Multicast in einem Campus-Netzwerk: CGMP- und IGMP-Snooping

Inhalt

Einleitung

Der Zweck von Cisco Group Management Protocol (CGMP)- und Internet Group Management Protocol (IGMP)-Snooping besteht in der Beschränkung des Multicast-Datenverkehrs in einem

Switch-Netzwerk. Standardmäßig überflutet ein LAN-Switch Multicast-Datenverkehr innerhalb der Broadcast-Domäne. Wenn viele Multicast-Server Streams an das Segment senden, kann dies sehr viel Bandbreite beanspruchen.

Vorbereitungen

Konventionen

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

Voraussetzungen

Es sind keine besonderen Voraussetzungen erforderlich, um den Inhalt dieses Dokuments nachzuvollziehen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Hintergrundinformationen

Der Multicast-Datenverkehr wird überflutet, da ein Switch in der Regel MAC-Adressen erfährt, indem er das Quelladressfeld aller empfangenen Frames überprüft. Eine Multicast-MAC-Adresse wird nie als Quelladresse für ein Paket verwendet. Solche Adressen werden nicht in der MAC-Adresstabelle angezeigt, und der Switch kann sie nicht erlernen.

Die erste Lösung für dieses Problem ist die Konfiguration statischer MAC-Adressen für jede Gruppe und jeden Client. Diese Lösung funktioniert gut, ist jedoch weder skalierbar noch dynamisch. Sie verwenden diese Lösung auf einem Catalyst Switch der Serien 4000, 5000 oder 6000, indem Sie einen der folgenden Befehle ausführen:

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

Diese beiden Befehle haben dieselbe Wirkung, mit der Ausnahme, dass die statischen Einträge beim Neustart verschwinden und permanente Einträge nicht.

Die zweite Lösung besteht in der Verwendung von CGMP, einem proprietären Cisco Protokoll, das zwischen dem Multicast-Router und dem Switch ausgeführt wird. Mit dem CGMP kann der Cisco Multicast-Router IGMP-Nachrichten verstehen, die von Hosts gesendet wurden, und den Switch über die im IGMP-Paket enthaltenen Informationen informieren.

Die letzte (und effizienteste) Lösung ist die Verwendung von IGMP-Snooping. Mit IGMP-Snooping fängt der Switch IGMP-Nachrichten vom Host selbst ab und aktualisiert seine MAC-Tabelle entsprechend. Zur Unterstützung von IGMP-Snooping ist erweiterte Hardware erforderlich.

Die in diesem Dokument angegebenen CGMP-Konfigurationen gelten für Catalyst Switches der Serien 4000 und 5000 mit CatOS (CGMP wird auf Catalyst 6000-Switches nicht unterstützt) und IGMP-Snooping-Konfigurationen für Catalyst Switches der Serien 5000 und 6000.

Im folgenden Abschnitt wird kurz eine Multicast-Adresse beschrieben, die Funktionen von IGMP erläutert und zusätzliche Details zu CGMP- und IGMP-Snooping bereitgestellt.

Multicast-Adresse

1. Multicast-IP-Adressen sind IP-Adressen der Klasse D. Daher sind alle IP-Adressen von 224.0.0.0 bis 239.255.255.255 Multicast-IP-Adressen. Sie werden auch als Group Destination Addresses (GDA) bezeichnet.
2. Für jede GDA gibt es eine zugeordnete MAC-Adresse. Diese MAC-Adresse besteht aus 01-00-5e, gefolgt von den letzten 23 Bit der GDA, die in Hexadezimalform umgewandelt wurden (siehe unten).239.20.20.20 entspricht MAC 01-00-5e-14-14-14-14.239.10.10.10 entspricht MAC 01-00-5e-0a-0a-0a.Daher ist dies keine Eins-zu-Eins-Zuordnung, sondern eine Eins-zu-Many-Zuordnung. Aus diesen beiden Adressen können Sie sehen, dass das erste Oktett (239) in der MAC-Adresse nicht verwendet wird. Die Multicast-Adressen mit denselben letzten drei Oktetten, aber unterschiedlichen ersten Oktetten haben also überlappende MAC-Adressen.
3. Einige Multicast-IP-Adressen sind für eine besondere Verwendung reserviert (siehe unten).224.0.0.1 - Alle Multicast-fähigen Hosts.224.0.0.2 - Alle Multicast-fähigen Router.224.0.0.5 und 224.0.0.6 werden von Open Shortest Path First (OSPF) verwendet.

Im Allgemeinen sind Adressen von 224.0.0.1 bis 224.0.0.255 reserviert und werden von verschiedenen Protokollen verwendet (Standard- oder proprietär, wie z. B. Hot Standby Router Protocol (HSRP)). Cisco empfiehlt, diese nicht für GDA in einem Multicast-Netzwerk zu verwenden. CGMP- und IGMP-Snooping funktionieren nicht mit diesem reservierten Adressbereich.

Internet Group Management-Protokoll

IGMP ist ein Standard, der in RFC 1112 für IGMPv1, in RFC 2236 für IGMPv2 und in RFC 3376 für IGMPv3 definiert ist. IGMP legt fest, wie ein Host sich bei einem Router registrieren kann, um bestimmten Multicast-Datenverkehr zu empfangen. Der nächste Abschnitt bietet einen kurzen Überblick über IGMP.

IGMPv1

IGMP Version 1 (IGMPv1)-Nachrichten werden in IP-Datagrammen übertragen und enthalten die folgenden Felder:

- Version: 1
- Typ: Es gibt zwei Arten von IGMP-Nachrichten: Mitgliedschaftsabfrage und Mitgliedschaftsbericht.
- Prüfsumme
- GDA

Mitgliedschaftsberichte werden von Hosts ausgegeben, die eine bestimmte Multicast-Gruppe (GDA) empfangen möchten. Die Mitgliedschaftsabfragen werden von Routern in regelmäßigen Abständen durchgeführt, um zu überprüfen, ob in diesem Segment noch ein Host Interesse an der GDA hat.

Berichte über die Hostmitgliedschaft werden entweder unaufgefordert (wenn der Host zuerst GDA-

Datenverkehr empfangen möchte) oder als Antwort auf eine Mitgliedschaftsabfrage ausgegeben. Sie werden mit den folgenden Feldern gesendet:

L2-Informationen

- Quell-MAC: Host-MAC-Adresse
- Ziel-MAC: Ziel-MAC für die GDA

L3-Informationen

- Quell-IP: IP-Adresse des Hosts
- Ziel-IP: GDA

IGMP-Paket

- IGMP-Daten enthalten darüber hinaus die GDA und einige andere Felder.

