# Risoluzione dei problemi relativi alle reti multicast con gli strumenti CLI

## Sommario

# Introduzione

In questo documento vengono descritti diversi strumenti e tecniche utilizzati per risolvere i problemi relativi alle reti multicast.

# Prerequisiti

## Requisiti

Nessun requisito specifico previsto per questo documento.

## 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.

# Risoluzione dei problemi relativi alle strategie

Quando si risolvono i problemi relativi alle reti multicast, è opportuno considerare il protocollo di segnalazione utilizzato nella rete e nel flusso dei pacchetti. Il protocollo di segnalazione viene utilizzato per configurare e interrompere le sessioni multicast (ad esempio, PIM dense mode, PIM sparse mode e DVMRP), e il flusso di pacchetto è l'effettivo invio, replica e ricezione dei pacchetti multicast tra l'origine e il destinatario, in base alla tabella di inoltro creata dal processo di segnalazione.

Questa tabella consente di verificare il corretto funzionamento di ciascuna informazione relativa al pezzo da risolvere e di controllare il corretto funzionamento di ciascuna sezione della tabella:

| | Origine | Rete | Ricevitori |
|---|---|---|---|
| Segnalazione | N/D | Verifica segnalazione di rete | Segnalazione ricevitore assegno |
| Flusso dei pacchetti | Verifica flusso pacchetti di origine | Verifica flusso pacchetti di rete | Verifica flusso pacchetti ricevitore |

Nelle sezioni seguenti vengono descritti in dettaglio gli strumenti di risoluzione dei problemi che è possibile utilizzare per verificare e risolvere i problemi più comuni.

## Verifica flusso pacchetti di origine

Completare questa procedura per determinare se i pacchetti sono stati inviati dall'origine e se sono stati inseriti i campi del pacchetto corretti:

1. Controllare i contatori dell'interfaccia sull'host. Controllare innanzitutto i contatori di interfaccia (se si utilizza un sistema UNIX, utilizzare il comando netstat) sull'host di origine per verificare se invia i pacchetti. In caso contrario, verificare la presenza di errori di configurazione o di bug nello stack host e nell'applicazione.

2. Usare il comando show ip igmp groups <interface-name> per controllare il router upstream e vedere se ha ricevuto un report di appartenenza al join sull'interfaccia direttamente connessa all'origine.

3. Controllare il valore TTL dei pacchetti nell'applicazione multicast; deve essere maggiore di 1. Se l'applicazione invia pacchetti con un valore TTL inferiore a 1, il traffico verrà scartato sul primo router upstream. Per verificarlo, usare il comando show ip traffic e cercare un aumento del valore del contatore "bad hop count". Qualsiasi pacchetto il cui valore TTL è 1 o inferiore alla soglia TTL impostata dall'interfaccia con il comando ip multicast ttl-threshold viene scartato e il contatore "bad hop-count" viene aumentato di un'unità. Utilizzare il comando show ip igmp interface <nome-interfaccia> per verificare il valore di soglia TTL dell'interfaccia.

4. Usare i comandi show ip route count e show ip route active per controllare il primo router o switch upstream e verificare se vede pacchetti multicast provenienti dall'origine. L'output del comando mostra le statistiche del flusso del traffico per ciascuna coppia (S,G). Se non si osserva alcun traffico, controllare la segnalazione del ricevitore.

5. Usare il comando debug ip mpacket sul router a monte più vicino, con l'argomento detail o acl per la granularità.

---

⚠ Attenzione: utilizzare questo comando con cautela in caso di traffico multicast intenso sulla rete. Solo se necessario, usare il comando debug ip mpacket sul router. Utilizzare l'argomento detail per visualizzare le intestazioni dei pacchetti nell'output di debug e gli elenchi degli accessi per controllare il traffico proveniente da origini specifiche. Tenere presente che questo comando può avere un grave impatto sulle prestazioni di altri tipi di traffico.

---

## Verifica segnalazione di rete

Si tratta della procedura di risoluzione dei problemi più complessa e importante di qualsiasi rete. Dipende dal protocollo di segnalazione di rete utilizzato, ad esempio PIM modalità sparse, PIM modalità dense e DVMRP. Si consiglia l'approccio in più fasi descritto in questa sezione.

