Problemen met multicast verkeer oplossen in hetzelfde VLAN op Catalyst Switches

Inhoud

Inleiding

Dit document beschrijft hoe u een multicast toepassingsfout kunt verhelpen wanneer deze in hetzelfde VLAN tussen Catalyst-switches wordt geïmplementeerd.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Catalyst 6500 met Supervisor Engine 720 waarop Cisco IOS®-softwarerelease 12.2(18)SXD5 wordt uitgevoerd
- Catalyst 3750 Series met een Cisco IOS-softwarerelease 12.2(25)SEB2-afbeelding

- Elke Catalyst switch die een Cisco IOS-softwarerelease uitvoert en ook ondersteuning biedt voor IGMP-snooping (Internet Group Management Protocol)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Achtergrondinformatie

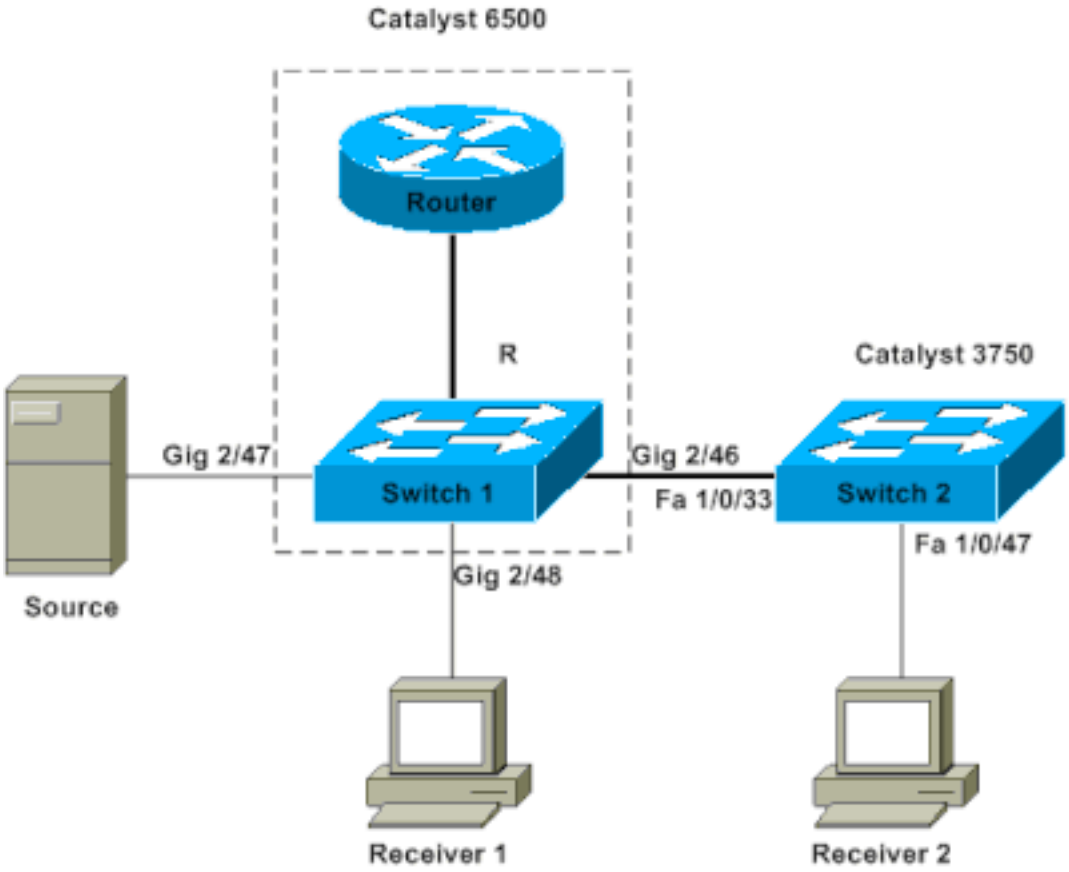
Bovendien kunnen sommige servers/toepassingen die multicastpakketten gebruiken voor de cluster/high-Availability-bewerking niet werken als u de switches niet goed configureert. Dit wordt ook in dit artikel behandeld.

