Behebung von Problemen mit Multicast-Datenverkehr im selben VLAN auf Catalyst-Switches

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie einen Fehler bei einer Multicast-Anwendung beheben, wenn diese im gleichen VLAN zwischen Catalyst-Switches bereitgestellt wird.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Catalyst 6500 mit Supervisor Engine 720, auf der die Cisco IOS® Software Version 12.2(18)SXD5 ausgeführt wird
- Catalyst 3750 mit Cisco IOS Software, Version 12.2(25)SEB2-Image
- Alle Catalyst Switches mit Cisco IOS Software und Unterstützung für IGMP-Snooping (Internet Group Management Protocol)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Hintergrundinformationen

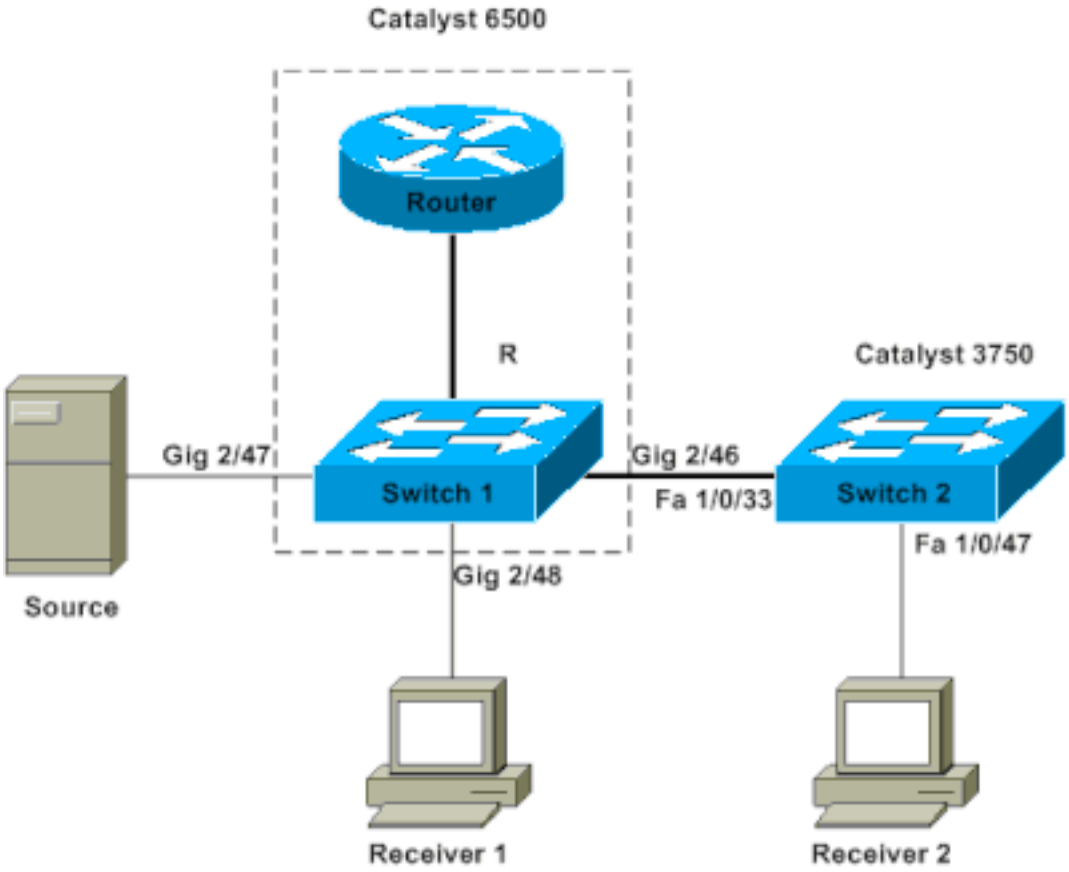
Darüber hinaus können einige Server/Anwendungen, die Multicast-Pakete für den Cluster-/Hochverfügbarkeitsbetrieb verwenden, fehlschlagen, wenn Sie die Switches nicht ordnungsgemäß konfigurieren. Dies wird auch in diesem Artikel behandelt.

> **Hinweis:** Informationen zur Identifizierung dieser Switches finden Sie im Abschnitt *zur Unterstützung* der *IGMP-Snooping-Funktion* der Catalyst Switch-*Unterstützungsmatrix* im Dokument Multicast Catalyst Switches Support Matrix.

