

Lesen Sie den Konfigurationsleitfaden für IP Multicast Quick Start.

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Hintergrundinformationen](#)

[Dense-Modus](#)

[Sparse Mode mit einem RP](#)

[Sparse Mode mit mehreren RPs](#)

[Auto-RP mit einem RP](#)

[Auto-RP mit mehreren RPs](#)

[DVMRP](#)

[MBGP](#)

[MSDP](#)

[Stub-Multicast-Routing](#)

[IGMP UDLR für Satellitenverbindungen](#)

[PIMv2-BSR](#)

[CGMP](#)

[IGMP-Snooping](#)

[PGM](#)

[MRM](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument werden die Grundlagen der Multicast-Konfiguration für verschiedene Netzwerkszenarien beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in diesem Thema verfügen:

- Internet Protocol (IP) Multicast

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 verstehen.

Konventionen

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

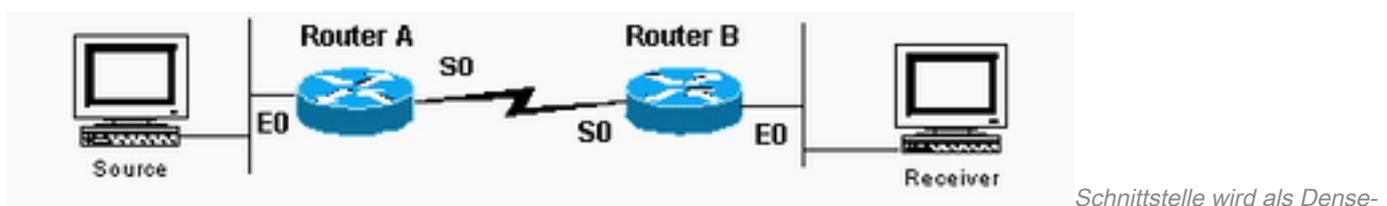
Hintergrundinformationen

IP-Multicasting ist eine bandbreitensparende Technologie, die den Datenverkehr reduziert, da Tausende von Empfängern und Privathaushalten gleichzeitig einen einzigen Informationsstrom erhalten. Zu den Anwendungen, die Multicast nutzen, gehören Videokonferenzen, die Unternehmenskommunikation, Fernunterricht und die Verteilung von Software, Aktiennotierungen und Nachrichten.

Dense-Modus

Cisco empfiehlt die Verwendung des Sparse Mode (PIM, Protocol Independent Multicast), insbesondere des Auto-RP, wo dies möglich ist, und insbesondere für neue Bereitstellungen. Wenn der Dense-Modus gewünscht wird, konfigurieren Sie den globalen Befehl **ip multicast-routing** und den Schnittstellenbefehl **ip pim sparse-dense-mode** auf jeder Schnittstelle, die Multicast-Datenverkehr verarbeiten muss. Die allgemeine Anforderung für alle Konfigurationen in diesem Dokument besteht darin, Multicasting global zu konfigurieren und PIM auf den Schnittstellen zu konfigurieren. Ab der Cisco IOS® Software-Version 11.1 können Sie die Schnittstellenbefehle **ip pim dense-mode** und **ip pim sparse-mode** gleichzeitig mit dem Befehl **ip pim sparse-dense-mode** konfigurieren. In diesem Modus wird die Schnittstelle als Dense-Modus behandelt, wenn sich die Gruppe im Dense-Modus befindet. Befindet sich die Gruppe im Sparse-Mode (z. B. wenn ein RP bekannt ist), wird die Schnittstelle als Sparse-Mode behandelt.

Hinweis: Die Quelle in den Beispielen in diesem Dokument stellt die Quelle für Multicast-Datenverkehr dar, und der Empfänger stellt den Empfänger für Multicast-Datenverkehr dar.



Modus behandelt, wenn sich Gruppe im Dense-Modus befindet

Konfiguration von Router A

```
ip multicast-routing

interface ethernet0
ip address <address> <mask>
ip pim sparse-dense-mode
```

```
interface serial0
ip address <address> <mask>
ip pim sparse-dense-mode
```

Router B-Konfiguration

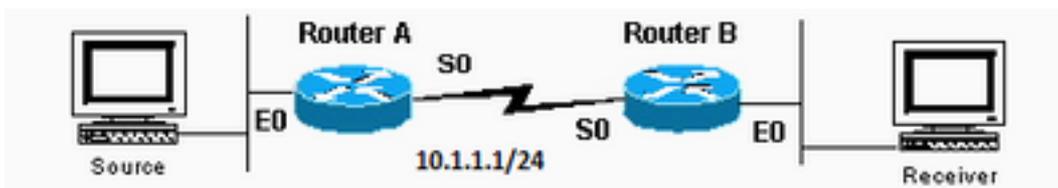
```
ip multicast-routing
```

```
interface serial0
ip address <address> <mask>
ip pim sparse-dense-mode
```

```
interface ethernet0
ip address <address> <mask>
ip pim sparse-dense-mode
```

Sparse Mode mit einem RP

In diesem Beispiel ist Router A der RP, der normalerweise der Router ist, der der Quelle am nächsten liegt. Für die statische RP-Konfiguration müssen auf allen Routern in der PIM-Domäne die gleichen `p-pim-rp-address`-Befehle konfiguriert sein. Sie können mehrere RPs konfigurieren, es kann jedoch nur einen RP pro Gruppe geben.



vorhanden sein, aber nur ein RP pro spezifischer Gruppe

Es können mehrere RPs

Konfiguration von Router A

```
ip multicast-routing
ip pim rp-address 10.1.1.1
```

```
interface ethernet0
ip address <address> <mask>
ip pim sparse-dense-mode
```

```
interface serial0
ip address 10.1.1.1 255.255.255.0
ip pim sparse-dense-mode
```

