Multicast in una rete campus: Snooping CGMP e IGMP

Sommario

Introduzione

Lo snooping CGMP (Cisco Group Management Protocol) e IGMP (Internet Group Management Protocol) ha lo scopo di limitare il traffico multicast in una rete a commutazione. Per impostazione

predefinita, uno switch LAN propaga il traffico multicast all'interno del dominio di trasmissione, e ciò può richiedere una notevole quantità di larghezza di banda se molti server multicast inviano flussi al segmento.

Operazioni preliminari

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Prerequisiti

Non sono previsti prerequisiti specifici per questo documento.

Componenti usati

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

Premesse

Il traffico multicast viene inondato perché uno switch in genere apprende gli indirizzi MAC cercando nel campo dell'indirizzo di origine di tutti i frame che riceve. Un indirizzo MAC multicast non viene mai utilizzato come indirizzo di origine per un pacchetto. Questi indirizzi non vengono visualizzati nella tabella degli indirizzi MAC e lo switch non dispone di un metodo per impararli.

La prima soluzione a questo problema è configurare indirizzi MAC statici per ogni gruppo e ogni client. Questa soluzione, tuttavia, non è né scalabile né dinamica. Per utilizzare questa soluzione su uno switch Catalyst 4000, 5000 o 6000, usare uno dei seguenti comandi:

- **set cam static**
- **set cam permanent**

Questi due comandi hanno lo stesso effetto, ad eccezione del fatto che le voci statiche scompaiono al riavvio e le voci permanenti no.

La seconda soluzione è usare CGMP, un protocollo proprietario di Cisco in esecuzione tra il router multicast e lo switch. CGMP consente al router multicast Cisco di comprendere i messaggi IGMP inviati dagli host e informa lo switch delle informazioni contenute nel pacchetto IGMP.

L'ultima (e la più efficiente) soluzione è lo snooping IGMP. Con lo snooping IGMP, lo switch intercetta i messaggi IGMP dall'host stesso e aggiorna la relativa tabella MAC di conseguenza. Per il supporto dello snooping IGMP è necessario hardware avanzato.

Le configurazioni CGMP riportate in questo documento sono valide per gli switch Catalyst 4000 e 5000 con software CatOS (il protocollo CGMP non è supportato sugli switch Catalyst 6000), mentre le configurazioni dello snooping IGMP sono valide per gli switch Catalyst 5000 e 6000 con software CatOS.

La sezione seguente descrive brevemente un indirizzo multicast, illustra le funzionalità di IGMP e fornisce ulteriori dettagli sullo snooping CGMP e IGMP.

Indirizzo multicast

1. Gli indirizzi IP multicast sono indirizzi IP di classe D. Pertanto, tutti gli indirizzi IP compresi tra 224.0.0.0 e 239.255.255.255 sono indirizzi IP multicast. Sono anche chiamati indirizzi di destinazione del gruppo (GDA).
2. A ogni GDA è associato un indirizzo MAC. Questo indirizzo MAC è formato da 01-00-5e, seguito dagli ultimi 23 bit del GDA convertiti in formato esadecimale, come mostrato di seguito.239.20.20.20 corrisponde a MAC 01-00-5e-14-14-14.239.10.10.10 corrisponde a MAC 01-00-5e-0a-0a-0a.Di conseguenza, non si tratta di un mapping uno-a-uno, bensì di un mapping uno-a-molti. Da questi due indirizzi, è possibile vedere che il primo ottetto (239) non è usato nell'indirizzo MAC. Quindi gli indirizzi multicast con gli stessi ultimi tre ottetti ma diversi per il primo ottetto si sovrappongono.
3. Alcuni indirizzi IP multicast sono riservati per un utilizzo speciale, come mostrato di seguito.24.0.0.1 - Tutti gli host con supporto multicast.24.0.0.2 - Tutti i router con supporto per multicast.224.0.0.5 e 224.0.0.6 sono utilizzati da Open Shortest Path First (OSPF).

In generale, gli indirizzi da 224.0.0.1 a 224.0.0.255 sono riservati e utilizzati da vari protocolli (standard o proprietari, ad esempio HSRP (Hot Standby Router Protocol)). Cisco consiglia di non utilizzarli per GDA in una rete multicast. Lo snooping CGMP e IGMP non funziona con questo intervallo di indirizzi riservato.

Protocollo Internet Group Management

IGMP è uno standard definito nella RFC112 per IGMPv1, nella RFC236 per IGMPv2 e nella RFC3376 per IGMPv3. IGMP specifica come un host può registrarsi su un router per ricevere traffico multicast specifico. La sezione successiva fornisce una breve panoramica su IGMP.

IGMPv1

I messaggi IGMP versione 1 (IGMPv1) vengono trasmessi in datagrammi IP e contengono i seguenti campi:

- Version: 1
- Tipo: Esistono due tipi di messaggi IGMP: Query appartenenza e Report appartenenza.
- Checksum
- GDA

I report sull'appartenenza vengono generati dagli host che desiderano ricevere un gruppo multicast specifico (GDA). Le query di appartenenza vengono emesse dai router a intervalli regolari per verificare se un host è ancora interessato al GDA in quel segmento.

I report sull'appartenenza dell'host vengono emessi non sollecitati (quando l'host desidera ricevere prima il traffico GDA) o in risposta a una query sull'appartenenza. Vengono inviati con i seguenti campi:

Informazioni L2

- MAC di origine: Indirizzo MAC host
- MAC di destinazione: MAC di destinazione per GDA

Informazioni L3

- IP di origine: Indirizzo IP dell'host
- IP di destinazione: GDA

Pacchetto IGMP

- I dati IGMP contengono inoltre la GDA e alcuni altri campi.

Le query sull'appartenenza dell'host vengono inviate dal router all'indirizzo multicast: 224.0.0.1. Queste query utilizzano 0.0.0.0 nel campo GDA IGMP. È necessario che un host per ogni gruppo risponda alla query oppure il router interrompe l'inoltro del traffico di quel GDA a quel segmento (dopo tre tentativi). Il router conserva una voce di routing multicast per ciascuna origine e la collega a un elenco di interfacce in uscita (interfaccia da cui proviene il report IGMP). Dopo tre tentativi di query IGMP senza risposta, questa interfaccia viene cancellata dall'elenco delle interfacce in uscita per tutte le voci collegate a quella GDA.

> **Nota:** IGMPv1 non ha alcun meccanismo di uscita. Se un host non desidera più ricevere il traffico, si limita a uscire. Se si tratta dell'ultimo host della subnet, il router non riceve alcuna risposta alla query ed elimina il GDA per la subnet.

IGMPv2

In IGMP versione 2 (IGMPv2), il campo versione è stato rimosso e il campo tipo può ora accettare valori diversi. I tipi sono illustrati di seguito.

- Query appartenenza
- Rapporto appartenenza IGMPv1
- Rapporto appartenenza versione 2
- Lascia gruppo

Di seguito sono elencate le descrizioni delle nuove funzioni più importanti aggiunte in IGMPv2.

- Messaggio IGMP Leave: quando un host desidera uscire da un gruppo, deve inviare un messaggio IGMP Leave Group alla destinazione 24.0.0.2 (invece di uscire automaticamente come in IGMPv1).
- Un router può ora inviare una query specifica del gruppo inviando una query di appartenenza al GDA del gruppo anziché inviarla a 0.0.0.0.

IGMPv3

In IGMP versione 3 (ICMPv3), esiste un campo di tipo che può avere i seguenti valori:

- Query appartenenza
- Rapporto di appartenenza alla versione 3

Un'implementazione di IGMPv3 *deve* inoltre supportare i seguenti tre tipi di messaggi, per l'interoperabilità con le versioni precedenti di IGMP:

- Rapporto di appartenenza alla versione 1 [RFC112]
- Rapporto di appartenenza alla versione 2 [RFC2236]

- Uscire dal gruppo versione 2 [RFC2236]

IGMPv3 aggiunge il supporto per il filtro di origine, ossia la capacità di un sistema di segnalare l'interesse nella ricezione di pacchetti da indirizzi di origine specifici o da **tutti gli** indirizzi di origine **tranne** specifici inviati a uno specifico indirizzo multicast. Questa funzionalità è anche denominata SSM (Source Specific Multicast).

