O Multicast não trabalha no mesmo VLAN nos Catalyst Switches

Índice

Introdução

Este documento discute um problema comum que ocorre na implantação de um aplicativo multicast pela primeira vez em uma rede de switch Cisco Catalyst e o multicast não funciona. Além disso, alguns servidores/aplicativos que usam pacotes multicast para uma operação de cluster/alta disponibilidade podem não funcionar caso os switches não sejam configurados adequadamente. O documento também abrange esse problema.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Catalyst 6500 com Supervisor Engine 720 que executa o Software Release 12.2(18)SXD5 de Cisco IOS®
- Catalizador 3750 que executa uma imagem do Cisco IOS Software Release 12.2(25)SEB2

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Produtos Relacionados

Este documento pode igualmente ser usado com estes versão de hardware e software:

- Algum Catalyst Switch que executa um Cisco IOS Software Release que apoie a verificação do Protocolo de Gerenciamento do Grupo da Internet (IGMP)**Nota:** Refira a seção da *Matriz de Suporte de Catalyst Switch de Recurso de Espionagem IGMP da* matriz de suporte dos Catalyst Switches do Multicast do documento a fim identificar este Switches.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Problema

O tráfego multicast não parece passar através dos Catalyst Switches, mesmo no mesmo VLAN. Figura 1 descreve um cenário típico:

Figura 1 – Instalação de rede com origem de transmissão múltipla e receptores

O origem de transmissão múltipla é conectado a Switch1, que é um Catalyst 6500 Switch com Supervisor Engine 720 que execute o Cisco IOS Software. O receptor 1 é conectado a Switch1, e o receptor 2 é conectado para comutar 2. Switch2 é um catalizador 3750. Há um link da camada 2, acesso ou tronco, entre Switch1 e Switch2.

Nesta instalação, você encontra esse receptor 1, que está no mesmo interruptor que a fonte, obtém o fluxo de transmissão múltipla sem problemas. Contudo, o receptor 2 não obtém nenhum tráfego multicast. Este documento aponta resolver esta edição.

Revisite alguns conceitos chaves do Multicast

Antes que você explore a solução e as opções que diferentes você tem, você deve ser claro em determinados conceitos chaves do Multicast da camada 2. Esta seção define estes conceitos.

Nota: Esta seção fornece uma explicação muito simples e direta essa focos somente nesta questão particular. Veja a seção Informação Relacionada deste documento para mais explicação

detalhada destes termos.

IGMP

O IGMP é um protocolo que permita host finais (receptores) de informar um Multicast Router (IGMP mais investigado) da intenção do host final receber o tráfego multicast particular. Assim este é um protocolo que as corridas entre um roteador e host finais e permitam:

- Roteadores para pedir host finais se precisam um fluxo de transmissão múltipla particular (pergunta IGMP)
- Host finais a dizer ou responder ao roteador se procuram um fluxo de transmissão múltipla particular (relatórios IGMP)

Espionagem de IGMP

O IGMP Snooping é um mecanismo para forçar o tráfego multicast somente às portas que têm os receptores anexados. O mecanismo adiciona a eficiência porque permite um switch de Camada 2 de mandar seletivamente pacotes de transmissão múltipla somente nas portas que as precisam. Sem IGMP Snooping, o interruptor inunda os pacotes em cada porta. O interruptor “escuta” a troca dos mensagens IGMP pelo roteador e pelos host finais. Desta maneira, o interruptor constrói uma tabela do IGMP Snooping que tenha uma lista de todas as portas que pediram um grupo de transmissão múltipla particular.

Porta do mrouter

A porta do mrouter é simplesmente a porta do ponto de vista do interruptor que conecta a um Multicast Router. A presença pelo menos de uma porta do mrouter é absolutamente essencial para que a operação do IGMP Snooping trabalhe através do Switches. A compreensão o problema e suas soluções seciona deste documento discute esta exigência com maiores detalhes.

Multicast no L2

Todo o tráfego da versão IP 4 (IPv4) com um IP de destino na escala de 224.0.0.0 a 239.255.255.255 é um fluxo de transmissão múltipla. Todos os pacotes de transmissão múltipla do IPv4 traçam a um MAC address predefinido da IEEE que tenha o formato 01.00.5e.xx.xx.xx.

Nota: O IGMP Snooping trabalha somente se os mapas de endereço MAC de transmissão múltipla a este MAC Ieee-complacente variam. Algumas escalas reservados do Multicast são excluídas de ser snooped pelo projeto. Se um pacote de transmissão múltipla nonconforming é originado em uma rede comutada, o pacote está inundado durante todo esse VLAN, assim que significa que está tratado como o tráfego de broadcast.

