Risoluzione dei problemi di traffico multicast nella stessa VLAN sugli switch Catalyst

Sommario

Introduzione

In questo documento viene descritto come risolvere un errore di un'applicazione multicast quando viene distribuita nella stessa VLAN tra switch Catalyst.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Catalyst 6500 con Supervisor Engine 720 con software Cisco IOS® versione 12.2(18)SXD5
- Catalyst 3750 con software Cisco IOS versione 12.2(25)SEB2 image

- Qualsiasi switch Catalyst con software Cisco IOS e che supporta anche lo snooping IGMP (Internet Group Management Protocol)

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

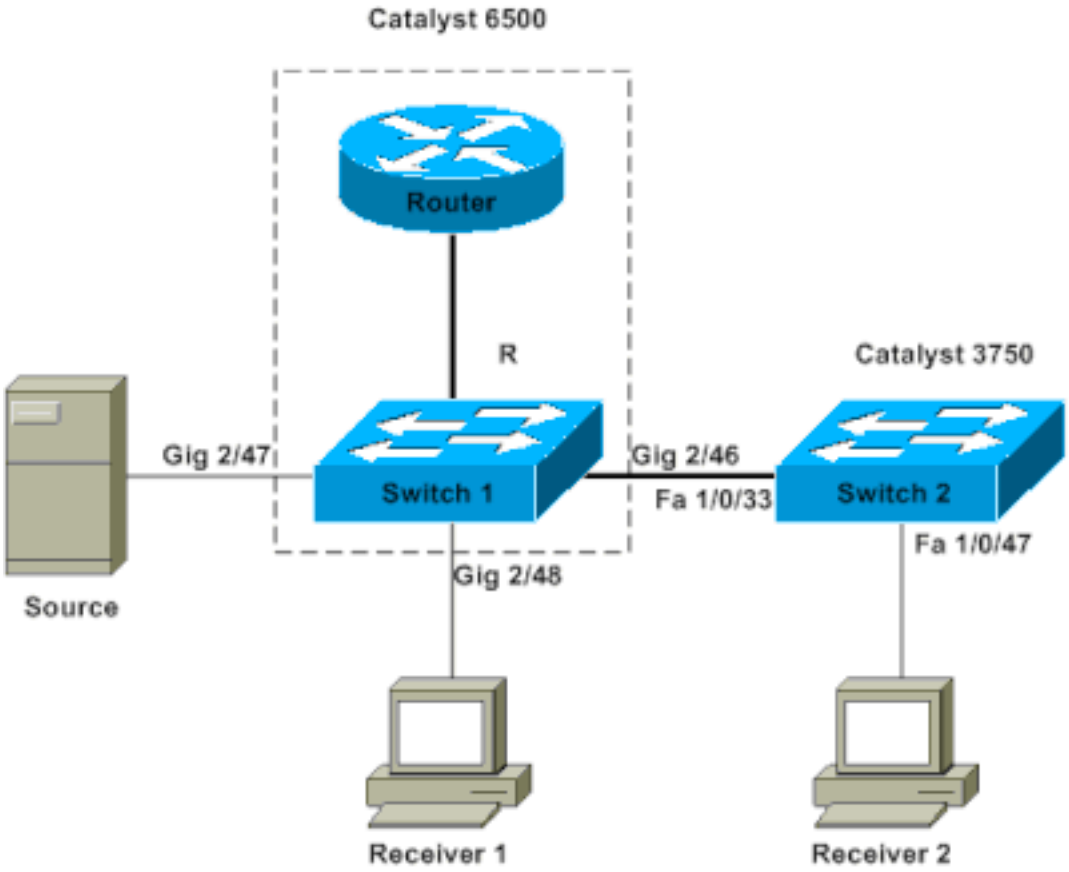
Inoltre, alcuni server/applicazioni che utilizzano pacchetti multicast per l'operazione cluster/elevata disponibilità potrebbero non funzionare correttamente se gli switch non vengono configurati correttamente. Questo argomento viene trattato anche in questo articolo.

> **Nota**: per individuare questi switch, consultare la sezione *IGMP Snooping Feature Catalyst Switch Support Matrix* del documento Multicast Catalyst Switch Support Matrix.

Problema

Il traffico multicast non passa attraverso gli switch Catalyst, neanche nella stessa VLAN. La figura 1 illustra questo scenario.