Router B-Konfiguration

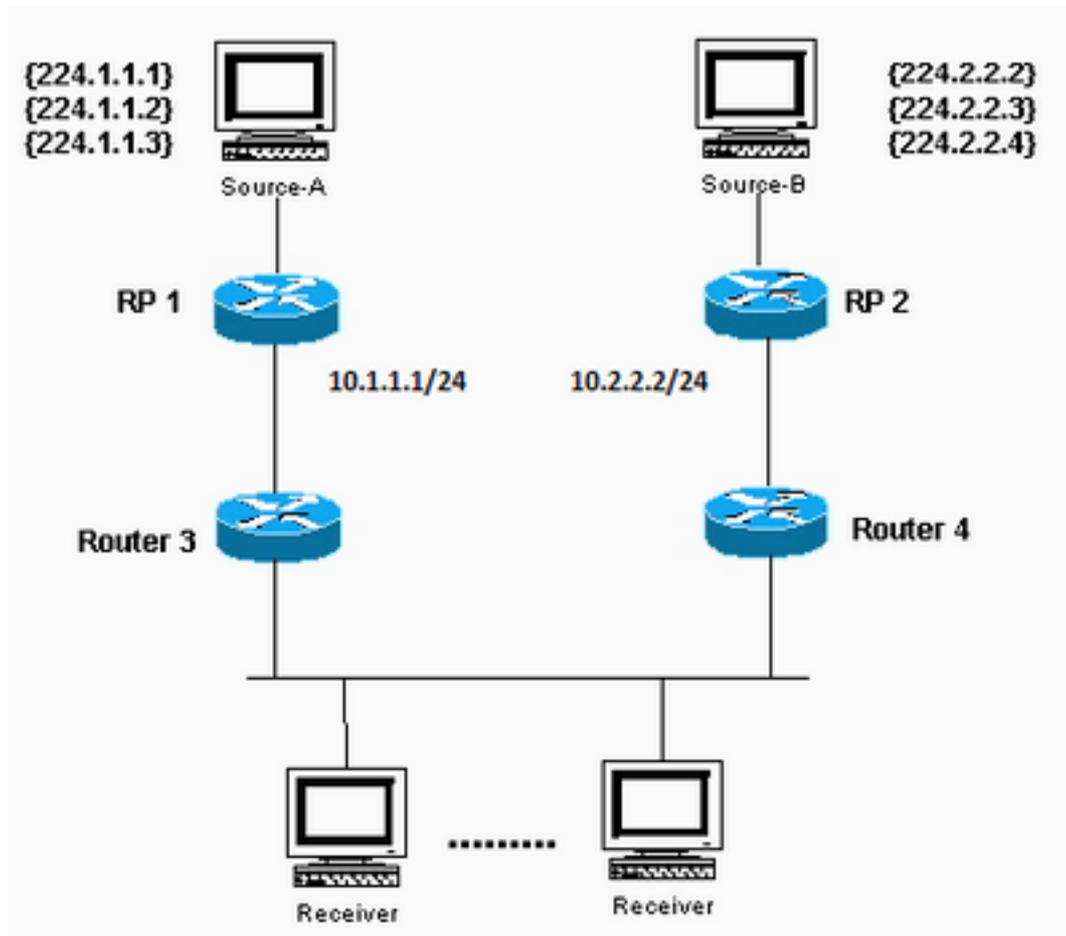
```
ip multicast-routing
ip pim rp-address 10.1.1.1
```

```
interface serial0
ip address <address> <mask>
ip pim sparse-dense-mode
```

```
interface ethernet0
ip address <address> <mask>
ip pim sparse-dense-mode
```

Sparse Mode mit mehreren RPs

In diesem Beispiel sendet Source-A Daten an 224.1.1.1, 224.1.1.2 und 224.1.1.3. Source-B sendet an 224.2.2.2, 224.2.2.3 und 224.2.2.4. Es kann sich um einen Router handeln, entweder RP 1 oder RP 2, der RP für alle Gruppen ist. Wenn jedoch verschiedene RPs unterschiedliche Gruppen verarbeiten sollen, müssen Sie alle Router so konfigurieren, dass sie die Gruppen enthalten, für die die RPs zuständig sind. Für diese Art der statischen RP-Konfiguration müssen auf allen Routern in der PIM-Domäne die gleichen Befehle für `ip pim rp-address acl` konfiguriert sein. Sie können [Auto-RP](#) auch verwenden, um dieselbe Konfiguration zu erreichen, die einfacher zu konfigurieren ist.



Quelle-A sendet an 224.1.1.1,

224.1.1.2 und 224.1.1.3; Quelle-B sendet an 224.2.2.2, 224.2.2.3 und 224.2.2.4.

Konfiguration von RP 1

```
ip multicast-routing
```

```
ip pim RP-address 10.1.1.1 2
ip pim RP-address 10.2.2.2 3
```

```
access-list 2 permit 224.1.1.1
access-list 2 permit 224.1.1.2
access-list 2 permit 224.1.1.3
access-list 3 permit 224.2.2.2
access-list 3 permit 224.2.2.3
access-list 3 permit 224.2.2.4
```

RP 2-Konfiguration

```
ip multicast-routing
```

```
ip pim RP-address 10.1.1.1 2
ip pim RP-address 10.2.2.2 3
```

```
access-list 2 permit 224.1.1.1
```

```

access-list 2 permit 224.1.1.2
access-list 2 permit 224.1.1.3
access-list 3 permit 224.2.2.2
access-list 3 permit 224.2.2.3
access-list 3 permit 224.2.2.4

```

Konfiguration für Router 3 und 4

```

ip multicast-routing
ip pim RP-address 10.1.1.1 2
ip pim RP-address 10.2.2.2 3

```

```

access-list 2 permit 224.1.1.1
access-list 2 permit 224.1.1.2
access-list 2 permit 224.1.1.3
access-list 3 permit 224.2.2.2
access-list 3 permit 224.2.2.3
access-list 3 permit 224.2.2.4

```

Auto-RP mit einem RP

Für die automatische RP müssen Sie die RPs so konfigurieren, dass ihre Verfügbarkeit als RPs und Zuordnungsagenten bekannt gegeben wird. Die RPs senden ihre Ankündigungen über 224.0.1.39. Der RP-Zuordnungs-Agent hört die angekündigten Pakete von den RPs ab und sendet dann RP-Gruppen-Zuordnungen in einer Ermittlungsnachricht, die an 224.0.1.40 gesendet wird. Diese Erkennungsmeldungen werden von den verbleibenden Routern für die Zuordnung zwischen RP und Gruppe verwendet. Sie können einen RP verwenden, der auch als Zuordnungsagent dient, oder Sie können mehrere RPs und mehrere Zuordnungsagenten aus Redundanzgründen konfigurieren.