Compreenda o problema e suas soluções

Àrevelia, os Catalyst Switches têm o IGMP Snooping permitido. Com IGMP Snooping, as espiões do interruptor (ou escuta) para mensagens IGMP em todas as portas. O interruptor constrói uma tabela do IGMP Snooping que trace basicamente um grupo de transmissão múltipla a todas as portas de switch que o pediram.

Supõe que, sem nenhuma configuração anterior, o receptor 1 e o receptor 2 sinalizaram suas intenções receber um fluxo de transmissão múltipla para 239.239.239.239 esse mapas ao endereço MAC de transmissão múltipla L2 de 01.00.5e.6f.ef.ef. Switch1 e Switch2 criam uma entrada em suas tabelas da espião para estes receptores em resposta ao IGMP relatam que os receptores gerenciem. Switch1 entra nas portas de Ethernet em gigabit 2/48 em sua tabela, e Switch2 inscreve o Fast Ethernet 1/0/47 da porta em sua tabela.

Nota: Neste momento, o origem de transmissão múltipla não começou seu tráfego, e nenhum do Switches sabe sobre a porta do mrouter do interruptor.

Quando a fonte em Switch1 começa fluir o tráfego multicast, Switch1 “viu” o relatório IGMP do receptor 1. em consequência, Switch1 entrega as portas de Ethernet em gigabit 2/48 do Multicast para fora. Mas, desde que Switch2 “absorvido” o relatório IGMP do receptor 2 como parte do processo do IGMP Snooping, Switch1 não vê um relatório IGMP (solicitação multicast) nas portas de Ethernet em gigabit 2/46. Em consequência, Switch1 não envia nenhum tráfego multicast para fora a Switch2. Consequentemente, o receptor 2 nunca obtém todo o tráfego multicast, mesmo que o receptor 2 esteja no mesmo VLAN mas meramente em um interruptor diferente do que o origem de transmissão múltipla.

A razão para esta edição é que o IGMP Snooping não está apoiado realmente em nenhuma plataforma do Catalyst sem um mrouter. O mecanismo “divide” na ausência de uma porta do mrouter. Se você quer um reparo para esta solução, você deve mandar o Switches de algum modo aprender ou saber de uma porta do mrouter. A seção das soluções deste documento explica o procedimento. Mas como a presença de uma porta do mrouter no Switches remedeia a situação?

Basicamente, quando o Switches aprende ou sabe estaticamente sobre uma porta do mrouter, duas coisas críticas ocorrem:

- O interruptor “retransmite” os relatórios IGMP dos receptores à porta do mrouter, assim que significa que os relatórios IGMP vão para o Multicast Router. O interruptor não retransmite todos os relatórios IGMP. Em lugar de, o interruptor envia somente alguns dos relatórios ao mrouter. Com a finalidade desta discussão, o número de relatórios não é importante. As necessidades do Multicast Router somente de saber se há pelo menos um receptor que está interessado ainda no Multicast rio abaixo. A fim fazer a determinação, o Multicast Router recebe os relatórios periódicos IGMP em resposta a suas perguntas IGMP.
- Em uma encenação do Multicast da fonte-somente, em que nenhum receptor tem ainda “juntou-se” dentro, o interruptor envia somente ao fluxo de transmissão múltipla para fora sua porta do mrouter.

Quando o Switches conhece sua porta do mrouter, Switch2 retransmite para fora o relatório IGMP que o interruptor recebeu do receptor 2 a sua porta do mrouter. Esta porta é o Fast Ethernet 1/0/33. Switch1 obtém este relatório IGMP no Gigabit Ethernet 2/46 da porta de switch. Da perspectiva de Switch1, o interruptor recebeu um meramente outro relatório IGMP. O interruptor adiciona que porta em sua tabela do IGMP Snooping e começa a mandar também o tráfego multicast nessa porta. Neste momento, ambos os receptores recebem o tráfego multicast pedido, e o aplicativo trabalha como esperado.

Mas como o Switches identifica sua porta do mrouter de modo que o IGMP Snooping trabalhe enquanto se espera trabalhar em um ambiente simples como este? A seção das soluções dá algumas respostas.

Soluções

Use estas soluções para resolver o problema.

Solução 1: Permita o PIM na relação da camada 3 Router/VLAN

Todas as plataformas do Catalyst têm a capacidade para aprender dinamicamente sobre a porta do mrouter. O Switches escuta passivamente os hellos da transmissão múltipla independente de protocolo (PIM) ou os mensagens de consulta de IGMP que um Multicast Router manda periodicamente.

