Fehlerbehebung bei Multicast-Netzwerken mit CLI-Tools

Inhalt

Einleitung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Konventionen
Strategien zur Fehlerbehebung
Quell-Paketfluss prüfen
Netzwerksignalisierung überprüfen
Fehlerbehebung: PIM Sparse Mode
Überprüfung des Netzwerkpaketflusses
Empfängersignalisierung überprüfen
Empfängerpaketfluss überprüfen
Power CLI-Tools
mstat
Marinefo
mtrace
Ping
show-Befehle
ip igmp-Gruppen anzeigen
show ip igmp-Schnittstelle
show ip pim neighbor
show ip pim interface
show ip mroute summary
show ip mroute
show ip mroute active
show ip rpf
show ip mcache
show ip mroute count
show ip route
show ip pim rp mapping
debug-Befehle
debug ip igmp
debug ip mpacket
debug ip mrouting
debug ip pim
Zugehörige Informationen

Einleitung

In diesem Dokument werden verschiedene Tools und Techniken zur Fehlerbehebung bei Multicast-Netzwerken beschrieben.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

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

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 kennen.

Konventionen

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

Strategien zur Fehlerbehebung

Bei der Fehlerbehebung in Multicast-Netzwerken ist es ratsam, das im Netzwerk und Paketfluss verwendete Signalisierungsprotokoll zu berücksichtigen. Das Signalisierungsprotokoll dient zum Einrichten und Beenden der Multicast-Sitzungen (z. B. PIM Dense Mode, PIM Sparse Mode und DVMRP). Der Paketfluss ist das tatsächliche Senden, Replizieren und Empfangen der Multicast-Pakete zwischen Quelle und Empfänger, basierend auf der vom Signalisierungsprozess erstellten Weiterleitungstabelle.

Diese Tabelle hilft bei der Überprüfung der zu behebenden Informationen und überprüft, ob die einzelnen Abschnitte der Tabelle ordnungsgemäß funktionieren:

	Quelle	Netzwerk	Empfänger
Signalisierung	NA	Netzwerksignalisierung überprüfen	Empfängersignalisierung überprüfen
Paketfluss	Quell-Paketfluss prüfen	Überprüfung des Netzwerkpaketflusses	Empfängerpaketfluss überprüfen

In den nächsten Unterabschnitten werden die Tools zur Fehlerbehebung beschrieben, mit denen Sie häufige Probleme überprüfen und beheben können.

Quell-Paketfluss prüfen

Gehen Sie wie folgt vor, um festzustellen, ob die Quelle die Pakete gesendet hat und ob die richtigen Paketfelder eingefügt wurden:

1. Überprüfen Sie die Schnittstellenzähler auf dem Host. Überprüfen Sie zunächst die Schnittstellenzähler (wenn Sie sich auf einem UNIX-System befinden, verwenden Sie den Befehl **netstat**) auf dem Quellhost, um festzustellen, ob Pakete gesendet werden. Ist dies nicht der Fall, überprüfen Sie den Host-Stack und die Anwendung auf fehlerhafte Konfigurationen oder Fehler.

2. Überprüfen Sie mit dem Befehl **show ip igmp groups <Schnittstellenname>**, ob der Upstream-Router an der direkt mit der Quelle verbundenen Schnittstelle einen Bericht über die Join-Mitgliedschaft erhalten hat.

3. Überprüfen Sie den TTL-Wert für die Pakete in der Multicast-Anwendung; er muss größer als 1 sein. Wenn die Anwendung Pakete mit einem TTL-Wert kleiner als 1 sendet, muss der Datenverkehr am ersten Upstream-Router verworfen werden. Verwenden Sie den Befehl **show ip traffic**, um den Wert des Zählers für die "bad hop count" (fehlerhafte Hop-Anzahl) zu überprüfen. Jedes Paket mit einem TTL-Wert von 1 oder weniger als dem TTL-Schwellenwert, der von der Schnittstelle mit dem **ip multicast ttl-threshold-**Befehl festgelegt wurde, wird verworfen, und der Zähler für die "schlechte Hop-Anzahl" wird um eins erhöht. Verwenden Sie den Befehl **show ip igmp interface <Schnittstellenname>**, um den TTL-Grenzwert für die Schnittstelle anzuzeigen.

4. Verwenden Sie die Befehle **show ip mroute count** und **show ip mroute active**, um den ersten Upstream-Router oder Switch zu überprüfen, ob er Multicast-Pakete von der Quelle erkennt. Die Befehlsausgabe zeigt die Datenverkehrsfluss-Statistiken für jedes (S,G)-Paar an. Wenn Sie keinen Datenverkehr beobachten, überprüfen Sie die Empfängersignalisierung.

5. Verwenden Sie den Befehl **debug ip mpacket** auf dem nächstgelegenen Upstream-Router mit dem Argument **detail** oder **acl** für die Detailgenauigkeit.

Vorsicht: Verwenden Sie diesen Befehl mit Vorsicht, wenn im Netzwerk ein hoher Multicast-Verkehr verzeichnet wird. Verwenden Sie den Befehl debug ip mpacket auf der Route nur, wenn dies erforderlich ist. Verwenden Sie das **detail-**Argument, um Paket-Header in der **Debug-**Ausgabe anzuzeigen, sowie Zugriffslisten, um den Datenverkehr bestimmter Quellen zu überprüfen. Denken Sie daran, dass dieser Befehl erhebliche Auswirkungen auf die Leistung des anderen Datenverkehrs haben kann.

Netzwerksignalisierung überprüfen

Dies ist die komplexeste und wichtigste Komponente zur Fehlerbehebung in einem Netzwerk. Dies hängt vom verwendeten Netzwerksignalisierungsprotokoll ab, z. B. PIM Sparse Mode, PIM Dense Mode und DVMRP. Wir empfehlen den in diesem Abschnitt beschriebenen mehrstufigen Ansatz.

Fehlerbehebung: PIM Sparse Mode

Gehen Sie wie folgt vor, um die Fehlerbehebung für den PIM Sparse Mode durchzuführen:

1. Überprüfen Sie, ob IP-Multicast-Routing auf allen Multicast-Routern aktiviert ist.

2. Verwenden Sie den Befehl **show ip pim neighbor,** um den Ablauf-Timer und den Modus zu überprüfen, um eine erfolgreiche Einrichtung des PIM-Nachbarn sicherzustellen, und suchen Sie nach möglichen Verbindungs- und Zeitgeberproblemen, die die Einrichtung von PIM-Nachbarn verhindern können. Falls erforderlich, verwenden Sie den Unterbefehl **ip pim [version] [dense-mode] [sparse-mode] [sparse-dense-mode] Schnittstellenebene,** um den korrekten Modus und die richtige Version festzulegen, damit die PIM-Nachbarn erfolgreich eingerichtet werden können.