Beachten Sie, dass Sie bei der Auswahl einer Schnittstelle, von der RP-Ankündigungen bezogen werden sollen, eine Schnittstelle wie z. B. Loopback anstelle einer physischen Schnittstelle verwenden sollten. Darüber hinaus können Switched VLAN Interfaces (SVIs) verwendet werden. Wenn die RP-Adresse über eine VLAN-Schnittstelle angekündigt wird, muss die Option **interface-type** in der **ip pim [vrf vrf-name] send-rp-announce {interface-type interface-number} angegeben werden. | ip-address} scope** Der Befehl **ttl-value** muss die VLAN-Schnittstelle und die VLAN-Nummer enthalten. Der Befehl sieht beispielsweise aus wie **ip pim send-rp-announceVlan500 scope 100**. Wenn Sie sich für eine physische Schnittstelle entscheiden, ist diese Schnittstelle immer verfügbar. Dies ist nicht immer der Fall, und der Router stellt sich selbst nicht mehr als RP bereit, sobald die physische Schnittstelle ausfällt. Bei einer Loopback-Schnittstelle ist sie immer aktiv und wird nie deaktiviert. So wird sichergestellt, dass der RP sich selbst über alle verfügbaren Schnittstellen als RP ankündigt. Dies gilt auch dann, wenn eine oder mehrere physische Schnittstellen ausfallen. Die Loopback-Schnittstelle muss PIM-fähig sein und von einem Interior Gateway Protocol (IGP) angekündigt werden, oder sie muss über statisches Routing erreichbar sein.



Die Loopback-Schnittstelle

muss PIM-fähig sein und über ein Interior Gateway Protocol (PIM) angekündigt werden. Alternativ dazu muss sie mit statischem Routing erreichbar sein.

Konfiguration von Router A

```
ip multicast-routing
```

```
ip pim send-rp-announce loopback0 scope 16
```

```
ip pim send-rp-discover scope 16 interface loopback0 ip address <address> <mask> ip pim sparse-dense-mode  
interface ethernet0 ip address <address> <mask> ip pim sparse-dense-mode interface serial0 ip address  
<address> <mask> ip pim sparse-dense-mode
```

Router B-Konfiguration

```
ip multicast-routing
```

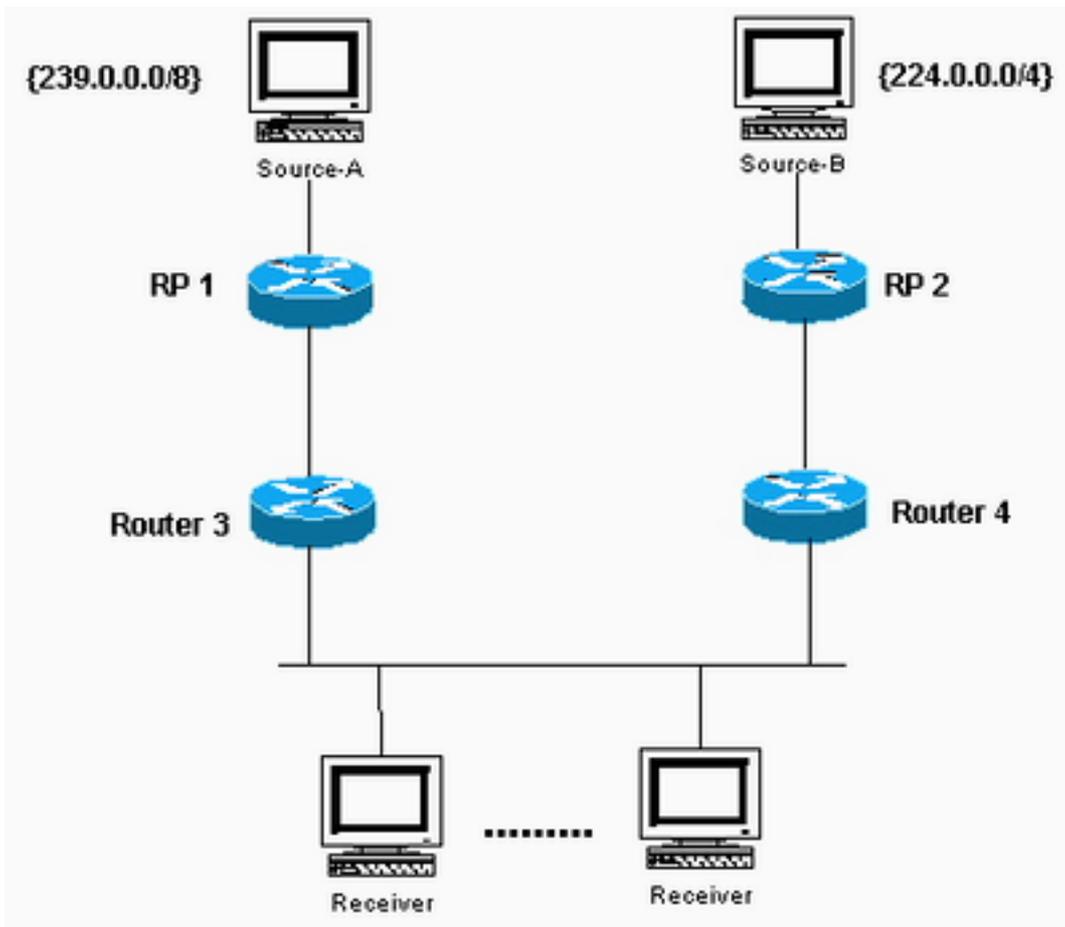
```
interface ethernet0  
ip address <address> <mask>  
ip pim sparse-dense-mode
```

```
interface serial0  
ip address <address> <mask>  
ip pim sparse-dense-mode
```

Auto-RP mit mehreren RPs

Mithilfe der Zugriffslisten in diesem Beispiel können die RPs nur für die gewünschten Gruppen als RP verwendet werden. Wenn keine Zugriffsliste konfiguriert ist, sind die RPs für alle Gruppen als RP verfügbar. Wenn zwei RPs ihre Verfügbarkeit als RPs für dieselbe(n) Gruppe(n) bekannt geben, lösen die Zuordnungsagenten diese Konflikte mit der Regel "Höchste IP-Adresse wird gewonnen".