Risoluzione dei problemi relativi alla modalità sparse di PIM

Completare la procedura seguente per risolvere i problemi relativi alla modalità sparse PIM:

1. Verificare che il routing multicast IP sia abilitato su tutti i router multicast.
2. Utilizzare il comando show ip pim neighbors per controllare il timer e la modalità di scadenza per verificare che i router adiacenti PIM siano stati stabiliti correttamente e cercare eventuali problemi di connettività e del timer che potrebbero impedire la definizione di router adiacenti PIM. Se necessario, utilizzare il sottocomando ip pim [version] [dense-mode] [sparse-mode] [sparse-dense-mode] interface level per impostare la modalità e la versione corrette per stabilire correttamente i vicini PIM.
3. Utilizzare il comando show ip pim rp mapping per verificare la corretta mappatura del gruppo RP e per controllare il timer di scadenza se è configurato l'RP automatica. Per risolvere eventuali errori di auto-RP, usare il comando debug ip pim auto-rp. Se non viene visualizzato alcun mapping da gruppo PIM a RP, controllare la configurazione automatica di RP o configurare i mapping statici da gruppo a RP con il comando ip pim indirizzo ip ip indirizzo ip di RP [access-list] [named-accesslist] [override]. La configurazione auto-RP può essere eseguita con i comandi ip pim send-rp-notice interface-id scope valore TTL e ip pim send-rp-discovery interface-id scope valore TTL. Questi comandi devono essere configurati solo se sono presenti configurazioni auto-RP.
4. Utilizzare il comando show ip rpf <indirizzo ip dell'origine> per verificare l'errore RPF per l'indirizzo di origine. La modalità dense PIM e la modalità sparse PIM restituiscono i messaggi Prune all'origine se il traffico arriva su un'interfaccia point-to-point non RPF. Il comando debug ip pim aiuta a identificare le possibili cause di un errore in una rete PIM e confronta l'output tipico con quello visualizzato. Usate questo output per identificare le tre fasi discrete nella modalità sparse PIM: unione, registrazione e switchover SPT. Il comando show ip mroute consente di controllare le voci null negli elenchi dell'interfaccia in uscita e le voci eliminate nella tabella mroute.

Verifica flusso pacchetti di rete

Utilizzare questi comandi per controllare il flusso dei pacchetti multicast nella rete:

- Utilizzare il comando mtrace per controllare la traccia multicast hop-by-hop
- mstat
- ping
- show ip route count
- show ip route active
- debug ip mpacket

Segnalazione ricevitore assegno

Completare questi passaggi per controllare la segnalazione del ricevitore:

1. Usare il comando show ip igmp groups sul primo router upstream collegato al ricevitore per verificare che l'interfaccia sia stata unita al gruppo.
2. Utilizzare il comando ping per verificare la raggiungibilità dell'host e del primo router upstream.
3. Per controllare la versione IGMP dell'interfaccia, usare il comando show ip igmp interface.

> Nota: un router configurato con IGMP versione 1 considera non validi i pacchetti IGMP versione 2 ricevuti dall'host. Questi pacchetti IGMP non si uniscono al gruppo finché il router non riceve un pacchetto IGMP versione 1 dall'host.

4. Usare il comando debug ip igmp per risolvere ulteriormente i problemi di segnalazione del ricevitore.

Verifica flusso pacchetti ricevitore

Completare questa procedura per controllare il flusso del pacchetto del destinatario:

1. Usare il comando netstat su un sistema UNIX per controllare le statistiche dell'interfaccia del ricevitore.
2. Verificare che lo stack TCP/IP sia stato installato e configurato correttamente.
3. Verificare che l'applicazione client di ricezione multicast sia stata installata e configurata correttamente.
4. Controllare la presenza di pacchetti multicast duplicati su un segmento ad accesso multiplo.

# Strumenti Power CLI

I comandi riportati in questa sezione possono essere utili anche per la risoluzione dei problemi, in particolare quando si esegue il test del flusso dei pacchetti di rete e si individuano i punti di errore nella rete multicast.

## mstat

Questo comando visualizza il percorso multicast in formato grafico ASCII. Traccia il percorso tra due punti qualsiasi della rete, mostra le perdite e i duplicati, i TTL e i ritardi in ogni nodo della rete. È molto utile quando si devono individuare punti di congestione nella rete o concentrarsi su un router con conteggi di drop/duplicati elevati. I duplicati vengono indicati nell'output come perdite "negative".