Affinché un computer supporti SSM, deve supportare IGMPv3. Tuttavia, sono relativamente pochi i sistemi operativi che supportano IGMPv3. Windows XP supporta IGMPv3 e sono disponibili patch di supporto per IGMPv3 per FreeBSD e Linux.

Gli amministratori devono distinguere tra il supporto IGMPv3 a livello di router e lo snooping IGMPv3 a livello di switch. Sono due caratteristiche diverse.

Supporto di IGMPv3 sugli switch Catalyst (L2)

- Catalyst 6000 con software in modalità ibrida (CatOS sul Supervisor e software Cisco IOS® sull'MSFC) supporta ufficialmente lo snooping IGMPv3 a partire dalla versione 7.5(1).
- Nelle versioni precedenti alla 7.5(1), lo switch Catalyst 6000 non disponeva di supporto ufficiale per IGMPv3, ma normalmente dovrebbe essere in grado di gestire pacchetti IGMPv3.
- Catalyst 6000 con software Integrated IOS supporta IGMPv3 a livello di router (interfaccia L3) a partire dalla versione 12.1(8a)E.
- Catalyst 4000 supporta solo IGMPv3 a livello di router su Supervisor III e IV. Non supporta lo snooping IGMPv3.

Supporto di IGMPv3 sui router Cisco (L3)

IGMPv3 è supportato su tutte le piattaforme con software Cisco IOS® versione 12.1(5)T e successive.

Avvertenze

Quando uno switch esegue lo snooping IGMP, intercetta i pacchetti IGMP e popola la tabella di inoltro statica di layer 2 (L2) in base al contenuto dei pacchetti intercettati. Quando sulla rete sono presenti host IGMPv1 o v2, lo switch legge i join e le foglie IGMP per determinare quali host desiderano ricevere quale flusso multicast o interrompere la ricezione del flusso multicast.

IGMPv3 è più complicato, in quanto utilizza non solo l'indirizzo di gruppo (indirizzo multicast), ma anche le origini da cui è previsto il traffico. A parte lo switch Catalyst 6000 con CatOS 7.5 o versioni successive e Native IOS 12.1(8a)E o versioni successive, nessun altro switch è attualmente in grado di bloccare efficacemente i pacchetti e creare una tabella di inoltro basata su queste informazioni. Pertanto, lo snooping IGMP deve essere disattivato quando sullo switch è presente un host IGMPv3. Quando lo snooping IGMP è disattivato, lo switch non può generare dinamicamente una tabella di inoltro L2 per i flussi multicast. In altre parole, lo switch invia i flussi multicast.

Quando lo snooping IGMP è disabilitato, una soluzione consiste nel configurare manualmente le voci CAM (Content-Addressable Memory) dinamiche multicast per evitare di inondare la subnet con il traffico multicast. Si tratta tuttavia di un onere amministrativo e non di una soluzione dinamica. Quando un client non desidera più ricevere il traffico, la voce CAM non viene rimossa dallo switch (a meno che non si proceda manualmente), in modo che il traffico di rete sia ancora

indirizzato all'host.

Inoltre, quando si usa IGMPv3 nella rete, gli switch che usano CGMP funzionano normalmente a parte il fatto che CGMP Fastleave non funziona. Se CGMP Fastleave è necessario, è consigliabile ripristinare IGMPv2.

Le avvertenze specifiche della piattaforma in sospeso sono riportate nelle note sulla versione dei rispettivi switch.

Interoperabilità tra IGMPv1 e IGMPv2

Con IGMPv1 e IGMPv2, solo un router per subnet IP invia query. Questo router è denominato router di query. In IGMPv1, il router di query viene scelto con l'aiuto del protocollo di routing multicast. In IGMPv2, viene scelto dall'indirizzo IP più basso tra i router. Di seguito sono riportate diverse possibilità:

Scenario 1: Router IGMPv1 con una combinazione di host IGMPv1 e IGMPv2

Il router non è in grado di interpretare il report IGMPv2, quindi tutti gli host devono utilizzare solo il report IGMPv1.

Scenario 2: Router IGMPv2 con una combinazione di host IGMPv2 e IGMPv3

Gli host IGMPv1 non sono in grado di comprendere la query IGMPv2 o la query di appartenenza al gruppo IGMPv2. Il router deve utilizzare solo IGMPv1 e sospendere l'operazione di uscita.

Scenario 3: Router IGMPv1 e router IGMPv2 situati sullo stesso segmento

Il router IGMPv1 non ha modo di rilevare il router IGMPv2. Pertanto, il router IGMPv2 deve essere configurato dall'amministratore come router IGMPv1. In ogni caso, è possibile che non siano in accordo sul router di query.

Interoperabilità tra IGMPv1/IGMPv2 e IGMPv3

In tutte le versioni di IGMP, solo un router per subnet IP invia query. Questo router è denominato router di query. In IGMPv1, il router di query viene scelto con l'aiuto del protocollo di routing multicast. In IGMPv2 e IGMPv3, viene scelto dall'indirizzo IP più basso tra i router. Di seguito sono riportate diverse opzioni di interoperabilità.

Scenario 1: Router IGMPv1/IGMPv2 con una combinazione di host IGMPv1/IGMPv2 e IGMPv3

Poiché il router non è in grado di interpretare i report IGMPv3, tutti gli host utilizzano i report IGMPv1/IGMPv2.

Scenario 2: Router IGMPv3 con una combinazione di host IGMPv1/IGMPv2 e IGMPv3

Gli host IGMPv1/IGMPv2 non sono in grado di interpretare la query IGMPv3 o la query di appartenenza IGMPv3. Il router deve utilizzare solo la versione IGMP corrispondente alla versione client IGMP più bassa presente. Se sono presenti client IGMPv3 e IGMPv2, il router utilizza

IGMPv2. Se sono presenti client IGMPv1, IGMPv2 e IGMPv3, il router utilizza IGMPv1.

Scenario 3: Versione diversa dei router sullo stesso segmento

Quando sullo stesso segmento sono presenti router di versioni diverse, i router delle versioni inferiori non hanno modo di rilevare i router delle versioni superiori. Pertanto, i diversi router devono essere configurati dall'amministratore con la stessa versione. Questa versione deve corrispondere alla versione più bassa su qualsiasi router di query presente.

IGMP su un router

Se, per impostazione predefinita, non vi sono utenti registrati in un gruppo specifico di una subnet, il router non inoltra il traffico multicast di quel gruppo nella subnet. Ciò significa che un router deve ricevere un report IGMP per un GDA per poterlo aggiungere alla tabella di routing multicast e avviare l'inoltro del traffico per quel gruppo.

Su un router, è necessario eseguire le seguenti azioni:

1. Abilitare il routing multicast in modalità globale, come mostrato di seguito.

   ```
   ip multicast-routing
   ```

2. Configurare un protocollo di routing multicast sull'interfaccia interessata, come mostrato di seguito.

   ```
   ip pim dense-mode
   ```

3. Monitorare IGMP, come illustrato di seguito.

   ```
   show ip igmp interface
   show ip igmp group
   show ip mroute
   ```

4. Configurare un router per inviare il report IGMP (sull'interfaccia), come mostrato di seguito.

   ```
   ip igmp join-group [GDA_ip_address]
   ip igmp version [1 | 2 | 3]
   ```

Esempio pratico su un router

Un router è configurato per effettuare il routing tra due sottointerfacce, Fast-Ethernet 0.2 e Fast-Ethernet 0.3. Entrambe le interfacce sono configurate anche per eseguire IGMP. Nell'output seguente è possibile visualizzare la versione IGMP, il gruppo aggiunto e così via.