> **Opmerking**: raadpleeg de sectie *IGMP Snooping Feature Catalyst Switch Support Matrix* van de ondersteunende matrix voor Switches van Multicast Catalyst om deze switches te helpen identificeren.

Probleem

Multicastverkeer gaat niet over Catalyst-switches, zelfs niet in hetzelfde VLAN.Afbeelding 1 toont een dergelijk scenario.

Afbeelding 1 - Network Setup met multicast bronnen en ontvangers



Netwerkdiagram

De multicast bron is verbonden met Switch 1, die een Catalyst 6500 Switch met Supervisor Engine 720 is die Cisco IOS-software draait. Ontvanger 1 is aangesloten op Switch 1 en ontvanger 2 op Switch 2. Switch 2 is een Catalyst 3750. Er is een Layer 2-koppeling, toegang of trunk, tussen Switch 1 en Switch 2.

In deze opstelling, vindt u dat Ontvanger 1, die op de zelfde switch zoals de bron is, de multicast stroom zonder problemen krijgt. Ontvanger 2 *krijgt* echter geen multicastverkeer. Dit document is bedoeld om deze kwestie op te lossen.

Belangrijke multicastconcepten opnieuw bekijken

Alvorens u de oplossing en de verschillende opties onderzoekt die u hebt, moet u duidelijk zijn over bepaalde belangrijke concepten van Layer 2 multicast. In deze paragraaf worden deze begrippen gedefinieerd.

> **Opmerking**: in dit gedeelte wordt een zeer eenvoudige en directe uitleg gegeven die alleen over dit specifieke onderwerp gaat. Zie het gedeelte **Verwante informatie** aan het eind van dit document voor een gedetailleerde uitleg van deze bepalingen.

IGMP

IGMP is een protocol dat eindhosts (ontvangers) in staat stelt een multicast router (IGMP-query) te informeren over de intentie van de eindhost om bepaald multicast verkeer te ontvangen. Dit is dus een protocol dat tussen een router en eindhosts loopt en het volgende toestaat:

- Routers om eindhosts te vragen of ze een bepaalde multicast stream (IGMP-query) nodig

hebben
- Eindhosts om de router te informeren of erop te reageren als zij een bepaalde multicast-stroom zoeken (IGMP-rapporten)

IGMP-controle

IGMP-spionage is een mechanisme om multicast-verkeer te beperken tot alleen de poorten waaraan ontvangers zijn gekoppeld. Het mechanisme voegt efficiëntie toe omdat het een Layer 2-switch in staat stelt om selectief multicastpakketten op alleen de poorten die ze nodig hebben te sturen. Zonder IGMP-snooping overspoelt de switch de pakketten op elke poort. De switch "luistert" naar de uitwisseling van IGMP-berichten door de router en de eindhosts. Op deze manier maakt de switch een IGMP-spionagetabel met een lijst van alle poorten die om een bepaalde multicast groep hebben gevraagd.

Mrouter-poort

De routerpoort is simpelweg de poort vanuit het oogpunt van de switch die verbinding maakt met een multicast router. De aanwezigheid van ten minste één routerpoort is absoluut noodzakelijk voor de IGMP-spionagefunctie om over switches te werken. Zie de sectie Het probleem en zijn oplossingen van dit document voor meer informatie.

Multicast op L2

Een IP versie 4 (IPv4)-verkeer met een IP-bestemming in het bereik van 224.0.0.0 tot 239.255.255.255 is een multicaststroom. Alle IPv4 multicast-pakketten worden toegewezen aan een vooraf gedefinieerd IEEE MAC-adres met het formaat 01.00.5e. *xx*. *xx*. *xx* .

> **Opmerking**: IGMP-spionage werkt alleen als het multicast MAC-adres aan dit IEEE-conforme MAC-bereik wordt toegewezen. Sommige gereserveerde multicast reeksen zijn uitgesloten van die gesnooped door ontwerp. Als een niet-conform multicast pakket afkomstig is van een switched netwerk, wordt het pakket overspoeld door dat VLAN, wat betekent dat het wordt behandeld als uitzendingsverkeer.