<#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
```

## mrinfo

Questo comando mostra le informazioni sui router adiacenti multicast, le funzionalità e la versione del codice del router, le informazioni sull'interfaccia multicast, le soglie TTL, le metriche, il protocollo e lo stato. È utile quando è necessario verificare i router adiacenti multicast, verificare che esista un'adiacenza bidirezionale e verificare che i tunnel siano attivi in entrambe le direzioni.

<#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]
```

I flag nell'output indicano:

- P = con possibilità di eliminazione
- M = compatibile con mtrace
- S = compatibile con SNMP
- A = compatibile con Auto-RP

## mtrace

Questo comando mostra il percorso multicast tra l'origine e il destinatario e traccia il percorso tra i punti nelle reti, che mostra le soglie TTL e il ritardo su ciascun nodo. Durante la risoluzione dei problemi, utilizzare il comando mtrace per individuare il punto in cui il flusso di traffico multicast si arresta, verificare il percorso del traffico multicast e identificare i percorsi non ottimali.

<#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

Durante la risoluzione dei problemi, il comando ping è il modo più semplice per generare traffico multicast nel lab e testare l'albero multicast, in quanto esegue il ping di tutti i membri del gruppo e tutti i membri rispondono.

<#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
```

# Comandi show

I comandi in questa sezione consentono di raccogliere informazioni utili per la risoluzione di un problema multicast. Per informazioni più dettagliate su questi comandi show, consultare la guida di riferimento dei comandi di Cisco IOS IP Multicast.

---

Suggerimento: se le risposte del comando show sono lente, la causa più probabile è che il router esegua attualmente una ricerca di dominio IP per gli indirizzi IP nel comando show. Per disabilitare la ricerca del dominio IP, è possibile disabilitare la ricerca del dominio IP usando il comando no ip domain-lookup in modalità di configurazione globale del router. In questo modo si interrompe la ricerca del dominio IP e si aumenta la velocità di output del comando show.

---

## show ip igmp groups

Con questo comando vengono visualizzati i gruppi multicast connessi direttamente al router e quelli appresi tramite IGMP (Internet Group Management Protocol). È possibile utilizzare questo comando per verificare che un'origine o un destinatario sia stato effettivamente aggiunto al gruppo target sull'interfaccia del router. La colonna Last Reporter mostra un solo host IGMP, che indica che ha inviato un join IGMP o un report IGMP non richiesto in risposta a una query IGMP dal router PIM per quel particolare gruppo. È necessario visualizzare un solo ultimo reporter per indirizzo di gruppo.

<#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 interface

Utilizzare questo comando per visualizzare informazioni relative al multicast su un'interfaccia e per verificare che IGMP sia abilitato, che la versione in esecuzione sia corretta, che i timer, il valore di soglia TTL (Time To Live) e il router query IGMP siano impostati correttamente. Non è necessario configurare IGMP su un'interfaccia. Per impostazione predefinita, è attivata quando si configura ip pim {dense-mode|sparse-mode|sparse-dense-mode}.

<#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 neighbors

Utilizzare questo comando per elencare i router adiacenti PIM (Protocol Independent Multicast) rilevati dal software Cisco IOS®.

<#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**

I dettagli relativi a ciascun campo sono illustrati di seguito:

- Indirizzo router adiacente: specifica l'indirizzo IP di un router adiacente PIM
- Interfaccia: interfaccia in cui è stato individuato un router adiacente PIM
- Tempo di attività: il tempo di attività totale del sistema adiacente
- Scade: il tempo prima del timeout di un vicino e fino alla ricezione del prossimo saluto PIM
- Ver: versione di PIM sull'interfaccia del router adiacente

- DR Prio: i valori possibili sono 0-4294967294 o "N"

  Si tratta di una nuova colonna che tiene traccia della priorità di un'interfaccia PIM per la scelta di DR. La funzione per configurare un DR in base alla priorità più alta rispetto all'indirizzo IP più alto è stata introdotta nei software Cisco IOS versioni 12.1(2)T e 12.2 e nelle immagini Cisco IOS con Bidir-PIM. È possibile utilizzare il comando ip pim dr-priority <0-4294967294>interface per impostare la priorità del ripristino di emergenza. La priorità di ripristino di emergenza predefinita è impostata su 1. Per garantire l'interoperabilità, se un router adiacente PIM esegue una versione precedente di Cisco IOS che non supporta la funzione di priorità DR, nella colonna "DR Prior" viene visualizzato il valore "N". Se il router adiacente è l'unico router a visualizzare "N" per l'interfaccia, diventa il DR, a prescindere dal router che in realtà ha l'indirizzo IP più alto. Se ci sono diversi vicini PIM con "N" elencato sotto questa colonna, l'interruttore è l'indirizzo IP più alto tra loro.

- Modalità: informazioni su DR e altre funzionalità PIM.

  In questa colonna vengono elencati il DR oltre alle funzionalità supportate dal sistema adiacente PIM:

DR- Il PIM adiacente è un router designato

Funzionalità B- PIM bidirezionale (Bidir-PIM)

S- Aggiornamenti dello stato compatibili (applicabile solo in modalità densa)

Quando si esegue la risoluzione dei problemi, utilizzare questo comando per verificare che tutti i router adiacenti siano attivi e che utilizzino la modalità, la versione e il timer di scadenza appropriati. È inoltre possibile controllare la configurazione del router o utilizzare il comando show ip pim interface per verificare la modalità (modalità PIM sparsa o densa). Utilizzare il comando debug ip pim per osservare lo scambio di messaggi tramite query pim.

## show ip pim interface

Utilizzare questo comando per visualizzare informazioni sulle interfacce configurate per PIM. Inoltre, è possibile utilizzare questo comando per verificare che sull'interfaccia sia configurata la modalità PIM corretta (densa o sparsa), che il numero di router adiacenti sia corretto e che il router designato (DR) sia corretto (condizione critica per la modalità sparsa PIM). I segmenti ad accesso multiplo (come Ethernet, Token Ring, FDDI) selezionano un DR in base all'indirizzo IP più alto. I collegamenti point-to-point non visualizzano le informazioni di DR.

<#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 route summary

Utilizzare questo comando per visualizzare un riepilogo del contenuto della tabella di routing multicast IP. È inoltre possibile utilizzarlo per verificare i gruppi multicast attivi e i mittenti multicast attivi quando si esaminano i timer e i flag.

<#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 route

Utilizzare questo comando per visualizzare il contenuto completo della tabella di routing multicast IP. Quando si esegue la risoluzione dei problemi, utilizzare questo comando per verificare:

- Voci di stato (S,G) e (*,G) dai flag.
- L'interfaccia in ingresso è corretta. In caso contrario, controllare la tabella di routing unicast.
- Le interfacce in uscita sono corrette. In caso di eliminazione non corretta, controllare lo stato nel router a valle.

<#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 route active

Utilizzare questo comando per visualizzare le origini e i gruppi di traffico attivi oltre la soglia. Quando si esegue la risoluzione dei problemi, utilizzarlo per verificare i gruppi di origine attivi, la velocità del traffico per ogni coppia di gruppi di origine (S,G) (è necessario passare alla struttura ad albero del percorso più breve (SPT)) e per controllare se il traffico multicast del gruppo di destinazione è stato ricevuto. Se il traffico non viene ricevuto, cercare il traffico attivo che inizia dalla sorgente verso il destinatario.

