Identificar e Solucionar Problemas de IGMP para Implantações de NLB em Switches Catalyst 9000

Contents

Introdução

Este documento descreve como o recurso IGMP nos Catalyst 9000 Series Switches se comporta em uma implantação do Microsoft Network Load Balancer (NLB).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Modos de operação do Microsoft NLB
- Multicast IGMP

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O NLB é uma tecnologia de cluster disponível em todos os sistemas da família Windows 2000 Server e Windows 2003 Server. Ele fornece um único endereço IP virtual para todos os clientes como o endereço IP de destino para todo o cluster.

O NLB pode ser usado para distribuir solicitações de clientes através de um conjunto de servidores. Para garantir que os clientes tenham níveis de desempenho aceitáveis, o NLB oferece a capacidade de adicionar

servidores adicionais para expandir aplicativos stateless (como servidores Web baseados em IIS) à medida que a carga do cliente aumenta. Além disso, reduz o tempo de inatividade causado pelo mau funcionamento do servidor.

Você pode configurar o NLB para funcionar em um destes três modos:

- Modo unicast
- Modo multicast
- modo de Internet Group Management Protocol (IGMP)

> **Dica**: as implantações de modo unicast e multicast têm a mesma configuração e verificação descritas no documento Exemplo de Configuração de Switches Catalyst para Balanceamento de Carga de Rede Microsoft

---

Este documento se concentra no modo Internet Group Management Protocol (IGMP).

Melhores práticas

Os switches Catalyst 9000 Series rastream os cabeçalhos da camada 3 dos pacotes IGMP para preencher a tabela de rastreamento. Devido ao modo como o NLB deve ser configurado no switch usando um MAC multicast estático, a tabela de rastreamento IGMP não é preenchida e ocorre inundação na VLAN de destino. Em outras palavras, o IGMP Snooping no Catalyst 9000 não contém automaticamente a inundação de multicast quando o servidor NLB está no modo IGMP (o encaminhamento no Catalyst 9000 é baseado no IP de multicast e não no endereço MAC de multicast).

> **Observação**: no Catalyst 9000, a inundação ocorre em todos os três modos de NLB. A inundação não ocorre na VLAN do usuário, uma vez que o destino dos pacotes deve ser o gateway padrão. Somente após a regravação do cabeçalho na VLAN de destino, ocorre a inundação.

Portanto, considere estas práticas recomendadas para implantações bem-sucedidas:

- Use uma VLAN dedicada para restringir a inundação apenas para o cluster NLB.
- Utilize entradas MAC estáticas para limitar as portas em que a inundação ocorre dentro da VLAN NLB.

Modo IGMP

Neste modo, o MAC virtual do cluster NLB se enquadra no intervalo IANA (Internet Assigned Numbers Authority) e começa com 0100.5exx.xxxx. O IGMP Snooping O recurso configurado no switch não programa na tabela de endereços MAC o endereço MAC multicast virtual do cluster. Como essa programação dinâmica está ausente, o tráfego multicast recebido pelo switch do cluster NLB é enviado para todas as portas membros da mesma VLAN. ID de bug da Cisco CSCvw18989.

Para as topologias em que os servidores NLB estão em VLAN diferentes dos usuários, como o endereço IP virtual do cluster usa um endereço MAC multicast, ele não pode ser alcançado fora da sub-rede local. Para resolver isso, você deve configurar uma entrada ARP estática em cada dispositivo com uma interface de camada 3 na VLAN do cluster.