3. Verwenden Sie den Befehl **show ip pim rp mapping**, um die richtige Zuordnung der RP-Gruppe sicherzustellen und den Ablaufzeitpunkt zu überprüfen, wenn auto-RP konfiguriert ist. Verwenden Sie den Befehl **debug ip pim auto-rp**, um etwaige Fehler beim automatischen Erstellen zu ermitteln. Wenn keine PIM Group-to-RP-Zuordnungen angezeigt werden, überprüfen Sie die Auto-RP-Konfiguration, oder konfigurieren Sie statische Group-RP-Zuordnungen mit der **IP-Adresse ip pim rp-address des** Befehls **RP [access-list] [named-accesslist] [override].** Die automatische RP-Konfiguration kann mit den Befehlen **ip pim send-rp-announce interface-id scope TTL value** und **ip pim send-rp-discovery interface-id scope TTL value** durchgeführt werden. Diese Befehle müssen nur konfiguriert werden, wenn automatische RP-Konfigurationen vorhanden sind.

4. Verwenden Sie den Befehl **show ip rpf <ip address of source>**, um den RPF-Fehler für die Quelladresse zu überprüfen. Der PIM Dense Mode und der PIM Sparse Mode senden Prune-Nachrichten an die Quelle zurück, wenn der Datenverkehr an einer Point-to-Point-Schnittstelle ankommt, die keine RPF-Schnittstelle ist. Mit dem Befehl **debug ip pim** können Sie mögliche Ursachen für einen Fehler in einem PIM-Netzwerk ermitteln. Er vergleicht die typische Ausgabe mit dem, was Sie sehen. Verwenden Sie diese Ausgabe, um die drei diskreten Stufen im PIM Sparse Mode zu identifizieren: Join, Registering und SPT-Switchover. Mit dem Befehl **show ip mroute** können Sie die Nulleinträge in den Listen der ausgehenden Schnittstellen und die bereinigten Einträge in der mroute-Tabelle überwachen.

Überprüfung des Netzwerkpaketflusses

Verwenden Sie diese Befehle, um den Fluss von Multicast-Paketen im Netzwerk zu überprüfen:

- Verwenden Sie den Befehl **mtrace**, um Multicast Trace Hop-by-Hop zu überprüfen.
- **mstat**
- **Ping**
- **show ip mroute count**
- **show ip mroute active**
- **debug ip mpacket**

Empfängersignalisierung überprüfen

Gehen Sie wie folgt vor, um die Empfängersignalisierung zu überprüfen:

1. Verwenden Sie den Befehl **show ip igmp groups** auf dem ersten Upstream-Router, der mit dem Empfänger verbunden ist, um zu überprüfen, ob die Schnittstelle der Gruppe beigetreten ist.
2. Verwenden Sie den Befehl **ping**, um die Erreichbarkeit des Hosts und des ersten Upstream-Routers zu überprüfen.
3. Verwenden Sie den Befehl **show ip igmp interface**, um die IGMP-Version der Schnittstelle zu überprüfen.

> **Hinweis**: Beachten Sie, dass ein mit IGMP Version 1 konfigurierter Router IGMP Version 2-Pakete, die vom Host empfangen wurden, als ungültig betrachtet. Diese IGMP-Pakete werden erst in die Gruppe aufgenommen, wenn der Router ein IGMP-Paket der Version 1 vom Host empfängt.

---

4. Verwenden Sie den Befehl **debug ip igmp**, um weitere Fehler bei der Empfängersignalisierung zu beheben.

Empfängerpaketfluss überprüfen

Führen Sie die folgenden Schritte aus, um den Paketfluss des Empfängers zu überprüfen:

1. Verwenden Sie den Befehl **netstat** auf einem UNIX-System, um die Statistiken der Empfängerschnittstelle zu überprüfen.

2. Überprüfen Sie, ob der TCP/IP-Stack ordnungsgemäß installiert und konfiguriert wurde.

3. Überprüfen Sie, ob die Multicast Receiver-Clientanwendung installiert und ordnungsgemäß konfiguriert wurde.

4. Achten Sie auf duplizierte Multicast-Pakete in einem Multizugriffssegment.

Power CLI-Tools

Die Befehle in diesem Abschnitt können auch bei der Fehlerbehebung nützlich sein, insbesondere wenn Sie den Netzwerkpaketfluss testen und die Fehlerpunkte im Multicast-Netzwerk ermitteln.

mstat

Dieser Befehl zeigt den Multicast-Pfad im ASCII-Grafikformat an. Es verfolgt den Pfad zwischen zwei beliebigen Punkten im Netzwerk, zeigt Verwerfungen und Duplikate, TTLs und Verzögerungen an jedem Knoten im Netzwerk an. Es ist sehr nützlich, wenn Sie Engpässe im Netzwerk lokalisieren müssen oder sich auf einen Router mit hoher Anzahl an Verlusten/Duplikaten konzentrieren müssen. Duplikate werden in der Ausgabe als "negative" Drops angezeigt.

<#root>

```
Router#
```

mstat lwei-home-ss2 172.16.58.88 224.0.255.255

```
Type escape sequence to abort
Mtrace from 172.16.143.27 to 172.16.58.88 via group 224.0.255.255
>From source (lwei-home-ss2.cisco.com) to destination (lwei-ss20.cisco.com)
Waiting to accumulate statistics......
Results after 10 seconds:

  Source        Response Dest    Packet Statistics For    Only For Traffic
172.16.143.27    172.16.62.144    All Multicast Traffic     From 172.16.143.27
     |       __/  rtt 48   ms   Lost/Sent = Pct  Rate     To 224.0.255.255
     v      /     hop 48   ms   ---------------------     --------------------
172.16.143.25   lwei-cisco-isdn.cisco.com
     |     ^      ttl   1
     v     |      hop 31   ms    0/12 = 0%      1 pps    0/1 = --%  0 pps
172.16.121.84
172.16.121.45   eng-frmt12-pri.cisco.com
     |     ^      ttl   2
     v     |      hop -17  ms    -735/12 = --%      1 pps    0/1 = --%  0 pps
172.16.121.4
172.16.5.27     eng-cc-4.cisco.com
     |     ^      ttl   3
     v     |      hop -21  ms    -678/23 = --%      2 pps    0/1 = --%  0 pps
172.16.5.21
172.16.62.130   eng-ios-2.cisco.com
     |     ^      ttl   4
     v     |      hop 5    ms    605/639 = 95%      63 pps    1/1 = --%  0 pps
172.16.62.144
172.16.58.65    eng-ios-f-5.cisco.com
     |      \__   ttl   5
     v         \  hop 0    ms        4         0 pps           0    0 pps
172.16.58.88    172.16.62.144
  Receiver      Query Source
```

Marinefo

Dieser Befehl zeigt Informationen zu den Multicast-Nachbarroutern, den Routerfunktionen und der Codeversion, Informationen zu den Multicast-Schnittstellen, TTL-Schwellenwerten, Metriken, Protokollen und Status an. Sie ist nützlich, wenn Sie Multicast-Nachbarn überprüfen, überprüfen müssen, ob bidirektionale Nachbarn-Adjacency vorhanden ist, und überprüfen müssen, ob Tunnel in beide Richtungen verfügbar sind.