```
<#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

Utilizzare questo comando per visualizzare il modo in cui il routing multicast IP esegue il reverse path Forwarding (RPF). Quando si esegue la risoluzione dei problemi, utilizzarla per verificare che le informazioni RPF siano corrette. In caso contrario, verificare l'indirizzo di origine nella tabella di routing unicast. Utilizzare inoltre i comandi ping e trace sull'indirizzo di origine per verificare che il routing unicast funzioni. È possibile utilizzare route DVMRP (Distance Vector Multicast Routing Protocol) o route statiche per correggere eventuali incoerenze unicast-multicast.

```
<#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

Questo comando consente di verificare la cache di commutazione rapida multicast IP e di eseguire il debug dei bug di commutazione rapida.

```
<#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 route count

Utilizzare questo comando per verificare che il traffico multicast sia stato ricevuto e per controllare le relative velocità di flusso e cadute. Se non si riceve traffico, lavorare dalla sorgente al destinatario fino a individuare il punto in cui il traffico si arresta. È inoltre possibile utilizzare questo comando per verificare che il traffico venga inoltrato. In caso contrario, usare il comando show ip route per cercare "Null Outgoing interface list" e gli errori RPF.

<#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

Utilizzare questo comando per controllare la tabella di routing unicast e correggere gli errori RPF nella tabella di routing mroute.