Wenn zwei RPs für diese Gruppe angekündigt werden, können Sie für jeden Router eine Loopback-Adresse konfigurieren, um zu beeinflussen, welcher Router der RP für eine bestimmte Gruppe ist. Platzieren Sie die höhere IP-Adresse auf dem bevorzugten RP, und verwenden Sie dann die Loopback-Schnittstelle als Quelle für die Ankündigungspakete, z. B. **ip pim send-RP-announce loopback0**. Wenn mehrere Mapping-Agenten verwendet werden, kündigen sie die gleiche Gruppe den RP-Zuordnungen zur 224.0.1.40 Discovery-Gruppe an.



Platzieren Sie die höhere IP-Adresse auf dem bevorzugten RP.

Adresse auf dem bevorzugten RP.

Konfiguration von RP 1

```
ip multicast-routing

interface loopback0
ip address <address> <mask>
ip pim sparse-dense-mode

ip pim send-RP-announce loopback0 scope 16 group-list 1
ip pim send-RP-discovery scope 16 access-list 1 permit 239.0.0.0 0.255.255.255
```

RP 2-Konfiguration

```
ip multicast-routing

interface loopback0
ip address <address> <mask>
ip pim sparse-dense-mode

ip pim send-RP-announce loopback0 scope 16 group-list 1 ip pim send-RP-discovery scope 16 access-list 1
239.0.0.0 0.255.255.255 access-list 1 permit 224.0.0.0 10.255.255.255
```

DVMRP

Ihr Internet Service Provider (ISP) könnte vorschlagen, dass Sie einen Distance Vector Multicast Routing Protocol (DVMRP)-Tunnel zum ISP erstellen, um Zugriff auf den Multicast-Backbone im Internet (mbone) zu erhalten. Die Mindestbefehle zum Konfigurieren eines DVMRP-Tunnels sind hier aufgeführt:

```

interface tunnel0
ip unnumbered <any pim interface>
tunnel source <address of source>
tunnel destination <address of ISPs mrouterd box>
tunnel mode dvmrp
ip pim sparse-dense-mode

```

Normalerweise lässt Sie der ISP einen Tunnel zu einem UNIX-System herstellen, das "mrouterd" (DVMRP) ausführt. Wenn Sie vom ISP stattdessen einen Tunnel zu einem anderen Cisco Gerät einrichten, verwenden Sie den standardmäßigen GRE-Tunnelmodus.

Wenn Sie Multicast-Pakete für andere Benutzer auf dem Knochen generieren möchten, um sie zu sehen anstatt Multicast-Pakete zu empfangen, müssen Sie die Quell-Subnetze ankündigen. Wenn die Adresse des Multicast-Quell-Hosts 172.16.108.1 lautet, müssen Sie dem mbone die Existenz dieses Subnetzes ankündigen. Direkt verbundene Netzwerke werden standardmäßig mit Metrik 1 angekündigt.

Wenn Ihre Quelle nicht direkt mit dem Router mit dem DVMRP-Tunnel verbunden ist, konfigurieren Sie dies unter interface tunnel0:

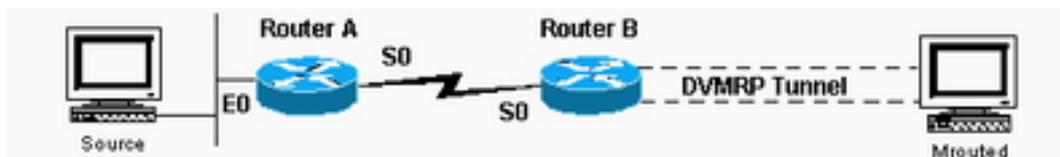
```

ip dvmrp metric 1 list 3
access-list 3 permit 172.16.108.0 0.0.0.255

```

Hinweis: Sie müssen diesem Befehl eine Zugriffsliste hinzufügen, um zu verhindern, dass die gesamte Unicast-Routing-Tabelle für den Mbone angekündigt wird.

Wenn die Konfiguration der hier gezeigten ähnelt und Sie DVMRP-Routen über die Domäne verbreiten möchten, konfigurieren Sie den Befehl **ip dvmrp unicast-routing** auf den seriellen0-Schnittstellen der Router A und B. Mit diesem Vorgang werden DVMRP-Routen an PIM-Nachbarn weitergeleitet, die dann über eine DVMRP-Routing-Tabelle für die Umkehrpfadweiterleitung (Reverse Path Forwarding, RPF) verfügen. Von DVMRP übernommene Routen haben RPF-Vorrang vor allen anderen Protokollen, mit Ausnahme der direkt verbundenen Routen.

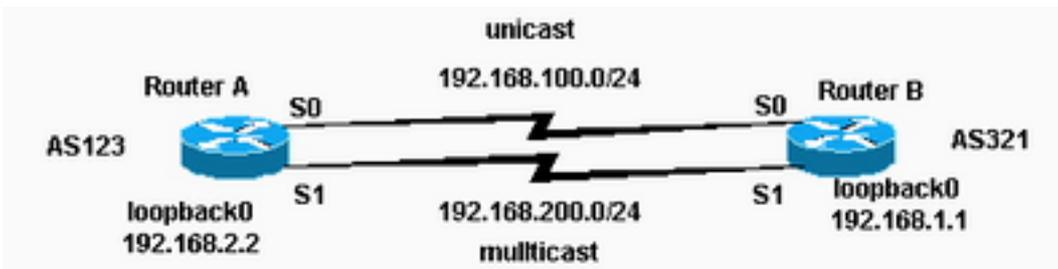


über die Domäne

Verteilen von DVMRP-Routen

MBGP

Das Multiprotocol Border Gateway Protocol (MBGP) ist eine grundlegende Methode zur Übertragung zweier Routensätze: ein Satz für Unicast-Routing und ein Satz für Multicast-Routing. MBGP stellt die erforderliche Kontrolle bereit, um zu entscheiden, wohin Multicast-Pakete übertragen werden dürfen. PIM verwendet die dem Multicast-Routing zugeordneten Routen, um Datenverteilungsstrukturen zu erstellen. Das MBGP stellt den RPF-Pfad bereit, nicht die Erstellung eines Multicast-Zustands. PIM wird weiterhin benötigt, um die Multicast-Pakete weiterzuleiten.



