Consultare la guida alla configurazione iniziale rapida del multicast IP

Sommario

Introduzione

Prerequisiti

- Requisiti
- Componenti usati
- Convenzioni

Premesse

Modalità Dense

Modalità sparse con un RP

Modalità sparse con più RP

Auto-RP con un RP

Auto-RP con più RP

DVMRP

MBGP

MSDP

Stub Multicast Routing

IGMP UDLR per collegamenti satellitari

PIMv2 BSR

CGMP

Snooping IGMP

PGM

MRM

Risoluzione dei problemi

Informazioni correlate

Introduzione

Questo documento descrive le nozioni di base su come configurare il multicast per vari scenari di rete.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di questo argomento:

- Multicast IP (Internet Protocol).

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.

Premesse

Il multicasting IP è una tecnologia che riduce il traffico e consente di distribuire un singolo flusso di informazioni a migliaia di destinatari e abitazioni aziendali.

Le applicazioni che sfruttano il multicast includono videoconferenze, comunicazioni aziendali, formazione a distanza e distribuzione di software, quotazioni di borsa e notizie.

Modalità Dense

Cisco consiglia di utilizzare la modalità sparse PIM (Protocol Independent Multicast), in particolare Auto-RP, dove possibile e soprattutto per nuove distribuzioni.

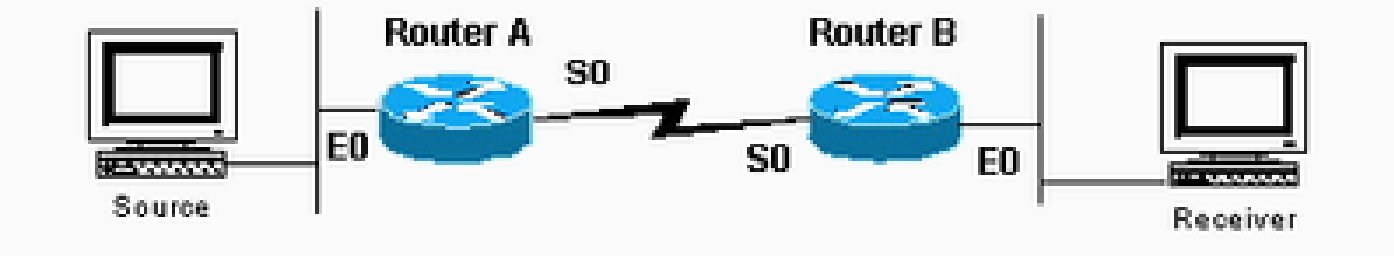
Tuttavia, se si desidera la modalità densa, configurare il comando globale ip multicast-routing e il comando di interfaccia ip pim sparse-dense-mode su ciascuna interfaccia che deve elaborare il traffico multicast.

In tutte le configurazioni descritte in questo documento, il requisito comune è configurare il multicasting a livello globale e configurare il protocollo PIM sulle interfacce.

A partire dal software Cisco IOS® versione 11.1, è possibile configurare i comandi di interfaccia ip pim dense-mode e ip pim sparse-mode contemporaneamente al comando ip pim sparse-dense-mode.

In questa modalità, l'interfaccia viene considerata in modalità dense se se il gruppo è in modalità dense. Se il gruppo è in modalità sparse (ad esempio, se è noto un RP), l'interfaccia viene trattata come modalità sparse.

Nota: La "Sorgente" negli esempi di questo documento rappresenta l'origine del traffico multicast, mentre il "Ricevitore" rappresenta il destinatario del traffico multicast.



Interfaccia trattata come modalità Dense se Group è in modalità Dense

Configurazione 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`

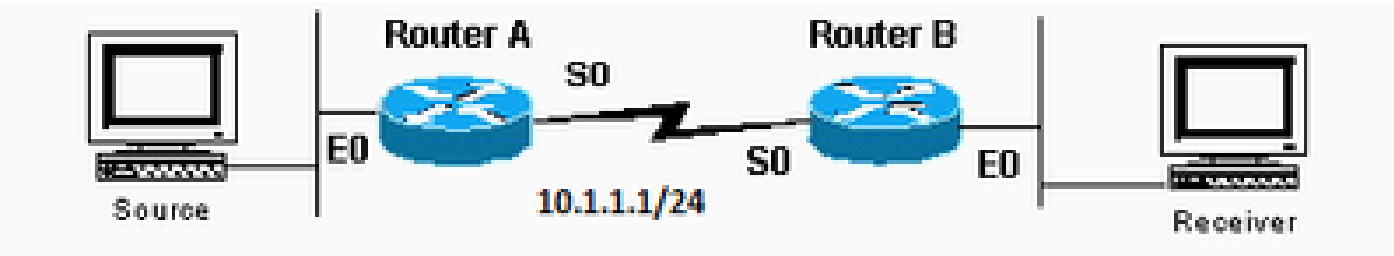
Configurazione router B

`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`

Modalità sparse con un RP

Nell'esempio, il router A è l'RP, in genere il router più vicino all'origine. La configurazione RP statica richiede che per tutti i router del dominio PIM siano configurati i comandi samei p pim rp-address.

È possibile configurare più RP, ma può esistere un solo RP per gruppo specifico.