<#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

Utilizzare questo comando per controllare l'assegnazione RP in base all'intervallo di gruppi multicast e per verificare che l'origine dell'apprendimento RP (statico o automatico) e la mappatura siano corrette. Se viene rilevato un errore, controllare la configurazione del router locale o la configurazione di RP automatica.

<#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 (?)**

# Comandi debug

In questa sezione viene illustrato l'aspetto di determinati output del comando debug in una rete funzionante. Quando si esegue la risoluzione dei problemi, è possibile distinguere tra l'output di debug corretto e quello che indica un problema nella rete. Per informazioni più dettagliate su questi comandi di debug, consultare la guida di riferimento dei comandi di debug di Cisco IOS.

## debug ip igmp

Usare il comando debug ip igmp per visualizzare i pacchetti IGMP ricevuti e trasmessi e gli eventi correlati all'host IGMP. La forma no di questo comando disabilita l'output di debug.

Questo output consente di determinare se i processi IGMP funzionano. In generale, se il protocollo IGMP non funziona, il processo del router non rileva mai un altro host sulla rete configurato per ricevere pacchetti multicast. In modalità PIM dense, ciò significa che i pacchetti vengono consegnati in modo intermittente (alcuni ogni tre minuti). In modalità sparse PIM, non vengono mai consegnati.

<#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

L'output precedente mostra che il router invia un'interrogazione IGMP versione 2 all'interfaccia Ethernet 1 all'indirizzo multicast 24.0.0.1 (tutti i sistemi multicast su questa subnet). L'interfaccia Ethernet 1 è un membro del gruppo 24.0.1.40 (è possibile usare il comando show ip igmp interface per verificare questa condizione), che imposta un tempo di ritardo del report di 9,4 secondi (determinato in modo casuale). Poiché non riceve alcun report da un altro sistema per il gruppo multicast 24.0.1.40 per i prossimi 9.4 secondi, invia un report versione 2 della sua appartenenza, che viene ricevuto dal router stesso su Ethernet 1. Riceve inoltre il report IGMP versione 1 dall'host 192.168.9.1, collegato direttamente all'interfaccia Ethernet 1 per il gruppo 239.255.0.1.

Questo output di debug è utile quando si verifica che l'interfaccia del router invii delle query e si determina l'intervallo di query (nel caso precedente, 60 secondi). È inoltre possibile utilizzare il comando per determinare la versione di IGMP utilizzata dai client.

## debug ip mpacket

Usare il comando debug ip mpacket per visualizzare tutti i pacchetti multicast IP ricevuti e trasmessi. La forma no di questo comando disabilita l'output di debug.

```
<#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
```

Questo comando decodifica il pacchetto multicast e visualizza se il pacchetto viene inoltrato (mforward) o scartato. Quando si esegue il debug dei problemi di flusso dei pacchetti nella rete, è utile esaminare il valore TTL e il motivo per cui un pacchetto è stato scartato.

---

⚠ Attenzione: prestare attenzione quando si attiva l'output di debug a livello di pacchetto, in particolare quando il pacchetto multicast elevato dei servizi router viene caricato.

---

## debug ip mrouting

Questo comando è utile per la manutenzione delle tabelle di routing. Utilizzarlo per verificare che il percorso alternativo (S,G) sia installato nella tabella di routing distribuito. In caso contrario, verificarne il motivo. Le informazioni chiave in questo output sono l'interfaccia RPF. In caso di errore del controllo RPF, l'installazione del mroute (S,G) nella tabella di mrouting non riesce.

```
<#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

Usare il comando debug ip pim per visualizzare i pacchetti PIM ricevuti e trasmessi e gli eventi correlati a PIM. La forma no di questo comando disabilita l'output di debug.

In questa sezione viene illustrato un esempio per comprendere l'output del comando debug della modalità sparse PIM e mostrare un output di debug tipico.

Di seguito è riportato l'output del comando debug ip pim su R1:

<#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
```

Di seguito è riportato il significato di ogni riga di output: R1 e R2 stabiliscono i vicini PIM quando vengono scambiati i messaggi Hello. Questi messaggi Hello periodici, scambiati in secondi di intervallo query tra R1 (E0) e R2 (E0), tengono traccia dei vicini PIM.