Figura 1 - Configurazione della rete con origine multicast e ricevitori



Esempio di rete

L'origine multicast è collegata allo switch 1, uno switch Catalyst 6500 con Supervisor Engine 720 con software Cisco IOS. Il ricevitore 1 è collegato allo switch 1, il ricevitore 2 allo switch 2. Lo switch 2 è un Catalyst 3750. Tra lo switch 1 e lo switch 2 è presente un collegamento di layer 2, accesso o trunk.

In questa configurazione, il ricevitore 1, che si trova sullo stesso switch della sorgente, riceve il flusso multicast senza problemi. Tuttavia, il ricevitore 2 non *riceve* alcun traffico multicast. Questo documento ha lo scopo di risolvere il problema.

Revisione dei concetti principali del multicast

Prima di esplorare la soluzione e le diverse opzioni disponibili, è necessario conoscere chiaramente alcuni concetti chiave del multicast di layer 2. In questa sezione vengono descritti i concetti di base.

> **Nota**: questa sezione fornisce una spiegazione molto semplice e diretta che si concentra solo su questo particolare problema. Per una spiegazione dettagliata dei termini, vedere la sezione **Informazioni correlate** alla fine di questo documento.

IGMP

IGMP è un protocollo che consente agli host terminali (ricevitori) di informare un router multicast (interrogante IGMP) dell'intenzione dell'host terminale di ricevere un particolare traffico multicast. Si tratta quindi di un protocollo che viene eseguito tra un router e gli host terminali e consente:

- I router devono chiedere agli host finali se hanno bisogno di un particolare flusso multicast

(query IGMP)
- Gli host finali possono comunicare o rispondere al router se cercano un particolare flusso multicast (report IGMP)

Snooping IGMP

Lo snooping IGMP è un meccanismo che vincola il traffico multicast solo alle porte a cui sono collegati dei ricevitori. Il meccanismo migliora l'efficienza perché consente a uno switch di layer 2 di inviare selettivamente pacchetti multicast solo sulle porte che li richiedono. Senza lo snooping IGMP, lo switch invia i pacchetti a tutte le porte. Lo switch "resta in ascolto" per lo scambio di messaggi IGMP da parte del router e degli host terminali. In questo modo, lo switch crea una tabella di snooping IGMP che contiene un elenco di tutte le porte che hanno richiesto un particolare gruppo multicast.

Porta Mrouter

La porta del router è semplicemente la porta dal punto di vista dello switch che si connette a un router multicast. La presenza di almeno una porta del router è assolutamente essenziale per il funzionamento dello snooping IGMP tra gli switch. Per ulteriori informazioni, vedere la sezione Comprendere il problema e le relative soluzioni di questo documento.

Multicast a L2

Qualsiasi traffico IP versione 4 (IPv4) con IP di destinazione compreso tra 224.0.0.0 e 239.255.255.255 è un flusso multicast. Tutti i pacchetti multicast IPv4 vengono mappati a un indirizzo MAC IEEE predefinito con formato 01.00.5e. *xx* . *xx* . *xx*.

> **Nota**: lo snooping IGMP funziona solo se l'indirizzo MAC multicast è mappato su questo intervallo MAC compatibile con IEEE. Alcuni intervalli multicast riservati sono esclusi da quelli sottoposti a snooping per progettazione. Se un pacchetto multicast non conforme viene inviato a una rete commutata, il pacchetto viene trasmesso su tutta la VLAN, ossia viene trattato come traffico broadcast.

Comprendere il problema e le relative soluzioni

Per impostazione predefinita, sugli switch Catalyst lo snooping IGMP è abilitato. Con lo snooping IGMP, lo switch snooping (o resta in ascolto) dei messaggi IGMP su tutte le porte. Lo switch crea una tabella di snooping IGMP che fondamentalmente mappa un gruppo multicast a tutte le porte dello switch che lo hanno richiesto.

Si supponga che, senza alcuna configurazione precedente, il ricevitore 1 e il ricevitore 2 abbiano segnalato la loro intenzione di ricevere un flusso multicast per 239.239.239.239 che mappa all'indirizzo MAC multicast L2 di 01.00.5e.6f.ef.ef. Sia lo switch 1 che lo switch 2 creano una voce nelle rispettive tabelle di snooping per questi ricevitori in risposta ai rapporti IGMP generati dai ricevitori. Lo switch 1 entra nella tabella delle porte Gigabit Ethernet 2/48 e lo switch 2 entra nella tabella delle porte Fast Ethernet 1/0/47.