PIM ist für die Weiterleitung

der Multicast-Pakete weiterhin erforderlich.

Konfiguration von Router A

```
ip multicast-routing

interface loopback0
ip pim sparse-dense-mode
ip address 192.168.2.2 255.255.255.0

interface serial0
ip address 192.168.100.1 255.255.255.0

interface serial1
ip pim sparse-dense-mode
ip address 192.168.200.1 255.255.255.0

router bgp 123
network 192.168.100.0 nlri unicast
network 192.168.200.0 nlri multicast
neighbor 192.168.1.1 remote-as 321 nlri unicast multicast
neighbor 192.168.1.1 ebgp-multihop 255
neighbor 192.168.100.2 update-source loopback0
neighbor 192.168.1.1 route-map setNH out

route-map setNH permit 10
match nlri multicast
set ip next-hop 192.168.200.1

route-map setNH permit 20
```

Router B-Konfiguration

```
ip multicast-routing

interface loopback0
ip pim sparse-dense-mode
ip address 192.168.1.1 255.255.255.0

interface serial0
ip address 192.168.100.2 255.255.255.0

interface serial1
ip pim sparse-dense-mode
ip address 192.168.200.2 255.255.255.0
```

```

router bgp 321
network 192.168.100.0 nlri unicast
network 192.168.200.0 nlri multicast
neighbor 192.168.2.2 remote-as 123 nlri unicast multicast
neighbor 192.168.2.2 ebgp-multihop 255
neighbor 192.168.100.1 update-source loopback0
neighbor 192.168.2.2 route-map setNH out

```

```

route-map setNH permit 10
match nlri multicast
set ip next-hop 192.168.200.2

```

```

route-map set NH permit 20

```

Wenn Ihre Unicast- und Multicast-Topologien kongruent sind (wenn sie z. B. über denselben Link geleitet werden), besteht der Hauptunterschied in der Konfiguration im Befehl **nlri unicast multicast**. Hier sehen Sie ein Beispiel:

```

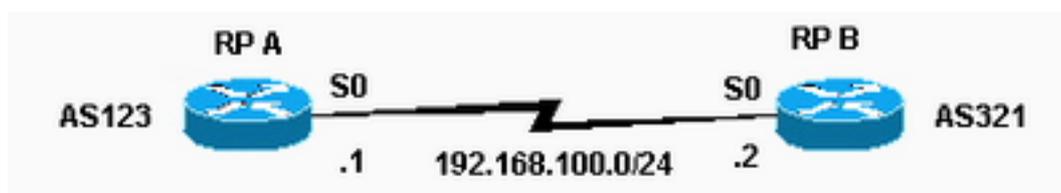
network 192.168.100.0 nlri unicast multicast

```

Übereinstimmende Topologien mit MBGP haben einen Vorteil: Obwohl der Datenverkehr dieselben Pfade durchläuft, können für Unicast-BGP andere Richtlinien als für Multicast-BGP angewendet werden.

MSDP

Das Multicast Source Discovery Protocol (MSDP) verbindet mehrere PIM-SM-Domänen. Jede PIM-SM-Domäne verwendet ihren eigenen unabhängigen RP und muss sich nicht auf RPs in anderen Domänen verlassen. Mit MSDP können Domänen Multicast-Quellen aus anderen Domänen erkennen. Wenn Sie auch BGP-Peering mit dem MSDP-Peer durchführen, müssen Sie für MSDP dieselbe IP-Adresse wie für BGP verwenden. Wenn MSDP Peer-RPF-Prüfungen durchführt, erwartet MSDP, dass die MSDP-Peer-Adresse mit der Adresse übereinstimmt, die BGP/MBGP ihr zuweist, wenn es eine Routing-Tabellen-Suche nach dem RP in der SA-Nachricht durchführt. Wenn zwischen den MSDP-Peers ein BGP/MBGP-Pfad besteht, müssen Sie BGP/MBGP nicht mit dem MSDP-Peer ausführen. Wenn es keinen BGP/MBGP-Pfad und mehr als einen MSDP-Peer gibt, müssen Sie den Befehl **ip msdp default-peer** verwenden. Das Beispiel hier zeigt, dass RP A der RP für seine Domäne und RP B der RP für seine Domäne ist.



Multicast Source Discovery

Protocol (MSDP) verbindet mehrere PIM-SM-Domänen

Konfiguration von Router A

```

ip multicast-routing

```

```

ip pim send-RP-announce loopback0 scope 16 group-list 1
ip pim send-RP-discovery scope 16
ip msdp peer 192.168.100.2 ip msdp sa-request 192.168.100.2 interface loopback0 ip address <address> <mask>
ip pim sparse-dense-mode interface serial0 ip address 192.168.100.1 255.255.255.0 ip pim sparse-dense-m