R1 invia un messaggio Join/Prune all'indirizzo RP 192.168.7.2. L'RP (R2) risponde con un messaggio Ricevuto RP raggiungibile a R1 per il gruppo 239.255.0.1. In questo modo viene aggiornato il timer di scadenza RP in R1. Il timer di scadenza imposta un checkpoint per garantire che l'RP esista ancora; in caso contrario, è necessario individuare un nuovo RP. Utilizzare il comando show ip pim rp per osservare l'ora di scadenza dell'RP.

A questo punto, esaminare l'output del comando debug tra R1 e R2 quando un ricevitore multicast per il gruppo 239.255.0.1 si unisce a R1.

Osservare innanzitutto l'output in R1:

<#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)

Osservare ora l'output in R2:

<#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
```

Nella riga 1 precedente, il ricevitore multicast per il gruppo 239.255.0.1 si unisce a R1. Verrà installata una voce (*, 239.255.0.1) nella tabella route. Quindi, nella riga 2, il ricevitore multicast invia un join IGMP a R2 (RP) per unirsi alla struttura condivisa.

Quando il join IGMP arriva su R2, R2 installa una route (*, 239.255.0.1), come mostrato nelle righe da 12 a 15 dell'output R2.

Una volta installato (*, 239.255.0.1) nella tabella di routing, R2 aggiunge l'interfaccia dalla quale ha

ricevuto il messaggio Join/Prune all'elenco di interfacce in uscita (OIL) nello stato forward. Quindi invia un messaggio RP-reachability sull'interfaccia su cui ha ricevuto il messaggio Join/Prune. Questa operazione è indicata alle righe da 15 a 21 della produzione R2.

R1 riceve il messaggio RP-reachable per il gruppo 239.255.0.1 e aggiorna il proprio timer di scadenza per RP. Per impostazione predefinita, questo scambio si ripete una volta al minuto e aggiorna lo stato di inoltro multicast, come mostrato nelle righe 7 e 8 dell'output R1.

Nelle righe successive, viene visualizzato l'output del comando debug tra R2 (RP) e R3. L'origine (collegata direttamente a R3) ha iniziato a inviare i pacchetti per il gruppo 239.255.0.1.

Osservate innanzitutto l'output in R3:

<#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)

Di seguito è riportato l'output di R2, l'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
```

La linea 1 mostra che R3, che è collegato direttamente all'origine tramite Ethernet0/0, riceve il traffico multicast per il gruppo 239.255.0.1. Crea una voce (* , 239.255.0.1) e invia un messaggio di join all'RP.

Le righe 16 e 17 mostrano che R2, che è l'RP, riceve anche il messaggio Join/Prune e invia le informazioni sulla raggiungibilità RP a R3.

Nelle righe 5 e 6, R3 aggiorna il proprio timer di scadenza RP dopo aver ricevuto le informazioni raggiungibili RP. Le righe 7 e 8 precedenti mostrano che R3 utilizza la voce (*,G) per inviare i dati al protocollo RP incapsulato in un pacchetto Register con l'origine che avvia la trasmissione al gruppo 239.255.0.1.

Le righe da 18 a 20 mostrano che R2 ha ricevuto il pacchetto Register, lo ha decapsulato e inoltrato verso la struttura con una voce preesistente (*, 239.255.0.1) nella tabella di routing.

Le righe 21 e 29 mostrano che R2 invia un messaggio di join verso R3 e installa una voce (S,G) (192.168.33.32, 239.255.0.1) nella tabella di route.

Le righe da 9 a 11 mostrano che R3 riceve il messaggio Join da R2, installa una voce (S,G) (192.168.33.32,239.255.0.1) nella tabella mroute e mette l'interfaccia collegata a RP in modalità forward, che costruisce l'albero SPT multicast (S,G) verso la sorgente.

Alla riga 23, R2 inizia a ricevere (S,G) il traffico verso il basso SPT e invia un messaggio Register-Stop (e un messaggio Join) verso l'origine.

Le righe da 12 a 15 mostrano che R3 riceve il messaggio Register-Stop, cancella il flag di registro e arresta il traffico (S,G) dell'incapsulamento.

I messaggi di unione/eliminazione periodici vengono scambiati tra l'RP e l'R3 per mantenere la struttura multicast.

## Informazioni correlate

- Guida alla risoluzione dei problemi del multicast IP
- Guida rapida alla configurazione del multicast
- Pagina di supporto per il multicast IP
- Pagina di supporto per il routing IP

- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).