Possono esistere più RP, ma solo un RP per gruppo specifico

Configurazione 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`

Configurazione router B

`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`

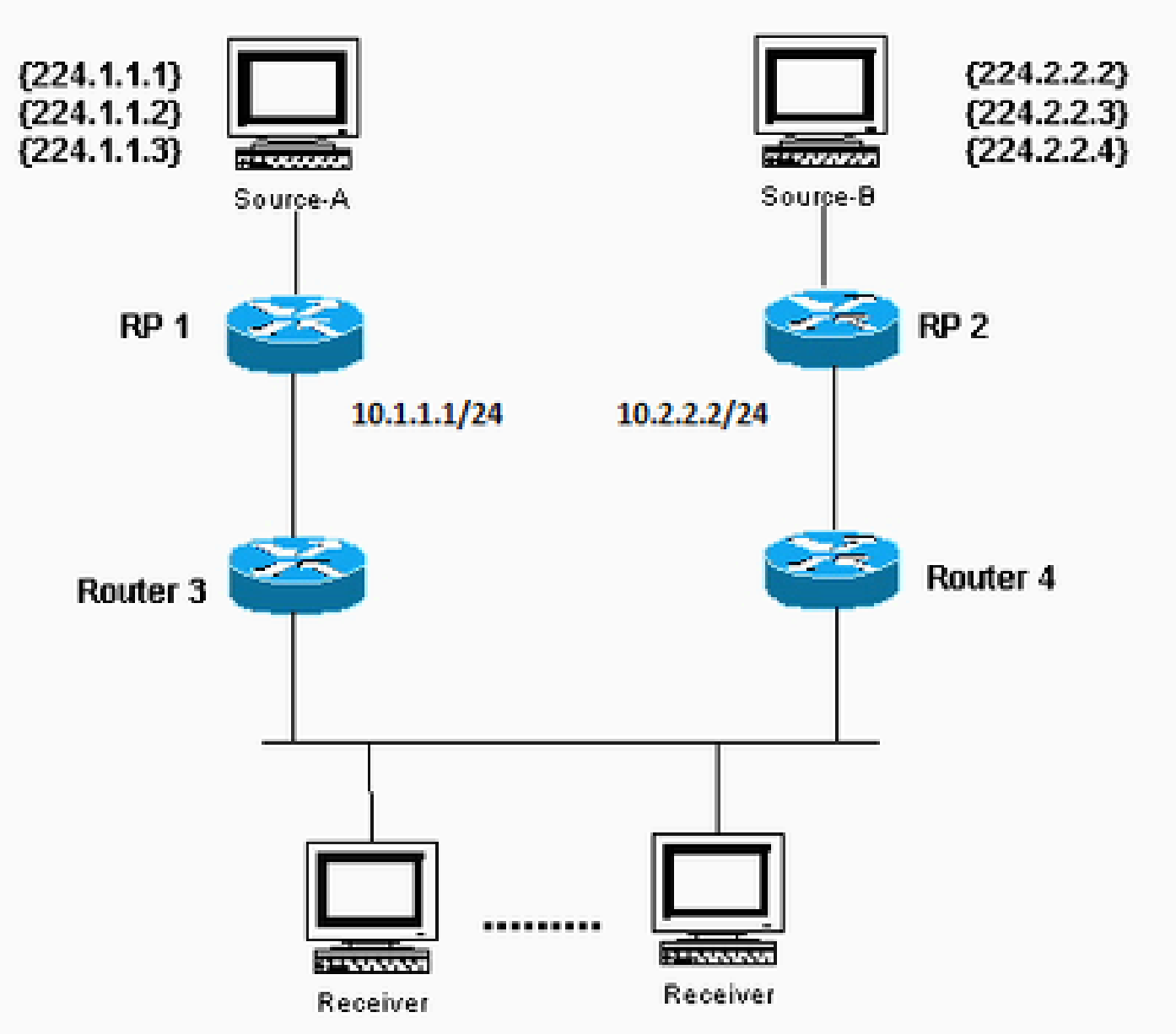
Modalità sparse con più RP

Nell'esempio, l'origine A invia a 224.1.1.1, 224.1.1.2 e 224.1.1.3. L'origine B invia a 224.2.2.2, 224.2.2.3 e 224.2.2.4. È possibile avere un router, RP 1 o RP 2, che sia l'RP per tutti i gruppi.

Tuttavia, se si desidera che RP diversi gestiscano gruppi diversi, è necessario configurare tutti i router in modo che includano i gruppi che gli RP possono servire.

Per questo tipo di configurazione RP statica è necessario che tutti i router del dominio PIM dispongano dello stesso comando acl indirizzo ip pim configurato.

È inoltre possibile utilizzare Auto-RP per ottenere la stessa impostazione, che è più facile da configurare.



La sorgente A invia i dati ai punti 224.1.1.1, 224.1.1.2 e 224.1.1.3; La sorgente B invia a 224.2.2.2, 224.2.2.3 e 224.2.2.4.

Configurazione 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`

Configurazione RP 2

```
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
```

Configurazione per i router 3 e 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 con un RP

L'Auto-RP richiede la configurazione degli RP per annunciarne la disponibilità come RP e agenti di mapping. Le RP utilizzano 224.0.1.39 per inviare i loro annunci.

L'agente di mapping RP resta in ascolto dei pacchetti annunciati dagli RP, quindi invia i mapping RP-a-gruppo in un messaggio di individuazione inviato a 24.0.1.40.

Questi messaggi di individuazione vengono utilizzati dai router residui per la mappa da RP a gruppo.

È possibile utilizzare un RP che funga anche da agente di mapping oppure configurare più RP e più agenti di mapping a scopo di ridondanza.