Host-Mitgliedschaftsabfragen werden vom Router an die reine Multicast-Adresse gesendet: 224.0.0.1. Diese Abfragen verwenden 0.0.0.0 im IGMP-GDA-Feld. Ein Host für jede Gruppe muss auf diese Abfrage antworten, oder der Router beendet die Weiterleitung des Datenverkehrs für diese GDA an dieses Segment (nach drei Versuchen). Der Router führt für jede Quelle einen Multicast-Routing-Eintrag und verknüpft diesen mit einer Liste ausgehender Schnittstellen (Schnittstelle, von der aus der IGMP-Bericht stammt). Nach drei IGMP-Abfrageversuchen ohne Antwort wird diese Schnittstelle für alle mit dieser GDA verknüpften Einträge aus der Liste der ausgehenden Schnittstellen gelöscht.

> **Anmerkung:** IGMPv1 verfügt über keinen Mechanismus zum Hinterlassen. Wenn ein Host den Datenverkehr nicht mehr empfangen möchte, beendet er ihn einfach. Wenn es sich um den letzten Host im Subnetz handelt, erhält der Router keine Antwort auf seine Abfrage und löscht die GDA für dieses Subnetz.

IGMPv2

In IGMP Version 2 (IGMPv2) wurde das Versionsfeld entfernt, und das Typfeld kann nun verschiedene Werte annehmen. Die Typen sind unten aufgeführt.

- Mitgliedschaftsabfrage
- IGMPv1-Mitgliedschaftsbericht
- Version 2 Bericht über die Mitgliedschaft
- Gruppe verlassen

Nachfolgend werden die wichtigsten neuen Funktionen von IGMPv2 beschrieben.

- IGMP-Nachricht hinterlassen: Wenn ein Host eine Gruppe verlassen möchte, sollte er eine IGMP-Nachricht für die Leave-Gruppe an das Ziel 224.0.0.2 senden (statt wie in IGMPv1 stumm zu bleiben).
- Ein Router kann nun eine gruppenspezifische Abfrage senden, indem er eine Mitgliedschaftsabfrage an die GDA-Gruppe sendet, anstatt diese an 0.0.0.0 zu senden.

IGMPv3

In IGMP Version 3 (ICMPv3) gibt es ein Typfeld mit den folgenden Werten:

- Mitgliedschaftsabfrage
- Version 3 Bericht über die Mitgliedschaft

Eine IGMPv3-Implementierung *muss* die folgenden drei Meldungstypen für die Zusammenarbeit mit früheren IGMP-Versionen unterstützen:

- Version 1 Mitgliedschaftsbericht [RFC112]
- Version 2 Mitgliedschaftsbericht [RFC2236]
- Version 2 Leave Group (RFC2236)

IGMPv3 bietet zusätzliche Unterstützung für die Quellfilterung, d. h. die Möglichkeit, dass ein System Interesse am Empfang von Paketen von bestimmten Quelladressen oder von **allen, aber** bestimmten Quelladressen meldet, die an eine bestimmte Multicast-Adresse gesendet werden. Diese Funktion wird auch als Source Specific Multicast (SSM) bezeichnet.

Damit ein Computer SSM unterstützt, muss er IGMPv3 unterstützen. Relativ wenige Betriebssysteme unterstützen jedoch IGMPv3. Windows XP unterstützt IGMPv3, und es gibt IGMPv3-Support-Patches für FreeBSD und Linux.

Administratoren müssen zwischen IGMPv3-Unterstützung auf Router- und IGMPv3-Snooping auf Switch-Ebene unterscheiden. Es gibt zwei verschiedene Funktionen.

Unterstützung von IGMPv3 auf Catalyst Switches (L2)

- Der Catalyst 6000 mit Hybrid-Mode-Software (CatOS auf Supervisor und Cisco IOS® Software auf MSFC) unterstützt IGMPv3-Snooping ab Version 7.5(1) offiziell.
- In Versionen vor 7.5(1) hatte der Catalyst 6000-Switch keine offizielle Unterstützung für IGMPv3, sollte aber normalerweise IGMPv3-Pakete verarbeiten können.
- Der Catalyst 6000 mit integrierter IOS-Software unterstützt IGMPv3 auf Router-Ebene (L3-Schnittstelle) ab Version 12.1(8a)E.
- Der Catalyst 4000 unterstützt IGMPv3 nur auf Routerebene auf der Supervisor III- und der Supervisor IV-Plattform. IGMPv3-Snooping wird nicht unterstützt.

Unterstützung von IGMPv3 auf Cisco Routern (L3)

IGMPv3 wird auf allen Plattformen unterstützt, auf denen die Cisco IOS® Software, Version 12.1(5)T und höher, ausgeführt wird.

Hinweise

Wenn ein Switch IGMP-Snooping ausführt, fängt er die IGMP-Pakete ab und füllt die statische L2-Weiterleitungstabelle (Layer 2) auf Basis des Inhalts der abgefangenen Pakete auf. Wenn im Netzwerk IGMPv1- oder v2-Hosts vorhanden sind, liest der Switch die IGMP-Joins und -Leaves, um zu bestimmen, welche Hosts welchen Multicast-Stream empfangen oder den Empfang des Multicast-Streams beenden möchten.

IGMPv3 ist komplizierter, da es nicht nur die Gruppenadresse (Multicast-Adresse) verwendet,

sondern auch die Quellen, von denen Datenverkehr erwartet wird. Außer dem Catalyst Switch der Serie 6000 mit CatOS 7.5 oder höher und der Native IOS Version 12.1(8a)E oder höher können derzeit keine anderen Switches diese Pakete effektiv schnappen und eine Weiterleitungstabelle auf der Grundlage dieser Informationen erstellen. Daher sollte IGMP-Snooping deaktiviert werden, wenn ein IGMPv3-Host auf dem Switch vorhanden ist. Wenn IGMP-Snooping deaktiviert ist, kann der Switch keine L2-Weiterleitungstabelle für die Multicast-Streams dynamisch erstellen. Mit anderen Worten, der Switch überflutet die Multicast-Streams.

