0a
MCAST-TIMER:IGMPLeaveTimer:delete leave timer


Switch_B (enable) show cam static
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN Dest MAC/Route Des [CoS] Destination Ports or VCs / [Protocol Type]
---- ------------------ ----- -------------------------------------------
3    01-00-5e-0a-0a-0a         3/1,3/3
```

6. O host na porta 3/3 sai o grupo e envia uma mensagem de IGMP Leave. A única diferença do ponto anterior é que a mensagem de IGMP Leave é finalmente encaminhada para porta do roteador.

```
MCAST-IGMPQ:recvd an IGMP Leave on the port 3/3 vlanNo 3 GDA 224.10.10.10
MCAST-SEND:Transmitting IGMP Mac Based GS Query msg on port 3/3 vlanNo 3
MCAST-SEND:  Transmit Succeeded for IGMP Group Specific Query msg on
             port 3/3 vlanNo 3
MCAST-TIMER:IGMPLeaveTimer expired on port 3/3 vlanNo 3 GDA
             01-00-5e-0a-0a-0a
MCAST-TIMER:IGMPLeaveTimer expiry: Transmit IGMP Leave on port 3/1
             vlanNo 3
MCAST-SEND:Transmitting IGMP Leave msg on port 3/1 vlanNo 3
MCAST-SEND: Inband Transmit Succeeded for IGMP Leave Message on port 3/1
             vlanNo 3
MCAST-TIMER:IGMPLeaveTimer:delete leave timer
```

A configuração da sub-rede agora voltou para o início, seu estado no Passo 1. A entrada multicast desapareceu do **show cam static** Saída do comando.

Para concluir, veja um exemplo de **show igmp static** saída do comando, conforme mostrado abaixo.

```
Switch_B (enable) show igmp stat 2
IGMP enabled

IGMP statistics for vlan 2:
Total valid pkts rcvd:           329
Total invalid pkts recvd         0
General Queries recvd            82
Group Specific Queries recvd     0
MAC-Based General Queries recvd  0
Leaves recvd                     0
Reports recvd                    82
Queries  Xmitted                 0
GS Queries Xmitted               0
Reports Xmitted                  0
Leaves Xmitted                   0
Failures to add GDA to EARL      0
Topology Notifications rcvd      0

Switch_B (enable) show igmp stat 3
IGMP enabled

IGMP statistics for vlan 3:
```

```
Total valid pkts rcvd:           360
Total invalid pkts recvd         0
General Queries recvd            93
Group Specific Queries recvd     6
MAC-Based General Queries recvd  0
Leaves recvd                     11
Reports recvd                    64
Queries  Xmitted                 0
GS Queries Xmitted               14
Reports Xmitted                  0
Leaves Xmitted                   10
Failures to add GDA to EARL      0
Topology Notifications rcvd      1
Switch_B (enable)
```

Informações Relacionadas

- Matriz de suporte de Switches de transmissão múltipla Catalyst
- Página de Suporte ao Multicast IP
- Suporte à Tecnologia Cisco
- suporte ao produto Cisco
- Suporte Técnico e Documentação - Cisco Systems