Configurazione

```
ip multicast-routing
```

```
interface FastEthernet0
 no ip address
 no ip directed-broadcast
!
interface FastEthernet0.2
 encapsulation isl 2
 ip address 10.2.2.1 255.255.255.0
 no ip redirects
 no ip directed-broadcast
 ip pim dense-mode
!
interface FastEthernet0.3
 encapsulation isl 3
 ip address 10.3.3.1 255.255.255.0
 no ip redirects
 no ip directed-broadcast
 ip pim dense-mode
!
```

show ip igmp interface

```
 Fa0.2 is up, line protocol is up
 Internet address is 10.2.2.1/24
 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
 Inbound IGMP access group is not set
 IGMP activity: 3 joins, 2 leaves
 Multicast routing is enabled on interface
 Multicast TTL threshold is 0
 Multicast designated router (DR) is 10.2.2.1 (this system)
 IGMP querying router is 10.2.2.1 (this system)
 Multicast groups joined: 224.0.1.40

 Fa0.3 is up, line protocol is up
 Internet address is 10.3.3.1/24
 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
 Inbound IGMP access group is not set
 IGMP activity: 1 joins, 1 leaves
 Multicast routing is enabled on interface
 Multicast TTL threshold is 0
 Multicast designated router (DR) is 10.3.3.1 (this system)
 IGMP querying router is 10.3.3.1 (this system)
 No multicast groups joined
```

show ip mroute and show ip igmp group

```
 Router_A#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
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode


(*, 239.10.10.10), 00:01:15/00:02:59, RP 0.0.0.0, flags: DJC
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    FastEthernet0.3, Forward/Dense, 00:01:16/00:00:00

(10.2.2.2, 239.10.10.10), 00:00:39/00:02:20, flags: CT
  Incoming interface: FastEthernet0.2, RPF nbr 0.0.0.0
  Outgoing interface list:
    FastEthernet0.3, Forward/Dense, 00:00:39/00:00:00

Router_A#show ip igmp groups
IGMP Connected Group Membership
Group Address    Interface            Uptime    Expires   Last Reporter
239.10.10.10     Fa0.3                00:02:48  00:02:04  10.3.3.2
Router_A#
```

Protocollo Cisco Group Management

Per il supporto del protocollo CGMP sugli switch Catalyst, consultare il documento sulla matrice di supporto degli switch Catalyst multicast.

Frame CGMP e tipi di messaggio

CGMP è stato implementato per la prima volta da Cisco per limitare il traffico multicast in una rete L2. Essenzialmente, uno switch non è in grado di esaminare i pacchetti L3, quindi non è in grado di distinguere un pacchetto IGMP. Con il protocollo CGMP, il router fornisce l'interfaccia tra gli host. I router "parlano" con IGMP e gli switch "parlano" con CGMP.

I frame CGMP sono frame Ethernet con indirizzo MAC di destinazione 01-00-0c-dd-dd-dd e intestazione SNAP (Subnetwork Access Protocol) con valore 0x2001. I frame CGMP contengono i seguenti campi:

- Version: 1 o 2.
- Tipo messaggio: Partecipa o esci.
- Conteggio: Numero di coppie di indirizzi multicast/unicast nel messaggio.
- GDA: Indirizzo MAC a 48 bit del gruppo multicast.
- Indirizzo origine unicast (USA): L'indirizzo unicast MAC a 48 bit dei dispositivi che vogliono unirsi al GDA.

  Nota: Il valore del campo conteggio determina il numero di visualizzazioni degli ultimi due campi.

Per impostazione predefinita, i processori di uno switch (denominato NMP in Catalyst) ascoltano gli indirizzi multicast solo quando **show cam system** il comando. Quando si abilita CGMP su uno switch, l'indirizzo 01-00-0c-dd-dd-dd viene aggiunto al **show cam system** output del comando.

Nella tabella seguente vengono elencati tutti i possibili messaggi CGMP.

GDA	Stati Uniti	Partecipa/ Esci	Significato

MAC Mcast	MAC client	Partecipa	Aggiungere una porta al gruppo.
MAC Mcast	MAC client	Esci	Elimina porta dal gruppo.
00-00-00-00-00-00	MAC router	Partecipa	Assegnare la porta del router.
00-00-00-00-00-00	MAC router	Esci	Annullare l'assegnazione della porta del router.
MAC Mcast	00-00-00-00-00-00	Esci	Elimina gruppo.
00-00-00-00-00-00	00-00-00-00-00-00	Esci	Elimina tutti i gruppi.

Apprendimento delle porte dei router

Lo switch deve essere a conoscenza di tutte le porte del router in modo che vengano aggiunte automaticamente alle nuove voci multicast. Lo switch apprende le porte del router quando riceve un join CGMP a GDA 00-00-00-00-00-00 con Router MAC USA (terzo tipo di messaggio nella tabella). Questi messaggi vengono generati dal router su tutte le interfacce configurate per eseguire CGMP. Tuttavia, è disponibile anche un metodo statico per configurare le porte del router sullo switch.

Aggiunta a un gruppo con CGMP

- Un nuovo client richiede di ricevere il traffico per un GDA, quindi il client invia un messaggio di rapporto appartenenza IGMP.
- Il router riceve il report IGMP, lo elabora e invia un messaggio CGMP allo switch. Il router copia l'indirizzo MAC di destinazione nel campo GDA del join CGMP e l'indirizzo MAC di origine negli Stati Uniti del join CGMP. e quindi lo rimanda allo switch.
- uno switch con CGMP abilitato deve ascoltare gli indirizzi CGMP 01-00-0c-dd-dd-dd. Il processore dello switch cerca nella tabella CAM per gli Stati Uniti. Una volta che gli Stati Uniti sono stati visualizzati nella tabella CAM, lo switch riconosce su quale porta si trovano gli Stati Uniti ed effettua una delle seguenti operazioni:Crea una nuova voce statica per GDA e collega la porta USA a tale voce insieme a tutte le porte del router.Aggiunge la porta USA all'elenco delle porte per questo GDA (se la voce statica esiste già).

Come lasciare un gruppo con CGMP

Le voci statiche imparate con il protocollo CGMP sono permanenti, a meno che la VLAN non subisca una modifica della topologia dello spanning tree o che il router non invii uno degli ultimi messaggi di uscita CGMP della tabella precedente.

Quando l'host è IGMPv1, non inviare messaggi di abbandono IGMP. Il router invia messaggi

Leave solo se non riceve una risposta a tre query IGMP consecutive. Ciò significa che nessuna porta viene eliminata da un gruppo se altri utenti sono ancora interessati a quel gruppo.

Con l'introduzione di IGMPv2 e la presenza di IGMP Leave, Cisco è stato aggiunto alla specifica CGMP originale (CGMPv2). Questa aggiunta è denominata CGMP Fast-Leave.

L'elaborazione CGMP Fast-Leave consente allo switch di rilevare i messaggi IGMPv2 Leave inviati all'indirizzo multicast di tutti i router (24.0.0.2) dagli host su una qualsiasi delle porte del modulo supervisor engine. Quando il modulo supervisor engine riceve un messaggio di uscita, avvia un timer di risposta alla query e invia un messaggio sulla porta su cui è stata ricevuta l'uscita per determinare se esiste ancora un host disposto a ricevere questo gruppo multicast su quella porta. Se il timer scade prima della ricezione di un messaggio di aggiunta CGMP, la porta viene eliminata dalla struttura multicast per il gruppo multicast specificato nel messaggio di uscita originale. Se si tratta dell'ultima porta del gruppo multicast, inoltra il messaggio IGMP Leave a tutte le porte del router. Il router avvia quindi il normale processo di eliminazione inviando una query specifica del gruppo. Poiché non viene ricevuta alcuna risposta, il router rimuove il gruppo dalla tabella di routing multicast per l'interfaccia. Inoltre, invia un messaggio CGMP Leave allo switch per cancellare il gruppo dalla tabella statica. L'elaborazione Fast-Leave assicura una gestione ottimale della larghezza di banda per tutti gli host di una rete commutata, anche quando si utilizzano contemporaneamente più gruppi multicast.

Quando l'opzione CGMP Leave è abilitata, al menu **show cam system** come mostrato di seguito.

```
01-00-5e-00-00-01
01-00-5e-00-00-02
```

In IGMP Leave viene utilizzato 224.0.0.2 e in IGMP Query viene utilizzato 224.0.0.1.