Wenn IGMP-Snooping deaktiviert ist, besteht eine Lösung in der manuellen Konfiguration von Multicast Dynamic Content-Addressable Memory (CAM)-Einträgen, um zu verhindern, dass das Subnetz durch Multicast-Datenverkehr überflutet wird. Dies ist jedoch ein Verwaltungsaufwand und keine dynamische Lösung. Wenn ein Client den Datenverkehr nicht mehr empfangen möchte, wird der CAM-Eintrag nicht vom Switch entfernt (es sei denn, dies geschieht durch manuelle Eingriffe), sodass der Netzwerkverkehr weiterhin an den Host adressiert wird.

Bei der Verwendung von IGMPv3 im Netzwerk funktionieren Switches mit CGMP auch normal, abgesehen davon, dass CGMP Fastleave nicht funktioniert. Wenn ein CGMP-Schnellurlaub erforderlich ist, sollte am besten auf IGMPv2 zurückgekehrt werden.

Die herausragenden plattformspezifischen Probleme finden Sie in den Versionshinweisen für die jeweiligen Switches.

Interoperabilität zwischen IGMPv1 und IGMPv2

Bei IGMPv1 und IGMPv2 sendet nur ein Router pro IP-Subnetz Abfragen. Dieser Router wird als Abfrage-Router bezeichnet. In IGMPv1 wird der Abfrage-Router mithilfe des Multicast-Routing-Protokolls ausgewählt. In IGMPv2 wird er von der niedrigsten IP-Adresse der Router gewählt. Im Folgenden finden Sie einige Möglichkeiten:

Szenario 1: IGMPv1-Router mit einer Kombination aus IGMPv1- und IGMPv2-Hosts

Der Router versteht den IGMPv2-Bericht nicht. Daher dürfen alle Hosts nur den IGMPv1-Bericht verwenden.

Szenario 2: IGMPv2-Router mit einer Kombination aus IGMPv2- und IGMPv3-Hosts

IGMPv1-Hosts verstehen die IGMPv2-Abfrage oder die IGMPv2-Gruppenmitgliedschaftsabfrage nicht. Der Router darf nur IGMPv1 verwenden und den Vorgang für den Austritt aussetzen.

Szenario 3: IGMPv1-Router und IGMPv2-Router im selben Segment

Der IGMPv1-Router kann den IGMPv2-Router nicht erkennen. Aus diesem Grund muss der IGMPv2-Router vom Administrator als IGMPv1-Router konfiguriert werden. Auf jeden Fall ist es möglich, dass sie sich nicht auf den Abfrage-Router einigen.

Interoperabilität zwischen IGMPv1/IGMPv2 und IGMPv3

Bei allen IGMP-Versionen sendet nur ein Router pro IP-Subnetz Abfragen. Dieser Router wird als Abfrage-Router bezeichnet. In IGMPv1 wird der Abfrage-Router mithilfe des Multicast-Routing-Protokolls ausgewählt. In IGMPv2 und IGMPv3 wird er von der niedrigsten IP-Adresse der Router

gewählt. Nachfolgend sind einige Interoperabilitätsoptionen aufgeführt.

Szenario 1: IGMPv1/IGMPv2-Router mit einer Kombination aus IGMPv1/IGMPv2- und IGMPv3-Hosts

Da der Router die IGMPv3-Berichte nicht versteht, verwenden alle Hosts die IGMPv1/IGMPv2-Berichte.

Szenario 2: IGMPv3-Router mit einer Kombination aus IGMPv1/IGMPv2- und IGMPv3-Hosts

Die IGMPv1/IGMPv2-Hosts verstehen die IGMPv3-Abfrage oder die IGMPv3-Mitgliedschaftsabfrage nicht. Der Router darf nur die IGMP-Version verwenden, die der niedrigsten vorhandenen IGMP-Client-Version entspricht. Wenn IGMPv3- und IGMPv2-Clients vorhanden sind, verwendet der Router IGMPv2. Wenn IGMPv1-, IGMPv2- und IGMPv3-Clients vorhanden sind, verwendet der Router IGMPv1.

Szenario 3: Verschiedene Version-Router im gleichen Segment

Wenn Router verschiedener Versionen auf demselben Segment vorhanden sind, können die Router der unteren Version die Router der höheren Version nicht erkennen. Daher müssen die verschiedenen Router vom Administrator als gleiche Version konfiguriert werden. Diese Version muss mit der niedrigsten Version auf einem vorhandenen Abfragerouter übereinstimmen.

IGMP auf einem Router

Wenn in einem Subnetz standardmäßig kein Benutzer für eine bestimmte Gruppe registriert ist, leitet der Router keinen Multicast-Datenverkehr für diese Gruppe an dieses Subnetz weiter. Das bedeutet, dass ein Router einen IGMP-Bericht für eine GDA erhalten muss, um diesen zur Multicast-Routing-Tabelle hinzuzufügen und die Weiterleitung des Datenverkehrs für diese Gruppe zu starten.

Auf einem Router müssen Sie die folgenden Aktionen durchführen:

1. Aktivieren Sie Multicast-Routing im globalen Modus, wie unten gezeigt.

   ```
   ip multicast-routing
   ```

2. Konfigurieren Sie ein Multicast-Routing-Protokoll auf der beteiligten Schnittstelle (siehe unten).

   ```
   ip pim dense-mode
   ```

3. Überwachen Sie IGMP, wie unten gezeigt.

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

4. Konfigurieren Sie einen Router, um den IGMP-Bericht (über die Schnittstelle) zu senden (siehe unten).

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

Praktisches Beispiel auf einem Router

Ein Router ist für die Weiterleitung zwischen zwei Subschnittstellen konfiguriert, Fast-Ethernet 0.2 und Fast-Ethernet 0.3. Beide Schnittstellen sind auch für die Ausführung von IGMP konfiguriert. In der unten stehenden Ausgabe sehen Sie die IGMP-Version, die beigefügte Gruppe usw.

Konfiguration

```
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#
```

Cisco Group Management-Protokoll

Informationen zur CGMP-Unterstützung auf Catalyst Switches finden Sie in der Multicast Catalyst Switches Support Matrix.

