

Multicast su tunnel GRE

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene fornita una configurazione di esempio per il multicast su un tunnel GRE (Generic Routing Encapsulation).

In molti scenari di rete si desidera configurare la rete in modo che utilizzi i tunnel GRE per inviare traffico PIM (Protocol Independent Multicast) e multicast tra router. In genere, questo si verifica quando l'origine e il destinatario multicast sono separati da un cloud IP non configurato per il routing multicast IP. In tali scenari di rete, la configurazione di un tunnel attraverso un cloud IP con PIM permette di trasportare i pacchetti multicast verso il destinatario. In questo documento vengono descritti la configurazione, la verifica e i problemi correlati relativi al multicast su un tunnel GRE.

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Una conoscenza di base di multicast e PIM è utile. Per ulteriori informazioni sul multicast e sul PIM, consultare la [guida alla configurazione multicast](#) con [avvio rapido](#).

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Come mostra il diagramma di rete, l'origine multicast (10.1.1.1) è connessa a R102 ed è configurata per il gruppo multicast 239.1.1.20. Il ricevitore multicast (10.2.2.3) è connesso a R104 ed è configurato per ricevere pacchetti multicast per il gruppo 239.1.1.20. Separando R102 e R104 si ottiene un cloud IP, non configurato per il routing multicast.

Viene configurato un tunnel tra i router R102 e R104 con le relative interfacce di loopback. Il comando **ip pim sparse-dense mode** è configurato sulle interfacce del tunnel e il routing multicast è abilitato sui router R102 e R104. La configurazione della modalità sparse-dense sulle interfacce del tunnel consente l'inoltro dei pacchetti in modalità sparse o densa sul tunnel a seconda della configurazione del punto di rendering (RP) per il gruppo.

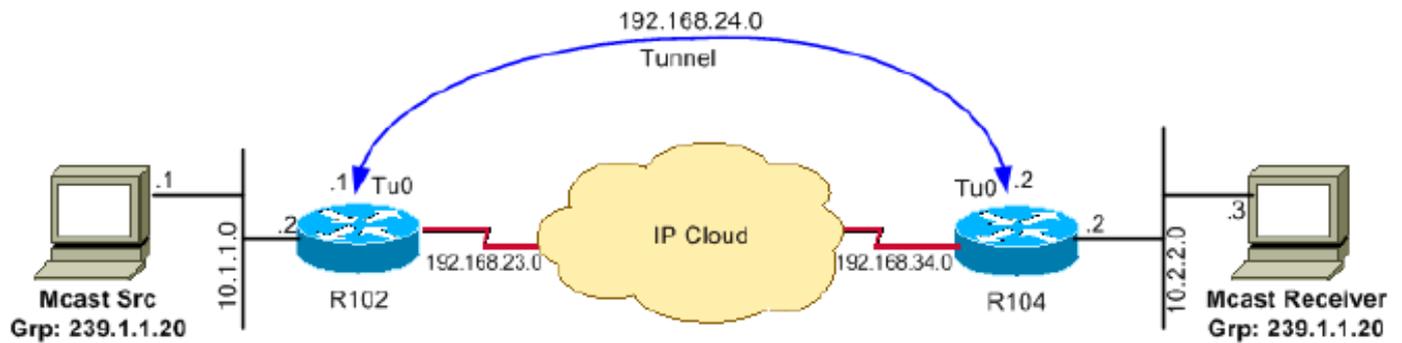
Nota: *Per la modalità densa:* con la modalità densa PIM configurata sul tunnel, un comando **ip route 10.1.1.0 255.255.255.0 tunnel 0** viene configurato su R104 per garantire la riuscita di un RPF per l'indirizzo di origine multicast 10.1.1.1. I pacchetti multicast in arrivo (10.1.1.1, 239.1.1.20) su Tunnel0 (Tu0) vengono controllati per l'inoltro di percorso inverso (RPF) utilizzando questa istruzione route. Dopo aver superato il controllo, i pacchetti multicast vengono inoltrati alle interfacce dell'elenco di interfacce in uscita (OIL).

Nota: *Per la modalità sparse:* con la modalità sparse PIM configurata sul tunnel, verificare che siano presi in considerazione i seguenti punti:

- Per una corretta verifica RPF del traffico multicast che scorre sull'albero condiviso (*,G) da RP, è necessario configurare un comando **ip mroute rp-address nexthop** per l'indirizzo RP, che punta all'interfaccia del tunnel. Supponendo che R102 sia l'RP (indirizzo RP 2.2.2.2) in questo caso, il router intermedio è il comando **ip mroute 2.2.2.2 255.255.255.255 tunnel 0**, che assicura il corretto controllo delle richieste RPF per il traffico che attraversa la struttura condivisa.
- Per una corretta verifica da parte di RPF del traffico multicast (S,G) che attraversa l'albero del percorso più breve (SPT), è necessario configurare un comando **ip mroute source-address nexthop** per l'origine multicast, che punta all'interfaccia del tunnel. In questo caso, quando il traffico SPT scorre sull'interfaccia del tunnel, un comando **ip route 10.1.1.0 255.255.255.0 tunnel 0** viene configurato su R104 per garantire la riuscita della verifica RPF dei pacchetti multicast in arrivo (10.1.1.1, 239.1.1.20) sull'interfaccia Tu0.