O recurso de rastreamento de IGMP nos Catalyst 9000 Series Switches não usa o endereço MAC multicast para encaminhamento. Eles usam o endereço IP multicast, é por isso que ele não pode programar automaticamente o endereço MAC multicast na tabela MAC como outras plataformas legadas fazem (como a série Catalyst 6000). Todas as novas plataformas usam o método de encaminhamento de endereço IP

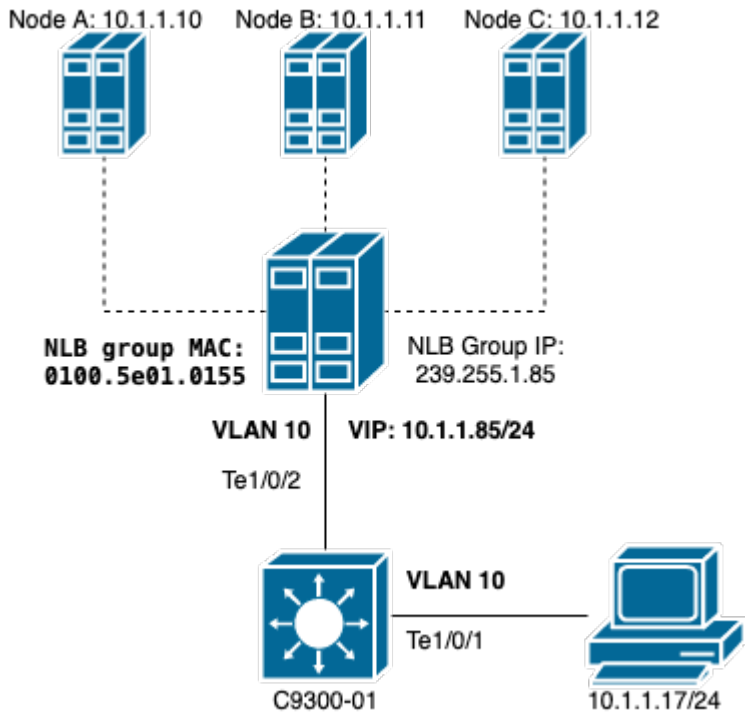
multicast para evitar o problema de sobreposição de endereços encontrado nos switches herdados.

> **Observação**: um endereço MAC de multicast Ethernet tem alguma sobreposição. O mesmo endereço MAC é atribuído a 32 grupos multicast diferentes. Se um usuário em um segmento ethernet se inscrever no grupo multicast 225.1.1.1 e outro usuário se inscrever em 230.1.1.1, ambos os usuários receberão os dois fluxos multicast (o endereço MAC é o mesmo 01-00-5e-01-01-01). Na engenharia de redes multicast em segmentos de LAN, essa sobreposição precisa ser observada e projetada especificamente para evitar o problema.

Configurar

Origem e Destino na mesma VLAN

Diagrama de Rede



Esta seção descreve como configurar o NLB quando o cluster e os usuários estão na mesma VLAN.

1. Verifique se a VLAN NLB foi criada. É recomendável ter uma VLAN dedicada para o tráfego NLB devido à inundação.

<#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 uma entrada de endereço MAC estático para as portas que devem obter esse tráfego NLB. Esse comando deve incluir todas as portas de tronco ou portas de acesso no caminho em direção ao cluster NLB na VLAN NLB. No diagrama, há apenas um caminho em direção ao NLB via Tengig1/0/2.