<#root>

```
Router#
```

mrinfo

```
  192.168.7.37 (b.cisco.com) [version cisco 11.1] [flags: PMSA]:
  192.168.7.37 -> 192.168.7.34 (s.cisco.com) [1/0/pim]
  192.168.7.37 -> 192.168.7.47 (d.cisco.com) [1/0/pim]
  192.168.7.37 -> 192.168.7.44 (d2.cisco.com) [1/0/pim]
  192.168.9.26  -> 192.168.9.29 (su.bbnplanet.net) [1/32/pim]
```

Die Markierungen in der Ausgabe zeigen Folgendes an:

- P = pflaumenfähig
- M = mtrace-fähig
- S = SNMP-fähig
- A = Auto-RP-fähig

mtrace

Dieser Befehl zeigt den Multicast-Pfad von der Quelle zum Empfänger sowie den Pfad zwischen den Punkten in den Netzwerken an. Dieser Befehl zeigt TTL-Grenzwerte und Verzögerungen an jedem Knoten an. Verwenden Sie bei der Fehlerbehebung den Befehl **mtrace,** um zu ermitteln, wo der Multicast-Datenverkehrsfluss endet, um den Pfad des Multicast-Datenverkehrs zu überprüfen und um suboptimale Pfade zu identifizieren.

<#root>

```
Router#
```

mtrace 192.168.215.41 192.168.215.67 239.254.254.254

```
Type escape sequence to abort.
Mtrace from 192.168.215.41 to 192.168.215.67 via group 239.254.254.254
From source (?) to destination (?)
Querying full reverse path...
0  192.168.215.67
-1  192.168.215.67 PIM  thresh^ 0  0 ms
-2  192.168.215.74 PIM  thresh^ 0  2 ms
-3  192.168.215.57 PIM  thresh^ 0  894 ms
-4  192.168.215.41 PIM  thresh^ 0  893 ms
```

```
-5  192.168.215.12 PIM  thresh^ 0  894 ms
-6  192.168.215.98 PIM  thresh^ 0  893 ms
```

Ping

Bei der Fehlerbehebung ist der Befehl **ping** die einfachste Methode, Multicast-Datenverkehr im Labor zu generieren, um die Multicast-Struktur zu testen, da alle Mitglieder der Gruppe gepingt werden und alle Mitglieder reagieren.

<#root>

```
R3#
```

ping 239.255.0.1

```
 Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 239.255.0.1, timeout is 2 seconds:
Reply to request 0 from 172.16.12.2, 16 ms
Reply to request 0 from 172.16.7.2, 20 ms
```

show-Befehle

Die Befehle in diesem Abschnitt helfen Ihnen beim Sammeln nützlicher Informationen, wenn Sie Probleme mit Multicast beheben. Ausführlichere Informationen zu diesen **show**-Befehlen finden Sie im Cisco IOS IP Multicast Command Reference Guide.

> **Tipp:** Wenn die Antworten des Befehls **show** träge sind, führt der Router wahrscheinlich derzeit eine IP-Domänensuche nach IP-Adressen im Befehl **show** durch. Sie können die IP-Domänensuche deaktivieren, indem Sie den Befehl **no ip domain-lookup** im globalen Konfigurationsmodus des Routers verwenden, um die IP-Domänensuche zu deaktivieren. Dadurch wird die IP-Domänensuche beendet und die Ausgabegeschwindigkeit des Befehls **show** erhöht.

---

ip igmp-Gruppen anzeigen

Dieser Befehl zeigt an, welche Multicast-Gruppen direkt mit dem Router verbunden sind und welche über das Internet Group Management Protocol (IGMP) erfasst werden. Mit diesem Befehl können Sie überprüfen, ob eine Quelle oder ein Empfänger der Zielgruppe an der Router-Schnittstelle tatsächlich beigetreten ist. In der Spalte "**Last Reporter**" wird nur ein IGMP-Host angezeigt, der angibt, dass er als Antwort auf eine IGMP-Abfrage des PIM-Routers für diese Gruppe entweder einen unaufgeforderten IGMP-Join- oder einen IGMP-Bericht gesendet hat. Es darf nur ein **letzter Reporter** pro Gruppenadresse angezeigt werden.

<#root>

```
R1#
```

show ip igmp groups

```
IGMP Connected Group Membership
Group Address    Interface      Uptime          Expires         Last Reporter
```

```
239.255.0.1      Ethernet1      00:10:54        00:01:10        192.168.9.1
224.0.1.40       Ethernet0      01:36:27        00:02:45        192.168.10.2
224.0.1.40       Ethernet1      01:48:15        never           192.168.9.3
```

show ip igmp-Schnittstelle

Verwenden Sie diesen Befehl, um Multicast-bezogene Informationen über eine Schnittstelle anzuzeigen. Um zu überprüfen, ob IGMP aktiviert ist, wird die richtige Version ausgeführt, und die Timer, der TTL-Schwellenwert (Time To Live) und der IGMP Querier-Router sind richtig festgelegt. IGMP muss nicht für eine Schnittstelle konfiguriert werden. Sie ist standardmäßig aktiviert, wenn Sie **ip pim {dense-mode|sparse-mode|sparse-dense-mode} konfigurieren**.