CGMP-Frames und Nachrichtentypen

CGMP wurde erstmals von Cisco implementiert, um den Multicast-Verkehr in einem L2-Netzwerk zu beschränken. Da ein Switch im Wesentlichen nicht in der Lage ist, L3-Pakete zu betrachten, kann er ein IGMP-Paket nicht unterscheiden. Mit CGMP stellt der Router die Schnittstelle zwischen den Hosts bereit. Die Router "sprechen" IGMP und die Switches "sprechen" CGMP.

CGMP-Frames sind Ethernet-Frames mit der MAC-Zieladresse 01-00-0c-dd-dd und mit einem Subnetz Access Protocol (SNAP)-Header mit dem Wert 0x2001. Die CGMP-Frames enthalten die folgenden Felder:

- Version: 1 oder 2.

- Meldungstyp: Treten Sie bei oder verlassen Sie.
- Anzahl: Die Anzahl der Multicast-/Unicast-Adresspaare in der Nachricht.
- GDA: Die 48-Bit-MAC-Adresse der Multicast-Gruppe.
- Unicast-Quelladresse (USA): Die 48-Bit-MAC-Unicast-Adresse der Geräte, die der GDA beitreten möchten.

Anmerkung: Der Wert des Zählfelds bestimmt, wie oft die letzten beiden Felder angezeigt werden.

Standardmäßig lauschen die Prozessoren eines Switches (in Catalyst NMP genannt) nur Multicast-Adressen, wenn die **show cam system** wird ausgegeben. Wenn Sie CGMP auf einem Switch aktivieren, wird die Adresse 01-00-0c-dd-dd-dd zum Switch **show cam system** Befehlsausgabe.

In der folgenden Tabelle sind alle möglichen CGMP-Nachrichten aufgelistet.

GDA	USA	Beitreten/Verlassen	Bedeutung
Multicast-MAC	Client-MAC	Beitreten	Zu Gruppe Port hinzufügen
Multicast-MAC	Client-MAC	Urlaub	Port aus Gruppe löschen
00-00-00-00-00-00	Router-MAC	Beitreten	Router-Port zuweisen
00-00-00-00-00-00	Router-MAC	Urlaub	Entfernen Sie den Router-Port.
Multicast-MAC	00-00-00-00-00-00	Urlaub	Gruppe löschen.
00-00-00-00-00-00	00-00-00-00-00-00	Urlaub	Löschen Sie alle Gruppen.

Learning Router-Ports

Der Switch muss alle Router-Ports kennen, damit sie automatisch zu allen neu erstellten Multicast-Einträgen hinzugefügt werden. Der Switch erkennt Router-Ports, wenn er eine CGMP-Join-Nachricht an GDA 00-00-00-00-00-00 mit Router MAC USA (dritter Nachrichtentyp in der Tabelle) empfängt. Diese Meldungen werden vom Router auf allen für die Ausführung von CGMP konfigurierten Schnittstellen generiert. Es gibt jedoch auch eine statische Methode zum Konfigurieren der Router-Ports am Switch.

Einem CGMP beitreten

- Ein neuer Client fordert den Empfang von Datenverkehr für eine GDA an, sodass der Client eine Meldung über den IGMP-Mitgliedschaftsbericht sendet.
- Der Router empfängt den IGMP-Bericht, verarbeitet ihn und sendet eine CGMP-Meldung an den Switch. Der Router kopiert die Ziel-MAC-Adresse in das GDA-Feld der CGMP-Join-Nachricht und kopiert die Quell-MAC-Adresse in die USA des CGMP-Joins. Anschließend wird es an den Switch zurückgesendet.
- Ein Switch mit aktiviertem CGMP muss die CGMP-Adressen 01-00-0c-dd-dd überwachen. Der Switch-Prozessor überprüft die CAM-Tabelle für die USA. Sobald die USA in der CAM-Tabelle aufgeführt sind, weiß der Switch, auf welchem Port sich die USA befinden, und führt einen der folgenden Schritte aus:Erstellt einen neuen statischen Eintrag für die GDA und verbindet den USA-Port mit ihm sowie allen Router-Ports.Fügt der Liste der Ports für diese GDA den USA-Port hinzu (falls der statische Eintrag bereits vorhanden ist).

Verlassen einer Gruppe mit CGMP

Die mit dem CGMP erfassten statischen Einträge sind permanent, es sei denn, es erfolgt eine Änderung der Spanning-Tree-Topologie im VLAN, oder der Router sendet eine der letzten CGMP-Leave-Nachrichten in der vorherigen Tabelle.

Wenn IGMPv1 der Host ist, senden Sie keine IGMP Leave-Nachrichten. Der Router sendet Leave-Nachrichten nur, wenn er keine Antwort auf drei aufeinander folgende IGMP-Abfragen erhält. Das bedeutet, dass kein Port aus einer Gruppe gelöscht wird, wenn Benutzer noch an dieser Gruppe interessiert sind.

Mit der Einführung von IGMPv2 und dem Vorhandensein von IGMP Leave hat Cisco die ursprüngliche CGMP-Spezifikation (CGMPv2) erweitert. Diese Ergänzung wird als CGMP Fast-Leave bezeichnet.

Die CGMP Fast-Leave-Verarbeitung ermöglicht dem Switch die Erkennung von IGMPv2 Leave-Nachrichten, die an die All-Router-Multicast-Adresse (224.0.0.2) von Hosts an einem der Modulports der Supervisor Engine gesendet werden. Wenn das Supervisor Engine-Modul eine Leave-Nachricht empfängt, startet es einen Abfrageantwort-Timer und sendet eine Nachricht an den Port, an dem der Urlaub empfangen wurde, um festzustellen, ob noch ein Host bereit ist, diese Multicast-Gruppe an diesem Port zu empfangen. Wenn dieser Timer abläuft, bevor eine CGMP-Join-Nachricht empfangen wird, wird der Port aus der Multicast-Struktur für die in der ursprünglichen Urlaubsmeldung angegebene Multicast-Gruppe entfernt. Wenn es sich um den letzten Port in der Multicast-Gruppe handelt, wird die IGMP-Leave-Nachricht an alle Router-Ports weitergeleitet. Der Router startet dann den normalen Löschvorgang, indem er eine gruppenspezifische Abfrage sendet. Da keine Antworten empfangen werden, entfernt der Router diese Gruppe aus der Multicast-Routing-Tabelle für diese Schnittstelle. Außerdem wird eine CGMP-Leave-Meldung an den Switch gesendet, mit der die Gruppe aus der statischen Tabelle gelöscht wird. Die Fast-Leave-Verarbeitung gewährleistet eine optimale Bandbreitenverwaltung für alle Hosts in einem Switch-Netzwerk, selbst wenn mehrere Multicast-Gruppen gleichzeitig verwendet werden.