Si noti che, quando si sceglie un'interfaccia dalla quale originare gli annunci RP, Cisco consiglia di utilizzare un'interfaccia quale un loopback anziché un'interfaccia fisica.

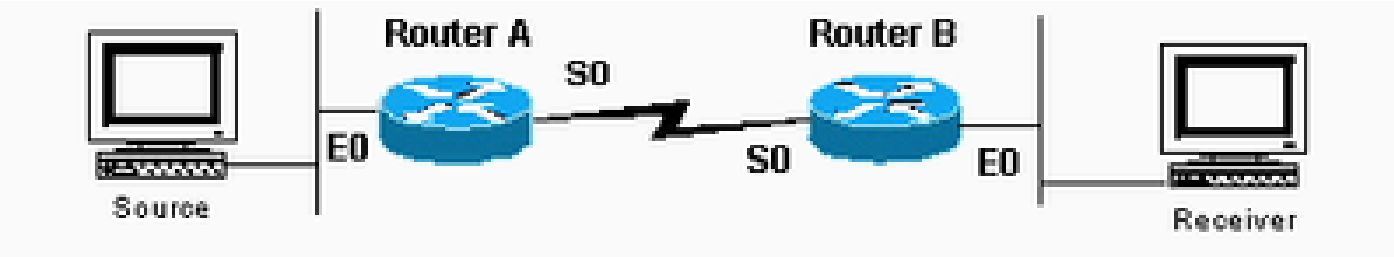
Inoltre, è possibile utilizzare interfacce VLAN commutate (SVI). Se si usa un'interfaccia VLAN per annunciare l'indirizzo RP, l'opzione interface-type nel comando ip pim [vrf vrf-name] send-rp-notice {interface-type-number | ip-address} il comando ttl-value dell'ambito deve contenere l'interfaccia VLAN e il numero VLAN. Ad esempio, il comando ha il formato ip pim send-rp-noticeVlan500 scope 100 .

Se si sceglie un'interfaccia fisica, è necessario che l'interfaccia sia sempre attiva. Ciò non accade

sempre e il router smette di pubblicizzarsi come RP una volta che l'interfaccia fisica si interrompe.

Con un'interfaccia di loopback, è sempre attivo e non si abbassa mai, il che assicura che l'RP continui a farsi pubblicità attraverso qualsiasi interfaccia disponibile come un RP.

Ciò avviene anche se si verifica un errore in una o più interfacce fisiche. L'interfaccia di loopback deve essere abilitata per PIM e pubblicizzata da un IGP (Interior Gateway Protocol) oppure deve essere raggiungibile con il routing statico.



L'interfaccia di loopback deve essere abilitata per PIM e annunciata da un protocollo gateway interno o raggiungibile con routing statico

Configurazione router A

```
ip multicast-routing

ip pim send-rp-annouce 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
```

Configurazione router B

```
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 con più RP

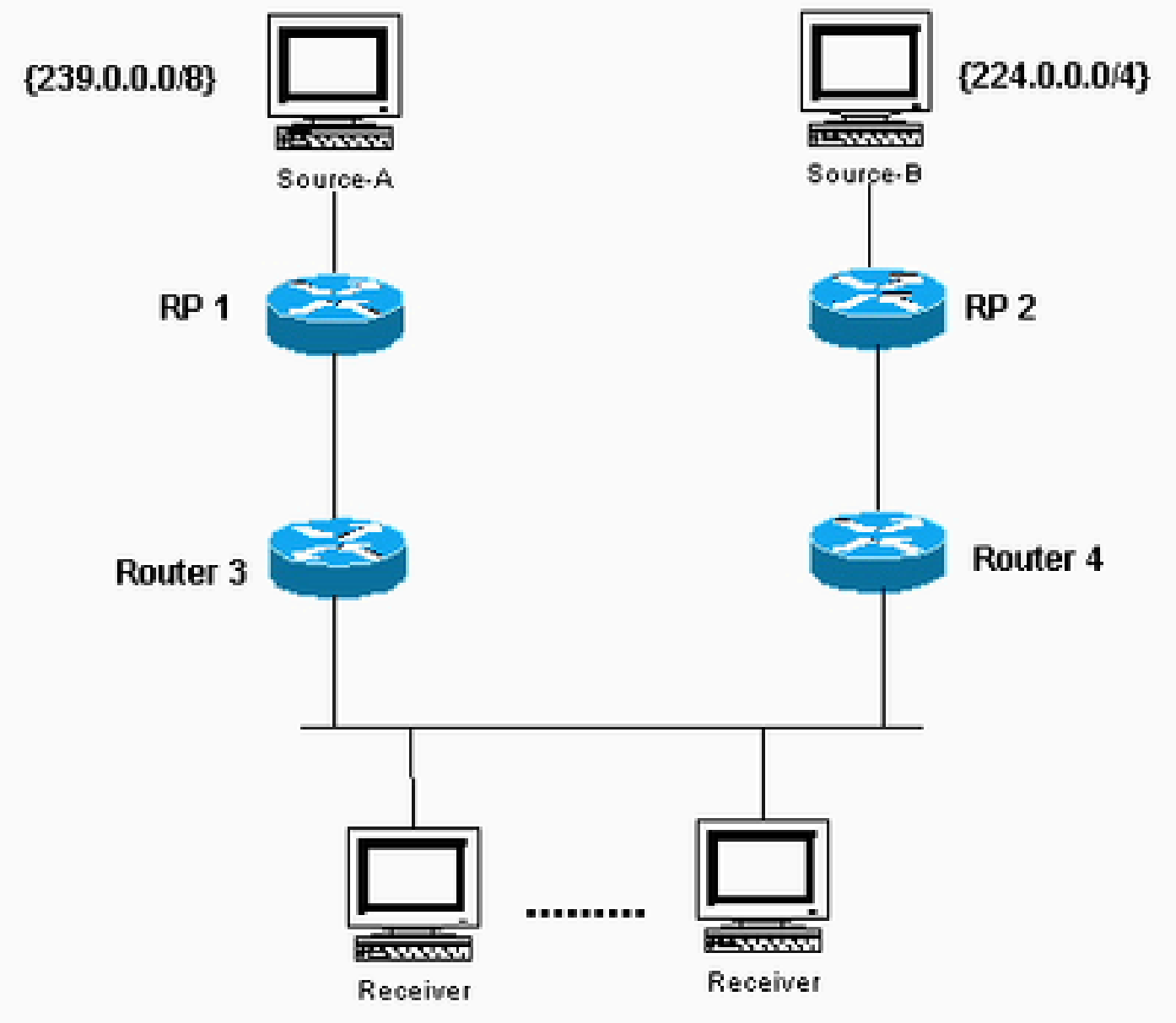
Gli elenchi degli accessi di questo esempio consentono di utilizzare gli RP solo per i gruppi desiderati. Se non è configurato alcun elenco degli accessi, gli RP sono disponibili come RP per tutti i gruppi.

Se due RP dichiarano di essere RP per lo stesso gruppo, gli agenti di mapping risolvono questi conflitti con la regola "l'indirizzo IP più alto prevale".

Quando due RP sono annunciati per quel gruppo, è possibile configurare ciascun router con un indirizzo di loopback in modo da influenzare quale router sia l'RP per un particolare gruppo.

Posizionare l'indirizzo IP più alto sull'RP preferito, quindi utilizzare l'interfaccia di loopback come origine dei pacchetti di annuncio; ad esempio, ip pim send-RP-indeceloopback0 .

Quando si utilizzano più agenti di mapping, ciascuno annuncia lo stesso gruppo ai mapping RP al gruppo di rilevamento 224.0.1.40.



Inserire l'indirizzo IP superiore nell'RP preferita

Configurazione 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`

Configurazione RP 2
`ip multicast-routing`

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

access-list 1 deny 239.0.0.0 0.255.255.255
access-list 1 permit 224.0.0.0 10.255.255.255
```

