

# Multicast über einen GRE-Tunnel

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Konfigurieren](#)

[Netzwerkdigramm](#)

[Konfigurationen](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

## Einführung

Dieses Dokument enthält eine Beispielkonfiguration für Multicasting über einen Generic Routing Encapsulation (GRE)-Tunnel.

In vielen Netzwerkszenarien möchten Sie Ihr Netzwerk so konfigurieren, dass GRE-Tunnel zum Senden von Protocol Independent Multicast (PIM)- und Multicast-Datenverkehr zwischen Routern verwendet werden. In der Regel werden Multicast-Quelle und -Empfänger durch eine IP-Cloud getrennt, die nicht für IP-Multicast-Routing konfiguriert ist. In solchen Netzwerkszenarien wird bei der Konfiguration eines Tunnels über eine IP-Cloud mit PIM-aktivierter Übertragung Multicast-Pakete zum Empfänger übertragen. In diesem Dokument werden die Konfiguration, die Überprüfung und die damit verbundenen Probleme im Zusammenhang mit Multicasting über einen GRE-Tunnel beschrieben.

## Voraussetzungen

### Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Ein grundlegendes Verständnis von Multicast und PIM ist hilfreich. Weitere Informationen zu Multicast und PIM finden Sie im [Multicast Quick-Start-Konfigurationshandbuch](#).

### Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren

(Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Konventionen

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

## Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Wie das Netzwerkdiagramm zeigt, ist die Multicast-Quelle (10.1.1.1) mit R102 verbunden und für die Multicast-Gruppe 239.1.1.20 konfiguriert. Der Multicast-Empfänger (10.2.2.3) ist mit R104 verbunden und für den Empfang von Multicast-Paketen für die Gruppe 239.1.1.20 konfiguriert. Die Trennung von R102 und R104 ist eine IP-Cloud, die nicht für Multicast-Routing konfiguriert ist.

Zwischen R102 und R104 wird ein Tunnel konfiguriert, der über die Loopback-Schnittstellen bereitgestellt wird. Der Befehl **ip pim sparse-dense mode** wird auf Tunnelschnittstellen konfiguriert, und Multicast-Routing ist auf R102 und R104 aktiviert. Die Konfiguration des Sparse-Dense-Modus an den Tunnelschnittstellen ermöglicht die Weiterleitung von Sparse-Mode- oder Dense-Mode-Paketen über den Tunnel, abhängig von der Rendezvous Point (RP)-Konfiguration für die Gruppe.

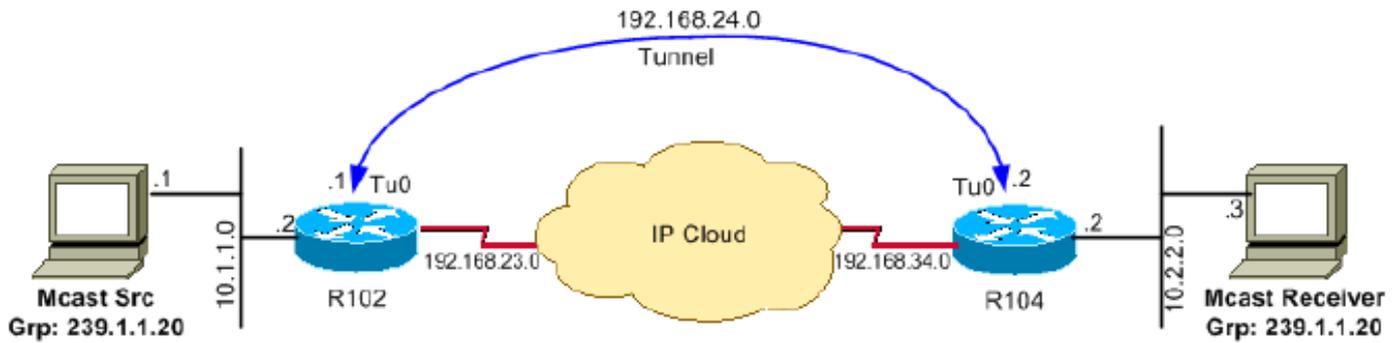
**Hinweis:** *Für den Dense-Modus* - Bei konfigurierter PIM-Dense-Modus über den Tunnel wird ein Befehl **ip mroute 10.1.1.0 255.255.255.0 tunnel 0** auf R104 konfiguriert, um eine erfolgreiche RPF für die Multicast-Quelladresse 10.11.1.1.1.1.1.111 zu gewährleisten. Eingehende (10.1.1.1, 239.1.1.20) Multicast-Pakete über Tunnel0 (Tu0) werden mit dieser mroute-Anweisung auf Reverse Path Forwarding (RPF) geprüft. Nach einer erfolgreichen Prüfung werden die Multicast-Pakete an die OIL-Schnittstellen (Outgoing Interface List) weitergeleitet.