<#root>

```
R1#
```

show ip igmp interface

```
Ethernet1 is up, line protocol is up
  Internet address is 192.168.9.3/24
```

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
  Last member query response interval is 1000 ms
  Inbound IGMP access group is not set
  IGMP activity: 22 joins, 18 leaves
  Multicast routing is enabled on interface
  Multicast TTL threshold is 0
  Multicast designated router (DR) is 192.168.9.5
  IGMP querying router is 192.168.9.3 (this system)
  Multicast groups joined (number of users):
      224.0.1.40(1)
```

show ip pim neighbor

Mit diesem Befehl können Sie die von der Cisco IOS®-Software erkannten Protocol Independent Multicast (PIM)-Nachbarn auflisten.

<#root>

```
R1#
```

show ip pim neighbor

```
PIM Neighbor Table
Neighbor          Interface               Uptime/Expires    Ver   DR
Address                                                           Prio/Mode
```

```
10.10.10.1        Ethernet0/0              02:19:41/00:01:38 v2    1 / DR B S
```

Einzelheiten zu den einzelnen Feldern finden Sie hier:

- **Nachbar-Adresse**: Gibt eine IP-Adresse des PIM-Nachbarn an.
- **Schnittstelle** - Eine Schnittstelle, bei der ein PIM-Nachbar erkannt wurde.
- **Betriebszeit** - Die Gesamtbetriebszeit des Nachbarn
- **Läuft ab** - Die Zeit, bevor ein Timeout für einen Nachbarn auftritt und bis der nächste PIM-Hello empfangen wird.
- **Ver** - Die PIM-Version auf der Nachbarschnittstelle
- **DR Prio**- Mögliche Werte sind 0 bis 4294967294 oder "N"

  Dies ist eine neue Spalte, die die Priorität einer PIM-Schnittstelle für die DR-Auswahl verfolgt. Die Funktion zum Konfigurieren eines DR auf der Grundlage der höchsten Priorität im Vergleich zur höchsten IP-Adresse wurde in den Cisco IOS Software-Versionen 12.1(2)T und 12.2 und Cisco IOS-Images mit Bidir-PIM eingeführt. Sie können den Schnittstellenbefehl **eip pim dr-priority <0-4294967294>** verwenden, um die DR-Priorität festzulegen. Die Standard-DR-Priorität ist auf 1 festgelegt. Wenn ein PIM-Nachbar eine ältere Cisco IOS-Version ausführt, die die DR-Prioritätsfunktion nicht unterstützt, wird in der Spalte "DR Prior" aus Interoperabilitätsgründen "N" angezeigt. Wenn der Nachbar der einzige Router ist, der "N" für die Schnittstelle anzeigt, wird er zum DR, unabhängig davon, welcher Router tatsächlich die höchste IP-Adresse hat. Wenn in dieser Spalte mehrere PIM-Nachbarn mit "N" aufgeführt sind, ist der Timer-Breaker die höchste IP-Adresse unter diesen Nachbarn.
- **Modus**: Informationen zum DR und anderen PIM-Funktionen

  In dieser Spalte wird der DR zusätzlich zu den vom PIM-Nachbarn unterstützten Funktionen aufgeführt:

DR - Der PIM-Nachbar ist ein designierter Router.

B- Bidirectional PIM (Bidir-PIM)-fähig

S- State Refresh-fähig (gilt nur für den Dense-Modus)

Verwenden Sie bei der Fehlerbehebung diesen Befehl, um zu überprüfen, ob alle Nachbarn aktiv sind und den richtigen Modus, die richtige Version und den richtigen Ablaufzeitpunkt verwenden. Sie können auch die Router-Konfiguration überprüfen oder den Modus mit dem Befehl show ip pim interface (PIM Sparse- oder Dense-Modus) überprüfen. Verwenden Sie den Befehl debug ip pim, um den Nachrichtenaustausch pim-query zu beobachten.

show ip pim interface

Verwenden Sie diesen Befehl, um Informationen über für PIM konfigurierte Schnittstellen anzuzeigen. Mit diesem Befehl können Sie außerdem überprüfen, ob der richtige PIM-Modus (Dense oder Sparse) für die Schnittstelle konfiguriert ist, die Anzahl der Nachbarn richtig ist und der designierte Router (DR) richtig ist (was für den PIM Sparse Mode wichtig ist). Segmente mit mehreren Zugriffen (z. B. Ethernet, Token Ring, FDDI) wählen einen DR basierend auf der höchsten IP-Adresse aus. Point-to-Point-Links zeigen keine DR-Informationen an.

<#root>

```
R1#
```

show ip pim interface

```
Address          Interface          Version/Mode    Nbr   Query     DR
                                                    Count Intvl
192.168.10.1     Ethernet0          v2/Sparse-Dense  1    30     192.168.10.2
192.168.9.3      Ethernet1          v2/Sparse-Dense  1    30     192.168.9.5
```

show ip mroute summary

Mit diesem Befehl können Sie den zusammengefassten Inhalt der IP-Multicast-Routing-Tabelle anzeigen. Sie können es auch verwenden, um die aktive(n) Multicast-Gruppe(n) zu überprüfen und festzustellen, welche Multicast-Absender aktiv sind, wenn Sie die Timer und Flags überprüfen.

<#root>

```
R1#
```

show ip mroute summary

```
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
       M - MSDP created entry, X - Proxy Join Timer Running
       A - Advertised via MSDP
Outgoing interface flags: H - Hardware switched
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 239.255.0.1), 01:57:07/00:02:59, RP 192.168.7.2, flags: SJCF
  (192.168.33.32, 239.255.0.1), 01:56:23/00:02:59, flags: CJT
  (192.168.9.1, 239.255.0.1), 01:57:07/00:03:27, flags: CFT

(*, 224.0.1.40), 1d00h/00:00:00, RP 192.168.7.2, flags: SJPCL
```

show ip mroute

Verwenden Sie diesen Befehl, um den vollständigen Inhalt der IP-Multicast-Routing-Tabelle anzuzeigen. Verwenden Sie bei der Fehlerbehebung diesen Befehl, um Folgendes zu überprüfen:

- Die Zustandseinträge (S,G) und (*,G) aus den Flags.
- Die Eingangsschnittstelle ist korrekt. Ist dies nicht der Fall, überprüfen Sie die Unicast-Routing-Tabelle.
- Die ausgehenden Schnittstellen sind richtig. Wenn sie nicht korrekt bereinigt wurde, überprüfen Sie den Status im Downstream-Router.

<#root>

```
R1#
```

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
       M - MSDP created entry, X - Proxy Join Timer Running
       A - Advertised via MSDP
Outgoing interface flags: H - Hardware switched
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode
```

(*, 239.255.0.1), 01:55:27/00:02:59, RP 192.168.7.2, flags: SJCF

```
  Incoming interface: Ethernet0, RPF nbr 192.168.10.2
  Outgoing interface list:
    Ethernet1, Forward/Sparse, 01:55:27/00:02:52
```

