Resolución de problemas de IGMP para implementaciones NLB en switches Catalyst 9000

Contenido

[Introducción](#)
[Prerequisites](#)
[Antecedentes](#)
[Configurar](#)
[Troubleshoot](#)
[Información Relacionada](#)

Introducción

Este documento describe cómo se comporta la función IGMP en los switches Catalyst de la serie 9000 en una implementación de Equilibrador de carga de red (NLB) de Microsoft.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Modos de funcionamiento de Microsoft NLB
- Multidifusión IGMP

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Catalyst 9200
- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Catalyst 9600

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

NLB es una tecnología de clúster disponible en todos los sistemas de la familia Windows 2000 Server y Windows 2003 Server. Proporciona una única dirección IP virtual para todos los clientes como dirección IP de destino para todo el clúster.

NLB se puede utilizar para distribuir las solicitudes de cliente a través de un conjunto de servidores. Con el fin de garantizar que los clientes experimenten niveles de rendimiento aceptables, NLB proporciona la

capacidad de agregar servidores adicionales para ampliar aplicaciones sin estado (como servidores web basados en IIS) a medida que aumenta la carga del cliente. Además, reduce el tiempo de inactividad provocado por un mal funcionamiento del servidor.

Puede configurar NLB para que funcione en uno de estos tres modos:

- Modo unidifusión
- Modo de multidifusión
- Modo de protocolo de administración de grupos de Internet (IGMP)

> **Sugerencia**: Las implementaciones de modo unidifusión y modo multidifusión tienen la misma configuración y verificación descritas en el documento Ejemplo de configuración de switches Catalyst para el equilibrio de carga de red de Microsoft

---

Este documento se centra en el modo de protocolo de administración de grupos de Internet (IGMP).

Mejores medidas

Los switches Catalyst de la serie 9000 indagan los encabezados de capa 3 de los paquetes IGMP para llenar la tabla de indagación. Debido a cómo se debe configurar NLB en el switch mediante una MAC de multidifusión estática, la tabla de detección IGMP no se rellena y se produce una inundación en la VLAN de destino. En otras palabras, la indagación IGMP en Catalyst 9000 no contiene automáticamente la inundación multicast cuando el servidor NLB está en modo IGMP (el reenvío en Catalyst 9000 se basa en IP multicast y no en dirección MAC multicast).

> **Nota**: En Catalyst 9000, la inundación ocurre en los tres modos de NLB. La inundación no ocurre en la VLAN del usuario, dado que el destino de los paquetes tiene que ser su gateway predeterminado. Solo después de que el encabezado se reescriba en la VLAN de destino, se produce la inundación.

Por lo tanto, tenga en cuenta estas prácticas recomendadas para implementaciones satisfactorias:

- Utilice una VLAN dedicada para restringir la inundación sólo al clúster NLB.
- Utilice entradas MAC estáticas para limitar los puertos en los que se produce la inundación dentro de la VLAN NLB.

Modo IGMP

En este modo, la dirección MAC virtual del clúster NLB se encuentra dentro del intervalo de la Autoridad de números asignados de Internet (IANA) y comienza por 0100.5exx.xxxx. IGMP Snooping función configurada en el switch no programa en la tabla de direcciones MAC la dirección MAC de multidifusión virtual del clúster. Dado que esta programación dinámica está ausente, el tráfico multicast recibido por el switch desde el clúster NLB se inunda a todos los puertos miembros de la misma VLAN. Id. de error de Cisco CSCvw18989.

Para las topologías en las que los servidores NLB están en una VLAN diferente a la de los usuarios, dado que la dirección IP virtual del clúster utiliza una dirección MAC de multidifusión, no se puede alcanzar fuera de la subred local. Para resolver esto, debe configurar una entrada ARP estática en cada dispositivo con una interfaz de capa 3 en la VLAN del clúster.

