

Configurar rastreamento IGMP em switches CBS220 Series

Objetivo

O objetivo deste documento é mostrar a você como configurar o Internet Group Management Protocol (IGMP) Snooping nos Cisco Business 220 Series Switches.

Dispositivos aplicáveis | Versão do software

- Série CBS220 ([Data Sheet](#)) | 2.0.0.17

Introduction

Multicast é a técnica da camada de rede usada para transmitir pacotes de dados de um host para hosts selecionados na rede. Na camada inferior, o switch transmite o tráfego multicast em todas as portas, mesmo que apenas um host precise recebê-lo. A espionagem do Internet Group Management Protocol (IGMP) é usada para encaminhar o tráfego multicast do Internet Protocol versão 4 (IPv4) para o host desejado.

Quando o IGMP está ativado, ele detecta as mensagens IGMP trocadas entre o roteador IPv4 e os hosts multicast conectados às interfaces. Em seguida, ele mantém uma tabela que restringe o tráfego multicast IPv4 e os encaminha dinamicamente às partes que precisam recebê-los.

As seguintes configurações são pré-requisitos para a configuração do IGMP:

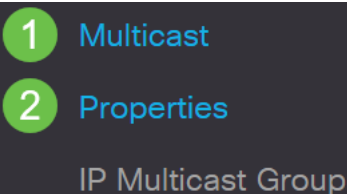
- [Configurar rede local virtual \(VLAN\)](#)
- Ativar a filtragem multicast de ponte (etapas mostradas na próxima seção)

Habilitar rastreamento IGMP e ação multicast

Para que o IGMP Snooping funcione, a filtragem Multicast de Bridge deve estar habilitada. O IGMP Snooping deve ser ativado globalmente e para cada VLAN relevante na página IGMP Snooping.

Passo 1

Faça login no utilitário de configuração da Web e escolha **Multicast > Properties**.



Passo 2

Verifique se o IGMP Snooping está ativado. Selecione o procedimento para *Ação multicast desconhecida*. As opções são *Drop*, *Flood* ou *Forward to Router Port*.

Properties

IGMP Snooping:	<input checked="" type="checkbox"/> Enable
MLD Snooping:	<input type="checkbox"/> Enable

Unknown Multicast Action:	<input type="radio"/> Drop
	<input checked="" type="radio"/> Flood
	<input type="radio"/> Forward to Router Port

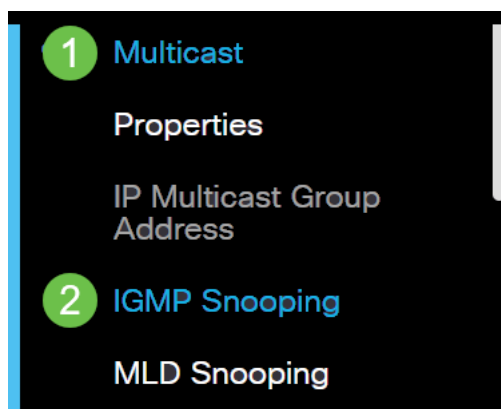
Etapa 3

Clique em Apply.

Configurar rastreamento IGMP

Passo 1

Faça login no utilitário baseado na Web e escolha **Multicast > IGMP Snooping**.



Passo 2

Selecione o botão de opção para a versão IGMP que você deseja usar. Suas opções são IGMPv2 ou IGMPv3.

A supressão de relatório está ativada por padrão. Se você desabilitar esse recurso, todos os relatórios IGMP serão encaminhados para roteadores Multicast.

A supressão de relatórios IGMP só é suportada quando a consulta Multicast tem relatórios

IGMPv1 e IGMPv2. Este recurso não é suportado quando a consulta inclui relatórios IGMPv3. O switch usa a supressão de relatório IGMP para encaminhar apenas um relatório IGMP por consulta de roteador Multicast para dispositivos Multicast. Quando a supressão de relatórios IGMP está ativada, o switch envia o primeiro relatório IGMP de todos os hosts de um grupo para todos os roteadores Multicast. O switch não envia os relatórios IGMP restantes para o grupo aos roteadores Multicast. Este recurso evita que relatórios duplicados sejam enviados aos dispositivos Multicast. O switch sempre encaminha somente o primeiro relatório IGMPv1 ou IGMPv2 de todos os hosts de um grupo para todos os roteadores Multicast, independentemente da consulta do roteador Multicast também inclui solicitações para relatórios IGMPv3.

IGMP Snooping

IGMP Snooping Version: IGMPv2

IGMPv3

Report Suppression: Enable

Etapa 3

Selecione uma VLAN e clique no ícone de edição.

IGMP Snooping Table



2

Entry No. VLAN ID IGMP Snooping Operational Status

1 1 Disabled

1 2 2 Disabled

Passo 4

Marque a caixa de seleção Enable (Habilitar) para *IGMP Snooping Status (Status de rastreamento IGMP)*. Isso ativará o rastreamento IGMP na VLAN. O dispositivo monitora o tráfego de rede para determinar quais hosts pediram para enviar o tráfego Multicast.

VLAN ID:

2

IGMP Snooping Status:

Enable

Etapa 5 (opcional)

Para permitir que o roteador multicast aprenda automaticamente as portas conectadas, marque a caixa de seleção Enable (Habilitar) para *MRouter Ports Auto*

Learn (Aprendizado automático das portas externas MR).

VLAN ID: ▾

IGMP Snooping Status: Enable

MRouter Ports Auto Learn: Enable

Etapa 6

Consulta robusta - Insira a variável robustez a ser usada se esse switch for o consultado.