Per risolvere i problemi relativi a CGMP, attenersi alla seguente procedura:

1. A causa di un conflitto con l'HSRP, l'elaborazione dell'uscita da CGMP è disabilitata per impostazione predefinita. HSRP utilizza l'indirizzo MAC 01-00-5e-00-00-02, che è lo stesso di IGMP Leave con IGMP versione 2. Con CGMP Fast-Leave, tutti i pacchetti HSRP passano alla CPU dello switch. Poiché un messaggio HSRP non è un pacchetto IGMP, lo switch rigenera tutti questi messaggi e li invia a tutte le porte del router. I router che ricevono `hello hsrp` o `i peer hsrp` perdono la connettività. Pertanto, nel debug dei problemi HSRP, provare a disabilitare l'opzione CGMP Fast-Leave.Per abilitare l'elaborazione del congedo CGMP, eseguire il comando **set cgmp leave enable**
2. Quando l'elaborazione CGMP Leave è abilitata, lo switch Catalyst 5000 apprende le porte del router tramite i messaggi PIM-v1, HSRP e CGMP Self-Join. Quando l'elaborazione CGMP Leave è disabilitata, lo switch Catalyst serie 5000 apprende le porte del router solo tramite i messaggi CGMP Self-Join.
3. CGMP non elimina il traffico multicast per gli indirizzi IP multicast mappati nell'intervallo di indirizzi MAC da 01-00-5E-00-00-00 a 01-00-5E-00-00-FF. Gli indirizzi multicast IP riservati, compresi tra 24.0.0.0 e 224.0.0.255, vengono utilizzati per inoltrare il traffico multicast IP locale in un singolo hop L3.

Rete CGMP e solo origine

Una rete di sola origine è un segmento con un solo multicast di origine e nessun client reale. Pertanto, è possibile che in tale segmento non vengano generati report IGMP. Tuttavia, il

protocollo CGMP deve limitare il flooding di questa fonte (solo per l'uso del router). Se un router rileva traffico multicast su un'interfaccia senza alcun report IGMP, viene identificato come rete solo origine multicast. Il router genera un messaggio CGMP Join per se stesso e lo switch si limita ad aggiungere questo gruppo (solo con la porta del router).

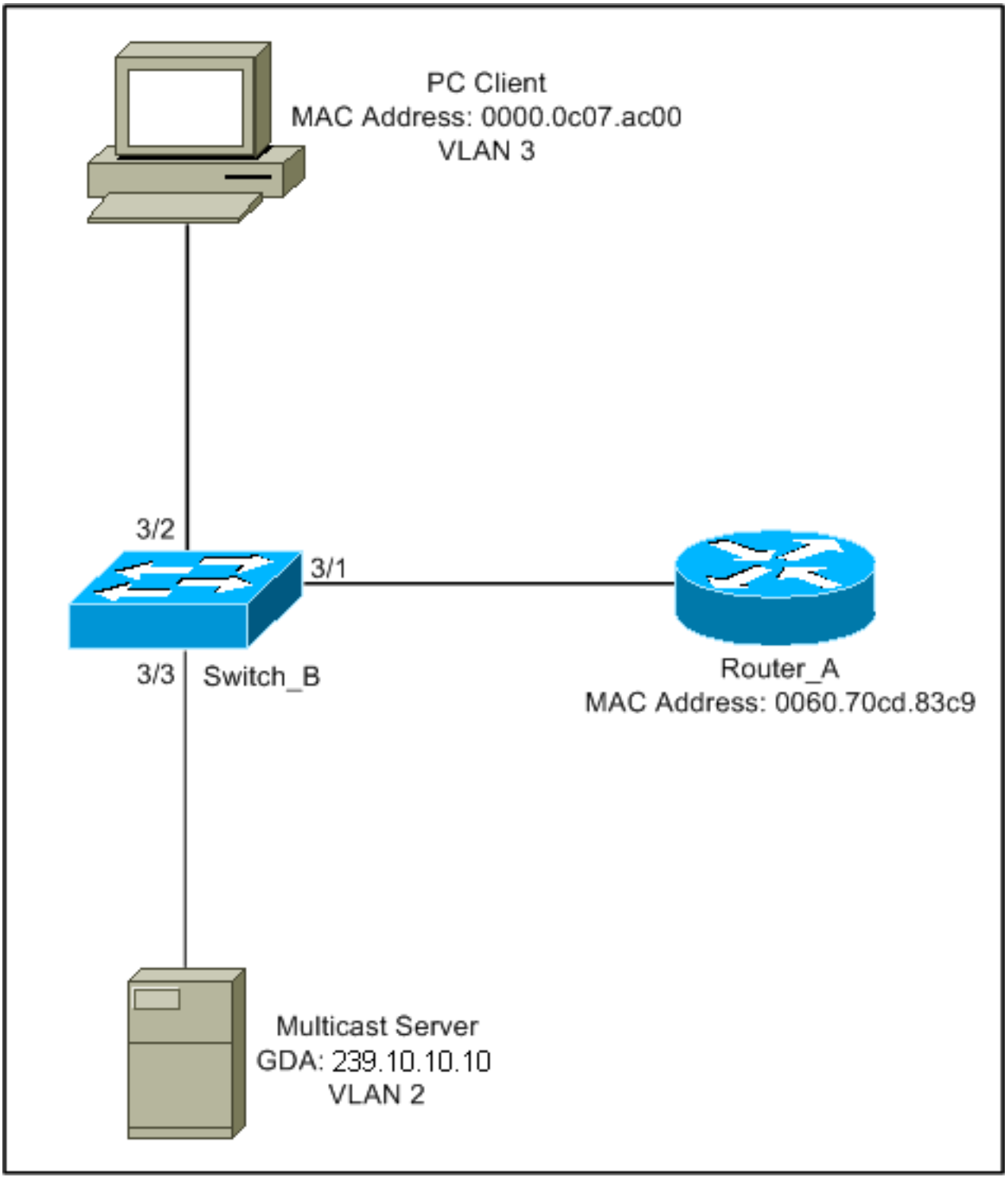
Configurazione di router e switch Cisco per abilitare CGMP

I comandi seguenti sono validi solo per Catalyst serie 4000 e 5000 (più 2901, 2902, 2926, 2948G e 4912).

- Multicast RouterAbilita multicast IP (comando globale):**ip multicast-routing**Abilitare ciascuna interfaccia che esegue CGMP (modalità interfaccia) con i seguenti comandi:**ip pimip igmpip cgmp**Eseguire il debug del problema multicast L2 con i seguenti comandi:**debug ip igmpdebug ip cgmp**
- Catalyst serie 4000 o 5000Abilitare/disabilitare CGMP con i seguenti comandi:**set cgmp**Abilitare/disabilitare la funzione CGMP Fast-Leave con i seguenti comandi:**set cgmp leave**Configurare il router multicast (statico) con i seguenti comandi:**set multicast router**Cancellare il router multicast con i seguenti comandi:**clear multicast router**Di seguito sono elencati vari comandi per verificare il funzionamento di CGMP.**show cam staticshow cgmp statisticshow cgmp leaveshow multicast routershow multicast groupshow multicast group cgmpshow multicast group count**

Esempio pratico di utilizzo del protocollo CGMP e dei comandi e dei risultati del debug

Questo è un esempio di configurazione pratica per un router Cisco e gli switch Catalyst.



Questa configurazione mostra le operazioni interessate quando un host viene aggiunto a un gruppo. Questa configurazione mostra anche le operazioni quando un host lascia un gruppo con la funzione di abbandono rapido abilitata. Inoltre, vengono fornite le tracce dello sniffer e la configurazione dello switch e del router.

Aggiunta a un gruppo con CGMP

Quando si unisce un gruppo a CGMP, attenersi alla seguente procedura.