Het probleem en de oplossingen ervan begrijpen

Standaard zijn IGMP-spionage ingeschakeld voor de Catalyst switches. Met IGMP-spionage snoopt de switch op alle poorten naar IGMP-berichten (of luistert ernaar). De switch bouwt een IGMP spioningstabel die een multicast groep in kaart brengt aan alle switch poorten die om het hebben gevraagd.

Veronderstel dat, zonder enige voorafgaande configuratie, Ontvanger 1 en Ontvanger 2 hun bedoelingen hebben gesignaleerd om een multicast stroom voor 239.239.239.239 te ontvangen die aan het L2 multicast adres van MAC van 01.00.5e.6f.ef.ef in kaart brengt. Zowel Switch 1 als Switch 2 creëren een ingang in hun snoopingstabellen voor deze ontvangers in antwoord op de IGMP-rapporten die de ontvangers genereren. Switch 1 voert poort Gigabit Ethernet 2/48 in in de tabel en Switch 2 voert poort Fast Ethernet 1/0/47 in in de tabel.

> **Opmerking**: op dit punt is de multicast-bron niet met zijn verkeer begonnen en geen van de switches weet van de switch-routerpoort.

Wanneer de bron op Switch 1 multicast verkeer begint te stromen, heeft Switch 1 het IGMP-rapport van ontvanger 1 "gezien". Hierdoor levert Switch 1 de multicast out-poort Gigabit Ethernet 2/48. Maar sinds Switch 2 het IGMP-rapport van ontvanger 2 "heeft geabsorbeerd" als deel van het IGMP-spionageproces, ziet Switch 1 geen IGMP-rapport (multicast-verzoek) op poort Gigabit Ethernet 2/46. Dientengevolge, stuurt Switch 1 geen multicast verkeer uit naar Switch 2. Daarom krijgt ontvanger 2 nooit een multicast verkeer, ook al is ontvanger 2 in hetzelfde VLAN maar alleen op een andere switch dan de multicast bron.

De reden voor dit probleem is dat IGMP-spionage niet echt wordt ondersteund op een Catalyst-platform zonder router. Het mechanisme "defect" bij afwezigheid van een router poort. Als u een oplossing voor deze oplossing wilt, moet u de switches op de een of andere manier leren of kennen van een routerpoort. Zie het gedeelte Oplossingen van dit document voor meer uitleg over de procedure. U moet nog ontdekken hoe de aanwezigheid van een routerpoort op de switches het probleem verhelpen.

Kort gezegd, wanneer de switches leren of statisch weten over een routerpoort, gebeuren er twee cruciale dingen:

- De switch "relayeert" de IGMP-rapporten van de ontvangers naar de routerpoort, wat betekent dat de IGMP-rapporten naar de multicast router gaan. De switch geeft niet alle IGMP-rapporten door. In plaats daarvan stuurt de switch slechts een paar rapporten naar de router. Voor deze discussie is het aantal verslagen niet belangrijk. De multicast router hoeft alleen te weten of er ten minste één ontvanger is die nog steeds geïnteresseerd is in de multicast downstream. Om dit te kunnen bepalen, ontvangt de multicast router de periodieke IGMP-rapporten in antwoord op zijn IGMP-vragen.
- In een bron-enige multicast scenario, waarin nog geen ontvangers "zijn toegetreden" in, de switch verstuurt alleen de multicast stream zijn routerpoort.

Wanneer de switches hun routerhaven kennen, geeft Switch 2 uit het IGMP- rapport dat de switch van Ontvanger 2 aan zijn routerhaven ontving. Deze poort is Fast Ethernet 1/0/33. Switch 1 krijgt dit IGMP-rapport over de switch-poort Gigabit Ethernet 2/46. Vanuit het oogpunt van Switch 1 heeft de switch slechts nog een IGMP-verslag ontvangen. De switch voegt die poort toe aan de IGMP-spionagetabel en begint ook het multicastverkeer op die poort te versturen. Op dit punt, zowel ontvangen de ontvangers het gevraagde multicast verkeer, en de toepassing werkt zoals verwacht.

Om te weten te komen hoe de switches hun routerpoort identificeren zodat IGMP-spionage werkt zoals verwacht wordt te werken in een eenvoudige omgeving, zie de Oplossingen sectie voor antwoorden.