DVMRP

Il provider di servizi Internet (ISP) potrebbe suggerire di creare un tunnel DVMRP (Distance Vector Multicast Routing Protocol) per l'ISP in modo da ottenere l'accesso alla backbone multicast in Internet (mbone).

Di seguito sono riportati i comandi minimi per configurare un tunnel DVMRP:

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

In genere, l'ISP consente di eseguire il tunnel su un computer UNIX che esegue "mrouted" (DVMRP). Se invece l'ISP dispone del tunnel a un altro dispositivo Cisco, utilizzare la modalità predefinita del tunnel GRE.

Se si desidera generare pacchetti multicast per gli altri utenti sulla barra multifunzione da visualizzare invece di ricevere pacchetti multicast, è necessario annunciare le subnet di origine.

Se l'indirizzo host di origine multicast è 172.16.108.1, è necessario annunciare l'esistenza di tale subnet al mbone. Per impostazione predefinita, le reti con connessione diretta vengono pubblicizzate con la metrica 1.

Se l'origine non è collegata direttamente al router con il tunnel DVMRP, configurarlo in interface tunnel0:

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

Nota: Con questo comando è necessario includere un elenco degli accessi per evitare che l'intera tabella di routing Unicast venga annunciata al mbone.

Se l'impostazione è simile a quella mostrata qui e si desidera propagare le route DVMRP attraverso il dominio, configurare il comando ip dvmrp unicast-routing sulle interfacce serial0 dei router A e B.

Questa azione consente di inoltrare route DVMRP ai router adiacenti PIM che dispongono di una tabella di routing DVMRP utilizzata per l'inoltro di percorsi inverso (RPF, Reverse Path Forwarding).

Le route apprese da DVMRP hanno la precedenza su tutti gli altri protocolli, ad eccezione delle route con connessione diretta.