1. Abilitare il protocollo CGMP sullo switch, come mostrato di seguito.

```
Switch_B (enable) set cgmp en
MCAST-CGMP: Set CGMP Sys Entrie
MCAST-CGMP: Set CGMP Sys Entrie
```

```
MCAST-CGMP: Set CGMP Sys Entrie
CGMP support for IP multicast enabled.
Switch_B (enable)
```

Come si può vedere di seguito, la voce 01-00-0c-dd-dd è inclusa per tutte le VLAN nella **show cam system** output del comando. Inoltre, poiché la rete esegue CGMP Fast-Leave, è possibile visualizzare le voci relative a 01-00-5e-00-00-01 e 01-00-5e-00-00-02.

```
Switch_B (enable) show cgmp leave

CGMP:       enabled
CGMP leave: enabled
Switch_B (enable) show cam system
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN  Dest MAC/Route Des [CoS]  Destination Ports or VCs / [Protocol Type]
----  ------------------ -----  -------------------------------------------
1     00-10-2f-00-14-00  #          7/1
1     00-e0-fe-4b-f3-ff  #          1/9
1     01-00-0c-cc-cc-cc  #          1/9
1     01-00-0c-cc-cc-cd  #          1/9
1     01-00-0c-dd-dd-dd  #          1/9
1     01-00-0c-ee-ee-ee  #          1/9
1     01-80-c2-00-00-00  #          1/9
1     01-80-c2-00-00-01  #          1/9
2     00-10-2f-00-14-00  #          7/1
2     01-00-0c-cc-cc-cc  #          1/9
2     01-00-0c-cc-cc-cd  #          1/9
2     01-00-0c-dd-dd-dd  #          1/9
2     01-80-c2-00-00-00  #          1/9
2     01-80-c2-00-00-01  #          1/9
3     01-00-0c-cc-cc-cc  #          1/9
3     01-00-0c-cc-cc-cd  #          1/9
3     01-00-0c-dd-dd-dd  #          1/9
3     01-80-c2-00-00-00  #          1/9
3     01-80-c2-00-00-01  #          1/9
Total Matching CAM Entries Displayed = 19
```

2. Il router invia un messaggio CGMP Join al GDA 00-00-00-00-00-00 con l'indirizzo MAC USA del router. Pertanto, la porta del router viene aggiunta all'elenco delle porte del router (vedere il primo esempio seguente).**Sul router**

```
6d01h: CGMP: Sending self Join on Fa0.3
6d01h:       GDA 0000.0000.0000, USA 0060.70cd.83c9
```

Sullo switch

```
MCAST-CGMP-JOIN: recvd CGMP JOIN msg on port 3/1 vlanNo 2
MCAST-CGMP-JOIN: join GDA 00-00-00-00-00-00 MCAST-CGMP-JOIN:USA
                 00-60-70-cd-83-c9
MCAST-ROUTER: Adding QUERIER port 3/1, vlanNo 2
MCAST-ROUTER: Creating RouterPortTimer for  port 3/1, vlanNo 2

Switch_B (enable) show multi router
CGMP enabled
IGMP disabled

Port       Vlan
---------  ----------------
 3/1       2-3

Total Number of Entries = 1
'*' - Configured
```

3. Il PC del 3/1 invia a IGMP un rapporto contenente la GDA: 239.10.10.10 (cfr. frame 2 in basso). Qui sotto è riportato il **show ip igmp group** output del comando sul router Router_A.Il router inoltra ora il traffico per le porte 24.10.10.10 a fa0.3 . Questa è una conseguenza della ricezione del report IGMP della versione 10.3.3.2, che è il PC client.

```
Router_A#show ip igmp groups
IGMP Connected Group Membership
Group Address    Interface            Uptime    Expires   Last Reporter
239.10.10.10     Fa0.3                00:02:48  00:02:04  10.3.3.2
Router_A#
```

4. Il router riceve il report e invia un messaggio di join CGMP insieme alle seguenti informazioni:MAC di origine: Indirizzo MAC del routerMAC di destinazione: 01-00-cc-dd-dd-ddSommario: Indirizzo MAC del PC client (USA): 00-00-0c-07-ac-00 indirizzo MAC del gruppo multicast: 01-00-5e-0a-0a-0a (vedere il frame 3 in basso)**Sul router**

```
6d01h: IGMP: Received v2 Report from 10.3.3.2 (Fa0.3) for 239.10.10.10
6d01h: CGMP: Received IGMP Report on Fa0.3
6d01h:       from 10.3.3.2 for 239.10.10.10
6d01h: CGMP: Sending Join on Fa0.3
```

5. Lo switch con 01-00-cc-dd-dd-dd nel **show cam system** nell'output del comando CGMP è abilitato. Lo switch è in grado di elaborare il pacchetto.Lo switch esegue una ricerca nella tabella della CAM dinamica per determinare su quale porta si trova l'indirizzo MAC del PC client. L'indirizzo si trova sulla porta 3/2 e lo switch crea una voce statica nella tabella CAM per 01-00-5e-0a-0a-0a limitata alla porta 3/2. Lo switch aggiunge anche la porta router 3/1 alla voce statica per quella GDA.**Sullo switch**

```
MCAST-CGMP-JOIN: recvd CGMP JOIN msg on port 3/1 vlanNo 3
MCAST-CGMP-JOIN: join GDA 01-00-5e-0a-0a-0a MCAST-CGMP-JOIN:USA 00-60-5c-f4-bd-e2
MCAST-CGMP-JOIN: 3/2/3: index 81
MCAST-CGMP-JOIN: recvd CGMP JOIN msg on port 3/1 vlanNo 2
MCAST-CGMP-JOIN: join GDA 01-00-5e-00-01-28 MCAST-CGMP-JOIN:USA 00-60-70-cd-83-c9
MCAST-CGMP-JOIN: 3/1/2: index 80
```

6. Tutto il traffico successivo per il gruppo multicast 239.10.10.10 viene inoltrato solo a questa porta nella VLAN. Di seguito è riportata la voce statica nello switch Catalyst dove 3/1 è la porta del router e 3/2 è la porta del client.

```
Switch_B (enable) show cam static
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN  Dest MAC/Route Des    [CoS]  Destination Ports or VCs / [Protocol Type]
----  ------------------    -----  ----------------------------------------
3     01-00-5e-0a-0a-0a             3/1-2
Total Matching CAM Entries Displayed = 3
Switch_B (enable)
```

Come lasciare un gruppo con la funzionalità CGMP Fast-Leave abilitata

L'esempio seguente richiede che il client sia un client IGMP versione 2 e che Fast-Leave sia abilitato sullo switch.

1. La procedura seguente attiva l'opzione CGMP Fast-Leave. Osservare la **show cgmp leave** per determinare se è attivato. Inoltre, osservate **show cam system** output del comando per determinare se lo switch sta ascoltando 01-00-5e-00-00-01 e 01-00-5e-00-00-02 (indirizzi usati per l'attesa).

```
Switch_B (enable) show cgmp leave

CGMP:       enabled
CGMP leave: enabled
Switch_B (enable) show cam sys
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN  Dest MAC/Route Des    [CoS]  Destination Ports or VCs / [Protocol Type]
----  ------------------    -----  -------------------------------------------
1     00-10-2f-00-14-00  #          7/1
1     00-e0-fe-4b-f3-ff  #          1/9
1     01-00-0c-cc-cc-cc  #          1/9
1     01-00-0c-cc-cc-cd  #          1/9
1     01-00-0c-dd-dd-dd  #          1/9
1     01-00-0c-ee-ee-ee  #          1/9
1     01-80-c2-00-00-00  #          1/9
1     01-80-c2-00-00-01  #          1/9
2     00-10-2f-00-14-00  #          7/1
2     01-00-0c-cc-cc-cc  #          1/9
2     01-00-0c-cc-cc-cd  #          1/9
2     01-00-0c-dd-dd-dd  #          1/9
2     01-00-5e-00-00-01  #          1/9
2     01-00-5e-00-00-02  #          1/9
2     01-80-c2-00-00-00  #          1/9
2     01-80-c2-00-00-01  #          1/9
3     01-00-0c-cc-cc-cc  #          1/9
3     01-00-0c-cc-cc-cd  #          1/9
3     01-00-0c-dd-dd-dd  #          1/9
3     01-00-5e-00-00-01  #          1/9
3     01-00-5e-00-00-02  #          1/9
3     01-80-c2-00-00-00  #          1/9
Do you wish to continue y/n [n]?  y
Total Matching CAM Entries Displayed = 22
```

2. Il client invia un messaggio IMPG Leave a 24.0.0.2. Lo switch lo intercetta e invia una query IGMP sulla porta su cui riceve il congedo. Di seguito viene indicato **debug** output sullo switch:

```
MCAST-IGMP-LEAVE:Recvd leave on port 3/2 vlanNo 3
MCAST-IGMP-LEAVE:router_port_tbl[vlanNo].QueryTime = 0
MCAST-IGMP-LEAVE:deletion_timer = 1
MCAST-SEND:Transmitting IGMP Mac Based GS Query msg on port 3/2 vlanNo 3
MCAST-SEND:  Transmit Succeeded for IGMP Group Specific Query msg on port 3/2 vlanNo 3
```