Problem

Multicast-Datenverkehr verläuft nicht über Catalyst Switches, selbst nicht im selben VLAN.Abbildung 1 zeigt ein solches Szenario.

Abbildung 1: Netzwerkeinrichtung mit Multicast-Quelle und -Empfängern



Netzwerkdiagramm

Die Multicast-Quelle ist mit Switch 1 verbunden, einem Catalyst Switch der Serie 6500 mit Supervisor Engine 720, auf dem die Cisco IOS Software ausgeführt wird. Der Empfänger 1 ist mit dem Schalter 1 verbunden, und der Empfänger 2 ist mit dem Schalter 2 verbunden. Switch 2 ist ein Catalyst 3750. Zwischen Switch 1 und Switch 2 besteht eine Layer-2-Verbindung, entweder über einen Access-Port oder einen Trunk.

In dieser Konfiguration stellen Sie fest, dass Receiver 1, der sich auf demselben Switch wie die Quelle befindet, den Multicast-Stream problemlos empfängt. Empfänger 2 *erhält* jedoch keinen Multicast-Verkehr. Mit diesem Dokument soll dieses Problem behoben werden.

Wichtige Multicast-Konzepte erneut durchgehen

Bevor Sie sich mit der Lösung und den verschiedenen verfügbaren Optionen vertraut machen, müssen Sie sich über bestimmte Schlüsselkonzepte von Layer-2-Multicast im Klaren sein. In diesem Abschnitt werden diese Konzepte definiert.

> **Hinweis**: Dieser Abschnitt enthält eine sehr einfache und direkte Erklärung, die sich nur auf dieses spezielle Problem konzentriert. Im Abschnitt **Zugehörige Informationen** am Ende dieses Dokuments finden Sie eine ausführliche Erläuterung dieser Begriffe.

IGMP

IGMP ist ein Protokoll, das es End-Hosts (Empfängern) ermöglicht, einen Multicast-Router (IGMP Querier) über die Absicht des End-Hosts zu informieren, bestimmten Multicast-Datenverkehr zu empfangen. Dieses Protokoll wird zwischen einem Router und End-Hosts ausgeführt und ermöglicht:

- Router fragen Endhosts, ob sie einen bestimmten Multicast-Stream benötigen (IGMP-Abfrage)
- End-Hosts, die den Router benachrichtigen oder auf diesen antworten, wenn sie einen bestimmten Multicast-Stream suchen (IGMP-Berichte)

IGMP-Snooping

IGMP-Snooping ist ein Mechanismus, der Multicast-Datenverkehr auf die Ports beschränkt, an die Empfänger angeschlossen sind. Der Mechanismus erhöht die Effizienz, da er es einem Layer-2-Switch ermöglicht, Multicast-Pakete selektiv nur an die Ports zu senden, die sie benötigen. Ohne IGMP-Snooping überflutet der Switch die Pakete an jedem Port. Der Switch überwacht den Austausch von IGMP-Nachrichten durch den Router und die End-Hosts. Auf diese Weise erstellt der Switch eine IGMP-Snooping-Tabelle mit einer Liste aller Ports, die eine bestimmte Multicast-Gruppe angefordert haben.

MRouter-Port

Aus Switch-Sicht ist der Router-Port einfach der Port, der mit einem Multicast-Router verbunden wird. Das Vorhandensein von mindestens einem Router-Port ist für die Switch-übergreifende Verwendung von IGMP-Snooping absolut erforderlich. Weitere Informationen finden Sie im Abschnitt "Das Problem und seine Lösungen verstehen" dieses Dokuments.

Multicast auf L2

Jeder IP-Verkehr der Version 4 (IPv4) mit einer Ziel-IP-Adresse im Bereich von 224.0.0.0 bis 239.255.255.255 ist ein Multicast-Stream. Alle IPv4-Multicast-Pakete werden einer vordefinierten IEEE-MAC-Adresse im Format 01.00.5e. *xx* . *xx* . *xx* zugeordnet.

> **Hinweis:** IGMP-Snooping funktioniert nur, wenn die Multicast-MAC-Adresse diesem IEEE-konformen MAC-Bereich zugeordnet ist. Einige reservierte Multicast-Bereiche sind von denjenigen ausgeschlossen, bei denen das Design einen Snooping ausführt. Wenn ein nicht konformes Multicast-Paket aus einem Switched-Netzwerk stammt, wird das Paket durch dieses VLAN geflutet, d. h. es wird wie Broadcast-Datenverkehr behandelt.