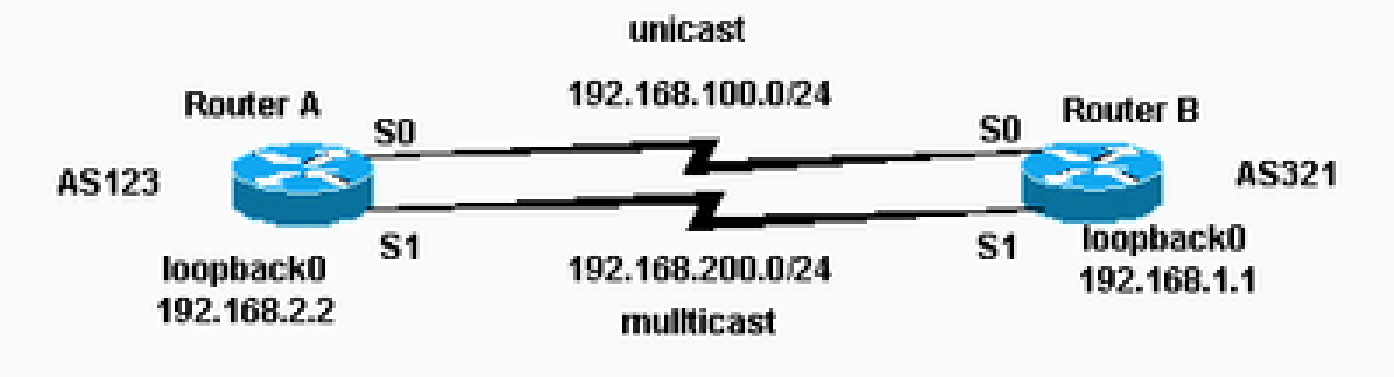
Propaga route DVMRP tramite il dominio

MBGP

Il protocollo MBGP (Multiprotocol Border Gateway Protocol) è un metodo di base per trasportare due set di route: una per il routing unicast e una per il routing multicast.

Il protocollo MBGP fornisce il controllo necessario per decidere dove consentire il flusso dei pacchetti multicast. PIM utilizza le route associate al routing multicast per creare strutture di distribuzione dei dati.

MBGP fornisce il percorso RPF, non la creazione dello stato multicast. PIM è ancora necessario per inoltrare i pacchetti multicast.



PIM è ancora necessario per inoltrare i pacchetti multicast

Configurazione 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
```

Configurazione router B

```
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
```

Se le topologie unicast e multicast sono congruenti (ad esempio, utilizzano lo stesso collegamento), la differenza principale nella configurazione è rappresentata dal comando multicast nlri.

Di seguito è riportato un esempio:

```
network 192.168.100.0 nlri unicast multicast
```

Le topologie congruenti con MBGP offrono un vantaggio: anche se il traffico attraversa gli stessi percorsi, è possibile applicare policy diverse a BGP unicast e BGP multicast.

MSDP

Il protocollo MSDP (Multicast Source Discovery Protocol) connette più domini PIM-SM.

Ogni dominio PIM-SM utilizza i propri RP indipendenti e non deve dipendere da RP in altri domini.

MSDP consente ai domini di individuare origini multicast da altri domini. Se si utilizza anche il peer BGP con il peer MSDP, è necessario utilizzare lo stesso indirizzo IP per MSDP e per BGP.

Quando MSDP esegue i controlli RPF peer, prevede che l'indirizzo peer MSDP corrisponda a quello fornito da BGP/MBGP quando esegue una ricerca della tabella di route sull'RP nel messaggio SA.

Tuttavia, non è necessario eseguire BGP/MBGP con il peer MSDP se tra i peer MSDP è presente un percorso BGP/MBGP.

Se non è presente alcun percorso BGP/MBGP e sono presenti più peer MSDP, è necessario utilizzare il comando ip msdp default-peer.

L'esempio mostra che RP A è l'RP per il proprio dominio e RP B è l'RP per il proprio dominio.

Protocollo MSDP (Multicast Source Discovery Protocol) per la connessione di più domini PIM-SM

Configurazione router A

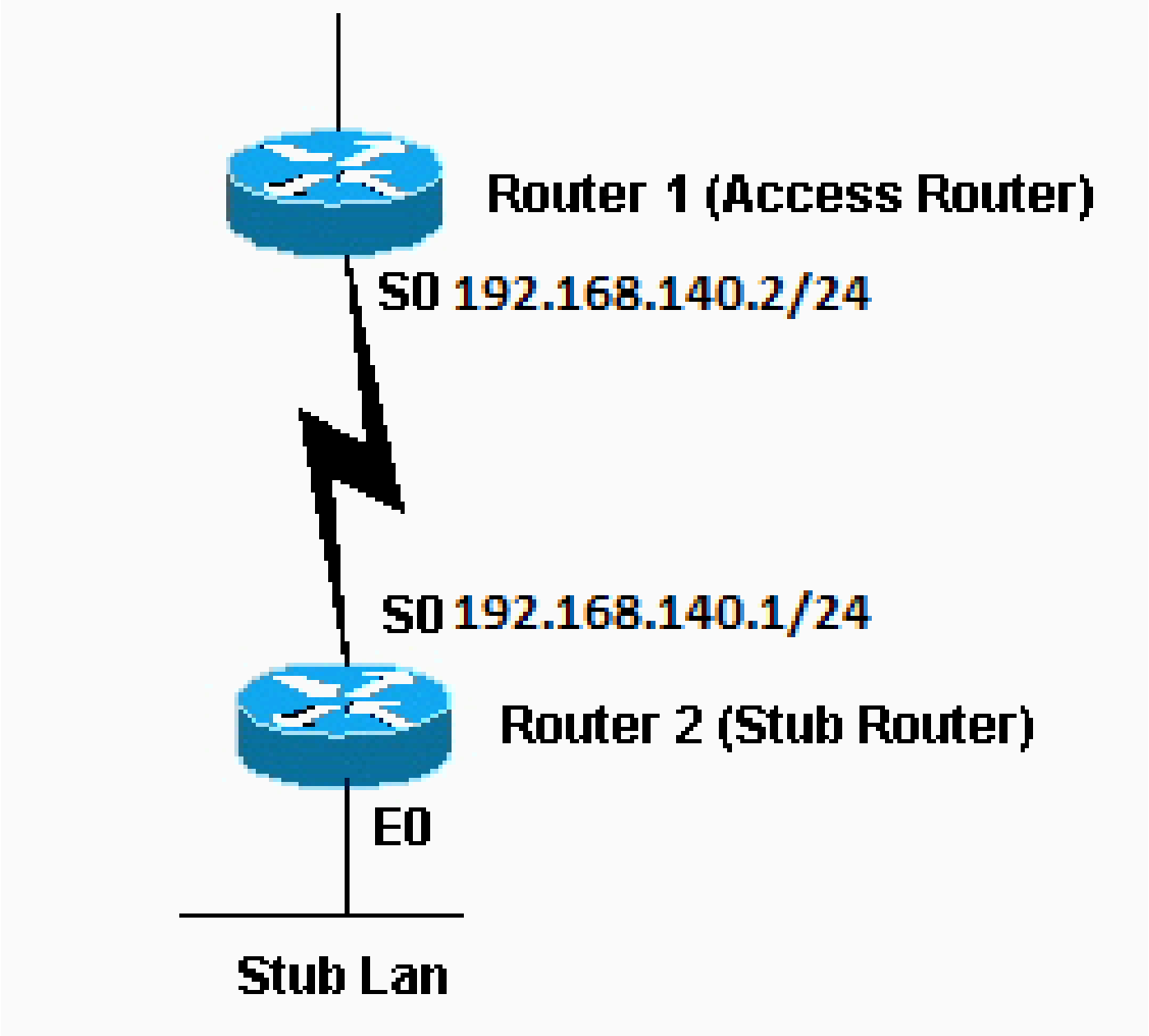
`ip multicast-routing`
 	
`ip pim send-RP-announce loopback0 scope 16 group-list 1`
`ip pim send-RP-discovery scope 16`
 	
`ip msdp peer 192.168.100.2`
`ip msdp sa-request 192.168.100.2`
 	
`interface loopback0`
`ip address <address> <mask>`
`ip pim sparse-dense-mode`
 	
`interface serial0`
`ip address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

Configurazione router B

`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 192.168.100.2 255.255.255.0`
`ip pim sparse-dense-mode`

Stub Multicast Routing

Stub multicast routing consente di configurare router remoti/stub come agenti proxy IGMP. Anziché partecipare completamente al PIM, questi router di stub inoltrano i messaggi IGMP dagli host al router multicast upstream.



I router di stub inoltrano i messaggi IGMP dagli host al router multicast upstream

Configurazione router 1

`int s0`
`ip pim sparse-dense-mode`
`ip pim neighbor-filter 1`
 	
`access-list 1 deny 192.168.140.1`

Il comando ip pim neighbors-filter è necessario per impedire al router 1 di riconoscere il router 2 come router adiacente PIM.

Se si configura il router 1 in modalità sparse, non è necessario utilizzare il filtro adiacente. Il router 2 non deve essere eseguito in modalità sparse.

In modalità densa, le sorgenti multicast di stub possono raggiungere i router della backbone.

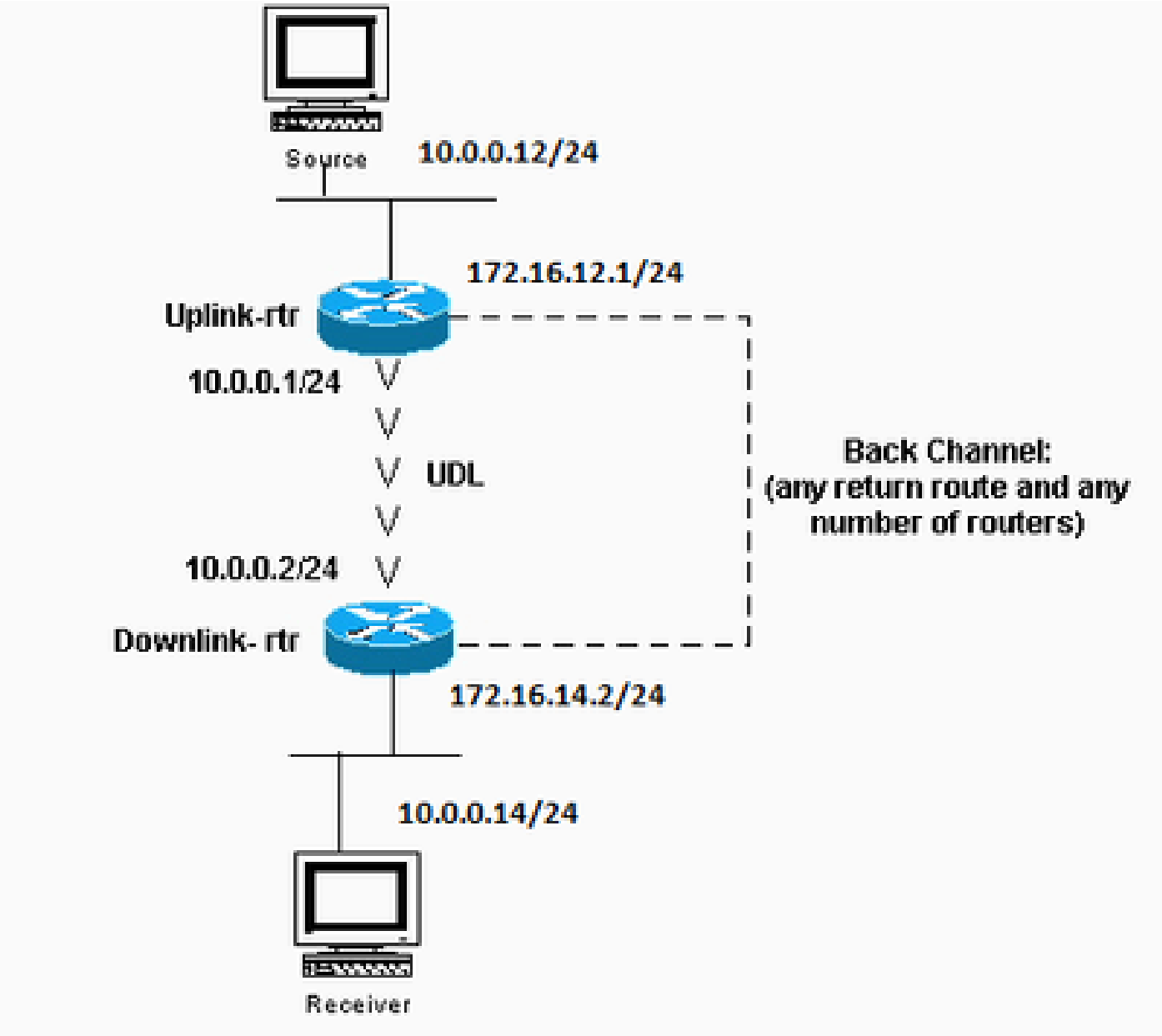
Configurazione router 2

`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 per collegamenti satellitari

UDLR (Unidirectional Link Routing) fornisce un metodo per l'inoltro di pacchetti multicast su un collegamento satellitare unidirezionale a reti stub con canale posteriore.

Questa procedura è simile al routing multicast di stub. Senza questa funzione, il router di uplink non è in grado di individuare dinamicamente gli indirizzi di gruppi multicast IP da inoltrare tramite il collegamento unidirezionale, in quanto il router di downlink non è in grado di inviare dati al mittente.



UDLR (Unidirectional Link Routing) Fornisce un metodo per l'inoltro di pacchetti multicast

Configurazione uplink-rtr

`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
```