```

Router B-Konfiguration

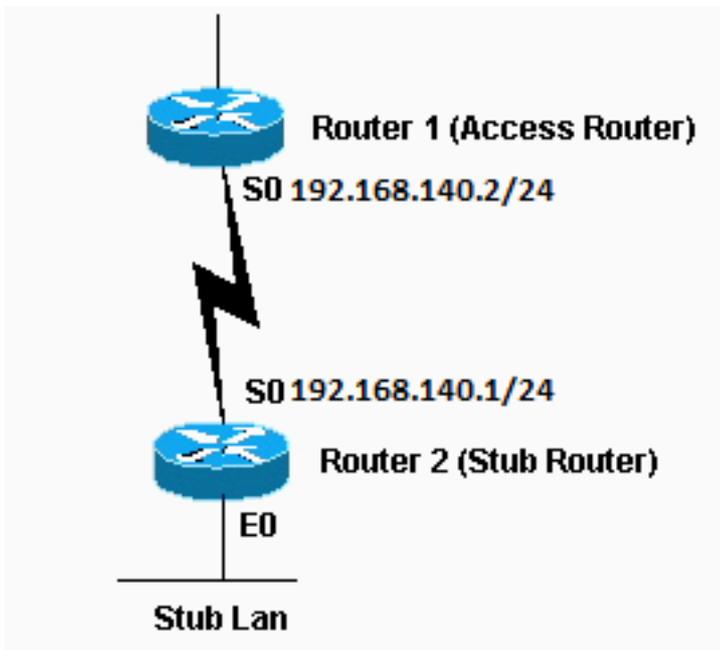
```
ip multicast-routing
```

```
ip pim send-RP-announce loopback0 scope 16 group-list 1
```

```
ip pim send-RP-discovery scope 16 ip msdp peer 192.168.100.1 ip msdp sa-request 192.168.100.1 interface loopback0 ip address <address> <mask> ip pim sparse-dense-mode interface serial0 ip address 192.168.100.255.255.255.0 ip pim sparse-dense-mode
```

Stub-Multicast-Routing

Mit Stub-Multicast-Routing können Sie Remote-/Stub-Router als IGMP-Proxy-Agenten konfigurieren. Anstatt vollständig am PIM teilzunehmen, leiten diese Stub-Router IGMP-Nachrichten von dem/den Host(en) an den Upstream-Multicast-Router weiter.



Stub-Router leiten IGMP-Nachrichten von den Hosts an den

Upstream-Multicast-Router weiter

Konfiguration von Router 1

```
int s0
ip pim sparse-dense-mode
ip pim neighbor-filter 1
```

```
access-list 1 deny 192.168.140.1
```

Der Befehl **ip pim neighbor-filter** ist erforderlich, damit Router 1 Router 2 nicht als PIM-Nachbarn erkennt. Wenn Sie Router 1 im Sparse-Mode konfigurieren, ist der Nachbarfilter nicht erforderlich. Router 2 darf nicht im Sparse-Mode ausgeführt werden. Im Dense-Modus können die Stub-Multicast-Quellen zu den Backbone-Routern geleitet werden.

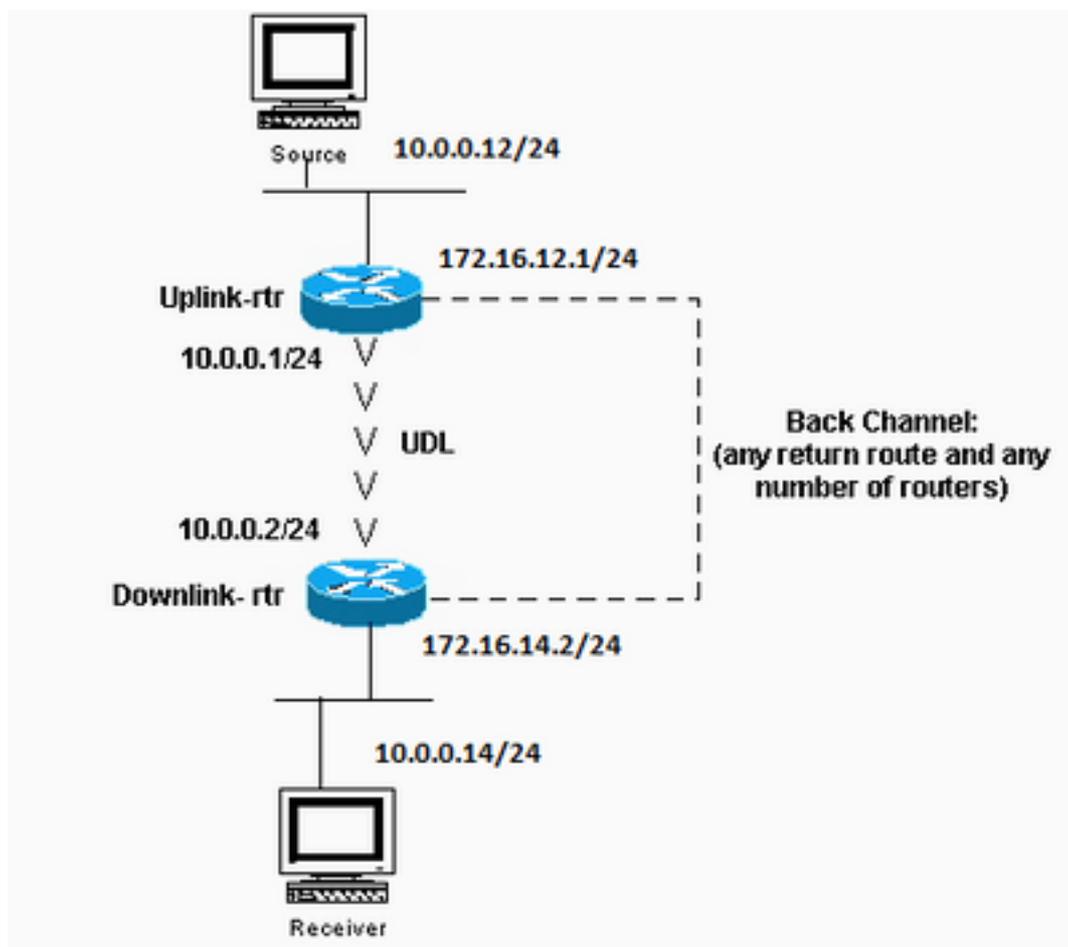
Konfiguration von Router 2

```
ip multicast-routing
int e0
ip pim sparse-dense-mode
ip igmp helper-address 192.168.140.2
```

```
int s0
ip pim sparse-dense-mode
```

IGMP UDLR für Satellitenverbindungen

Unidirectional Link Routing (UDLR) stellt ein Verfahren zum Weiterleiten von Multicast-Paketen über eine unidirektionale Satellitenverbindung an Stub-Netzwerke mit einem Rückkanal bereit. Dies ähnelt dem Stub-Multicast-Routing. Ohne diese Funktion kann der Uplink-Router nicht dynamisch ermitteln, welche IP-Multicast-Gruppenadressen über die unidirektionale Verbindung weitergeleitet werden sollen, da der Downlink-Router keine Daten zurücksenden kann.