Wenn CGMP Leave aktiviert ist, werden dem **show cam system** Befehlsausgabe, wie unten gezeigt.

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

`01-00-5e-00-00-02`
IGMP Leave verwendet 224.0.0.2 und IGMP Query 224.0.0.1.

Führen Sie die folgenden Schritte aus, um eine Fehlerbehebung für CGMP durchzuführen:

1. Aufgrund eines Konflikts mit dem HSRP ist die CGMP Leave-Verarbeitung standardmäßig deaktiviert. HSRP verwendet die MAC-Adresse 01-00-5e-00-00-02, die mit IGMP Leave in IGMP Version 2 identisch ist. Bei CGMP Fast-Leave gehen alle HSRP-Pakete an die Switch-CPU. Da eine HSRP-Nachricht kein IGMP-Paket ist, generiert der Switch alle diese Nachrichten neu und sendet sie an alle Router-Ports. Router, die `hsrp hello-` oder `hsrp-Peers` empfangen, verlieren die Verbindung. Versuchen Sie daher beim Debuggen von HSRP-Problemen, CGMP Fast-Leave zu deaktivieren.Um die CGMP Leave-Verarbeitung zu aktivieren, führen Sie den folgenden Befehl aus: **set cgmp leave enable** aus.
2. Wenn die CGMP-Leave-Verarbeitung aktiviert ist, erkennt der Catalyst Switch der Serie 500 Router-Ports über PIM-v1-, HSRP- und CGMP-Self-Join-Meldungen. Wenn die CGMP-Leave-Verarbeitung deaktiviert ist, erfährt der Catalyst Switch der Serie 500 Router-Ports nur über CGMP-Self-Join-Nachrichten.
3. Der CGMP deaktiviert keinen Multicast-Datenverkehr für IP-Multicast-Adressen, die dem MAC-Adressbereich 01-00-5E-00-00-00 bis 01-00-5E-00-00-FF zugeordnet sind. Die reservierten IP-Multicast-Adressen im Bereich von 224.0.0.0 bis 224.0.0.255 werden für die Weiterleitung des lokalen IP-Multicast-Datenverkehrs in einem einzelnen L3-Hop verwendet.

CGMP und Quellnetzwerk

Ein rein quellenbasiertes Netzwerk ist ein Segment, das nur über ein Quell-Multicast und keinen echten Client verfügt. Daher besteht die Möglichkeit, dass in diesem Segment keine IGMP-Berichte generiert werden. Der CGMP muss jedoch die Überflutung dieser Quelle (nur zur Verwendung durch Router) beschränken. Wenn ein Router Multicast-Datenverkehr an einer Schnittstelle ohne IGMP-Bericht erkennt, wird er als rein auf Multicast-Quellen basierendes Netzwerk identifiziert. Der Router generiert eine CGMP-Join-Nachricht für sich selbst, und der Switch fügt diese Gruppe einfach hinzu (nur mit dem Router-Port).

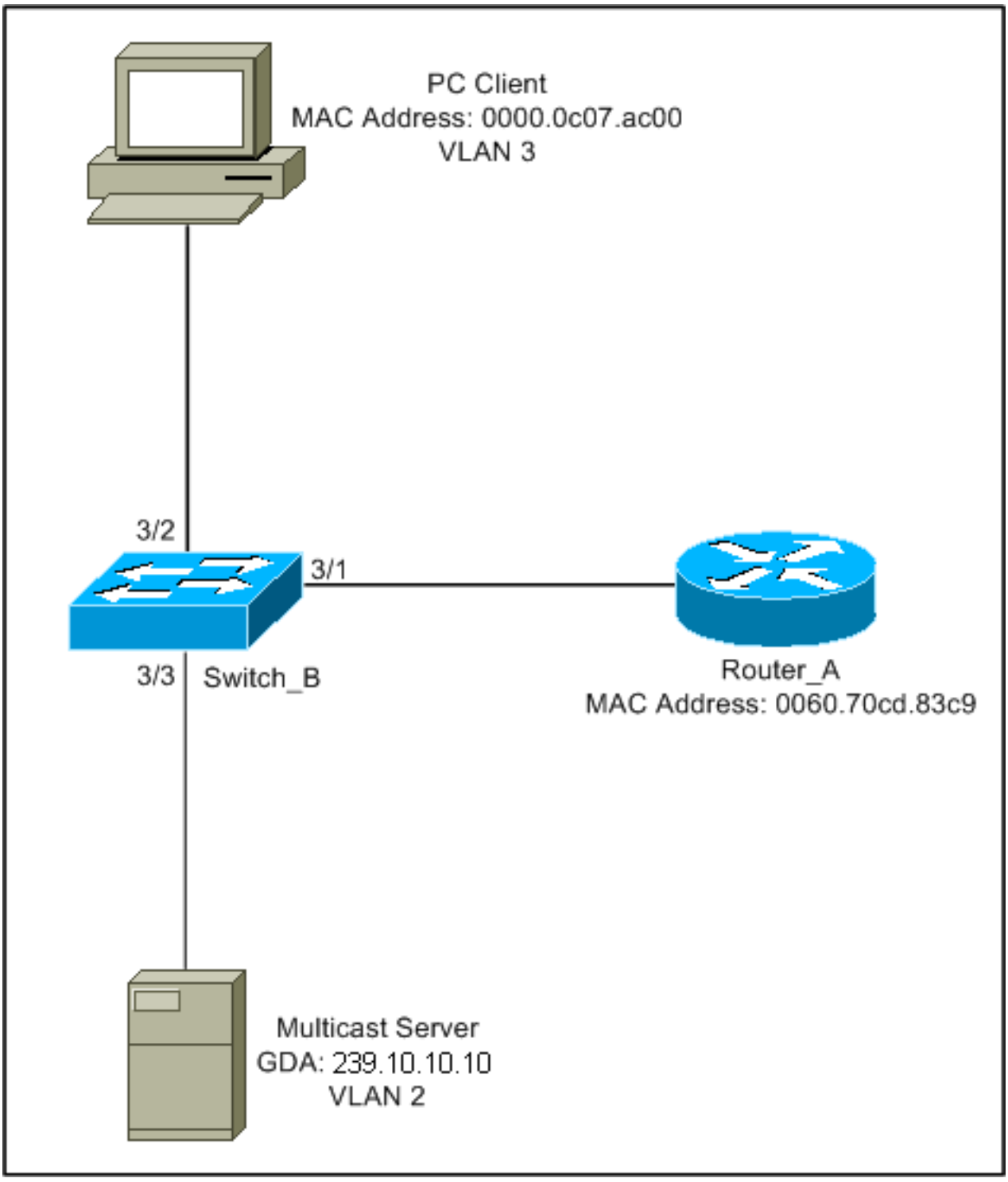
Konfigurieren von Cisco Routern und Switches zur Aktivierung des CGMP

Die folgenden Befehle gelten nur für die Catalyst Serien 4000 und 500 (plus 2901, 2902, 2926, 2948G und 4912).

