IGMP voor probleemoplossing voor NLB-implementaties op Catalyst 9000 Switches

Inhoud

Inleiding

Dit document beschrijft hoe de IGMP-functie op Catalyst 9000 Series switches zich gedraagt in een Microsoft Network Load Balancer (NLB) implementatie.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Microsoft NLB: werkingsmodi
- IGMP-multicast

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

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

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

NLB is een clustertechnologie die beschikbaar is in alle systemen van de Windows 2000-server en Windows 2003-serverreeks. Het biedt één virtueel IP-adres voor alle clients als het IP-adres van de bestemming voor het gehele cluster.

NLB kan worden gebruikt om clientaanvragen op een aantal servers te distribueren. Om ervoor te zorgen dat clients aanvaardbare prestatieniveaus ervaren, biedt NLB de mogelijkheid om extra servers toe te voegen om stateless toepassingen uit te breiden (zoals op IIS gebaseerde webservers) naarmate de clientbelasting

toeneemt. Bovendien vermindert het de downtime die door een serverstoring wordt veroorzaakt.

U kunt NLB zo configureren dat het op een van de volgende drie modi werkt:

- Unicast-modus
- Multicastmodus
- IGMP-modus (Internet Group Management Protocol)

> **Tip**: de implementaties van de unicastmodus en multicast-modus hebben dezelfde configuratie en verificatie als die worden beschreven in de Switches van document Catalyst voor Microsoft Network Load Balancing Configuration Voorbeeld

---

Dit document is gericht op de Internet Group Management Protocol (IGMP)-modus.

Best practices

Catalyst 9000 Series switches snoepen de Layer 3-headers van IGMP-pakketten om de Snooping-tabel te vullen. Gezien de manier waarop NLB op de switch moet worden geconfigureerd met behulp van een statische multicast MAC, is de IGMP-synchronisatietabel niet ingevuld en vindt overstroming in de bestemming VLAN plaats. Met andere woorden, IGMP-controle in Catalyst 9000 bevat niet automatisch de multicast overstroming wanneer de NLB-server in IGMP-modus staat (doorsturen in Catalyst 9000 is gebaseerd op multicast IP en niet op multicast MAC-adres).

> **Opmerking**: op Catalyst 9000 treedt overstroming op in alle drie de modi van NLB. Overstroming komt niet voor in de gebruiker VLAN, gezien dat de bestemming van de pakketten hun standaardgateway moet zijn. Alleen nadat de header is herschreven naar de bestemming VLAN, treedt de overstroming op.

Overweeg daarom deze best practices voor succesvolle implementaties:

- Gebruik een speciaal VLAN om de overstroming alleen tot het NLB-cluster te beperken.
- Gebruik statische MAC-vermeldingen om de poorten te beperken waarin de overstroming binnen NLB VLAN plaatsvindt.

IGMP-modus

In deze modus valt de virtuele MAC van het NLB-cluster binnen het bereik van de Internet Assigned Numbers Authority (IANA) en begint deze met 0100.5exx.xxxx. Het IGMP Snooping de functie die op de switch is geconfigureerd, programmeert in de MAC-adrestabel niet het virtuele multicast MAC-adres van het cluster. Aangezien deze dynamische programmering ontbreekt, wordt het multicast-verkeer dat de switch van het NLB-cluster ontvangt, overspoeld naar alle poortleden van hetzelfde VLAN. Cisco bug-id CSCvw18989.

Voor topologieën waar de NLB-servers in ander VLAN zijn dan de gebruikers, is het virtuele IP-adres van het cluster een multicast MAC-adres en is het onbereikbaar buiten het lokale subnet. Om dit aan te pakken moet u een statische ARP-ingang op elk apparaat configureren met een laag 3-interface in het cluster VLAN.