Das Problem und seine Lösungen verstehen

Standardmäßig ist IGMP-Snooping auf den Catalyst-Switches aktiviert. Bei IGMP-Snooping sucht (oder hört) der Switch nach IGMP-Nachrichten an allen Ports. Der Switch erstellt eine IGMP-Snooping-Tabelle, die im Prinzip allen Switch-Ports, die ihn angefordert haben, eine Multicast-Gruppe zuordnet.

Angenommen, Empfänger 1 und Empfänger 2 haben ohne vorherige Konfiguration ihre Absicht signalisiert, einen Multicast-Stream für 239.239.239.239 zu empfangen, der der L2-Multicast-MAC-Adresse von 01.00.5e.6f.ef.ef zugeordnet ist. Sowohl Switch 1 als auch Switch 2 erstellen einen Eintrag in ihren Snooping-Tabellen für diese Empfänger als Reaktion auf die von den Empfängern generierten IGMP-Berichte. Switch 1 geht in Port Gigabit Ethernet 2/48 in seine Tabelle und Switch 2 in Port Fast Ethernet 1/0/47 in seine Tabelle ein.

Hinweis: An diesem Punkt hat die Multicast-Quelle ihren Verkehr nicht gestartet, und keiner der Switches kennt den Switch-Router-Port.

Wenn die Quelle auf Switch 1 beginnt, Multicast-Datenverkehr zu streamen, hat Switch 1 den IGMP-Bericht von Receiver 1 "gesehen". So liefert Switch 1 den Multicast-Out-Port Gigabit Ethernet 2/48. Da Switch 2 jedoch den IGMP-Bericht von Receiver 2 im Rahmen des IGMP-Snooping-Prozesses "absorbiert" hat, sieht Switch 1 keinen IGMP-Bericht (Multicast-Anforderung) an Port Gigabit Ethernet 2/46. Daher sendet Switch 1 keinen Multicast-Datenverkehr an Switch 2. Aus diesem Grund erhält Empfänger 2 keinen Multicast-Verkehr, obwohl sich Empfänger 2 im selben VLAN befindet, sich aber lediglich auf einem anderen Switch als der Multicast-Quelle befindet.

Der Grund für dieses Problem ist, dass IGMP-Snooping auf keiner Catalyst-Plattform ohne einen Router unterstützt wird. Der Mechanismus "bricht zusammen", wenn kein Router-Port vorhanden ist. Wenn Sie diese Lösung reparieren möchten, müssen die Switches einen Router-Port kennen oder sich damit vertraut machen. Weitere Erläuterungen zum Verfahren finden Sie im Abschnitt "Lösungen" dieses Dokuments. Sie müssen jedoch noch ermitteln, wie das Problem durch das Vorhandensein eines Router-Ports auf den Switches behoben werden kann.

Wenn die Switches einen Router-Port kennen oder statisch wissen, sind im Wesentlichen zwei Dinge wichtig:

- Der Switch "leitet" die IGMP-Berichte von den Empfängern an den Router-Port weiter, was bedeutet, dass die IGMP-Berichte an den Multicast-Router weitergeleitet werden. Der Switch leitet nicht alle IGMP-Berichte weiter. Stattdessen sendet der Switch nur wenige Berichte an den Router. Für diese Diskussion ist die Anzahl der Berichte nicht von Bedeutung. Der Multicast-Router muss nur wissen, ob mindestens ein Empfänger noch am Downstream-Multicast interessiert ist. Zur Durchführung der Bestimmung erhält der Multicast-Router als Reaktion auf seine IGMP-Anfragen die periodischen IGMP-Berichte.
- In einem Multicast-Szenario, in dem noch keine Empfänger registriert sind, sendet der Switch den Multicast-Stream nur über seinen Router-Port.

Wenn die Switches ihren Router-Port kennen, leitet Switch 2 den IGMP-Bericht, den der Switch vom Receiver 2 erhalten hat, an seinen Router-Port weiter. Dieser Port ist Fast Ethernet 1/0/33. Switch 1 erhält diesen IGMP-Bericht auf dem Switch-Port Gigabit Ethernet 2/46. Aus Sicht von Switch 1 hat der Switch lediglich einen weiteren IGMP-Bericht erhalten. Der Switch fügt diesen Port seiner IGMP-Snooping-Tabelle hinzu und beginnt, den Multicast-Verkehr auch an diesen Port zu senden. An diesem Punkt empfangen beide Empfänger den angeforderten Multicast-Datenverkehr, und die Anwendung funktioniert wie erwartet.