VLAN ID: ▾

IGMP Snooping Status: Enable

MRouter Ports Auto Learn: Enable

Query Robustness: (Range: 1 - 7, Default: 2)

Etapa 7

Intervalo de consulta - Insira o intervalo entre as consultas gerais a serem usadas se esse switch for o consultante escolhido.

Query Robustness: (Range: 1 - 7, Default: 2)

Query Interval: sec (Range: 30 - 18000, Default: 125)

Passo 8

Intervalo de resposta máxima da consulta - Insira o atraso usado para calcular o código de resposta máxima inserido nas consultas gerais periódicas.

MRouter Ports Auto Learn: Enable

Query Robustness: (Range: 1 - 7, Default: 2)

Query Interval: sec (Range: 30 - 18000, Default: 125)

Query Max Response Interval: sec (Range: 5 - 20, Default: 10)

Passo 9

Contador de Consulta do Último Membro - O número de consultas específicas de grupo IGMP enviadas antes do dispositivo assumir que não há mais membros para o grupo se o dispositivo for o consultante eleito.

MRouter Ports Auto Learn: Enable

✳ Query Robustness: (Range: 1 - 7, Default: 2)

✳ Query Interval: sec (Range: 30 - 18000, Default: 125)

✳ Query Max Response Interval: sec (Range: 5 - 20, Default: 10)

✳ Last Member Query Counter: (Range: 1 - 7, Default: 2)

Passo 10

Último intervalo de consulta do membro - Insira o atraso máximo de resposta a ser usado se o switch não puder ler o valor máximo do tempo de resposta das consultas específicas do grupo enviadas pelo pesquisador eleito.

MRouter Ports Auto Learn: Enable

✳ Query Robustness: (Range: 1 - 7, Default: 2)

✳ Query Interval: sec (Range: 30 - 18000, Default: 125)

✳ Query Max Response Interval: sec (Range: 5 - 20, Default: 10)

✳ Last Member Query Counter: (Range: 1 - 7, Default: 2)

✳ Last Member Query Interval: sec (Range: 1 - 25, Default: 1)

Passo 11

Immediate Leave - Selecione para permitir que o switch remova uma interface que envia uma mensagem de saída da tabela de encaminhamento sem primeiro enviar consultas gerais baseadas em MAC para a interface. Quando a mensagem Immediate Leave an IGMP Leave Group é recebida de um host, o sistema remove a porta do host da entrada da tabela. Depois de retransmitir as consultas IGMP do roteador Multicast, ele exclui entradas periodicamente se não recebe nenhum relatório de associação IGMP dos clientes Multicast. Quando habilitado, esse recurso reduz o tempo necessário para bloquear o tráfego IGMP desnecessário enviado a uma porta do dispositivo.

MRouter Ports Auto Learn: Enable

✱ Query Robustness: (Range: 1 - 7, Default: 2)

✱ Query Interval: sec (Range: 30 - 18000, Default: 125)

✱ Query Max Response Interval: sec (Range: 5 - 20, Default: 10)

✱ Last Member Query Counter: (Range: 1 - 7, Default: 2)

✱ Last Member Query Interval: sec (Range: 1 - 25, Default: 1)

Immediate Leave: Enable

Etapa 12 (Opcional)

IGMP Querier Status - Selecione para habilitar este recurso. Esse recurso é necessário se não houver roteador Multicast.

MRouter Ports Auto Learn: Enable

✱ Query Robustness: (Range: 1 - 7, Default: 2)

✱ Query Interval: sec (Range: 30 - 18000, Default: 125)

✱ Query Max Response Interval: sec (Range: 5 - 20, Default: 10)

✱ Last Member Query Counter: (Range: 1 - 7, Default: 2)

✱ Last Member Query Interval: sec (Range: 1 - 25, Default: 1)

Immediate Leave: Enable

IGMP Querier Status: Enable

Passo 13

IGMP Querier Version - (Versão do questionário IGMP) Selecione a versão IGMP a ser usada se o dispositivo se tornar o consultado. Selecione IGMPv3 se houver switches e/ou roteadores Multicast na VLAN que executam o encaminhamento Multicast IP específico da origem. Caso contrário, selecione IGMPv2.

Neste exemplo, a versão 2 é escolhida. Permite que a consulta de associação seja geral e específica do grupo. A Consulta de Associação geral é usada para determinar todos os grupos de multicast aos quais as estações estão assinadas. A Consulta de associação específica do grupo é usada para determinar se há um assinante para um grupo específico.

MRouter Ports Auto Learn: Enable

✱ Query Robustness: (Range: 1 - 7, Default: 2)

✱ Query Interval: sec (Range: 30 - 18000, Default: 125)

✱ Query Max Response Interval: sec (Range: 5 - 20, Default: 10)

✱ Last Member Query Counter: (Range: 1 - 7, Default: 2)

✱ Last Member Query Interval: sec (Range: 1 - 25, Default: 1)

Immediate Leave: Enable

IGMP Querier Status: Enable

IGMP Querier Version: IGMPv2
 IGMPv3

Passo 14

Clique em Apply. O arquivo de configuração atual é atualizado.


Apply

Close

As alterações na configuração do temporizador de rastreamento IGMP (incluindo robustez da consulta, intervalo de consulta etc.) não têm efeito nos temporizadores já criados.

Etapa 15

Para salvar essa configuração da configuração atual para a configuração de inicialização, clique no **ícone salvar** no canto superior direito da tela.

 admin(Switch...) ▾

Conclusão

É tão simples quanto isso, agora você configurou o IGMP Snooping.

Para obter mais configurações, consulte o [Guia de Administração dos Switches Cisco Business 220 Series](#).

Se quiser ver mais artigos sobre os switches CBS220, consulte a [página de suporte da 220 Series](#).