**Hinweis:** Stellen Sie bei Konfiguration des PIM Sparse Mode über den Tunnel sicher, dass diese Punkte adressiert werden:

- Für eine erfolgreiche RPF-Verifizierung des Multicast-Datenverkehrs, der vom RP über den Shared Tree (\*,G) fließt, muss ein Befehl **ip mroute rp-address nexthop** für die RP-Adresse konfiguriert werden, der auf die Tunnelschnittstelle zeigt. Unter der Annahme, dass R102 der RP (RP-Adresse 2.2.2.2) ist, ist mroute der Befehl **ip mroute 2.2.2 255.255.255.255 Tunnel 0**, der eine erfolgreiche RPF-Überprüfung des Datenverkehrs sicherstellt, der über den Shared Tree fließt.
- Für eine erfolgreiche RPF-Verifizierung des Multicast-Datenverkehrs (S,G), der über den Shortest Path Tree (SPT) fließt, muss ein Befehl **ip mroute source-address nexthop** für die Multicast-Quelle konfiguriert werden, der auf die Tunnelschnittstelle verweist. Wenn SPT-Datenverkehr über die Tunnelschnittstelle fließt, wird der Befehl **ip mroute 10.1.1.0 255.255.255.0 tunnel 0** auf R104 konfiguriert, um eine erfolgreiche RPF-Verifizierung für eingehenden Datenverkehr sicherzustellen (10.1.1.1.1, 20, 20, 20, 20, 20, 20, 20, 220, 1.1.1.1.1.1.1.1.1.1.20) Multicast-Pakete über die Tu0-Schnittstelle.

## Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



## Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

- [R102](#)
- [R104](#)

Konfigurieren Sie Router 102 entsprechend dieser aktuellen Konfigurationsdatei:

### R102

```
version 12.2
!hostname r102
!
!ip subnet-zero
no ip domain-lookup
!--- It stops IP domain lookup, which improves
!--- the show command response time. ! ip multicast-routing !--- Enables IP multicast routing. ! interf
Loopback0 ip address 2.2.2.2 255.255.255.255 !--- Tunnel Source interface. ! interface Tunnel0 !--- Tun
interface configured for PIM and carrying
!--- multicast packets to R104. ip address 192.168.24.1 255.255.255.252 ip pim sparse-dense-mode tunnel
source Loopback0 tunnel destination 4.4.4.4 ! interface Ethernet0/0 !--- Interface connected to Source.
address 10.1.1.2 255.255.255.0 ip pim sparse-dense-mode ! ! interface Serial8/0 ip address 192.168.23.1
255.255.255.252 !--- Note IP PIM sparse-dense mode is
!--- not configured on Serial interface. !router ospf 1 log-adjacency-changes network 2.2.2.2 0.0.0.0 a
network 10.1.1.0 0.0.0.255 area 0 network 192.168.23.0 0.0.0.255 area 0 ! ip classless ip pim bidir-ena
line con 0 line aux 0 line vty 0 4 login ! end
```

Konfigurieren Sie Router 104 entsprechend dieser aktuellen Konfigurationsdatei:

### R104

```
r104#
version 12.2
!
hostname r104
!
!
```

```

ip subnet-zero
no ip domain-lookup
!--- It stops IP domain lookup, which improves
!--- the show command response time. ! ip multicast-routing !--- Enables IP multicast routing. ! interf
Loopback0 ip address 4.4.4.4 255.255.255.255 !--- Tunnel Source interface. ! interface Tunnel0 ip addre
192.168.24.2 255.255.255.252 !--- Tunnel interface configured for PIM
!--- and carrying multicast packets. ip pim sparse-dense-mode tunnel source Loopback0 tunnel destinatio
2.2.2.2 ! interface Ethernet0/0 ip address 10.2.2.2 255.255.255.0 ip pim sparse-dense-mode ! interface
Serial9/0 ip address 192.168.34.1 255.255.255.252 !--- Note IP PIM sparse-dense mode is not
!--- configured on Serial interface. ! ! router ospf 1 log-adjacency-changes network 4.4.4.4 0.0.0.0 ar
network 10.2.2.0 0.0.0.255 area 0 network 192.168.34.0 0.0.0.255 area 0 ! ip classless no ip http serve
pim bidir-enable ip mroute 10.1.1.0 255.255.255.0 Tunnel0 !--- This mroute ensures a successful RPF che
!--- for packets flowing from the source.
!--- 10.1.1.1 over Shared tree in case of Dense
!--- more and SPT in case of Sparse mode. ! ip mroute 2.2.2.2 255.255.255.255 tunnel 0 !--- This mroute
required for RPF check when
!--- Sparse mode multicast traffic is
!--- flowing from RP (assuming R102 with 2.2.2.2 as RP)
!--- towards receiver via tunnel
!--- before the SPT switchover. line con 0 line aux 0 line vty 0 4 login ! end

```

## Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Der [Cisco CLI Analyzer](#) (nur [registrierte](#) Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie den Cisco CLI Analyzer, um eine Analyse der **Ausgabe** des **Befehls show** anzuzeigen.

- **show ip igmp group** - Überprüft, ob der Empfänger seinen IGMP-Beitrittsantrag für die Gruppe 239.1.1.20 an R104 gesendet hat.

```

r104#show ip igmp groups
IGMP Connected Group Membership
Group Address      Interface          Uptime    Expires    Last Reporter
239.1.1.20         Ethernet0/0        00:00:04  00:02:55  10.2.2.3

```

- **show ip mroute group-address** - Verifiziert, dass R102 beim Start von Multicasting-Paketen für die Gruppe 239.1.1.20 durch die Quelle 10.1.1.1 die Pakete (\*,239.1.1.20) und (10.1.1.1, 239.1.1.20) Einträge in die R102 mroute-Tabelle. **Hinweis:** Im Eintrag (10.1.1.1, 239.1.1.20) lautet der OIL Tunnel0.

```

r102#show ip mroute 239.1.1.20
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, 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 - Candidate for MSDP Advertisement,
U - URD, I - Received Source Specific Host Report
Outgoing interface flags: H - Hardware switched
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 239.1.1.20), 00:00:09/00:02:59, RP 0.0.0.0, flags: D
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Tunnel0, Forward/Sparse-Dense, 00:00:09/00:00:00
    Ethernet0/0, Forward/Sparse-Dense, 00:00:09/00:00:00

(10.1.1.1, 239.1.1.20), 00:00:09/00:02:58, flags: T
  Incoming interface: Ethernet0/0, RPF nbr 0.0.0.0
  Outgoing interface list:
    Tunnel0, Forward/Sparse-Dense, 00:00:09/00:00:00

```

- **show ip mroute group-address** - Überprüft, ob der R104 die (\*,239.1.1.20) und (10.1.1.1, 239.1.1.20) Einträge hat, während er Multicast-Pakete für die Gruppe 239.1.1.20 weiterleitet, die von 1.20 stammen 1.1.1Hinweis: (10.1.1.1, 239.1.1.20) ist die eingehende Schnittstelle Tunnel0 und der RPF-Nachbar 192.168.24.1 - das Tunnelkopfende auf R102. Die RPF-Verifizierung erfolgt auf Basis der auf R104 konfigurierten Route, und die Multicast-Pakete werden an die OIL an den Empfänger weitergeleitet, der an der Ethernet 0/0-Schnittstelle angeschlossen ist.

```
r104#show ip mroute 239.1.1.20
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, 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 - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report
Outgoing interface flags: H - Hardware switched
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 239.1.1.20), 00:07:10/00:00:00, RP 0.0.0.0, flags: DCL
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Tunnel0, Forward/Sparse-Dense, 00:07:10/00:00:00
    Ethernet0/0, Forward/Sparse-Dense, 00:07:10/00:00:00

(10.1.1.1, 239.1.1.20), 00:01:13/00:02:24, flags: CLT
  Incoming interface: Tunnel0, RPF nbr 192.168.24.1, Mroute
  Outgoing interface list:
    Ethernet0/0, Forward/Sparse-Dense, 00:01:13/00:00:00
```

- **show ip rpf ip-address** - RPF-Überprüfung für Pakete, die von 10.1.1.1 stammen Im folgenden Beispiel wird bestätigt, dass RPF für 10.1.1.1 über Tunnel 0 erfolgt, auf dem die Multicast-Pakete (S,G) empfangen werden.

```
r104>show ip rpf 10.1.1.1
RPF information for ? (10.1.1.1)
  RPF interface: Tunnel0
  RPF neighbor: ? (192.168.24.1)
  RPF route/mask: 10.1.1.1/24
  RPF type: static
  RPF recursion count: 0
  Doing distance-preferred lookups across tables
```

## Fehlerbehebung

In diesem Abschnitt finden Sie eine Fehlerbehebung für Ihre Konfiguration.