(192.168.33.32 , 239.255.0.1), 01:54:43/00:02:59, flags: CJT

```
  Incoming interface: Ethernet0, RPF nbr 192.168.10.2
```

Outgoing interface list:
Ethernet1, Forward/Sparse, 01:54:43/00:02:52

```
(192.168.9.1, 239.255.0.1), 01:55:30/00:03:26, flags: CFT
  Incoming interface: Ethernet1, RPF nbr 0.0.0.0
  Outgoing interface list:
    Ethernet0, Forward/Sparse, 01:55:30/00:03:12

(*, 224.0.1.40), 1d00h/00:00:00, RP 192.168.7.2, flags: SJPCL
  Incoming interface: Ethernet0, RPF nbr 192.168.10.2
  Outgoing interface list: Null
```

show ip mroute active

Verwenden Sie diesen Befehl, um die aktiven Datenverkehrsquellen und -gruppen anzuzeigen, die den Schwellenwert überschreiten. Wenn Sie die Fehlerbehebung durchführen, überprüfen Sie mit diesem Befehl die aktiven Quellgruppen, die Datenverkehrsrate für jedes Quellgruppen-Paar (S,G) (Sie müssen auf Shortest Path Tree (SPT) umgeschaltet haben) und prüfen Sie, ob Multicast-Datenverkehr der Zielgruppe empfangen wird. Wenn der Datenverkehr nicht empfangen wird, suchen Sie nach aktivem Datenverkehr, der von der Quelle in Richtung Empfänger beginnt.

<#root>

```
R1#
```

show ip mroute active

```
Active IP Multicast Sources - sending >= 4 kbps

Group: 239.255.0.1, (?)
   Source: 192.168.33.32 (?)
   Rate: 10 pps/115 kbps(1sec), 235 kbps(last 23 secs), 87 kbps(life avg)
```

show ip rpf

Mit diesem Befehl können Sie anzeigen, wie das IP-Multicast-Routing das Reverse Path Forwarding (RPF) ausführt. Überprüfen Sie bei der Fehlerbehebung anhand dieser Informationen, ob die RPF-Informationen richtig sind. Ist dies nicht der Fall, überprüfen Sie die Unicast-Routing-Tabelle für die Quelladresse. Verwenden Sie außerdem die Befehle **ping** und **trace** an der Quelladresse, um zu überprüfen, ob Unicast-Routing funktioniert. Sie können Distance Vector Multicast Routing Protocol (DVMRP)-Routen oder statische Routen verwenden, um Unstimmigkeiten zwischen Unicast und Multicast zu beheben.

<#root>

```
R1#
```

show ip rpf 192.168.33.32

```
RPF information for ? (192.168.33.32)
```

RPF interface: Ethernet0

```
  RPF neighbor: ? (192.168.10.2)
  RPF route/mask: 192.168.33.0/16
  RPF type: unicast (eigrp 1)
  RPF recursion count: 0
  Doing distance-preferred lookups across tables
```

show ip mcache

Dieser Befehl kann den IP-Multicast-Fast Switching-Cache überprüfen und Fast-Switching-Fehler beheben.

<#root>

```
R1#
```

show ip mcache

```
IP Multicast Fast-Switching Cache
(192.168.33.32/32, 239.255.0.1), Ethernet0, Last used: 00:00:00
  Ethernet1       MAC Header: 01005E7F000100000C13DBA90800
(192.168.9.1/32, 239.255.0.1), Ethernet1, Last used: 00:00:00
  Ethernet0       MAC Header: 01005E7F000100000C13DBA80800
```

show ip mroute count

Verwenden Sie diesen Befehl, um zu überprüfen, ob Multicast-Datenverkehr empfangen wird, und um seine Flussraten und Verluste zu überprüfen. Wenn kein Datenverkehr eingeht, arbeiten Sie von der Quelle zum Empfänger, bis Sie feststellen, wo der Datenverkehr stoppt. Sie können mit diesem Befehl auch überprüfen, ob Datenverkehr weitergeleitet wird. Ist dies nicht der Fall, suchen Sie mit dem Befehl show ip mroute nach "Null Outgoing interface list" und RPF-Fehlern.

<#root>

```
R1#
```

show ip mroute count

```
   IP Multicast Statistics
    routes using 2406 bytes of memory
   2 groups, 1.00 average sources per group
   Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
   Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)
   Group: 239.255.0.1, Source count: 2, Group pkt count: 11709
  RP-tree: Forwarding: 3/0/431/0, Other: 3/0/0
```

Source: 192.168.33.32/32, Forwarding: 11225/6/1401/62, Other: 11225/0/0
Source: 192.168.9.1/32, Forwarding: 481/0/85/0, Other: 490/0/9

```
  Group: 224.0.1.40, Source count: 0, Group pkt count:
```

show ip route

Verwenden Sie diesen Befehl, um die Unicast-Routing-Tabelle zu überprüfen und die RPF-Fehler in der mroute-Tabelle zu beheben.

<#root>

R2#

show ip route

```
   Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is not set
D    192.168.9.0/24 [90/307200] via 192.168.10.1, 00:59:45,    Ethernet0
   C    192.168.10.0/24 is directly connected, Ethernet0
   D    192.168.4.0/24 [90/11040000] via 192.168.7.1, 23:21:00,    Serial0
   D    192.168.5.0/24 [90/11023872] via 192.168.7.1, 23:21:02,    Serial0
   C    192.168.7.0/24 is directly connected, Serial0
   D    192.168.33.0/16 [90/2195456] via 192.168.7.1, 1d23h, Serial0
   D    192.168.1.0/24 [90/11552000] via 192.168.7.1, 22:41:27,    Serial0
```

show ip pim rp mapping

Mit diesem Befehl können Sie die RP-Zuweisung nach Multicast-Gruppenbereich prüfen und überprüfen, ob die Quelle für RP-Learning (statisch oder automatisch) und die Zuordnung richtig sind. Wenn Sie einen Fehler finden, überprüfen Sie die lokale Router- oder Auto-RP-Konfiguration.