La función IGMP Snooping en los switches Catalyst de la serie 9000 no utiliza la dirección MAC de multidifusión para el reenvío. Utilizan la dirección IP de multidifusión, por lo que no puede programar automáticamente la dirección MAC de multidifusión en la tabla MAC como hacen otras plataformas

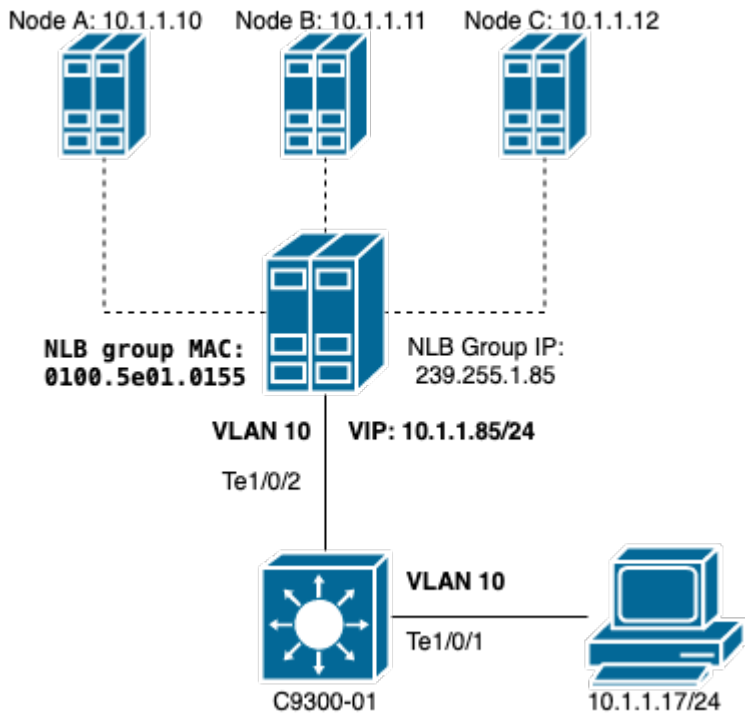
heredadas (como Catalyst serie 6000). Todas las plataformas nuevas utilizan el método de reenvío de direcciones IP de multidifusión para evitar el problema de superposición de direcciones que se encuentra en los switches heredados.

> **Nota**: Una dirección MAC de multidifusión Ethernet tiene cierto solapamiento. La misma dirección MAC se asigna a 32 grupos de multidifusión diferentes. Si un usuario en un segmento Ethernet se suscribe al grupo multicast 225.1.1.1 y otro usuario se suscribe a 230.1.1.1, ambos usuarios reciben ambos flujos multicast (la dirección MAC es la misma 01-00-5e-01-01-01). En la ingeniería de redes multidifusión en segmentos LAN, este solapamiento debe vigilarse y diseñarse específicamente para evitar el problema.

Configurar

Origen y destino en la misma VLAN

Diagrama de la red



Esta sección describe cómo configurar NLB cuando el clúster y los usuarios están en la misma VLAN.

1. Compruebe que se ha creado la VLAN NLB. Se sugiere tener una VLAN dedicada para el tráfico NLB debido a la inundación.

<#root>

C9300-01#

show vlan id 10

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
10   NLB                              active    Te1/0/1, Te1/0/2, Te1/0/3
```

```
VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
10   enet  100010     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

2. CConfigure una entrada de dirección MAC estática para los puertos que deben obtener este tráfico NLB. Este comando debe incluir todos los puertos troncales o puertos de acceso en la ruta hacia el clúster NLB en la VLAN NLB. En el diagrama, solo hay un trayecto hacia el NLB a través de Tengig1/0/2.