3. Poiché non è stata ricevuta alcuna risposta, Catalyst inoltra il messaggio IGMP Leave al router, come mostrato di seguito.

```
MCAST-TIMER:IGMPLeaveTimer expired on port 3/2 vlanNo 3 GDA 01-00-5e-0a-0a-0a
MCAST-TIMER:IGMPLeaveTimer expiry: Transmit IGMP Leave on port 3/1 vlanNo 3
MCAST-SEND:Transmitting IGMP Leave msg on port 3/1 vlanNo 3
MCAST-SEND: Inband Transmit Succeeded for IGMP Leave Message on port 3/1 vlanNo 3
```

4. Il router riceve un messaggio di uscita IGMP, quindi invia un messaggio di uscita CGMP allo switch ed elimina il gruppo dal relativo elenco di gruppi IGMP. Di seguito è riportata la **debug**

sul router.**Sul router**

```
IGMP: Received Leave from 10.200.8.108 (Fa0.3) for 239.10.10.10
IGMP: Send v2 Query on Fa0.3 to 239.10.10.10
IGMP: Send v2 Query on Fa0.3 to 239.10.10.10
CGMP: Sending Leave on Fa0.3
      GDA 0100.5e0a.0a0a, USA 0000.0000.0000
IGMP: Deleting 239.10.10.10 on Fa0.3
```

Tracce e configurazione CGMP

Telaio 1

Il frame 1 è un CGMP Join frame su GDA 00-00-00-00-00-00. Viene usato per aggiungere la porta del router all'elenco delle porte del router.

```
ISL: ----- ISL Protocol Packet -----
     ISL:
     ISL: Destination Address               = 01000C0000
     ISL: Type                              = 0 (Ethernet)
     ISL: User                              = 0 (Normal)
     ISL: Source Address                    = 8C958B7B1000
     ISL: Length                            = 76
     ISL: Constant value                    = 0xAAAA03
     ISL: Vendor ID                         = 0x8C958B
     ISL: Virtual LAN ID (VLAN)             = 2
     ISL: Bridge Protocol Data Unit (BPDU)  = 0
     ISL: Port Index                        = 193
     ISL: Reserved
     ISL:
ETHER: ----- Ethernet Header -----
     ETHER:
     ETHER: Destination = Multicast 01000CDDDDDD
!--- Send to the CGMP !--- macaddress present in show cam sys !--- command output.

     ETHER: Source      = Station Cisco11411E1
     ETHER: 802.3 length = 24
     ETHER:
LLC:  ----- LLC Header -----
     LLC:
     LLC:  DSAP Address = AA, DSAP IG Bit = 00 (Individual Address)
     LLC:  SSAP Address = AA, SSAP CR Bit = 00 (Command)
     LLC:  Unnumbered frame: UI
     LLC:
SNAP: ----- SNAP Header -----
     SNAP:
     SNAP: Vendor ID = Cisco1
     SNAP: Type = 2001 (CGMP)
     SNAP:
CGMP: ----- CGMP -----
     CGMP:
     CGMP: Version   = 16
     CGMP: Type      = 0 (Join)
     CGMP: Reserved
     CGMP: Count     = 1
     CGMP:
     CGMP: Group Destination Address and Unicast Source Address
     CGMP:
     CGMP:    GDA    =0000.0000.0000
```

```
     CGMP:    USA    =0000.0C14.11E1
!--- MAC address of the router. CGMP:
```

Il risultato del frame 1 è sullo switch, con 3/1 come porta collegata al router:

/Frame 2/

Il frame 2 è un report di appartenenza IGMP inviato dall'host per richiedere (o confermare) che gli utenti desiderino ricevere il traffico per il gruppo 239.10.10.10.

```
ISL: ----- ISL Protocol Packet -----
     ISL:
     ISL: Destination Address               = 01000C0000
     ISL: Type                              = 0 (Ethernet)
     ISL: User                              = 0 (Normal)
     ISL: Source Address                    = 8C958B7B1000
     ISL: Length                            = 76
     ISL: Constant value                    = 0xAAAA03
     ISL: Vendor ID                         = 0x8C958B
     ISL: Virtual LAN ID (VLAN)             = 2
     ISL: Bridge Protocol Data Unit (BPDU)  = 0
     ISL: Port Index                        = 195
     ISL: Reserved
     ISL:
ETHER: ----- Ethernet Header -----
     ETHER:
     ETHER: Destination = Multicast 01005E0A0A0A
!--- Destination is the GDA MAC. ETHER: Source = Station Cisco176DCCA !--- Sourced by the PC
connected in 3/1. ETHER: Ethertype = 0800 (IP) ETHER: IP: ----- IP Header ----- IP: IP: Version
= 4, header length = 20 bytes IP: Type of service = C0 IP: 110. .... = internetwork control IP:
...0 .... = normal delay IP: .... 0... = normal throughput IP: .... .0.. = normal reliability
IP: Total length = 28 bytes IP: Identification = 0 IP: Flags = 0X IP: .0.. .... = may fragment
IP: ..0. .... = last fragment IP: Fragment offset = 0 bytes IP: Time to live = 1 seconds/hops
IP: Protocol = 2 (IGMP) IP: Header checksum = CC09 (correct) IP: Source address = [10.1.1.2] IP:
Destination address = [224.10.10.10] IP: No options IP: IGMP: ----- IGMP header ----- IGMP:
IGMP: Version = 1 IGMP: Type = 6 (Ver2 Membership Report) IGMP: Unused = 0x00 IGMP: Checksum =
FFEA (correct) IGMP: Group Address = [224.10.10.10] IGMP:
```

Frame 3

Il frame 3 è il frame CGMP inviato dal router allo switch per comunicare allo switch di aggiungere una voce statica per 01-00-5e-0a-0a-0a.

```
ISL: ----- ISL Protocol Packet -----
     ISL:
     ISL: Destination Address               = 01000C0000
     ISL: Type                              = 0 (Ethernet)
     ISL: User                              = 0 (Normal)
     ISL: Source Address                    = 8C958B7B1000
     ISL: Length                            = 76
     ISL: Constant value                    = 0xAAAA03
     ISL: Vendor ID                         = 0x8C958B
     ISL: Virtual LAN ID (VLAN)             = 2
     ISL: Bridge Protocol Data Unit (BPDU)  = 0
     ISL: Port Index                        = 193
     ISL: Reserved
     ISL:
ETHER: ----- Ethernet Header -----
     ETHER:
     ETHER: Destination = Multicast 01000CDDDDDD
     ETHER: Source      = Station Cisco11411E1
```

```
     ETHER: 802.3 length = 24
     ETHER:
LLC:  ----- LLC Header -----
     LLC:
     LLC:  DSAP Address = AA, DSAP IG Bit = 00 (Individual Address)
     LLC:  SSAP Address = AA, SSAP CR Bit = 00 (Command)
     LLC:  Unnumbered frame: UI
     LLC:
SNAP: ----- SNAP Header -----
     SNAP:
     SNAP: Vendor ID = Cisco1
     SNAP: Type = 2001 (CGMP)
     SNAP:
CGMP: ----- CGMP -----
     CGMP:
     CGMP: Version   = 16
     CGMP: Type      = 0 (Join)
     CGMP: Reserved
     CGMP: Count     = 1
     CGMP:
     CGMP: Group Destination Address and Unicast Source Address
     CGMP:
     CGMP:    GDA    =0100.5E0A.0A0A
!--- GDA MAC added in show cam static !--- command output.

     CGMP:    USA    =0000.0C76.DCCA
!--- MAC of the PC in 3/1. CGMP:
```

Di seguito viene riportata la configurazione del router e dello switch.

```
 Router_A (router) Configuration:

 Router_A#write terminal
 Building configuration...

 Current configuration:
 !
 version 12.0
 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
 !
 hostname Router_A
 !
 !
 ip subnet-zero
 ip multicast-routing
 ip dvmrp route-limit 20000


 interface FastEthernet0
  no ip address
  no ip directed-broadcast
 !
 interface FastEthernet0.1
  encapsulation isl 1
  ip address 10.1.1.1 255.255.255.0
  no ip redirects
  no ip directed-broadcast
 !
 interface FastEthernet0.2
  encapsulation isl 2
  ip address 10.2.2.1 255.255.255.0
```

```
 no ip redirects
 no ip directed-broadcast
 ip pim dense-mode
 ip cgmp
!
interface FastEthernet0.3
 encapsulation isl 3
 ip address 10.3.3.1 255.255.255.0
 no ip redirects
 no ip directed-broadcast
 ip pim dense-mode
 ip cgmp
!

Switch_B configuration for CGMP:

#cgmp
set cgmp enable
set cgmp leave enable
!

CGMP statistics for VLAN 3:

Switch_B (enable) show cgmp sta 3
CGMP enabled

CGMP statistics for vlan 3:
valid rx pkts received           109
invalid rx pkts received         0
valid cgmp joins received        108
valid cgmp leaves received       1
valid igmp leaves received       1
valid igmp queries received      63
igmp gs queries transmitted      1
igmp leaves transmitted          1
failures to add GDA to EARL      0
topology notifications received  0
Switch_B (enable)
```

Snooping IGMP

Lo snooping IGMP è un'altra funzione che consente di acquisire direttamente i frame IGMP. Per il supporto dello snooping IGMP sugli switch Catalyst, consultare il documento sulla matrice di supporto degli switch Catalyst multicast.