- Multicast-RouterIP-Multicasting aktivieren (globaler Befehl):**ip multicast-routing**Aktivieren Sie jede CGMP-Schnittstelle (Schnittstellenmodus) mit den folgenden Befehlen:**ip pimip igmpip cgmp**Debuggen Sie das L2-Multicast-Problem mit den folgenden Befehlen:**debug ip igmpdebug ip cgmp**
- Catalyst Serie 4000 oder 5000Aktivieren/Deaktivieren von CGMP mit den folgenden Befehlen:**set cgmp**Aktivieren/Deaktivieren von CGMP Fast-Leave mit den folgenden Befehlen:**set cgmp leave**Konfigurieren Sie den Multicast-Router (statisch) mit den folgenden Befehlen:**set multicast router**Löschen Sie den Multicast-Router mit den folgenden Befehlen:**clear multicast router**Im Folgenden werden verschiedene Befehle zur Überprüfung des CGMP-Vorgangs aufgelistet.**show cam staticshow cgmp statisticshow cgmp leaveshow multicast routershow multicast groupshow multicast group cgmpshow multicast group count**

Praxisbeispiel für die Verwendung von CGMP sowie für Debug-Befehl und -Ausgabe

Dies ist ein praktisches Konfigurationsbeispiel für einen Cisco Router und Catalyst Switches.



Diese Konfiguration zeigt die Operationen an, die ein Host einer Gruppe beitritt. Diese Konfiguration zeigt auch die Vorgänge an, da ein Host eine Gruppe mit aktiviertem Fast-Leave-Befehl verlässt. Sniffer-Traces sowie die Konfiguration von Switch und Router sind ebenfalls enthalten.

Einem CGMP beitreten

Gehen Sie wie folgt vor, wenn Sie einer Gruppe mit dem CGMP beitreten.

1. Aktivieren Sie CGMP auf dem Switch, wie unten gezeigt.

```
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)
```

   Wie Sie unten sehen, ist der Eintrag 01-00-0c-dd-dd-dd für alle VLANs in der **show cam system** Befehlsausgabe. Da im Netzwerk CGMP Fast-Leave ausgeführt wird, können Sie außerdem die Einträge für 01-00-5e-00-00-01 und 01-00-5e-00-00-02 sehen.

```
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. Der Router sendet eine CGMP-Join-Nachricht an GDA 00-00-00-00-00-00 mit der USA-MAC des Routers. Aus diesem Grund wird der Router-Port der Router-Port-Liste hinzugefügt (siehe das erste Beispiel unten).**Auf dem Router**

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

   Am 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. Der PC am 3/1 sendet IGMP einen Bericht mit der GDA: 239.10.10.10 (siehe Bild 2 unten). Im Folgenden sehen Sie die **show ip igmp group** Ausgabe auf dem Router Router_A.Dies zeigt, dass der Router jetzt Datenverkehr für 224.10.10.10 an fa0.3 weiterleitet. Dies ist eine Folge des Empfangs des IGMP-Berichts vom 10.3.3.2, dem Client-PC.

```
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. Der Router empfängt den Bericht und sendet eine CGMP Join-Nachricht mit den folgenden Informationen:Quell-MAC: MAC-Adresse des RoutersZiel-MAC: 01-00-cc-dd-dd-dd-ddInhalt: MAC-Adresse des Client-PCs (USA): 00-00-0c-07-ac-00 MAC-Adresse der Multicast-Gruppe: 01-00-5e-0a-0a-0a (siehe Frame 3 unten)**Auf dem Router**

```
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. Der Switch mit dem Befehl 01-00-cc-dd-dd-dd im **show cam system** -Befehlsausgabe ist CGMP aktiviert. Der Switch kann das Paket verarbeiten.Der Switch sucht in der dynamischen CAM-Tabelle nach dem Port, an dem sich die MAC-Adresse des Client-PCs befindet. Die Adresse befindet sich an Port 3/2, und der Switch macht einen statischen Eintrag in die CAM-Tabelle für 01-00-5e-0a-0a-0a begrenzt auf Port 3/2. Der Switch fügt dem statischen Eintrag für diese GDA auch den Router-Port 3/1 hinzu.**Am 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. Der gesamte nachfolgende Datenverkehr für die Multicast-Gruppe 239.10.10.10 wird nur an diesen Port in diesem VLAN weitergeleitet. Unten sehen Sie den statischen Eintrag im Catalyst Switch, wobei 3/1 der Router-Port und 3/2 der Client-Port ist.

```
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)
```

Verlassen einer Gruppe mit aktiviertem CGMP Fast-Leave

Im folgenden Beispiel wird vorausgesetzt, dass der Client ein IGMP Version 2-Client ist und dass Fast-Leave auf dem Switch aktiviert ist.

1. Die folgende Prozedur aktiviert CGMP Fast-Leave. Sehen Sie sich **show cgmp leave** - Befehlsausgabe, um festzustellen, ob sie aktiviert ist. Schauen Sie sich auch die **show cam system** Ausgabe zu bestimmen, ob der Switch auf 01-00-5e-00-00-01 und 01-00-5e-00-00-02 hört (Adressen für den Urlaub).