Unidirectional Link Routing

(UDLR): Methode zur Weiterleitung von Multicast-Paketen

Uplink-RTR-Konfiguration

```
ip multicast-routing
```

```
interface Ethernet0
description Typical IP multicast enabled interface
ip address 172.16.12.1 255.0.0.0
ip pim sparse-dense-mode
```

```
interface Ethernet1
description Back channel which has connectivity to downlink-rtr
ip address 172.16.11.1 255.0.0.0
ip pim sparse-dense-mode
```

```
interface Serial0
```

```
description Unidirectional to downlink-rtr
ip address 10.0.0.1 255.0.0.0
ip pim sparse-dense-mode
ip igmp unidirectional-link
no keepalive
```

Downlink-rtr-Konfiguration

```
ip multicast-routing
```

```
interface Ethernet0
description Typical IP multicast enabled interface
ip address 172.16.14.2 255.0.0.0
ip pim sparse-dense-mode
ip igmp helper-address udl serial0
```

```
interface Ethernet1
description Back channel which has connectivity to downlink-rtr
ip address 172.16.13.2 255.0.0.0
ip pim sparse-dense-mode
```

```
interface Serial0
description Unidirectional to uplink-rtr
ip address 10.0.0.2 255.0.0.0
ip pim sparse-dense-mode
ip igmp unidirectional-link
no keepalive
```

PIMv2-BSR

Wenn auf allen Routern im Netzwerk PIMv2 ausgeführt wird, können Sie anstelle von Auto-RP einen BSR konfigurieren. BSR und Auto-RP sind sich sehr ähnlich. Eine BSR-Konfiguration erfordert die Konfiguration von BSR-Kandidaten (ähnlich wie RP-Announce in Auto-RP) und BSRs (ähnlich wie Auto-RP Mapping Agents). Um einen BSR zu konfigurieren, gehen Sie wie folgt vor:

1. Konfigurieren Sie auf den BSR-Kandidaten:

```
ip pim bsr-candidate interface hash-mask-len pref
```

Dabei enthält die **Schnittstelle** die Kandidaten-BSR-IP-Adresse. Es wird empfohlen (aber nicht erforderlich), dass **hash-mask-Len** für alle BSR-Kandidaten identisch ist. Ein BSR-Kandidat mit dem größten **pref**-Wert wird als BSR für diese Domäne ausgewählt. Ein Beispiel für die Befehlsverwendung wird angezeigt:

```
ip pim bsr-candidate ethernet0 30 4
```

Der PIMv2-BSR sammelt RP-Kandidateninformationen und verteilt RP-Set-Informationen, die jedem Gruppenpräfix zugeordnet sind. Um Single-Point-of-Failure zu vermeiden, können Sie mehrere Router in einer Domäne als Kandidaten-BSRs konfigurieren. Ein BSR wird auf Basis der konfigurierten Voreinstellungswerte automatisch unter den Kandidaten-BSRs ausgewählt. Um als BSR-Kandidaten zu fungieren, müssen die Router angeschlossen sein und sich im Backbone des Netzwerks befinden, anstatt im Einwahlbereich des Netzwerks.

2. Konfigurieren Sie mögliche RP-Router. Dieses Beispiel zeigt einen möglichen RP auf der Schnittstelle ethernet0 für den gesamten Admin-Bereich:

```
access-list 11 permit 239.0.0.0 0.255.255.255
ip pim rp-candidate ethernet0 group-list 11
```

CGMP

Um das Group Management Protocol (CGMP) zu konfigurieren, konfigurieren Sie dies auf der Router-Schnittstelle, die zum Switch zeigt:

```
ip pim sparse-dense-mode
ip cgmp
```

Konfigurieren Sie anschließend Folgendes auf dem Switch:

```
set cgmp enable
```

IGMP-Snooping

Internet Group Management Protocol (IGMP)-Snooping ist in Version 4.1 des Catalyst 5000 verfügbar. IGMP-Snooping erfordert eine Supervisor III-Karte. Zum Konfigurieren von IGMP-Snooping auf dem Router ist keine andere Konfiguration als PIM erforderlich. Ein Router mit IGMP-Snooping ist weiterhin erforderlich, um IGMP-Abfragen bereitzustellen.

Das hier gezeigte Beispiel zeigt, wie IGMP-Snooping auf dem Switch aktiviert wird:

```
Console> (enable) set igmp enable
IGMP Snooping is enabled.
CGMP is disabled.
```

Wenn Sie versuchen, IGMP zu aktivieren, CGMP jedoch bereits aktiviert ist, wird Folgendes angezeigt:

```
Console> (enable) set igmp enable
Disable CGMP to enable IGMP Snooping feature.
```

PGM

Pragmatic General Multicast (PGM) ist ein zuverlässiges Multicast-Transportprotokoll für Anwendungen, die eine geordnete, doppeltfreie Multicast-Datenübermittlung von mehreren Quellen an mehrere Empfänger erfordern. PGM garantiert, dass ein Empfänger in der Gruppe entweder alle Datenpakete von Übertragungen und Neuübertragungen empfängt oder einen nicht wiederherstellbaren Datenpaketverlust erkennen kann.