<#root>

C9300-01(config)#

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

C9300-01#

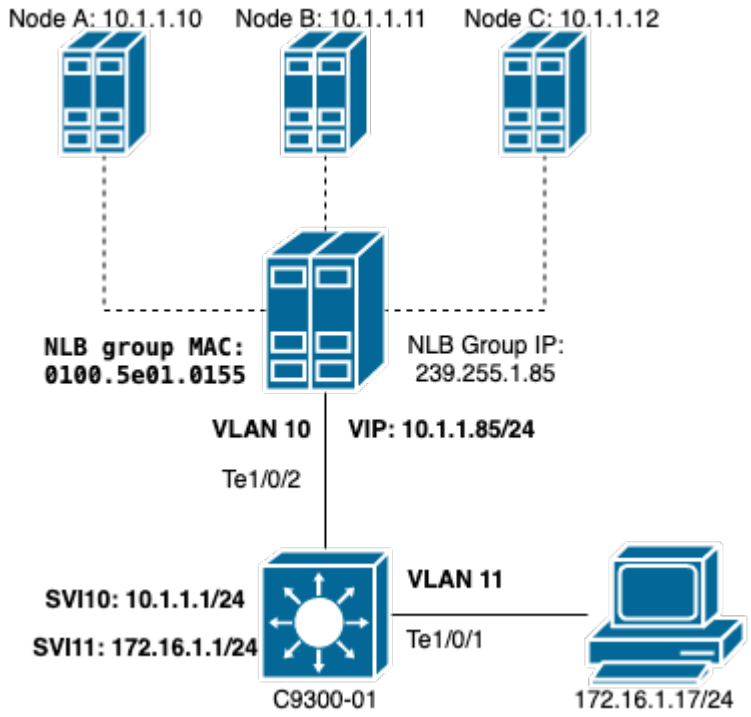
show run | in mac

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

> **Observação**: você pode ter quantas portas mapeadas na entrada de endereço MAC estático forem necessárias. Esse mapa de portas reduz a inundação esperada dentro da VLAN do NLB. No exemplo, a entrada MAC estática pode evitar que o tráfego em direção ao cluster NLB seja despejado de Te1/0/3.

Origem e Destino em VLANs diferentes

Diagrama de Rede



Esta seção descreve como configurar o NLB quando o cluster e os usuários estão em VLANs diferentes.

1. Configure a VLAN NLB e um endereço IP para ser o gateway padrão do cluster 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 uma entrada ARP estática para o endereço IP virtual dos servidores de cluster NLB. O ARP estático deve ser configurado em todos os dispositivos da camada 3 que têm uma interface virtual do switch (SVI) na VLAN do cluster. A finalidade do ARP estático é permitir que o switch tenha as informações de regravação necessárias para enviar pacotes roteados para a VLAN NLB.

<#root>

C9300-01(config)#

arp 10.1.1.85 0100.5e01.0155 arpa

3. Verifique a VLAN de usuário criada na camada de acesso e seu gateway padrão. É importante que você configure o gateway padrão em ambas as partes. (cluster NLB e usuários).

<#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
```

Observação: qualquer pacote que seja roteado após a regravação do cabeçalho MAC cujo MAC de destino não seja aprendido na SVI de saída, o pacote será então inundado na VLAN correspondente. Para atenuar a inundação, você precisa criar um gateway e uma VLAN separada apenas para os servidores NLB. Se você não quiser configurar uma VLAN dedicada para o tráfego NLB, poderá configurar uma entrada de endereço MAC estático para as portas que devem receber o tráfego NLB,

---

ou seja, **mac address-table static** *0100.5exx.xxxx* **vlan** # **interface** interface_name

Troubleshooting

1. Verifique se o endereço MAC estático está configurado para todas as portas de destino que precisam encaminhar o tráfego para o NLB.

<#root>

C9300-01#

show mac address multicast

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

2. Para implantações onde o cluster NLB está em sub-rede diferente dos clientes, verifique se há entradas ARP estáticas que mapeiem o IP Virtual do servidor NLB com seu endereço MAC multicast.

<#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. Faça um ping para o IP do Servidor NLB com um tamanho que não tenha sido usado com frequência. Limpe os controladores da porta e verifique com várias iterações do comando qual tamanho não foi usado 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 se os pings foram encaminhados para fora da porta de destino corretamente e se o mesmo teste de ping foi enviado para outras portas. Verifique isso com o mesmo comando controllers counters nas 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. Capture pacotes na porta de entrada com EPC e na porta de saída com SPAN e verifique se o switch está encaminhando os dados ou não.

<#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
```

> **Dica**: a funcionalidade Embedded Packet Capture (EPC) é confiável quando os pacotes são encaminhados na direção de entrada ou saída da camada 2. No entanto, se o tráfego for roteado pelo switch e encaminhado à porta de saída, o EPC não será confiável. Para capturar pacotes na saída após a ocorrência do roteamento da camada 3, use o recurso Switch Port Analyzer (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
```

Informações Relacionadas

- **Exemplo de configuração de switches do Catalyst para balanceamento de carga da rede Microsoft**
- **Suporte técnico e downloads da Cisco**

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.