```
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. Der Client sendet eine IMPG Leave-Nachricht an 224.0.0.2. Der Switch fängt es ab und sendet eine IGMP-Abfrage an den Port, an den er den Urlaub empfängt. Folgendes ist **debug** Ausgabe am 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. Da keine Antwort empfangen wurde, leitet der Catalyst die IGMP-Leave-Nachricht an den Router weiter (siehe unten).

```
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. Der Router empfängt eine IGMP-Leave-Nachricht, also sendet er eine CGMP-Leave-Nachricht an den Switch und löscht die Gruppe auch aus der IGMP-Gruppenliste. Im Folgenden finden Sie die **debug** Befehlsausgabe auf dem Router.**Auf dem Router**

```
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
```

CGMP-Ablaufverfolgungen und -Konfiguration

Bild 1

Frame 1 ist ein CGMP Join Frame zu GDA 00-00-00-00-00-00-00. Sie wird verwendet, um den Router-Port der Router-Port-Liste hinzuzufügen.

```
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:
```

Das Ergebnis "Frame 1" befindet sich auf dem Switch, wobei "3/1" der Port ist, der mit dem Router verbunden ist:

Bild 2

Frame 2 ist ein IGMP-Mitgliedschaftsbericht, den der Host sendet, um anzufordern (oder zu bestätigen), dass Benutzer Datenverkehr für die Gruppe 239.10.10.10 empfangen möchten.

```
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:
```

Bild 3

Frame 3 ist der vom Router an den Switch gesendete CGMP-Frame, der den Switch anweist, einen statischen Eintrag für 01-00-5e-0a-0a-0a hinzuzufügen.

```
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:
```

Im Folgenden sehen Sie die Konfiguration von Router und 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)
```

IGMP-Snooping

IGMP-Snooping ist eine weitere Funktion, mit der Sie IGMP-Frames direkt erfassen können. Informationen zur Unterstützung von IGMP-Snooping auf Catalyst-Switches finden Sie in der Multicast Catalyst Switches Support Matrix.

IGMP-Snooping - Übersicht

IGMP-Snooping ist eine Funktion, die es dem Switch ermöglicht, die IGMP-Konversation zwischen Hosts und Routern anzuhören. Wenn ein Switch einen IGMP-Bericht eines Hosts für eine bestimmte Multicast-Gruppe hört, fügt der Switch die Port-Nummer des Hosts der GDA-Liste für diese Gruppe hinzu. Wenn der Switch einen IGMP Leave hört, wird der Host-Port aus dem Eintrag

in der CAM-Tabelle entfernt.

Erlernen des Router-Ports

Der Switch empfängt die folgenden Meldungen, um Router-Ports mit IGMP-Snooping zu erkennen:

- IGMP-Mitgliedschaftsabfrage wird an 01-00-5e-00-00-01 gesendet
- PIMv1 Hello-Senden an 01-00-5e-00-00-02
- PIMv2 Hello an 01-00-5e-00-00-0d senden
- DVMRP-Probes werden an 01-00-5e-00-04 gesendet
- MOSPF-Nachricht an 01-00-5e-00-05 oder 06 senden

Durch Aktivieren von IGMP-Snooping auf einem Switch werden alle oben genannten MAC-Einträge dem **show cam system** Ausgabe des Snooping-Switches. Sobald ein Router-Port erkannt wurde, wird er der Port-Liste aller GDAs in diesem VLAN hinzugefügt.

Einem IGMP-Snooping beitreten

Es gibt zwei Zusammenfügeszenarien:

Szenario A: Host A ist der erste Host, der einer Gruppe im Segment beitritt.

1. Host A sendet einen nicht angeforderten IGMP-Mitgliedschaftsbericht.
2. Der Switch fängt den IGMP-Mitgliedschaftsbericht ab, der vom Host gesendet wurde, der der Gruppe beitreten wollte.
3. Der Switch erstellt einen Multicast-Eintrag für diese Gruppe und verbindet ihn mit dem Port, an dem er den Bericht empfangen hat, sowie mit allen Router-Ports.
4. Der Switch leitet den IGMP-Bericht an alle Router-Ports weiter. Dadurch erhält der Router auch den IGMP-Bericht und aktualisiert seine Multicast-Routing-Tabelle entsprechend.

Szenario B: Host B ist jetzt der zweite Host, der derselben Gruppe beitritt.

1. Host B sendet einen nicht angeforderten IGMP-Mitgliedschaftsbericht.
2. Der Switch fängt den IGMP-Mitgliedschaftsbericht ab, der vom Host gesendet wurde, der der Gruppe beitreten möchte.
3. Der Switch leitet den IGMP-Bericht nicht notwendigerweise an alle Router-Ports weiter. Tatsächlich leitet der Switch IGMP-Berichte mithilfe von Proxy-Berichten an Router-Ports weiter und leitet nur einen Bericht pro Gruppe innerhalb von 10 s weiter.

   Anmerkung: Um die Gruppenmitgliedschaft aufrechtzuerhalten, sendet der Multicast-Router alle 60 Sekunden eine IGMP-Abfrage. Diese Abfrage wird vom Switch abgefangen und an alle Ports am Switch weitergeleitet. Alle Hosts, die Mitglieder der Gruppe sind, beantworten diese Abfrage. Da der Switch jedoch auch den Antwortbericht abfängt, sieht der andere Host nicht alle anderen Berichte. Daher senden alle Hosts einen Bericht (statt eines Berichts pro Gruppe). Der Switch verwendet dann auch Proxy Reporting, um nur einen Bericht pro Gruppe unter allen empfangenen Antworten weiterzuleiten.

Angenommen, Host A möchte die Gruppe verlassen, Host B möchte jedoch die Gruppe trotzdem empfangen.

- Der Switch erfasst die IGMP-Leave-Nachricht von Host A.
- Der Switch gibt eine gruppenspezifische IGMP-Abfrage für die Gruppe an diesem Port (und nur an diesem Port) aus.
- Wenn der Switch keinen Bericht empfängt, verwirft er diesen Port aus dem Eintrag. Wenn er eine Antwort von diesem Port erhält, tut er nichts und verwirft den Urlaub.
- Host B ist weiterhin von dieser Gruppe an diesem Switch interessiert. Dies ist nicht der letzte Nicht-Router-Port im Eintrag. Daher leitet der Switch die Leave-Nachricht nicht weiter.

Nehmen wir nun an, Host B möchte die Gruppe verlassen, und Host B ist der letzte Benutzer, der von dieser Gruppe in diesem Segment interessiert ist.