IGMP-controle in de Catalyst 9000 Series switches maakt geen gebruik van het multicast MAC-adres voor doorsturen. Ze gebruiken het multicast IP-adres, daarom kan het multicast MAC-adres niet automatisch in de MAC-tabel worden geprogrammeerd, zoals andere legacy-platforms (zoals Catalyst 6000 Series). Alle nieuwe platformen gebruiken de multicast IP-adresdoorstuurmethode om de overlappende adresproblemen

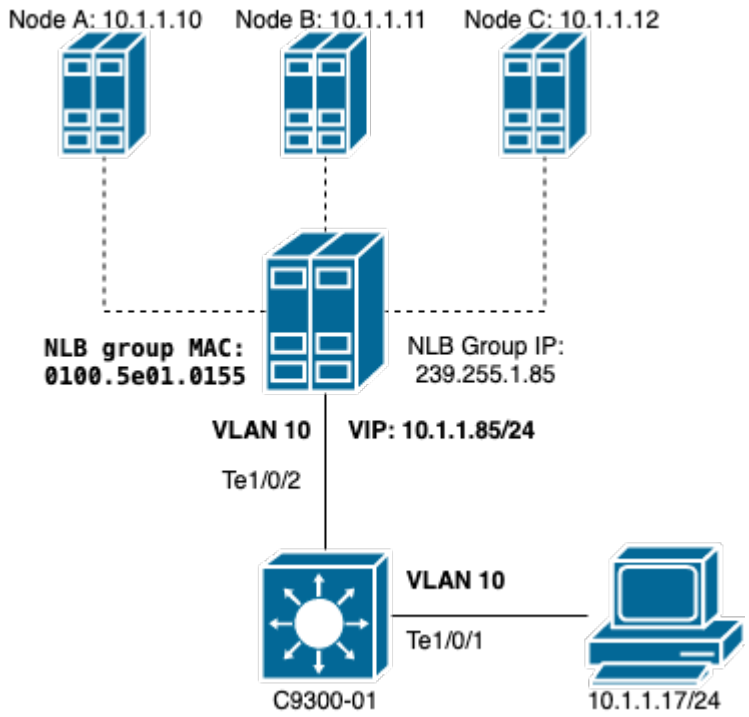
op oudere switches te voorkomen.

> **Opmerking**: Een Ethernet multicast MAC-adres heeft enige overlap. Het zelfde adres van MAC wordt toegewezen aan 32 verschillende multicast groepen. Als één gebruiker op een Ethernet-segment zich abonneert op multicast groep 225.1.1.1 en een andere gebruiker zich abonneert op 230.1.1.1, ontvangen beide gebruikers beide multicast streams (MAC-adres is hetzelfde 01-00-5e-01-01-01). In het ontwerpen van multicast netwerken op LAN-segmenten moet deze overlap specifiek worden bewaakt en ontworpen om het probleem te voorkomen.

Configureren

Bron en bestemming in hetzelfde VLAN

Netwerkdiagram



In dit gedeelte wordt beschreven hoe u NLB kunt configureren wanneer het cluster en de gebruikers zich in hetzelfde VLAN bevinden.

1. Controleer of NLB VLAN is gemaakt. Als gevolg van de overstroming wordt geadviseerd om een specifiek VLAN voor NLB-verkeer te hebben.

<#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. CConfigureer een statische MAC-adresinvoer voor de poorten die dit NLB-verkeer moeten krijgen. Deze opdracht moet alle trunkpoorten of toegangspoorten op het pad naar de NLB-cluster in NLB VLAN omvatten. In het diagram is er slechts één pad naar de 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#