Configurazione Downlink-Rtr

```
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

Se tutti i router della rete eseguono PIMv2, è possibile configurare un BSR anziché l'Auto-RP. BSR e Auto-RP sono molto simili.

Per una configurazione BSR è necessario configurare i candidati BSR (in modo analogo all'annuncio RP in Auto-RP) e i BSR (in modo analogo agli agenti di mapping Auto-RP). Per configurare un modulo BSR, attenersi alla seguente procedura:

1. Nei BSR candidati configurare:

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

   Dove interface contiene l'indirizzo IP dei BSR candidati. È consigliabile (ma non obbligatorio) che l'hash-mask-Len sia identico in tutti i BSR candidati. Un BSR candidato con il valore pref più grande viene scelto come BSR per questo dominio.

Di seguito è riportato un esempio di utilizzo del comando:

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

Il BSR PIMv2 raccoglie le informazioni RP candidate e diffonde le informazioni RP-set associate a ciascun prefisso di gruppo. Per evitare singoli punti di errore, è possibile configurare più router di un dominio come BSR candidati.

Tra i BSR candidati viene automaticamente selezionato un BSR in base ai valori delle preferenze configurati. Per poter fungere da BSR candidati, i router devono essere connessi e trovarsi nella backbone della rete anziché nell'area di connessione remota della rete.

2. Configurare i router RP candidati. L'esempio mostra un RP candidato, sull'interfaccia ethernet0, per l'intero intervallo di indirizzi dell'ambito di amministrazione:

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

CGMP

Per configurare il protocollo CGMP (Group Management Protocol), configurarlo sull'interfaccia del router rivolta allo switch:

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

Quindi, configurare questo sullo switch:

```
set cgmp enable
```

Snooping IGMP

Lo snooping IGMP (Internet Group Management Protocol) è disponibile nella versione 4.1 di Catalyst 5000. Lo snooping IGMP richiede una scheda Supervisor III.

Per configurare lo snooping IGMP sul router, non è necessaria alcuna configurazione diversa da PIM. È ancora necessario un router con snooping IGMP per fornire l'interrogazione IGMP.

L'esempio fornito qui mostra come abilitare lo snooping IGMP sullo switch:

<#root>

```
Console> (enable)

set igmp enable


IGMP Snooping is enabled.
CGMP is disabled.
```

Se si tenta di abilitare il protocollo IGMP ma il protocollo CGMP è già abilitato, viene visualizzato quanto segue:

<#root>

```
Console> (enable)