<#root>

R1#

show ip pim rp mapping

```
   PIM Group-to-RP Mappings

Group(s) 224.0.1.40/32
     RP 192.168.7.2 (?), v1


       Info source: local, via Auto-RP
            Uptime: 2d00h, expires: never


Group(s): 224.0.0.0/4, Static
       RP: 192.168.7.2 (?)
```

debug-Befehle

In diesem Abschnitt wird erläutert, wie bestimmte **Debug**-Befehlsausgaben in einem funktionierenden Netzwerk aussehen müssen. Bei der Fehlerbehebung können Sie zwischen der korrekten **Debugausgabe** und der unterscheiden, die auf ein Problem in Ihrem Netzwerk hinweist. Ausführliche Informationen zu diesen Debugbefehlen finden Sie in der Cisco IOS Debug Command Reference.

debug ip igmp

Verwenden Sie den Befehl **debug ip igmp**, um empfangene und übertragene IGMP-Pakete sowie IGMP-host-bezogene Ereignisse anzuzeigen. Die Debug-Ausgabe wird **nicht** durch diesen Befehl deaktiviert.

Mit dieser Ausgabe können Sie feststellen, ob die IGMP-Prozesse funktionieren. Wenn IGMP nicht funktioniert, erkennt der Router-Prozess im Allgemeinen nie einen anderen Host im Netzwerk, der für den Empfang von Multicast-Paketen konfiguriert ist. Im PIM-Dense-Modus bedeutet dies, dass die Pakete intermittierend (einige alle drei Minuten) zugestellt werden. Im PIM Sparse Mode werden sie nie ausgeliefert.

<#root>

```
R1#
```

debug ip igmp

```
12:32:51.065: IGMP: Send v2 Query on Ethernet1 to 224.0.0.1
12:32:51.069: IGMP: Set report delay time to 9.4 seconds for 224.0.1.40 on Ethernet1
12:32:56.909: IGMP: Received v1 Report from 192.168.9.1 (Ethernet1) for 239.255.0.1
12:32:56.917: IGMP: Starting old host present timer for 239.255.0.1 on Ethernet1
12:33:01.065: IGMP: Send v2 Report for 224.0.1.40 on Ethernet1
12:33:01.069: IGMP: Received v2 Report from 192.168.9.4 (Ethernet1) for 224.0.1.40
12:33:51.065: IGMP: Send v2 Query on Ethernet1 to 224.0.0.1
```

Die vorherige Ausgabe zeigt, dass der Router eine IGMP-Abfrage der Version 2 über die Schnittstelle Ethernet 1 mit der Multicast-Adresse 224.0.0.1 sendet (alle Multicast-Systeme in diesem Subnetz). Schnittstelle Ethernet 1 selbst ist ein Mitglied der Gruppe 224.0.1.40 (Sie können den Befehl show ip igmp interface verwenden, um dies zu bestimmen), der eine Berichtsverzögerungszeit von 9,4 Sekunden (zufällig bestimmt) festlegt. Da es für die nächsten 9,4 Sekunden keinen Bericht von einem anderen System für die Multicast-Gruppe 224.0.1.40 empfängt, sendet es einen Bericht über seine Mitgliedschaft in Version 2, der vom Router selbst über Ethernet 1 empfangen wird. Er empfängt auch den IGMP-Bericht, Version 1, von

Host 192.168.9.1, der direkt mit der Schnittstelle Ethernet 1 für die Gruppe 239.255.0.1 verbunden ist.

Diese **Debug-**Ausgabe ist nützlich, wenn Sie überprüfen, ob die Router-Schnittstelle Abfragen sendet, und das Abfragespaltintervall (im vorherigen Fall 60 Sekunden) bestimmen. Sie können den Befehl auch verwenden, um die IGMP-Version zu ermitteln, die von den Clients verwendet wird.

debug ip mpacket

Verwenden Sie den Befehl **debug ip mpacket**, um alle empfangenen und übertragenen IP-Multicast-Pakete anzuzeigen. Die Debug-Ausgabe wird **nicht** durch diesen Befehl deaktiviert.

<#root>

```
R1#
```

```
debug ip mpacket 239.255.0.1 detail
```

```
13:09:55.973: IP: MAC sa=0000.0c70.d41e (Ethernet0), IP last-hop=192.168.10.2
13:09:55.977: IP: IP tos=0x0, len=892, id=0xD3C1, ttl=12, prot=17
13:09:55.981: IP: s=192.168.33.32 (Ethernet0) d=239.255.0.1 (Ethernet1) len 906, mforward
```

Dieser Befehl decodiert das Multicast-Paket und zeigt an, ob das Paket weitergeleitet (mforward) oder verworfen wird. Beim Debuggen von Paketflussproblemen im Netzwerk ist es hilfreich, den TTL-Wert und den Grund zu untersuchen, aus dem ein Paket verworfen wurde.

> **Achtung:** Seien Sie vorsichtig, wenn Sie die Debug-Ausgabe auf Paketebene aktivieren, insbesondere, wenn der Router hohe Multicast-Paketlasten verarbeitet.

---

debug ip mrouting

Dieser Befehl ist für die Routingtabellenwartung nützlich. Überprüfen Sie, ob die (S,G)-Route in der Routing-Tabelle installiert ist, oder falls nicht, warum nicht. Die wichtigsten Informationen in dieser Ausgabe sind die RPF-Schnittstelle. Wenn eine RPF-Prüfung fehlschlägt, kann die (S,G) mroute nicht in der mrouting-Tabelle installiert werden.

<#root>

```
R1#
```

```
debug ip mrouting 239.255.0.1
```

```
13:17:27.821: MRT: Create (*, 239.255.0.1), RPF Null, PC 0x34F16CE
13:17:27.825: MRT: Create (192.168.33.32/32, 239.255.0.1), RPF Ethernet0/192.168.10.2,
PC 0x34F181A
13:17:30.481: MRT: Create (192.168.9.1/32, 239.255.0.1), RPF Ethernet1/0.0.0.0,
PC 0x34F18
```

debug ip pim

Verwenden Sie den Befehl **debug ip pim**, um die empfangenen und übertragenen PIM-Pakete sowie PIM-

bezogene Ereignisse anzuzeigen. Die No-Form dieses Befehls deaktiviert die Debugausgabe.

In diesem Abschnitt wird ein Beispiel verwendet, um die Debug-Ausgabe des PIM Sparse Mode zu verstehen und eine typische Debug-Ausgabe anzuzeigen.

Die Ausgabe von debug ip pim auf R1 lautet wie folgt:

<#root>

R1#

debug ip pim

```
 PIM: Send v2 Hello on Ethernet0
 PIM: Send v2 Hello on Ethernet1
 PIM: Received v2 Hello on Ethernet0 from 192.168.10.2
 PIM: Send v2 Hello on Ethernet0
 PIM: Send v2 Hello on Ethernet1
 PIM: Building Join/Prune message for 239.255.0.1
 PIM: v2, for RP, Join-list: 192.168.7.2/32, RP-bit, WC-bit, S-bit
 PIM: Send v2 periodic Join/Prune to RP via 192.168.10.2 (Ethernet0)
 PIM: Received RP-Reachable on Ethernet0 from 192.168.7.2 for group 239.255.0.1
 PIM: Update RP expiration timer (270 sec) for 239.255.0.1
```

Jede Ausgabezeile bezeichnet Folgendes: R1 und R2 stellen PIM-Nachbarn her, wenn Hello-Nachrichten ausgetauscht werden. Diese periodischen Hello-Nachrichten, die in **Abfrageintervall-**Sekunden zwischen R1 (E0) und R2 (E0) ausgetauscht werden, verfolgen PIM-Nachbarn.