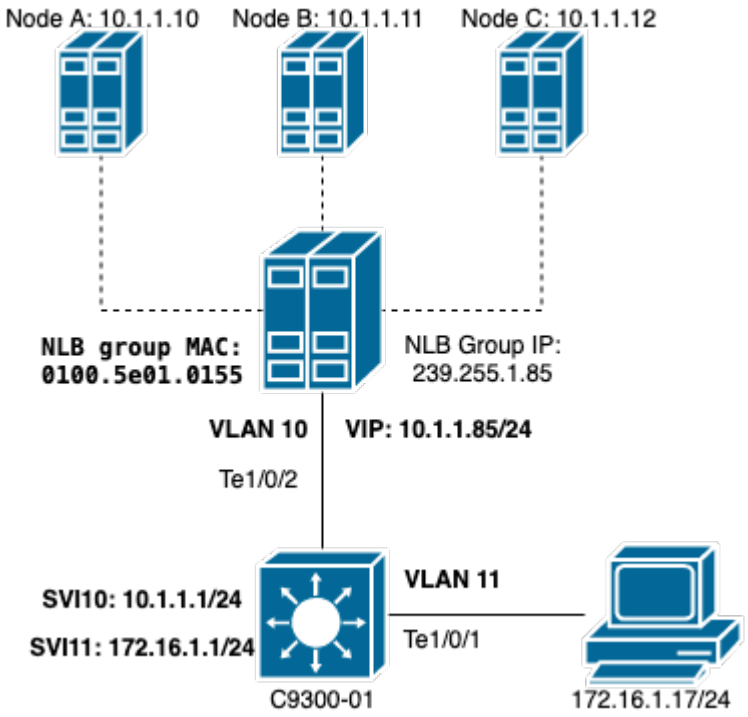
show run | in mac

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

> **Opmerking**: u kunt zoveel toegewezen poorten in de statische MAC-adresvermelding hebben als u nodig hebt. Deze kaart van poorten vermindert de verwachte overstroming in het VLAN van de NLB. In het voorbeeld kan de statische MAC-ingang voorkomen dat het verkeer naar de NLB-cluster overstroomt uit Te1/0/3.

Bron en bestemming in verschillend VLAN

Netwerkdiagram



In deze sectie wordt beschreven hoe u NLB kunt configureren wanneer het cluster en de gebruikers in verschillende VLANâ€™s zijn geïnstalleerd.

1. Configureer NLB VLAN en een IP-adres als de standaardgateway van het NLB-cluster.

<#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. Configureer een statische ARP-ingang voor het virtuele IP-adres van de NLB-clusterservers. De statische ARP moet worden geconfigureerd op alle Layer 3-apparaten die een Switch Virtual Interface (SVI) in het VLAN-cluster hebben. Het doel van statische ARP is de switch toe te staan om de herschrijfinformatie te hebben noodzakelijk om gerouteerde pakketten naar NLB VLAN te verzenden.

<#root>

C9300-01(config)#

arp 10.1.1.85 0100.5e01.0155 arpa

3. Controleer de gebruiker VLAN die op de toegangslaag is gemaakt en zijn standaardgateway. Het is belangrijk dat u de standaardgateway op beide partijen vormt. (NLB: cluster en gebruikers).

<#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
```

Opmerking: elk pakket dat na MAC-header wordt verstuurd, herschrijft de doelmap waarvan de MAC niet in uitgang SVI wordt geleerd, het pakket wordt dan overspoeld in het corresponderende VLAN. Om de overstroming te beperken, moet u alleen voor de NLB-servers een gateway en een

---

afzonderlijk VLAN maken. Als u geen specifiek VLAN voor het NLB-verkeer wilt configureren, kunt u een statische MAC-adresinvoer configureren voor de poorten die het NLB-verkeer moeten ontvangen, dat wil zeggen, **mac adrestabel statisch** *0100.5exx.xxxx* **VLAN #** **interface** *interface_name*

Problemen oplossen

1. Controleer of het statische MAC-adres is geconfigureerd voor alle doelpoorten die het verkeer naar NLB moeten doorsturen.

<#root>

C9300-01#

show mac address multicast

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

2. Controleer voor implementaties waarbij het NLB-cluster in andere subnetgebieden ligt dan de clients of er statische ARP-vermeldingen zijn die het virtuele IP van de NLB-server in kaart brengen met het multicast MAC-adres.

<#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. Pingel een keer naar de NLB-server voor IP met een grootte die niet vaak is gebruikt. Schakel de controllers van de poort uit en controleer met meerdere herhalingen van de opdracht welke grootte niet zo veel is gebruikt.

<#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. Controleer of de pings goed uit de bestemmingshaven zijn doorgestuurd en of dezelfde ping-test naar andere poorten is overstroomd. Controleer dit met dezelfde controllers tellers commando op de verschillende 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. Neem pakketopnamen op de toegangspoort met EPC en op de uitgangspoort met SPAN en controleer of de switch de gegevens doorstuurt of niet.

<#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
```

> **Tip**: de functionaliteit van Embedded Packet Capture (EPC) is betrouwbaar wanneer pakketten worden doorgestuurd in Layer 2 ingangen- of uitgangsrichting. Echter, als het verkeer wordt gerouteerd door de switch en vervolgens doorgestuurd naar de vertrekpoort, is EPC niet betrouwbaar. Als u pakketten na Layer 3-routing in uitgang wilt opnemen, gebruikt u de functie 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
```

Gerelateerde informatie

- **Catalyst-Switches voor Microsoft Configuration voorbeeld voor taakverdeling voor netwerken**
- **Cisco technische ondersteuning en downloads**

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.