> **Nota**: a questo punto, l'origine multicast non ha avviato il traffico e nessuno degli switch è a conoscenza della porta del router dello switch.

Quando l'origine sullo switch 1 inizia a trasmettere il traffico multicast, lo switch 1 ha "visto" il report IGMP del ricevitore 1. Di conseguenza, lo switch 1 fornisce la porta di uscita multicast Gigabit Ethernet 2/48. Tuttavia, poiché lo switch 2 ha "assorbito" il report IGMP dal ricevitore 2 come parte del processo di snooping IGMP, lo switch 1 non vede un report IGMP (richiesta multicast) sulla porta Gigabit Ethernet 2/46. Di conseguenza, lo switch 1 non invia traffico multicast allo switch 2. Pertanto, il ricevitore 2 non riceve mai traffico multicast, anche se il ricevitore 2 si trova sulla stessa VLAN ma solo su uno switch diverso rispetto alla sorgente multicast.

La ragione di questo problema è che lo snooping IGMP non è realmente supportato su nessuna piattaforma Catalyst senza un router. Il meccanismo si "interrompe" in assenza di una porta del router. Se si desidera risolvere il problema con questa soluzione, è necessario che gli switch siano a conoscenza o conoscano la presenza di una porta del router. Per ulteriori informazioni sulla procedura, vedere la sezione Soluzioni di questo documento. Per risolvere il problema, occorre scoprire come la presenza di una porta del router sugli switch.

Fondamentalmente, quando gli switch vengono a conoscenza o conoscono staticamente una porta del router, si verificano due situazioni critiche:

- Lo switch "inoltra" i rapporti IGMP dai ricevitori alla porta del router, il che significa che i rapporti IGMP vanno verso il router multicast. Lo switch non inoltra tutti i report IGMP. Al contrario, lo switch invia solo alcuni dei report al router. Ai fini della presente discussione, il numero di relazioni non è importante. Il router multicast deve solo sapere se esiste almeno un ricevitore ancora interessato al downstream multicast. Per effettuare la determinazione, il router multicast riceve i rapporti IGMP periodici in risposta alle proprie query IGMP.
- In uno scenario multicast solo sorgente, in cui nessun ricevitore si è ancora "unito" a un router, lo switch invia solo il flusso multicast fuori dalla porta del router.

Quando gli switch conoscono la porta del router, lo switch 2 invia il rapporto IGMP che lo switch ha ricevuto dal ricevitore 2 alla porta del router. Questa porta è Fast Ethernet 1/0/3. Lo switch 1 riceve questo report IGMP sulla porta dello switch Gigabit Ethernet 2/46. Dal punto di vista dello switch 1, lo switch ha ricevuto solo un altro report IGMP. Lo switch aggiunge tale porta nella relativa tabella di snooping IGMP e inizia a inviare il traffico multicast anche su tale porta. A questo punto, entrambi i ricevitori ricevono il traffico multicast richiesto e l'applicazione funziona come previsto.

Per informazioni su come gli switch identificano la porta del router in modo che lo snooping IGMP funzioni come previsto in un ambiente semplice, vedere la sezione Soluzioni per le risposte.

Soluzioni

Utilizzate queste soluzioni per risolvere il problema.

Soluzione 1: abilitare PIM sull'interfaccia router/VLAN di layer 3

Tutte le piattaforme Catalyst possono conoscere dinamicamente la porta del router. Gli switch ascoltano passivamente gli hellop PIM (Protocol Independent Multicast) o i messaggi di query IGMP inviati periodicamente da un router multicast.

Nell'esempio, viene configurata l'interfaccia virtuale con commutazione VLAN 1 (SVI) sullo switch Catalyst 6500 con `ip pim sparse-dense-mode` .

```
Switch1#show run interface vlan 1
!
interface Vlan1
 ip address 10.1.1.1 255.255.255.0
 ip pim sparse-dense-mode
end

Switch 1 now reflects itself (Actually the internal router port) as an Mrouter port.

Switch1#show ip igmp snooping mrouter
vlan            ports
-----+---------------------------------------
   1  Router

Switch 2 receives the same PIM hellos on its Fa 1/0/33 interface. So it assigns that
port as its Mrouter port.

Switch2#show ip igmp snooping mrouter
Vlan    ports
----    -----
   1    Fa1/0/33(dynamic)
```