set igmp enable


Disable CGMP to enable IGMP Snooping feature.
```

PGM

Pragmatic General Multicast (PGM) è un protocollo di trasporto multicast affidabile per applicazioni che richiedono la consegna di dati multicast ordinati, privi di duplicati, da più origini a più ricevitori.

PGM garantisce che il destinatario del gruppo riceva tutti i pacchetti di dati dalle trasmissioni e dalle ritrasmissioni o sia in grado di rilevare la perdita irreversibile dei pacchetti di dati.

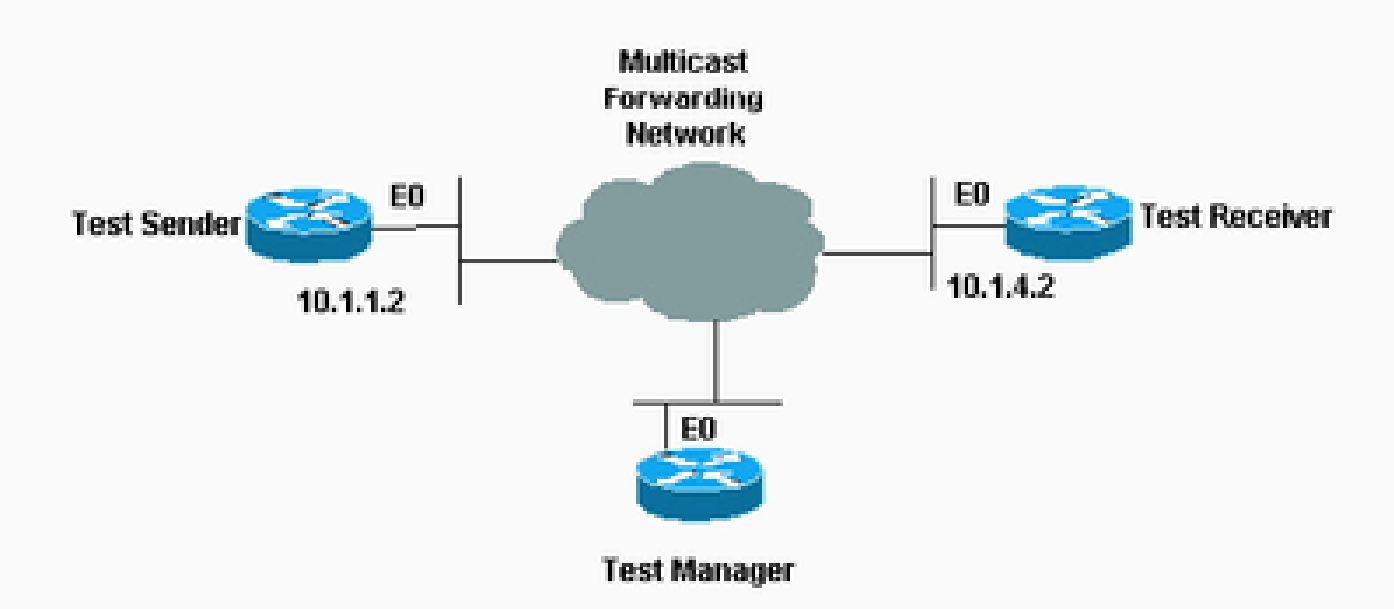
Nessun comando globale PGM. Il protocollo PGM viene configurato per ciascuna interfaccia con il comando ip pgm. È necessario abilitare il routing multicast sul router con PIM sull'interfaccia.

MRM

Multicast Routing Monitor (MRM) semplifica il rilevamento automatico degli errori in un'infrastruttura di routing multicast di grandi dimensioni. MRM è progettato per avvisare un amministratore di rete di problemi di routing multicast quasi in tempo reale.

MRM è costituito da due componenti: tester MRM e manager MRM. Il tester MRM è un mittente o un destinatario.

MRM è disponibile a partire da Cisco IOS versione 12.0(5)T. Solo i tester e i manager MRM devono eseguire la versione Cisco IOS supportata da MRM.



Multicast Routing Monitor (MRM) Facilita il rilevamento automatico degli errori in una grande infrastruttura di routing multicast

Test configurazione mittente
`interface Ethernet0` `  ip mrm test-sender`

Test configurazione ricevitore
`interface Ethernet0` `  ip mrm test-receiver`

Configurazione di Gestione test

`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`

Di seguito è riportato l'output del comando show ip mrm manager su Test Manager:

<#root>

```
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 p
```

Avviare il test con il comando indicato di seguito. Il gestore test invia messaggi di controllo al mittente e al destinatario del test come configurato nei parametri del test.

Il ricevitore di prova si unisce al gruppo e controlla i pacchetti di prova inviati dal mittente di prova.

<#root>

```
Test_Manager#
```

mrm start test1

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

Per visualizzare un report sullo stato per il gestore test, immettere questo comando:

<#root>

```
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#
```

L'output mostra che il destinatario ha inviato due rapporti di stato (una riga per ogni) a un determinato timestamp. Ogni report contiene una perdita di pacchetti durante la finestra dell'intervallo (valore predefinito: un secondo).

Il valore "Ehsr" mostra il valore stimato del numero di sequenza successivo del mittente del test. Se il ricevitore di prova rileva dei pacchetti duplicati, indica un numero negativo nella colonna "Pkt Loss/Dup".

Per interrompere il test, immettere questo comando:

<#root>

```
Test_Manager#
```

mrm stop test1

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

Durante l'esecuzione del test, il mittente MRM invia i pacchetti RTP all'indirizzo di gruppo configurato all'intervallo predefinito di 200 ms.

Il ricevitore controlla (prevede) gli stessi pacchetti allo stesso intervallo predefinito.

Se il destinatario rileva una perdita di pacchetto nell'intervallo di tempo predefinito di cinque secondi, invia un rapporto al manager MRM.

Per visualizzare il rapporto sullo stato inviato dal ricevitore, usare il comando show ip mrm status sul manager.

Risoluzione dei problemi

Alcuni dei problemi più comuni che si verificano quando si implementa il multicast IP in una rete sono quando il router non inoltra il traffico multicast a causa di un errore RPF o di impostazioni TTL.

Per una descrizione dettagliata di questi e altri problemi, sintomi e soluzioni comuni, consultare la guida alla risoluzione dei problemi del multicast IP.

Informazioni correlate

- Guida alla risoluzione dei problemi del multicast IP
- Risoluzione dei problemi relativi alle reti multicast con gli strumenti CLI
- Supporto IP multicast
- 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).