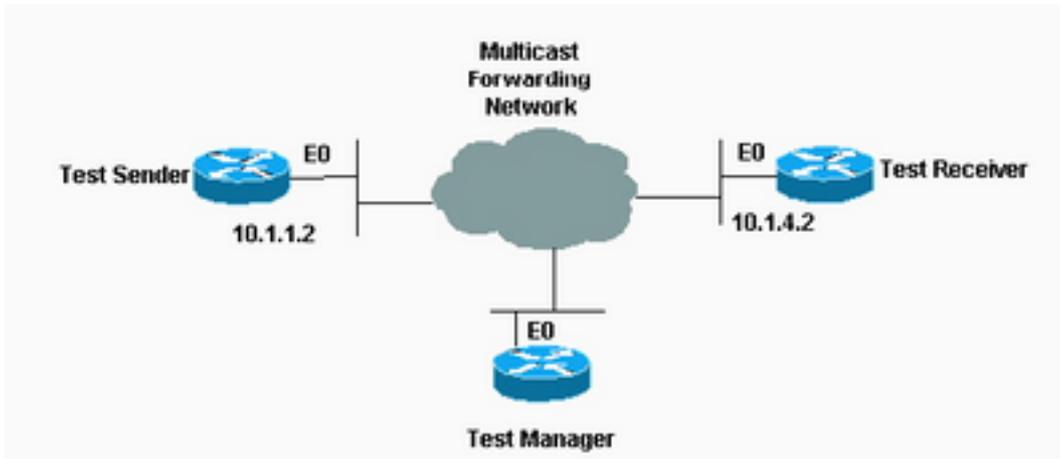
Es gibt keine globalen PGM-Befehle. PGM wird mithilfe des Befehls **ip pgm** für jede Schnittstelle konfiguriert. Sie müssen Multicast-Routing auf dem Router mit PIM auf der Schnittstelle aktivieren.

MRM

Multicast Routing Monitor (MRM) ermöglicht die automatische Fehlererkennung in einer großen Multicast-Routing-Infrastruktur. MRM wurde entwickelt, um Netzwerkadministratoren nahezu in Echtzeit über Probleme beim Multicast-Routing zu informieren.

MRM besteht aus zwei Komponenten: MRM-Tester und MRM-Manager. MRM-Tester ist ein Absender oder Empfänger.

MRM ist ab Version 12.0(5)T der Cisco IOS-Software verfügbar. Nur die MRM-Tester und -Manager benötigen die von MRM unterstützte Cisco IOS-Version.



Multicast Routing Monitor

(MRM) erleichtert die automatisierte Fehlererkennung in einer großen Multicast-Routing-Infrastruktur

Konfiguration des Testabsenders

```
interface Ethernet0
 ip mrm test-sender
```

Test Receiver-Konfiguration

```
interface Ethernet0
 ip mrm test-receiver
```

Test Manager-Konfiguration

```
ip mrm manager test1
manager e0 group 239.1.1.1
senders 1
receivers 2 sender-list 1

access-list 1 permit 10.1.1.2
access-list 2 permit 10.1.4.2
```

Die Ausgabe des Befehls `show ip mrm manager` auf dem Test Manager wird hier angezeigt:

```
Test_Manager# show ip mrm manager
  Manager:test1/10.1.2.2 is not running Beacon interval/holdtime/ttl:60/86400/32
Group:239.1.1.1, UDP port test-packet/status-report:16384/65535 Test sender: 10.1.1.2 Test
receiver: 10.1.4.2
```

Starten Sie den Test mit dem hier gezeigten Befehl. Der Testmanager sendet Kontrollnachrichten an den Testsender und den Testempfänger, wie in den Testparametern konfiguriert. Der Testempfänger tritt der Gruppe bei und überwacht die vom Testsender gesendeten Testpakete.

```
Test_Manager# mrm start test1
*Feb 4 10:29:51.798: IP MRM test test1 starts .....
Test_Manager#
```

Geben Sie den folgenden Befehl ein, um einen Statusbericht für den Test-Manager anzuzeigen:

```
Test_Manager# show ip mrm status

IP MRM status report cache:
```

| Timestamp | Manager | Test Receiver | Pkt Loss/Dup (%) | Ehsr |
|-----------------|----------|---------------|------------------|------|
| *Feb 4 14:12:46 | 10.1.2.2 | 10.1.4.2 | 1 (4%) | 29 |
| *Feb 4 18:29:54 | 10.1.2.2 | 10.1.4.2 | 1 (4%) | 15 |

Test_Manager#

Die Ausgabe zeigt, dass der Empfänger zwei Statusberichte (je eine Zeile) mit einem bestimmten Zeitstempel gesendet hat. Jeder Bericht enthält einen Paketverlust während des Intervallfensters (Standardwert: eine Sekunde). Der "Ehsr"-Wert zeigt den geschätzten Wert der nächsten Sequenznummer des Testsenders an. Wenn der Test-Empfänger doppelte Pakete erkennt, wird in der Spalte "Pkt Loss/Dup" eine negative Zahl angezeigt.

Um den Test zu beenden, geben Sie den folgenden Befehl ein:

```
Test_Manager# mrm stop test1
*Feb 4 10:30:12.018: IP MRM test test1 stops
Test_Manager#
```

Während des Tests sendet der MRM-Absender RTP-Pakete im Standardintervall von 200 ms an die konfigurierte Gruppenadresse. Der Empfänger überwacht (erwartet) dieselben Pakete im gleichen Standardintervall. Wenn der Empfänger einen Paketverlust im Standardfensterintervall von fünf Sekunden erkennt, sendet er einen Bericht an den MRM-Manager. Sie können den Statusbericht vom Empfänger anzeigen, wenn Sie den Befehl **show ip mrm status** auf dem Manager ausführen.

Fehlerbehebung

Zu den häufigsten Problemen, die bei der Implementierung von IP-Multicast in einem Netzwerk auftreten, gehören Probleme, wenn der Router aufgrund eines RPF-Fehlers oder der TTL-Einstellungen keinen Multicast-Datenverkehr weiterleitet. Im [Fehlerbehebungshandbuch](#) für [IP-Multicast](#) finden Sie eine detaillierte Beschreibung dieser und anderer häufiger Probleme, Symptome und Lösungen.

Zugehörige Informationen

- [Handbuch zur Fehlerbehebung bei IP-Multicast](#)
- [Fehlerbehebung bei Multicast-Netzwerken mit CLI-Tools](#)
- [IP-Multicast-Unterstützung](#)
- [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.