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Configurazioni

Nel documento vengono usate queste configurazioni:

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

Configurare il router 102 in base al seguente file di configurazione in esecuzione:

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 Serial18/0 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

```

Configurare il router 104 in base al seguente file di configurazione in esecuzione:

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

```

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

[Cisco CLI Analyzer \(solo utenti registrati\) supporta alcuni comandi show.](#) Usare Cisco CLI Analyzer per visualizzare un'analisi dell'output del comando **show**.

- **show ip igmp group:** verifica che il destinatario abbia inviato la richiesta di appartenenza ad IGMP per il gruppo da 239.1.1.20 a R104.

```

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 route group-address:** verifica che quando l'origine 10.1.1.1 avvia il multicasting dei pacchetti per il gruppo 239.1.1.20, R102 installa le voci (*.239.1.1.20) e (10.1.1.1, 239.1.1.20) nella tabella di route R102. **Nota:** nella voce (10.1.1.1, 239.1.1.20), l'OLIO è 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 route group-address:** verifica che R104 includa le voci (*.239.1.1.20) e (10.1.1.1, 239.1.1.20) durante l'inoltro dei pacchetti multicast per il gruppo 239.1.1.20 provenienti da

10.1.1.1.**Nota:** in (10.1.1.1, 239.1.1.20), l'interfaccia in entrata è Tunnel0 e il router adiacente RPF è 192.168.24.1 - l'headend del tunnel su R102. La verifica RPF viene eseguita in base al percorso configurato su R104 e i pacchetti multicast vengono inviati al router OIL al ricevitore collegato sull'interfaccia Ethernet 0/0.

```
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:** esegue una verifica RPF per i pacchetti provenienti da 10.1.1.1. L'esempio che segue conferma che RPF per 10.1.1.1 è collegato al tunnel 0, sul quale stiamo ricevendo i pacchetti multicast (S,G).

```
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
```

Risoluzione dei problemi

Utilizzare questa sezione per risolvere i problemi relativi alla configurazione.

[Cisco CLI Analyzer \(solo utenti registrati\) supporta alcuni comandi show.](#) Usare Cisco CLI Analyzer per visualizzare un'analisi dell'output del comando **show**.

Nota: consultare le [informazioni importanti sui comandi di debug](#) prima di usare i comandi di **debug**.

Se il multicast su tunnel GRE non funziona, una delle seguenti cause può essere:

- **Tunnel non UP/UP:** l'origine e la destinazione del tunnel non corrispondono su entrambe le estremità del tunnel. Ad esempio, se la destinazione del tunnel su R102 è stata modificata sull'indirizzo IP 10.2.2.2 invece di 2.2.2 mentre la configurazione su R104 è rimasta la stessa, il tunnel non verrebbe restituito. Usare il comando **show interface tunnel 0** per verificare lo stato del tunnel.
- **I pacchetti multicast vengono scartati a causa di un errore RPF.** Eseguire il comando **show ip**

route count. Di seguito è riportato un output di esempio di questo comando e dei relativi contatori crescenti per gli errori RPF:

```
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#
```

è possibile usare anche il comando **show ip rpf source**. Verificare che l'interfaccia RPF sia la stessa su cui vengono ricevuti i pacchetti multicast di origine - in questo esempio, tunnel 0. Per ulteriori informazioni sugli errori RPF, consultare la [guida alla risoluzione dei problemi relativi al multicast IP](#).

- **Router adiacenti PIM:** il router R102 non sta eseguendo l'inoltro tramite l'interfaccia Tunnel0 perché non vede un router adiacente PIM R104. Utilizzare i seguenti comandi: **show ip pim neighbors**: è possibile utilizzare il comando **show ip pim neighbors** su R102 per visualizzare il router adiacente R104 sul tunnel. **show ip pim int** - Per verificare la presenza di una porta adiacente, è possibile utilizzare anche il comando **show ip pim int.ip pim sparse-dense-mode**: verificare che il comando **ip pim sparse-dense-mode** a livello di interfaccia sia configurato su entrambe le estremità del tunnel e che il routing multicast IP sia abilitato.

Informazioni correlate

- [Guida rapida alla configurazione del multicast](#)
- [Guida alla risoluzione dei problemi del multicast IP](#)
- [Strumenti di base per la risoluzione dei problemi relativi al multicast](#)
- [Pagina di supporto per il multicast TCP/IP](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)