Soluzione 2: abilitare la funzione IGMP Querier su uno switch Catalyst di layer 2

Il querier IGMP è una funzione relativamente nuova sugli switch di layer 2. Quando una rete/VLAN non ha un router in grado di assumere il ruolo di router multicast e fornire il rilevamento del router sugli switch, è possibile attivare la funzione Query IGMP. Questa funzione consente allo switch di layer 2 di fungere da proxy per un router multicast e di inviare query IGMP periodiche in tale rete. In questo modo, lo switch viene considerato una porta router. Gli altri switch della rete definiscono semplicemente le rispettive porte del router come interfaccia su cui hanno ricevuto questa query IGMP.

```
Switch2(config)#ip igmp snooping querier

Switch2#show ip igmp snooping querier
Vlan      IP Address     IGMP Version   Port
-----------------------------------------------------------
1         10.1.1.2        v2             Switch
```

Lo switch 1 ora vede che la porta Gig 2/46 è collegata allo switch 2 come porta del router.

```
Switch1#show ip igmp snooping mrouter
vlan            ports
-----+---------------------------------------
   1  Gi2/46
```

Quando l'origine sullo switch 1 inizia a trasmettere il traffico multicast, lo switch 1 inoltra il traffico multicast al ricevitore 1 rilevato tramite snooping IGMP (ossia, porta di uscita Gig 2/48) e alla porta del router (ossia, porta di uscita Gig 2/46).

Soluzione 3: configurare la porta del router statico sullo switch

Il traffico multicast si interrompe all'interno della stessa VLAN di layer 2 per mancanza di una porta del router sugli switch. Per approfondire questo argomento, consultare la sezione Comprendere il problema e le relative soluzioni. Se si configura in modo statico una porta del router su tutti gli

switch, i report IGMP possono essere inoltrati nella VLAN a tutti gli switch. Questo permette di realizzare la multicast. Nell'esempio, è necessario configurare staticamente lo switch Catalyst 3750 in modo che abbia Fast Ethernet 1/0/33 come porta del router.

Nell'esempio, è necessaria una porta statica del router solo sullo switch 2:

```
Switch2(config)#ip igmp snooping vlan 1 mrouter interface fastethernet 1/0/33

Switch2#show ip igmp snooping mrouter
Vlan    ports
----    -----
   1    Fa1/0/33(static)
```

Soluzione 4: configurare le voci MAC multicast statiche su tutti gli switch

Èpossibile creare una voce statica CAM (Content-Addressable Memory) per l'indirizzo MAC multicast su tutti gli switch per tutte le porte del ricevitore e le porte dello switch a valle. Ogni switch rispetta le regole di immissione statiche della CAM e invia il pacchetto a tutte le interfacce specificate nella tabella CAM. Si tratta della soluzione meno scalabile per un ambiente con numerose applicazioni multicast.

```
Switch1(config)#mac-address-table static 0100.5e6f.efef vlan 1 interface
gigabitethernet 2/46 gigabitethernet 2/48

!--- Note: This command should be on one line. Switch1#show mac-address-table multicast vlan 1

 vlan   mac address     type    learn qos              ports
-----+---------------+--------+-----+---+--------------------------------
   1  0100.5e6f.efef    static  Yes          -    Gi2/46,Gi2/48


Switch2(config)#mac-address-table static 0100.5e6f.efef vlan 1 interface
fastethernet 1/0/47

!--- Note: This command should be on one line. Switch2#show mac-address-table multicast vlan 1
Vlan    Mac Address       Type       Ports
----    -----------       ----       -----
   1    0100.5e6f.efef    USER        Fa1/0/47
```

Soluzione 5: disabilitare lo snooping IGMP su tutti gli switch

Se si disabilita lo snooping IGMP, tutti gli switch considerano il traffico multicast come traffico broadcast. Il traffico viene instradato a *tutte le* porte della VLAN, a prescindere dal fatto che le porte abbiano o meno ricevitori interessati per il flusso multicast.

```
Switch1(config)#no ip igmp snooping

Switch2(config)#no ip igmp snooping
```

Informazioni correlate

- Multicast in una rete campus: snooping CGMP e IGMP
- Matrice di supporto per gli switch Multicast Catalyst
- Supporto IP multicast

- Note tecniche per la risoluzione dei problemi relativi al multicast IP
- Guida alla risoluzione dei problemi del multicast IP
- Supporto tecnico e download Cisco

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).