Der [Cisco CLI Analyzer](#) (nur [registrierte](#) Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie den Cisco CLI Analyzer, um eine Analyse der **Ausgabe** des **Befehls show** anzuzeigen.

**Hinweis:** Beachten Sie [vor der](#) Verwendung von **Debug**-Befehlen die [Informationen](#) zu [Debug-Befehlen](#).

Wenn Ihr Multicast über den GRE-Tunnel nicht funktioniert, kann eine der folgenden Ursachen vorliegen:

- **Tunnel not UP/UP (Tunnel not UP/UP)** - Quelle und Ziel des Tunnels stimmen nicht auf jedem Tunnelende überein. Wenn beispielsweise das Tunnelziel auf R102 auf die IP-Adresse

10.2.2.2 anstelle von 2.2.2.2 geändert wurde, während die Konfiguration auf R104 unverändert blieb, würde der Tunnel nicht angezeigt. Geben Sie den Befehl **show interface tunnel 0** ein, um den Status des Tunnels zu überprüfen.

- **Multicast-Pakete werden aufgrund eines RPF-Ausfalls verworfen.** Geben Sie den Befehl **show ip mroute count** ein. In dieser Ausgabe wird eine Beispielausgabe dieses Befehls und seiner steigenden Zähler für RPF-Fehler angezeigt:

```
r104#show ip mroute count
IP Multicast Statistics
3 routes using 1642 bytes of memory
2 groups, 0.50 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: 224.0.1.40, Source count: 0, Packets forwarded: 0, Packets received: 0

Group: 239.1.1.20, Source count: 1, Packets forwarded: 11, Packets received: 45
Source: 10.1.1.1/32, Forwarding: 11/0/100/0, Other: 25/14/0
```

```
!--- After some time, the show ip mroute count command
!--- is issued again. You can see the RPF failed counter increasing: r104#show ip mroute
count
IP Multicast Statistics
3 routes using 1642 bytes of memory
2 groups, 0.50 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: 224.0.1.40, Source count: 0, Packets forwarded: 0, Packets received: 0

Group: 239.1.1.20, Source count: 1, Packets forwarded: 11, Packets received: 50
Source: 10.1.1.1/32, Forwarding: 11/0/100/0, Other: 30/19/0
r104#
```

Sie können auch den Befehl **show ip rpf source** ausführen. Stellen Sie sicher, dass die RPF-Schnittstelle mit der Schnittstelle identisch ist, auf der die Quell-Multicast-Pakete empfangen werden - in diesem Beispiel Tunnel 0. Weitere Informationen zu RPF-Ausfällen finden Sie im [Leitfaden zur IP Multicast-Fehlerbehebung](#).

- **PIM Neighbors - Der Router R102 leitet nicht über die Tunnel0-Schnittstelle weiter, da er keinen PM-Nachbarn R104 sieht.** Geben Sie folgende Befehle ein: **show ip pim neighbor** - Sie können den Befehl **show ip pim neighbor** auf R102 verwenden, um den Nachbarn R104 über den Tunnel anzuzeigen. **show ip pim int** - Sie können auch den Befehl **show ip pim int** verwenden, um anzuzeigen, dass ein Nachbar vorhanden ist. **ip pim sparse-dense-mode** - Überprüfen Sie, ob der Befehl **ip pim sparse-dense-mode** auf Schnittstellenebene auf beiden Tunnelenden konfiguriert ist und ob IP-Multicast-Routing aktiviert ist.

## Zugehörige Informationen

- [Multicast-Schnellstartanleitung](#)
- [Leitfaden zur Fehlerbehebung bei IP-Multicast](#)
- [Grundlegende Tools zur Fehlerbehebung bei Multicast](#)
- [Support-Seite für TCP/IP-Multicast](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)