Este exemplo configura o Switched Virtual Interface VLAN1 (SVI) no Catalyst 6500 com `sparse-dense-mode do pim IP`.

```
Switch1#show run interface vlan 1 ! interface Vlan1  ip address 1.1.1.1 255.255.255.0  ip pim
sparse-dense-mode end Switch 1 now reflects itself (Actually the internal router port) as an
Mrouter port. Switch1#show ip igmp snooping mrouter vlan            ports -----+---------------
-----------------------    1  Router Switch 2 receives the same PIM hellos on its Fa 1/0/33
interface. So it assigns that port as its Mrouter port. Switch2#show ip igmp snooping mrouter
Vlan    ports ----    -----    1    Fa1/0/33(dynamic)
```

Solução 2: Permita a característica do IGMP mais investigado em um Catalyst Switch da camada 2

O IGMP mais investigado é relativamente uns novos recursos em switch de Camada 2. Quando um network/VLAN não tem um roteador que possa tomar no papel do Multicast Router e fornecer a descoberta de roteador m no Switches, você pode girar sobre a característica do IGMP mais investigado. A característica permite o switch de Camada 2 ao proxy para um Multicast Router e manda perguntas periódicas IGMP nessa rede. Esta ação faz com que o interruptor considere-se uma porta do mrouter. Os switch remanescente na rede definem simplesmente suas portas respectivas do mrouter como a relação em que receberam esta pergunta IGMP.

```
Switch2(config)#ip igmp snooping querier Switch2#show ip igmp snooping querier Vlan      IP
Address     IGMP Version   Port               ------------------------------------------------
---------- 1         1.1.1.2        v2             Switch
```

Switch1 vê agora a atuação 2/46 da porta ligar a Switch2 como uma porta do mrouter.

```
Switch1#show ip igmp snooping mrouter vlan            ports -----+------------------------------
----------    1  Gi2/46
```

Quando a fonte em Switch1 começar fluir o tráfego multicast, Switch1 para a frente que o tráfego multicast ao receptor 1 encontrou através do IGMP Snooping (isto é, mova para fora a atuação 2/48) e à porta do mrouter (isto é, mova para fora a atuação 2/46).

Solução 3: Configurar a porta estática do mrouter no interruptor

O tráfego multicast falha dentro da mesma camada 2 VLAN devido à falta de uma porta do mrouter no Switches, porque a compreensão o problema e sua seção das soluções discute. Se você configura estaticamente uma porta do mrouter em todo o Switches, os relatórios IGMP podem ser retransmitidos nesse VLAN a todo o Switches. Em consequência, multicasting é possível. Assim, no exemplo, você deve estaticamente configurar o Catalyst 3750 Switch para ter o Fast Ethernet 1/0/33 como uma porta do mrouter.

Neste exemplo, você precisa uma porta estática do mrouter em Switch2 somente:

```
Switch2(config)#ip igmp snooping vlan 1 mrouter interface fastethernet 1/0/33 Switch2#show ip
igmp snooping mrouter Vlan    ports ----    -----    1    Fa1/0/33(static)
```

Solução 4: Configurar entradas de MAC estáticas do Multicast em todo o Switches

Você pode fazer uma entrada estática da memória de conteúdo endereçável (CAM) para o endereço MAC de transmissão múltipla em todo o Switches para todas as portas do receptor *e as* portas de switch a jusante. Todo o interruptor obedece as regras da entrada de CAM estática e envia ao pacote para fora todas as relações que são especificadas na tabela CAM. Esta é a solução menos-escalável para um ambiente que tenha muitos aplicativos multicast.

```
Switch1(config)#mac-address-table static 0100.5e6f.efef vlan 1 interface gigabitethernet 2/46
gigabitethernet 2/48 !--- Note: This command should be on one line. Switch1#show mac-address-
table multicast vlan 1  vlan   mac address     type   learn qos             ports -----+--------
-------+--------+-----+---+--------------------------------    1  0100.5e6f.efef    static
Yes          -   Gi2/46,Gi2/48 Switch2(config)#mac-address-table static 0100.5e6f.efef vlan 1
interface fastethernet 1/0/47 !--- Note: This command should be on one line. Switch2#show mac-
address-table multicast vlan 1 Vlan    Mac Address       Type       Ports ----    -----------
       ----       -----    1    0100.5e6f.efef    USER        Fa1/0/47
```

Solução 5: IGMP Snooping do desabilitação em todo o Switches

Se você desabilita o IGMP Snooping, todo o Switches trata o tráfego multicast como um tráfego de broadcast. Isto inunda o tráfego a *todas as* portas nesse VLAN, apesar de se as portas interessaram receptores para esse fluxo de transmissão múltipla.

```
Switch1(config)#no ip igmp snooping Switch2(config)#no ip igmp snooping
```

Informações Relacionadas

- Transmissão múltipla em uma rede de campus: Espionagem de CGMP e IGMP
- Matriz de suporte de Switches de transmissão múltipla Catalyst
- Página de Suporte ao Multicast IP
- Protocolo IP multicast que pesquisa defeitos TechNotes
- Manual de Troubleshooting de IP Multicast
- Páginas de Suporte de Produtos de LAN
- Página de suporte da switching de LAN
- Suporte Técnico e Documentação - Cisco Systems