R1 sendet eine Join/Prune-Nachricht an die RP-Adresse 192.168.7.2. Der RP (R2) antwortet mit einer empfangenen RP Reachable-Nachricht an R1 für die Gruppe 239.255.0.1. Dadurch wird wiederum der RP-Ablaufzeitgeber auf R1 aktualisiert. Der Ablaufzeitgeber legt einen Prüfpunkt fest, um sicherzustellen, dass der RP noch vorhanden ist. Andernfalls muss ein neuer RP erkannt werden. Verwenden Sie den Befehl **show ip pim rp**, um die RP-Laufzeit zu überwachen.

Sehen Sie sich nun die **Debug-**Ausgabe zwischen R1 und R2 an, wenn ein Multicast-Empfänger für die Gruppe 239.255.0.1 zu R1 hinzukommt.

Schauen Sie sich zunächst die Ausgabe auf R1 an:

<#root>

1

```
 PIM: Check RP 192.168.7.2 into the
```

(*, 239.255.0.1) entry

2

```
 PIM:
```

Send v2 Join

```
 on Ethernet0 to 192.168.10.2 for (192.168.8.7.2/32, 239.255.0.1), WC-bit, RPT-bit, S-bit
```

3

PIM: Building batch join message for 239.255.0.1

4

PIM: Building Join/Prune message for 239.255.0.1

5

PIM: v2, for RP, Join-list: 192.168.7.2/32, RP-bit, WC-bit, S-bit

6

PIM: Send v2 periodic Join/Prune to RP via 192.168.10.2 (Ethernet0)

7

PIM: Received RP-Reachable on Ethernet0 from 192.168.7.2 : for group 239.255.0.1

8

PIM: Update RP expiration timer (270 sec) for 239.255.0.1

9

PIM: Building Join/Prune message for 239.255.0.1

10

PIM: v2, for RP, Join-list: 192.168.7.2/32, RP-bit, WC-bit, S-bit

11

PIM: Send v2 periodic Join/Prune to RP via 192.168.10.2 (Ethernet0)

Schauen Sie sich nun die Ausgabe auf R2 an:

<#root>

12

PIM:

Received v2 Join/Prune on Ethernet0 from 192.168.10.1

, to us

13

PIM: Join-list: (*, 239.255.0.1) RP 192.168.7.2

14

PIM: Check RP 192.168.7.2 into the (*, 239.255.0.1) entry, RPT-bit set, WC-bit set, S-bit set

15

PIM:

Add Ethernet0/192.168.10.1 to (*, 239.255.0.1), Forward state

16

PIM: Building Join/Prune message for 239.255.0.1

17

```
 PIM: Received v2 Join/Prune on Ethernet0 from 192.168.10.1, to us
18
 PIM: Join-list: (*, 239.255.0.1) RP 192.168.7.2, RPT-bit set, WC-bit set, S-bit set
19
 PIM: Add Ethernet0/192.168.10.1 to (*, 239.255.0.1), Forward state
20
 PIM: Building Join/Prune message for 239.255.0.1
21
 PIM:
Send RP-reachability for 239.255.0.1 on Ethernet0
22
 PIM: Received v2 Join/Prune on Ethernet0 from 192.168.10.1, to us
23
 PIM: Join-list: (*, 239.255.0.1) RP 192.168.7.2, RPT-bit set, WC-bit set, S-bit set
24
 PIM: Add Ethernet0/192.168.10.1 to (*, 239.255.0.1), Forward state
25
 PIM: Building Join/Prune message for 239.255.0.1
```

In Zeile 1 vor tritt der Multicast-Empfänger für die Gruppe 239.255.0.1 in R1 ein. Dadurch wird ein (*, 239.255.0.1) Eintrag in der mroute-Tabelle installiert. Anschließend sendet der Multicast-Empfänger in Zeile 2 eine IGMP-Join-Nachricht an R2 (RP), um der Shared Tree beizutreten.

Wenn der IGMP-Join auf R2 eingeht, installiert R2 eine (*, 239.255.0.1)-Route, wie in den Zeilen 12 bis 15 des R2-Ausgangs dargestellt.

Sobald R2 in seiner Routing-Tabelle (*, 239.255.0.1) installiert ist, fügt er die Schnittstelle, von der er die Join/Prune-Nachricht empfangen hat, seiner Outgoing-interface-list (OIL) im Weiterleitungsstatus hinzu. Anschließend wird eine RP-Erreichbarkeitsmeldung an die Schnittstelle zurückgesendet, an der die Join/Prune-Meldung empfangen wurde. Diese Transaktion ist in den Zeilen 15 bis 21 des R2-Ausgangs dargestellt.

R1 empfängt die Meldung "RP-reachable" (RP erreichbar) für die Gruppe 239.255.0.1 und aktualisiert ihren Ablaufzeitgeber für RP. Dieser Austausch wiederholt sich standardmäßig einmal pro Minute und aktualisiert seinen Multicast-Weiterleitungsstatus, wie in den Zeilen 7 und 8 des R1-Ausgangs dargestellt.

In den nächsten Zeilen ist die **Debug**-Ausgabe zwischen R2 (RP) und R3 zu sehen. Die Quelle (direkt mit R3 verbunden) begann, Pakete für die Gruppe 239.255.0.1 zu senden.