Informationen darüber, wie die Switches ihren Router-Port identifizieren, sodass IGMP-Snooping wie in einer einfachen Umgebung funktioniert, finden Sie im Abschnitt zu den Lösungen.

Lösungen

Verwenden Sie diese Lösungen, um das Problem zu lösen.

Lösung 1: Aktivieren von PIM auf der Layer-3-Router-/VLAN-Schnittstelle

Alle Catalyst-Plattformen haben die Möglichkeit, Informationen zum Router-Port dynamisch zu erfassen. Die Switches hören entweder die Protocol Independent Multicast (PIM)-Hellos oder die

IGMP-Abfragenachrichten passiv, die ein Multicast-Router regelmäßig sendet.

In diesem Beispiel wird die VLAN 1 Switched Virtual Interface (SVI) auf dem Catalyst 6500 mit 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)
```

Lösung 2: Aktivieren der IGMP Querier-Funktion auf einem Layer-2-Catalyst Switch

Der IGMP Querier ist eine relativ neue Funktion auf Layer-2-Switches. Wenn ein Netzwerk/VLAN keinen Router hat, der die Multicast-Router-Rolle übernehmen und die Router-Erkennung auf den Switches bereitstellen kann, können Sie die IGMP Querier-Funktion aktivieren. Mit dieser Funktion kann der Layer-2-Switch einen Proxy für einen Multicast-Router einrichten und in diesem Netzwerk regelmäßige IGMP-Abfragen senden. Dadurch betrachtet sich der Switch selbst als Router-Port. Die übrigen Switches im Netzwerk definieren einfach ihre jeweiligen Router-Ports als die Schnittstelle, an der sie diese IGMP-Abfrage empfangen haben.

```
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 sieht nun, dass Port Gig 2/46 mit Switch 2 als Router-Port verbunden ist.

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

Wenn die Quelle an Switch 1 beginnt, Multicast-Datenverkehr zu streamen, leitet Switch 1 den Multicast-Datenverkehr an den Empfänger 1 weiter, der über IGMP-Snooping gefunden wurde (d. h. an den Out-Port Gig 2/48), und an den Router-Port (d. h. an den Out-Port Gig 2/46).

Lösung 3: Konfigurieren des statischen Router-Ports auf dem Switch

Der Multicast-Datenverkehr fällt innerhalb desselben Layer-2-VLAN aus, da kein Router-Port an den Switches vorhanden ist. In diesem Abschnitt wird das Problem und die zugehörigen Lösungen behandelt. Wenn Sie einen Router-Port auf allen Switches statisch konfigurieren, können IGMP-Berichte in diesem VLAN an alle Switches weitergeleitet werden. Dadurch ist Multicasting möglich. In diesem Beispiel müssen Sie den Catalyst 3750-Switch statisch so konfigurieren, dass er Fast Ethernet 1/0/33 als Router-Port verwendet.

In diesem Beispiel benötigen Sie einen statischen Router-Port nur an Switch 2:

```
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)
```

Lösung 4: Konfigurieren statischer Multicast-MAC-Einträge auf allen Switches

Sie können einen statischen CAM-Eintrag (Content-Addressable Memory) für die Multicast-MAC-Adresse auf allen Switches für alle Empfänger-Ports und die Downstream-Switch-Ports erstellen. Jeder Switch befolgt die statischen CAM-Eingaberegeln und sendet das Paket über alle Schnittstellen, die in der CAM-Tabelle angegeben sind. Dies ist die am wenigsten skalierbare Lösung für eine Umgebung mit vielen Multicast-Anwendungen.

```
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
```

Lösung 5: Deaktivieren von IGMP-Snooping auf allen Switches

Wenn Sie IGMP-Snooping deaktivieren, behandeln alle Switches Multicast-Verkehr als Broadcast-Verkehr. Dadurch wird der Datenverkehr zu *allen* Ports in diesem VLAN geflutet, unabhängig davon, ob die Ports über interessierte Empfänger für diesen Multicast-Stream verfügen.

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

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

Zugehörige Informationen

- Multicast in einem Campus-Netzwerk: CGMP und IGMP Snooping
- Unterstützte Multicast-Catalyst-Switches
- IP-Multicast-Unterstützung
- Technische Hinweise zur Fehlerbehebung bei Problemen mit IP-Multicast
- Leitfaden zur Fehlerbehebung bei IP-Multicast
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.