- Der Switch erfasst die IGMP-Leave-Nachricht von Host A.
- Der Switch gibt eine gruppenspezifische IGMP-Abfrage für diese Gruppe an diesem Port aus.
- Wenn der Switch keinen Bericht empfängt, verwirft er diesen Port aus dem Eintrag.
- Dies ist der letzte Nicht-Router-Port für diese GDA. Der Switch leitet die IGMP-Leave-Nachricht an alle Router-Ports weiter und entfernt den Eintrag aus der Tabelle.

IGMP-/CGMP-Interaktion

In einigen Netzwerken können Sie IGMP-Snooping aufgrund von Hardware-Einschränkungen möglicherweise nicht auf allen Switches ausführen. In diesem Fall müssen Sie CGMP möglicherweise auf einigen Switches im gleichen Netzwerk ausführen.

Beachten Sie, dass es sich um einen Sonderfall handelt. Der Switch, auf dem IGMP-Snooping ausgeführt wird, erkennt CGMP-Nachrichten und erkennt, dass einige Switches im Netzwerk CGMP ausführen. Daher wechselt er in einen speziellen IGMP-CGMP-Modus und deaktiviert das Proxy-Reporting. Dies ist für den ordnungsgemäßen Betrieb des CGMP unbedingt erforderlich, da Router die Quell-MAC-Adresse des IGMP-Berichts verwenden, um eine CGMP-Join-Nachricht zu erstellen. Router, auf denen CGMP ausgeführt wird, müssen alle IGMP-Berichte anzeigen, daher muss die Proxy-Berichterstellung deaktiviert werden. Berichte, die an den Router gesendet werden, sollten nur für IGMP-Snooping erforderlich sein.

Multicast-Quellnetzwerk

Wenn das Segment nur einen Multicast-Server (Multicast-Quelle) und keinen Client enthält, kann es vorkommen, dass Sie in diesem Segment keine IGMP-Pakete haben, aber sehr viel Multicast-Datenverkehr. In diesem Fall leitet der Switch den Datenverkehr von dieser Gruppe einfach an alle Mitglieder des Segments weiter. Glücklicherweise kann ein Switch, der IGMP-Snooping ausführt, diese Multicast-Streams erkennen und einen Multicast-Eintrag für diese Gruppe mit nur dem Router-Port hinzufügen. Diese Einträge werden intern als `mcast_source_only` gekennzeichnet und werden alle 5 Minuten ausgeschaltet, oder wenn der Router-Port entfernt wird. Beachten Sie, dass die Adresse selbst nach dieser Alterung innerhalb weniger Sekunden neu gelernt wird, wenn der Datenverkehr anhält. Innerhalb der Lernphase kann es zu vorübergehenden Überflutungen im VLAN kommen. Um dies zu vermeiden und die Einträge beizubehalten, verwenden Sie die **set igmp flooding enable | disable** aus. Nachdem die Flooding deaktiviert wurde, werden die Quelleinträge nicht vom Switch verworfen.

Einschränkungen

Wie beim CGMP werden GDAs, die einer MAC-Adresse zugeordnet sind, die im Bereich 01-00-5e-00-00-xx liegt, nie durch IGMP-Snooping beschnitten.

Konfiguration von IGMP-Snooping auf Cisco Switches

Führen Sie den folgenden Befehl aus, um IGMP-Snooping zu aktivieren/deaktivieren:

- **set igmp**

Führen Sie zum Konfigurieren des Multicast-Routers (statisch) den folgenden Befehl aus:

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

Führen Sie die folgenden Befehle aus, um IGMP-Statistiken zu überwachen und zu überprüfen:

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

Praktisches Beispiel für IGMP-Snooping

Die Konfiguration für dieses Beispiel ähnelt der CGMP-Testphase, die zuvor in diesem Dokument verwendet wurde. Der einzige Unterschied besteht darin, dass die Ports 3/2 und 3/3 mit demselben VLAN verbunden sind und beide vom Client für die Verbindung zur Gruppe 224.10.10.10 konfiguriert sind.

Im folgenden Beispiel werden verschiedene Manipulationen erklärt, die Funktionsweise des Switches untersucht und die resultierende Ausgabe untersucht. Im folgenden Beispiel ist *Switch_B* ein Catalyst 5500 mit IGMP-Snooping und *Router_A* der mit Port 3/1 verbundene Multicast-Router.

1. Aktivieren Sie IGMP-Snooping auf dem Switch, und sehen Sie das Ergebnis, indem Sie **debug** aus. Beachten Sie, dass jeder Satz von Einträgen dem **show cam sys** Befehlsausgabe, die die Erkennung des Routerports über PIM, MOSPF usw. ermöglicht.

```
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. Der Switch empfängt ein PIMv2-Paket von Router_A und fügt den Router-Port hinzu.

```
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. Verbinden Sie einen neuen Host in Gruppe 224.10.10.10 (an Port 3/2). Dieser Host sendet einen IGMP-Mitgliedschaftsbericht. Der Bericht wird empfangen, vom Switch geschockt, der Eintrag hinzugefügt und der IGMP-Bericht an den Router weitergeleitet.**Ein 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. Fügen Sie einen weiteren Benutzer in VLAN 3 an Port 3/3 hinzu (siehe unten).

```
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. Entfernen Sie Port 3/2. Port 3/2 sendet eine IGMP Leave-Nachricht. Der Switch sendet eine gruppenspezifische IGMP-Abfrage an Port 3/2 zurück und startet einen Timer. Wenn der Timer abläuft, ohne eine Antwort zu erhalten, wird der Port aus der Gruppe gelöscht.

```
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. Der Host auf Port 3/3 verlässt die Gruppe und sendet eine IGMP Leave-Nachricht. Der einzige Unterschied zum vorherigen Punkt besteht darin, dass die IGMP-Leave-Nachricht schließlich an den Router-Port weitergeleitet wird.

```
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
```

Die Subnetzkonfiguration ist jetzt wieder am Anfang, ihr Zustand befindet sich in Schritt 1. Der Multicast-Eintrag ist aus dem **show cam static** Befehlsausgabe.

Zeigen Sie abschließend ein Beispiel des **show igmp static** Befehlsausgabe, wie unten gezeigt.

```
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)
```

Zugehörige Informationen

- Unterstützte Multicast-Catalyst-Switches
- Support-Seite für IP-Multicast
- Cisco Technologie-Support
- Cisco Produkt-Support
- Technischer Support und Dokumentation für Cisco Systeme