Schauen Sie sich zunächst die Ausgabe auf R3 an:

```
<#root>
1
```

```
 PIM:
Check RP 192.168.7.2 into the (*, 239.255.0.1) entry

2
 PIM: Building Join/Prune message for 239.255.0.1
3
 PIM: For RP, Join-list: 192.168.7.2/32, RP-bit, WC-bit
4
 PIM: Send periodic Join/Prune to RP via 192.168.7.2 (Serial4/0)
5
 PIM: Received RP-Reachable on Serial4/0 from 192.168.7.2
6
 PIM: Update RP expiration timer (270 sec) for 239.255.0.1
7
 PIM: Send Register to 192.168.7.2 for 192.168.33.32, group 239.255.0.1
8
 PIM: Send Register to 192.168.7.2 for 192.168.33.32, group 239.255.0.1
9
 PIM: Received Join/Prune on Serial4/0 from 192.168.7.2
10
 PIM: Join-list: (192.168.33.32/32, 239.255.0.1), S-bit set
11
 PIM: Add Serial4/0/192.168.7.2 to (192.168.33.32/32, 239.255.0.1), Forward state
12
 PIM:
Received Register-Stop on Serial4/0 from 192.168.7.2

13
 PIM: Clear register flag to 192.168.7.2 for (192.168.33.32/32, 239.255.0.1)
14
 PIM: Received Register-Stop on Serial4/0 from 192.168.7.2
15
 PIM: Clear register flag to 192.168.7.2 for (192.168.33.32/32, 239.255.0.1)
```

Hier ist der Ausgang von R2, der RP:

<#root>

16

PIM:

Received Join/Prune on Serial0 from 192.168.7.1

, to us

17

PIM:

Send RP-reachability for 239.255.0.1 on Serial0

18

PIM: Received Register on Serial0 from 192.168.7.1 for 192.168.33.32, group 239.255.0.1

19

PIM: Forward decapsulated data packet for 239.255.0.1 on Ethernet0

10

PIM: Forward decapsulated data packet for 239.255.0.1 on Serial0

21

PIM: Send Join on Serial0 to 192.168.7.1 for (192.168.33.32/32, 239.255.0.1), S-bit

22

PIM: Send Join on Serial0 to 192.168.7.1 for (192.168.33.32/32, 239.255.0.1), S-bit

23

PIM:

Send Register-Stop to 192.168.7.1 for 192.168.33.32, group 239.255.0.1

24

PIM: Received Join/Prune on Serial0 from 192.168.7.1, to us

25

PIM: Prune-list: (192.168.33.32/32, 239.255.0.1)

26

PIM: Received v2 Join/Prune on Ethernet0 from 192.168.10.1, to us

27

PIM: Join-list: (*, 239.255.0.1) RP 192.168.7.2, RPT-bit set, WC-bit set, S-bit set

28

PIM: Add Ethernet0/192.168.10.1 to (*, 239.255.0.1), Forward state

29

PIM: Add Ethernet0/192.168.10.1 to (192.168.33.32/32, 239.255.0.1)

30

PIM: Join-list: (192.168.33.32/32, 239.255.0.1), S-bit set

```
31
 PIM: Add Ethernet0/192.168.10.1 to (192.168.33.32/32, 239.255.0.1), Forward state
32
 PIM: Building Join/Prune message for 239.255.0.1
33
 PIM: For 192.168.7.1, Join-list: 192.168.33.32/32
34
 PIM: For 192.168.10.1, Join-list: 192.168.9.1/32
35
 PIM: Send v2 periodic Join/Prune to 192.168.10.1 (Ethernet0)
36
 PIM: Send periodic Join/Prune to 192.168.7.1 (Serial0)
37
 PIM: Received Join/Prune on Serial0 from 192.168.7.1, to us
38
 PIM: Join-list: (*, 239.255.0.1) RP 192.168.7.2, RP-bit set, WC-bit set, S-bit set
39
 PIM: Add Serial0/192.168.7.1 to (*, 239.255.0.1), Forward state
40
 PIM: Add Serial0/192.168.7.1 to (192.168.33.32/32, 239.255.0.1)
41
 PIM: Add Serial0/192.168.7.1 to (192.168.9.1/32, 239.255.0.1)
42
 PIM: Join-list: (192.168.9.1/32, 239.255.0.1), S-bit set
43
 PIM: Add Serial0/192.168.7.1 to (192.168.9.1/32, 239.255.0.1), Forward state
44
 PIM: Join-list: (*, 239.255.0.1) RP 192.168.7.2, RP-bit set, WC-bit set, S-bit set
45
 PIM: Add Serial0/192.168.7.1 to (*, 239.255.0.1), Forward state
```

Leitung 1 zeigt, dass R3, der direkt über Ethernet0/0 mit der Quelle verbunden ist, Multicast-Datenverkehr für Gruppe 239.255.0.1 empfängt. Es wird ein (*, 239.255.0.1)-Eintrag erstellt und eine Join-Nachricht an den RP gesendet.

Die Zeilen 16 und 17 zeigen, dass R2, der RP, auch die Join/Prune-Meldung empfängt und RP-Erreichbarkeitsinformationen an R3 zurücksendet.

In den Leitungen 5 und 6 aktualisiert R3 seinen RP-Ablaufzeitgeber, nachdem er die RP-Erreichbarkeitsinformationen erhalten hat. Die Zeilen 7 und 8 oben zeigen, dass R3 seinen (*,G)-Eintrag verwendet, um die Daten an einen RP zu senden, der in einem Registerpaket mit der Quelle gekapselt ist, die die Übertragung an die Gruppe 239.255.0.1 initiiert.

Die Zeilen 18 bis 20 zeigen, dass R2 das Registerpaket empfangen, entkapselt und mit einem bereits vorhandenen (*, 239.255.0.1) Eintrag in der Routing-Tabelle entlang des Baums weitergeleitet hat.

Die Zeilen 21 und 29 zeigen, dass R2 eine Join-Nachricht an R3 sendet und einen (S,G)-Eintrag (192.168.33.32, 239.255.0.1) in der mroute-Tabelle installiert.

Die Zeilen 9 bis 11 zeigen, dass R3 die Join-Nachricht von R2 empfängt, einen Eintrag (S,G) (192.168.33.32.239.255.0.1) in der Routing-Tabelle installiert und die mit dem RP verbundene Schnittstelle in den Weiterleitungsmodus versetzt, der den Multicast-SPT-Tree (S,G) erstellt. Quelle.

In Zeile 23 empfängt R2 (S,G)-Datenverkehr über SPT und sendet eine Register-Stopp-Nachricht (und eine Join-Nachricht) an die Quelle.

Die Zeilen 12 bis 15 zeigen an, dass R3 die Register-Stopp-Nachricht empfängt, das Register-Flag löscht und den Kapselungsverkehr (S,G) stoppt.

Zwischen dem RP und R3 werden periodische Join/Prune-Nachrichten ausgetauscht, um den Multicast-Tree aufrechtzuerhalten.

Zugehörige Informationen

- **Handbuch zur Fehlerbehebung bei IP-Multicast**
- **Schnellstart-Konfigurationsanleitung für Multicast**
- **IP Multicast-Support-Seite**
- **IP Routing-Support-Seite**
- **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.