Panoramica dello snooping IGMP

Lo snooping IGMP, come implica il nome, è una funzione che consente allo switch di "ascoltare" la conversazione IGMP tra host e router. Quando uno switch riceve un report IGMP da un host per un determinato gruppo multicast, aggiunge il numero di porta dell'host all'elenco GDA per quel gruppo. Inoltre, quando lo switch riceve un messaggio IGMP Leave, rimuove la porta dell'host dalla voce della tabella CAM.

Apprendimento della porta del router

Lo switch resta in ascolto dei seguenti messaggi per rilevare le porte del router con snooping

IGMP:

- Invio query appartenenza IGMP a 01-00-5e-00-00-01
- Invio saluti PIMv1 a 01-00-5e-00-00-02
- Invio saluti PIMv2 a 01-00-5e-00-00-0d
- Sonde DVMRP da inviare a 01-00-5e-00-04
- Messaggio MOSPF inviato a 01-00-5e-00-05 o 06

Abilitando lo snooping IGMP su uno switch, tutte le voci MAC precedenti vengono aggiunte al **show cam system** output del comando snooping switch. Una volta rilevata una porta del router, viene aggiunta all'elenco delle porte di tutti i GDA di tale VLAN.

Aggiunta a un gruppo con lo snooping IGMP

Di seguito sono riportati due scenari di unione:

Scenario A: L'host A è il primo host a unirsi a un gruppo nel segmento.

1. L'host A invia un report sull'appartenenza IGMP non richiesta.
2. Lo switch intercetta il report di appartenenza IGMP inviato dall'host che intendeva unirsi al gruppo.
3. Lo switch crea una voce multicast per quel gruppo e la collega alla porta su cui ha ricevuto il report e a tutte le porte del router.
4. Lo switch inoltra il report IGMP a tutte le porte del router. In questo modo, il router riceve anche il report IGMP e aggiorna di conseguenza la relativa tabella di routing multicast.

Scenario B: L'host B è ora il secondo host a unirsi allo stesso gruppo.

1. L'host B invia un report sull'appartenenza IGMP non richiesta.
2. Lo switch intercetta il report di appartenenza IGMP inviato dall'host che desidera unirsi al gruppo.
3. Lo switch non inoltra necessariamente il report IGMP a tutte le porte del router. In realtà, lo switch inoltra i report IGMP alle porte del router utilizzando il report sul proxy e inoltra solo un report per gruppo entro 10 secondi.

   Nota: Per mantenere l'appartenenza ai gruppi, il router multicast invia una query IGMP ogni 60 secondi. Questa query viene intercettata dallo switch e inoltrata a tutte le porte dello switch. Tutti gli host membri del gruppo rispondono alla query. Tuttavia, poiché lo switch intercetta anche il report di risposta, l'altro host non vede ognuno degli altri report e, di conseguenza, tutti gli host inviano un report (anziché uno per gruppo). Lo switch quindi utilizza anche Proxy Reporting per inoltrare solo un report per gruppo tra tutte le risposte ricevute.

Si supponga che l'host A desideri uscire dal gruppo, ma l'host B desideri ancora ricevere il gruppo.

- Lo switch acquisisce il messaggio IGMP Leave dall'host A.
- Lo switch esegue una query IGMP specifica del gruppo per il gruppo su quella porta (e solo su quella porta).
- Se lo switch non riceve un rapporto, elimina questa porta dalla voce. Se riceve una risposta da tale porta, non esegue alcuna operazione e scarta il permesso.
- L'host B è ancora interessato dal gruppo su tale switch. Questa non è l'ultima porta non router

della voce. Pertanto, lo switch non inoltra il messaggio Leave.

Si supponga ora che l'host B desideri uscire dal gruppo e che l'host B sia l'ultimo utente interessato dal gruppo in questo segmento.

- Lo switch acquisisce il messaggio IGMP Leave dall'host A.
- Lo switch esegue una query IGMP specifica per il gruppo su quella porta.
- Se lo switch non riceve un rapporto, elimina questa porta dalla voce.
- Questa è l'ultima porta non router per quel GDA. Lo switch inoltra il messaggio IGMP Leave a tutte le porte del router e rimuove la voce dalla relativa tabella.

Interazione IGMP/CGMP

In alcune reti, a causa di limitazioni hardware, potrebbe non essere possibile eseguire lo snooping IGMP su tutti gli switch. In questo caso, potrebbe essere necessario eseguire il protocollo CGMP su alcuni switch della stessa rete.

Si noti che si tratta di un caso particolare. Lo switch con snooping IGMP rileva i messaggi CGMP e rileva che alcuni switch nella rete eseguono CGMP. Pertanto, passa a una modalità IGMP-CGMP speciale e disabilita il report proxy. Ciò è assolutamente necessario per il corretto funzionamento di CGMP, in quanto i router utilizzano l'indirizzo MAC di origine del report IGMP per creare un join CGMP. I router che eseguono CGMP devono visualizzare tutti i report IGMP, quindi il report proxy deve essere disabilitato. I report inviati al router devono essere solo quelli strettamente necessari per lo snooping IGMP.

Rete solo origine multicast

Se il segmento contiene un solo server multicast (origine multicast) e nessun client, è possibile che si verifichi una situazione in cui non sono presenti pacchetti IGMP in quel segmento, ma il traffico multicast è elevato. In questo caso, lo switch inoltra semplicemente il traffico proveniente dal gruppo a tutti gli utenti del segmento. Fortunatamente, uno switch con snooping IGMP è in grado di rilevare questi flussi multicast e aggiunge una voce multicast per quel gruppo solo con la porta del router. Queste voci sono contrassegnate internamente come `mcast_source_only` e vengono eliminate ogni 5 minuti o quando la porta del router scompare. Notare che anche dopo questo invecchiamento, l'indirizzo viene riacquisito in pochi secondi se il traffico continua. Durante il periodo di riapprendimento, si possono verificare momentaneamente inondazioni sulla VLAN. Per evitare questo problema e mantenere le voci, utilizzare il **set igmp flooding enable | disable** Dopo aver disabilitato l'flooding, lo switch non invecchia le voci relative solo alla sorgente.

Limitazioni

Come con CGMP, i GDA che fanno riferimento a un MAC che rientra nell'intervallo 01-00-5e-00-00-xx non vengono mai potati dallo snooping IGMP.

Configurazione dello snooping IGMP sugli switch Cisco

Per abilitare/disabilitare lo snooping IGMP, eseguire il comando seguente:

- **set igmp**

Per configurare il router multicast (statico), eseguire il comando seguente:

- **set multicast router**
- **clear multicast router *port* | *all*>**

Per monitorare e controllare le statistiche IGMP, eseguire i seguenti comandi:

- **show igmp statistics**
- **show multicast router**

Esempio pratico di snooping IGMP

L'impostazione di questo esempio è simile a quella del test CGMP, utilizzata in precedenza in questo documento. L'unica differenza è che le porte 3/2 e 3/3 sono entrambe connesse alla stessa VLAN e sono entrambe configurate dal client per unirsi al gruppo 24.10.10.10.

Nell'esempio seguente vengono illustrate diverse manipolazioni, vengono esaminate le operazioni eseguite dallo switch e l'output risultante. Nell'esempio seguente, *lo switch B* è uno switch Catalyst 5500 con snooping IGMP e il router *A* è il router multicast collegato alla porta 3/1.