Oplossingen

Gebruik deze oplossingen om het probleem op te lossen.

Oplossing 1: Schakel PIM in op Layer 3 router/VLAN-interface

Alle Catalyst-platforms hebben de mogelijkheid om dynamisch meer te weten te komen over de routerpoort. De switches luisteren passief naar de Protocolonafhankelijke Multicast (PIM)-hellos of naar de IGMP-query-berichten die periodiek door een multicast-router worden verzonden.

In dit voorbeeld wordt de VLAN 1 switched Virtual Interface (SVI) op Catalyst 6500 geconfigureerd

met ip pim sparse-dense-mode .

```
Switch1#show run interface vlan 1
!
interface Vlan1
 ip address 10.1.1.1 255.255.255.0
 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)
```

Oplossing 2: IGMP Querier-functie inschakelen op een Layer 2 Catalyst-Switch

De IGMP querier is een relatief nieuwe functie op Layer 2-switches. Wanneer een netwerk/VLAN geen router heeft die de multicast routerrol kan overnemen en de routerontdekking op de switches kan verstrekken, kunt u de IGMP querierfunctie inschakelen. Met deze functie kan Layer 2-switch een proxy voor een multicast-router aanmaken en periodieke IGMP-vragen in dat netwerk verzenden. Deze actie zorgt ervoor dat de switch zichzelf als een routerpoort beschouwt. De rest van de switches in het netwerk definiëren hun respectievelijke routerpoorten gewoon als de interface waarop ze deze IGMP-query hebben ontvangen.

```
Switch2(config)#ip igmp snooping querier

Switch2#show ip igmp snooping querier
Vlan      IP Address     IGMP Version   Port
-----------------------------------------------------------
1         10.1.1.2        v2             Switch
```

Switch 1 ziet nu dat port Gig 2/46 naar Switch 2 koppelt als een routerpoort.

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

Wanneer de bron op Switch 1 multicast verkeer begint te streamen, door Switch 1 door:sturen het multicast verkeer aan Ontvanger 1 die via IGMP-snooping (namelijk out-poort Gig 2/48) wordt gevonden en aan de invoerrouterpoort (namelijk out-poort Gig 2/46).

Oplossing 3: Configureer de statische routerpoort op de Switch

Het multicast verkeer mislukt binnen dezelfde Layer 2 VLAN als gevolg van het ontbreken van een

routerpoort op de switches, de sectie Begrijp het probleem en de oplossingen ervan behandelt dit onderwerp. Als u een routerpoort op alle switches statisch configureert, kunnen IGMP-rapporten in dat VLAN worden doorgestuurd naar alle switches. Hierdoor is multicasting mogelijk. Zo, in het voorbeeld, moet u de Catalyst 3750 Switch statisch configureren om Fast Ethernet 1/0/33 als een routerpoort te hebben.

In dit voorbeeld hebt u alleen een statische routerpoort op Switch 2 nodig:

```
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)
```

Oplossing 4: Statische multicast MAC-vermeldingen op alle Switches configureren

U kunt een statische content-addressable memory (CAM)-ingang maken voor het multicast MAC-adres op alle switches voor alle ontvangerpoorten en downstream switch-poorten. Elke switch gehoorzaamt de statische CAM-ingangsregels en verstuurt het pakket alle interfaces die in de CAM-tabel zijn gespecificeerd. Dit is de minst schaalbare oplossing voor een omgeving met veel multicast-toepassingen.

```
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
```

Oplossing 5: IGMP-controle op alle Switches uitschakelen

Als u IGMP-spionage uitschakelt, behandelen alle switches multicast verkeer als een uitzendingsverkeer. Dit overspoelt het verkeer naar *alle* poorten in dat VLAN, ongeacht of de poorten geinteresseerde ontvangers hebben voor die multicast stroom.

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

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

Gerelateerde informatie

- Multicast in een Campus-netwerk: CGMP- en IGMP-controle

- Multicast Catalyst Switches-ondersteuningsmatrix
- IP-multicast ondersteuning
- TechNotes voor probleemoplossing met IP-multicast
- Handleiding voor IP-multicast probleemoplossing
- Cisco technische ondersteuning en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.