<#root>

C9300-01(config)#

mac address-table static 0100.5e01.0155 vlan 10 interface TenGigabitEthernet 1/0/2

C9300-01#

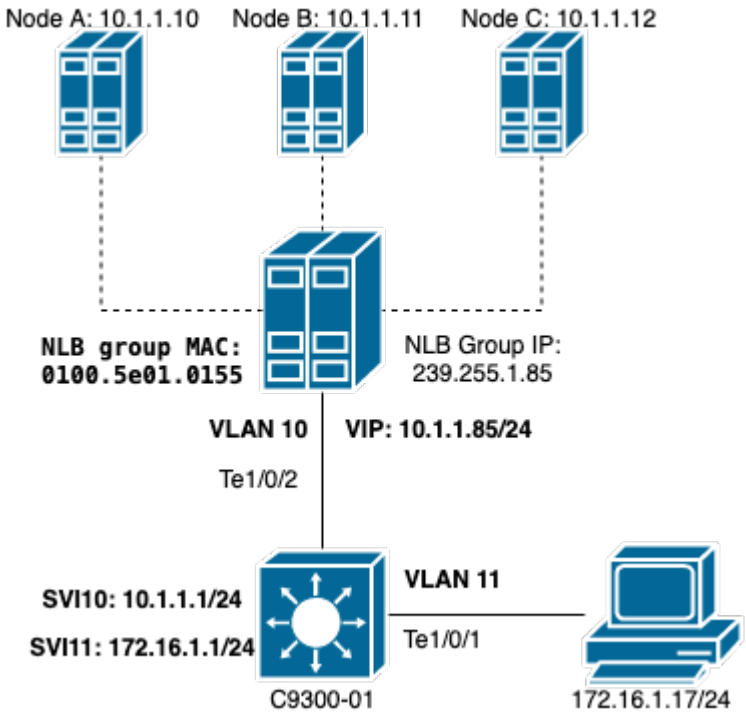
show run | in mac

```
mac address-table static 0100.5e01.0155 vlan 10 interface TenGigabitEthernet1/0/2
```

> **Nota**: Puede tener tantos puertos asignados en la entrada de dirección MAC estática como necesite. Este mapa de puertos reduce la inundación esperada dentro de la VLAN del NLB. En el ejemplo, la entrada MAC estática puede evitar que el tráfico hacia el clúster NLB se inunde con Te1/0/3.

Origen y destino en VLAN diferentes

Diagrama de la red



Esta sección describe cómo configurar NLB cuando el clúster y los usuarios están en VLAN diferentes.

1. Configure la VLAN de NLB y una dirección IP para que sean el gateway predeterminado del clúster NLB.

<#root>

C9300-01#

show vlan id 10

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
10   NLB                              active    Te1/0/2, Te1/0/3

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
10   enet  100010     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------

C9300-01#
```

show run interface vlan 10

```
Building configuration...

Current configuration : 59 bytes
!
interface Vlan10
 ip address 10.1.1.1 255.255.255.0
```

```
end
```

2. Configure una entrada ARP estática para la dirección IP virtual de los servidores del clúster NLB. El ARP estático debe configurarse en todos los dispositivos de capa 3 que tengan una interfaz virtual de switch (SVI) en la VLAN del clúster. El propósito del ARP estático es permitir que el switch tenga la información de reescritura necesaria para enviar paquetes enrutados hacia la VLAN NLB.

<#root>

C9300-01(config)#

arp 10.1.1.85 0100.5e01.0155 arpa

3. Verifique la VLAN de usuario creada en la capa de acceso y su gateway predeterminado. Es importante que configure el gateway predeterminado en ambas partes. (clúster NLB y usuarios).

<#root>

C9300-01#

show vlan id 11

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
11   Users2                           active    Te1/0/1, Te1/0/4

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
11   enet  100011     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

C9300-01#

show run interface vlan 11

```
Building configuration...

Current configuration : 59 bytes
!
interface Vlan11
 ip address 172.16.1.1 255.255.255.0
end
```

Nota: Cualquier paquete que se rutee después de la reescritura del encabezado MAC cuyo MAC de destino no se aprende en la SVI de salida, el paquete se inunda en la VLAN correspondiente. Para mitigar la inundación, debe crear un gateway y una VLAN independiente solo para los servidores

---

NLB. Si no desea configurar una VLAN dedicada para el tráfico NLB, puede configurar una entrada de dirección MAC estática para los puertos que deben recibir el tráfico NLB, es decir, **mac address-table static** *0100.5exx.xxxx* **vlan** # **interface** interface

Troubleshoot

1. Compruebe si la dirección MAC estática está configurada en todos los puertos de destino que necesitan reenviar el tráfico al NLB.

<#root>

C9300-01#

show mac address multicast