1. Abilitare lo snooping IGMP sullo switch e verificare il risultato emettendo il comando **debug** Ogni insieme di voci è stato aggiunto al **show cam sys** consentendo il rilevamento della porta del router tramite PIM, MOSPF e così via.

```
Switch_B (enable)  set igmp en

MCAST-IGMP: Set Sys Entries
MCAST-SYS-ENTRIES: Add system Entries in vlan 1
MCAST-IGMP: Set Sys Entries
MCAST-SYS-ENTRIES: Add system Entries in vlan 2
MCAST-IGMP: Set Sys Entries
MCAST-SYS-ENTRIES: Add system Entries in vlan 3

IGMP feature for IP multicast enabled

Switch_B (enable) show cam sys
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN  Dest MAC/Route Des [CoS]  Destination Ports or VCs / [Protocol Type]
----  ------------------ -----  -------------------------------------------
1     00-10-2f-00-14-00  #          7/1
1     00-e0-fe-4b-f3-ff  #          1/9
1     01-00-0c-cc-cc-cc  #          1/9
1     01-00-0c-cc-cc-cd  #          1/9
1     01-00-0c-dd-dd-dd  #          1/9
1     01-00-0c-ee-ee-ee  #          1/9
1     01-00-5e-00-00-01  #          1/9
1     01-00-5e-00-00-04  #          1/9
1     01-00-5e-00-00-05  #          1/9
1     01-00-5e-00-00-06  #          1/9
1     01-00-5e-00-00-0d  #          1/9
1     01-80-c2-00-00-00  #          1/9
1     01-80-c2-00-00-01  #          1/9
2     00-10-2f-00-14-00  #          7/1
2     01-00-0c-cc-cc-cc  #          1/9
2     01-00-0c-cc-cc-cd  #          1/9
2     01-00-0c-dd-dd-dd  #          1/9
2     01-00-5e-00-00-01  #          1/9
2     01-00-5e-00-00-04  #          1/9
2     01-00-5e-00-00-05  #          1/9
2     01-00-5e-00-00-06  #          1/9
2     01-00-5e-00-00-0d  #          1/9
```

2. Lo switch riceve un pacchetto PIMv2 dal router Router_A e aggiunge la porta del router.

```
MCAST-IGMPQ:recvd a PIM V2 packet of type HELLO on the port 3/1 vlanNo 2
MCAST-ROUTER: Adding port 3/1, vlanNo 2
MCAST-ROUTER: Creating RouterPortTimer for  port 3/1, vlanNo 2
MCAST-IGMPQ:recvd a PIM V2 packet of type HELLO on the port 3/1 vlanNo 3
MCAST-ROUTER: Adding port 3/1, vlanNo 3
MCAST-ROUTER: Creating RouterPortTimer for  port 3/1, vlanNo 3

Switch_B (enable) show multi router
CGMP disabled
IGMP enabled

Port       Vlan
---------  ----------------
 3/1       2-3

Total Number of Entries = 1
'*' - Configured
Switch_B (enable)
```

3. Collegare un nuovo host nel gruppo 24.10.10.10 (sulla porta 3/2). Questo host invia un rapporto di appartenenza IGMP. Il report viene ricevuto, scaricato dallo switch, viene aggiunta la voce e il report IGMP viene inoltrato al router.**Su switch_B**

```
MCAST-IGMPQ:recvd an IGMP V2 Report on the port 3/2 vlanNo 3
      GDA 224.10.10.10
MCAST-RELAY:Relaying packet on port 3/1 vlanNo 3
MCAST-SEND: Inband Transmit Succeeded for IGMP RELAY msg on port 3/1
      vlanNo 3

Switch_B (enable) show cam static
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN  Dest MAC/Route Des [CoS] Destination Ports or VCs / [Protocol Type]
----  ------------------ ----- -------------------------------------------
3     01-00-5e-0a-0a-0a         3/1-2
```

4. Aggiungere un altro utente nella VLAN 3 sulla porta 3/3, come mostrato di seguito.

```
Switch_B (enable) show cam static

  * = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.

  X = Port Security Entry

  VLAN Dest MAC/Route Des [CoS] Destination Ports or VCs / [Protocol Type]
  ---- ------------------ ----- -------------------------------------------
  3    01-00-5e-0a-0a-0a         3/1-3
```

5. Remove port 3/2. La porta 3/2 invia un messaggio IGMP Leave; lo switch invia una query IGMP specifica del gruppo sulla porta 3/2 e avvia un timer. Quando il timer scade senza ricevere una risposta, la porta viene eliminata dal gruppo.

```
MCAST-IGMPQ:recvd an IGMP Leave on the port 3/2 vlanNo 3 GDA 224.10.10.10
MCAST-IGMPQ-LEAVE:router_port_tbl[vlanNo].QueryTime = 0
MCAST-DEL-TIMER: Deletion Timer Value set to Random Value  1
MCAST-SEND:Transmitting IGMP Mac Based GS Query msg on port 3/2 vlanNo 3
```

```
MCAST-SEND:  Transmit Succeeded for IGMP Group Specific Query msg on port 3/2 vlanNo 3
MCAST-TIMER:IGMPLeaveTimer expired on port 3/2 vlanNo 3 GDA 01-00-5e-0a-0a-0a
MCAST-TIMER:IGMPLeaveTimer:delete leave timer


Switch_B (enable) show cam static
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN Dest MAC/Route Des [CoS] Destination Ports or VCs / [Protocol Type]
---- ------------------ ----- -------------------------------------------
3    01-00-5e-0a-0a-0a         3/1,3/3
```

6. L'host sulla porta 3/3 lascia il gruppo e invia un messaggio di abbandono IGMP. L'unica differenza rispetto al punto precedente è che il messaggio IGMP Leave viene inoltrato alla porta del router.

```
MCAST-IGMPQ:recvd an IGMP Leave on the port 3/3 vlanNo 3 GDA 224.10.10.10
MCAST-SEND:Transmitting IGMP Mac Based GS Query msg on port 3/3 vlanNo 3
MCAST-SEND:  Transmit Succeeded for IGMP Group Specific Query msg on
             port 3/3 vlanNo 3
MCAST-TIMER:IGMPLeaveTimer expired on port 3/3 vlanNo 3 GDA
             01-00-5e-0a-0a-0a
MCAST-TIMER:IGMPLeaveTimer expiry: Transmit IGMP Leave on port 3/1
             vlanNo 3
MCAST-SEND:Transmitting IGMP Leave msg on port 3/1 vlanNo 3
MCAST-SEND: Inband Transmit Succeeded for IGMP Leave Message on port 3/1
             vlanNo 3
MCAST-TIMER:IGMPLeaveTimer:delete leave timer
```

La configurazione della subnet è ora di nuovo all'inizio, con il relativo stato indicato al passaggio 1. La voce multicast è scomparsa dal **show cam static** output del comando.

Per terminare, visualizzare un esempio di **show igmp static** come mostrato di seguito.

```
Switch_B (enable) show igmp stat 2
IGMP enabled

IGMP statistics for vlan 2:
Total valid pkts rcvd:           329
Total invalid pkts recvd         0
General Queries recvd            82
Group Specific Queries recvd     0
MAC-Based General Queries recvd  0
Leaves recvd                     0
Reports recvd                    82
Queries  Xmitted                 0
GS Queries Xmitted               0
Reports Xmitted                  0
Leaves Xmitted                   0
Failures to add GDA to EARL      0
Topology Notifications rcvd      0

Switch_B (enable) show igmp stat 3
IGMP enabled

IGMP statistics for vlan 3:
Total valid pkts rcvd:           360
Total invalid pkts recvd         0
```

```
General Queries recvd            93
Group Specific Queries recvd     6
MAC-Based General Queries recvd  0
Leaves recvd                     11
Reports recvd                    64
Queries  Xmitted                 0
GS Queries Xmitted               14
Reports Xmitted                  0
Leaves Xmitted                   10
Failures to add GDA to EARL      0
Topology Notifications rcvd      1
Switch_B (enable)
```

Informazioni correlate

- Matrice di supporto per switch Multicast Catalyst
- Pagina di supporto per il multicast IP
- Supporto tecnologico Cisco
- Supporto dei prodotti Cisco
- Documentazione e supporto tecnico – Cisco Systems