

Catalyst-Switches configureren voor Microsoft NLB

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Unicast-modus](#)

[Multicast-modus](#)

[IGMP-modus](#)

[IGMP-modus: kanttekeningen](#)

[Netwerkdigram](#)

[Configureren](#)

[Configuratie voor multicast-modus](#)

[Configuratie voor IGMP-modus](#)

[Verifiëren](#)

[Verificatie van multicast-modus](#)

[Verificatie IGMP-modus](#)

[Problemen oplossen](#)

Inleiding

In dit document wordt beschreven hoe u Cisco Catalyst-switches configureert voor interactie met Microsoft Network Load Balancing (NLB).

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op en geconfigureerd voor deze software- en hardwareversies:

- Catalyst 6500 Sup2T switch met Cisco IOS Software 15.1(1)SY1
- Catalyst 4948 switch met Cisco IOS Software 15.0(2)SG7
- Microsoft Windows-servers



Opmerking: raadpleeg de juiste configuratiehandleiding voor de opdrachten die worden gebruikt om deze functies op andere Cisco-platforms in te schakelen.

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 de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

De NLB-technologie kan worden gebruikt om clientverzoeken over een reeks servers te verdelen. Om ervoor te zorgen dat clients altijd aanvaardbare prestatieniveaus ervaren, biedt Microsoft Windows NLB de mogelijkheid om extra servers toe te voegen, zodat u stateloze toepassingen, zoals op IIS gebaseerde webserver, kunt uitbreiden naarmate de belasting van de client toeneemt. Bovendien vermindert het de downtime die wordt veroorzaakt door servers die niet goed functioneren.

Microsoft Windows NLB is een clustertechnologie die wordt aangeboden als onderdeel van alle besturingssystemen van de Windows 2000 Server- en Windows 2003-serverfamilie. Het biedt één virtueel IP-adres voor alle clients als het IP-adres van de bestemming voor het hele cluster.

U kunt NLB configureren om in een van deze drie modi te werken:

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

Unicast-modus

Hier zijn enkele opmerkingen over het gebruik van NLB in Unicast-modus:

- In de Unicast-modus vervangt NLB het werkelijke MAC-adres (Media Access Control) van elke server in het cluster door een gemeenschappelijk NLB-MAC-adres. Wanneer alle servers in het cluster hetzelfde MAC-adres hebben, worden alle pakketten die naar dat adres worden doorgestuurd naar alle leden in het cluster verzonden. De NLB maakt een fictief MAC-adres en wijst dit toe aan elke server in het NLB-cluster. De NLB kent aan elke NLB-server een ander fictief MAC-adres toe, op basis van de host-ID van het lid. Dit adres wordt weergegeven in de koptekst van het Ethernet-frame.
- Het MAC-adres wordt gebruikt in de koptekst van het Address Resolution Protocol (ARP), niet in de Ethernet-koptekst. De switch gebruikt het MAC-adres in de Ethernet-header, niet de ARP-header. Dit veroorzaakt een probleem wanneer een pakket naar het NLB-cluster wordt verzonden met het MAC-adres van de bestemming als het MAC-adres van het cluster 00-bf-ac-10-00-01. De switch bekijkt de tabel Content Addressable Memory (CAM) voor het MAC-adres 00-bf-ac-10-00-01 en aangezien er geen poort is geregistreerd bij het NLB-cluster MAC-adres 00-bf-ac-10-00-01, wordt het frame geleverd aan alle switch-poorten. Dit

leidt tot unicast overstromingen. Om overstromingen te voorkomen, raadt Cisco u aan een speciaal VLAN voor NLB te gebruiken, zodat de overstroming wordt beperkt.