```
Vlan Mac Address Type Ports
---- ----------- ---- -----
10 0100.5e01.0155 USER Te1/0/2
```

2. En el caso de implementaciones en las que el clúster NLB se encuentra en una subred diferente a la de los clientes, compruebe si hay entradas ARP estáticas que asignen la IP virtual del servidor NLB con su dirección MAC de multidifusión.

<#root>

C9300-01#

show run | in arp

```
arp 10.1.1.85 0100.5e01.0155 ARPA
```

C9300-01#

show ip arp

```
Protocol Address Age (min) Hardware Addr Type Interface
Internet 10.1.1.1 - c4c6.0309.cf46 ARPA Vlan10
Internet 10.1.1.85 - 0100.5e01.0155 ARPA
Internet 172.16.1.1 - c4c6.0309.cf54 ARPA Vlan11
```

3. Haga un ping a la IP del servidor NLB con un tamaño que no se utilice con frecuencia. Borre los controladores del puerto y verifique con varias iteraciones del comando qué tamaño no se ha utilizado tanto.

<#root>

C9300-01#

show controllers ethernet-controller Te1/0/2 | in 1024

```
0 1024 to 1518 byte frames 0 1024 to 1518 byte frames
```

C9300-01#

clear controllers ethernet-controller Te1/0/2

```
HOST#
```

```
ping 10.1.1.85 time 0 rep 1000 size 1024
```

```
Type escape sequence to abort.
Sending 1000, 1024-byte ICMP Echos to 10.1.1.85, timeout is 0 seconds:
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................
Success rate is 0 percent (0/1000)
```

4. Verifique si los pings se han reenviado correctamente fuera del puerto de destino y si la misma prueba de ping se ha inundado a otros puertos. Verifique esto con el mismo comando controllers counters en las diferentes interfaces.

<#root>

```
C9300-01#
```

```
show controllers ethernet-controller Te1/0/1 | in 1024
```

```
 <-- Ingress Host port
0 1024 to 1518 byte frames 1000 1024 to 1518 byte frames
```

```
C9300-01#
```

```
show controllers ethernet-controller Te1/0/2 | in 1024
```

```
 <-- Egress port to NLB
1000 1024 to 1518 byte frames 0 1024 to 1518 byte frames
```

5. Tome capturas de paquetes en el puerto de ingreso con EPC y en el puerto de egreso con SPAN y verifique si el switch está reenviando los datos o no.

<#root>

```
C9300-01#
```

```
monitor capture tac buffer size 10 match any interface Te1/0/1 in
```

```
C9300-01#
```

```
monitor capture tac start
```

```
C9300-01#
```

```
monitor capture tac stop

C9300-01#

monitor capture tac export location flash:DataTraffic.pcap
```

> **Sugerencia**: la función de captura de paquetes integrada (EPC) es fiable cuando los paquetes se reenvían en la dirección de entrada o salida de la capa 2. Sin embargo, si el switch enruta el tráfico y luego lo reenvía al puerto de salida, el EPC no es confiable. Para capturar paquetes en salida después de que se produzca el routing de capa 3, utilice la función Analizador de puertos de switch (SPAN).

<#root>

C9300-01(config)#

```
monitor session 1 source interface Te1/0/2 tx

C9300-01(config)#

monitor session 1 destination interface Te1/0/3 encapsulation replicate


C9300-01#

show monitor session all

Session 1
---------
Type : Local Session
Source Ports :
TX Only : Te1/0/2
Destination Ports : Te1/0/3
Encapsulation : Replicate
Ingress : Disabled
```

Información Relacionada

- **Ejemplo de Configuración de Switches Catalyst para Balanceo de Carga de Red de Microsoft**
- **Asistencia técnica y descargas de Cisco**

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).