Multicast-modus

Hier zijn enkele opmerkingen over het gebruik van NLB in Multicast-modus:

- In de Multicast-modus klikt de systeembeheerder op de Multicast-knop in de Microsoft NLB-configuratie-GUI. Deze keuze instrueert de clusterleden om op de ARP's te reageren voor hun virtuele adres met behulp van een multicast-MAC-adres, zoals 0300.5e01.0101.
- Het ARP-proces is niet voltooid voor multicast MAC-adressen (dit breekt RFC 1812). Een statisch MAC-adres is vereist om het cluster buiten het lokale subnet te bereiken.
- Het virtuele IP-adres is 10.100.1.99 en het multicast MAC-adres is 0300.5e01.0101. Voer deze opdracht in om de ARP-tabel statisch te vullen:

<#root>

```
arp 10.100.1.99 0300.5e01.0101
```

- Aangezien de inkomende pakketten een unicast-bestemming-IP-adres en een multicast-bestemming-MAC hebben, negeert het Cisco-apparaat deze vermelding en overspoelt unicast elke clustergebonden pakketten. Om deze overstroming te voorkomen, voegt u een statische mac-adres-tabel in, zoals hieronder aangegeven, om clustergebonden pakketten in de switch te plaatsen.

<#root>

```
mac address-table static 0300.5e01.0101 vlan 200 interface TenGigabitEthernet1/4 TenGigabitEthernet1/5
```

 **Opmerking:** wanneer u een MAC-adres statisch toewijst aan meerdere poorten, wordt dit alleen ondersteund door de software op de switch van de Cisco Catalyst 4500-reeks. Het gebruik van deze configuratie op de switch van de Catalyst 4500-reeks kan ook een hoge CPU veroorzaken. Om dit probleem te voorkomen, kunt u de NLB isoleren naar een specifiek VLAN, alleen de statische ARP-vermeldingen toevoegen en overstromingen op dat VLAN toestaan.

 **Opmerking:** voor switches uit de Cisco Catalyst 6000/6500-reeks moet u de parameter disable-snooping toevoegen om het verkeer alleen naar de opgegeven poorten te beperken. Wanneer u een statische verbinding configureert, voert u het gereserveerde woord disable-snooping in om te voorkomen dat multicast-verkeer dat is geadresseerd aan het statisch geconfigureerde multicast-MAC-adres ook naar andere poorten in hetzelfde VLAN wordt



verzonden. (Deze opdracht is niet vereist op andere platforms).

IGMP-modus

Hier zijn enkele opmerkingen over het gebruik van NLB in IGMP-modus:

- Het gebruik van NLB in IGMP-modus vereist de minste handmatige configuratie. Het virtuele MAC-adres valt binnen het bereik van de Internet Assigned Numbers Authority (IANA) en begint met 0100.5exx.xxxx. Aangezien het MAC-adres nu voldoet aan de IANA-specificaties, kunnen de Cisco-switches het MAC-adres dynamisch programmeren met behulp van IGMP-snooping. Hierdoor hoeft het MAC-adres niet handmatig te worden geprogrammeerd op de poortkaarten die in de Multicast-modus vereist zijn om overstromingen naar het VLAN te voorkomen.
- De IGMP-snooping programmeert het virtuele MAC-adres voor u zodra de switch een lidmaatschapsrapport ontvangt van een lid in het cluster. Een Mrouter poort moet ook worden geprogrammeerd voor de NLB VLAN met het gebruik van ofwel Protocol Independent Multicast (PIM) of de IGMP querier functie.
- Aangezien het virtuele IP-adres een multicast MAC-adres gebruikt, is het onbereikbaar buiten het lokale subnet. Om dit aan te pakken, moet u een statische ARP-vermelding op elk apparaat configureren met een Layer 3 (L3)-interface in het cluster-VLAN. Dit doe je op dezelfde manier als bij Multicast. Als het virtuele IP-adres bijvoorbeeld 10.100.1.99 is en het multicast-MAC-adres 0100.5e01.0101, gebruikt u deze opdracht om de ARP-tabel statisch te vullen:

```
<#root>
```

```
arp 10.100.1.99 0100.5e01.0101
```

IGMP-modus: kanttekeningen

Hier zijn belangrijke opmerkingen om in gedachten te houden wanneer u NLB in IGMP-modus gebruikt:



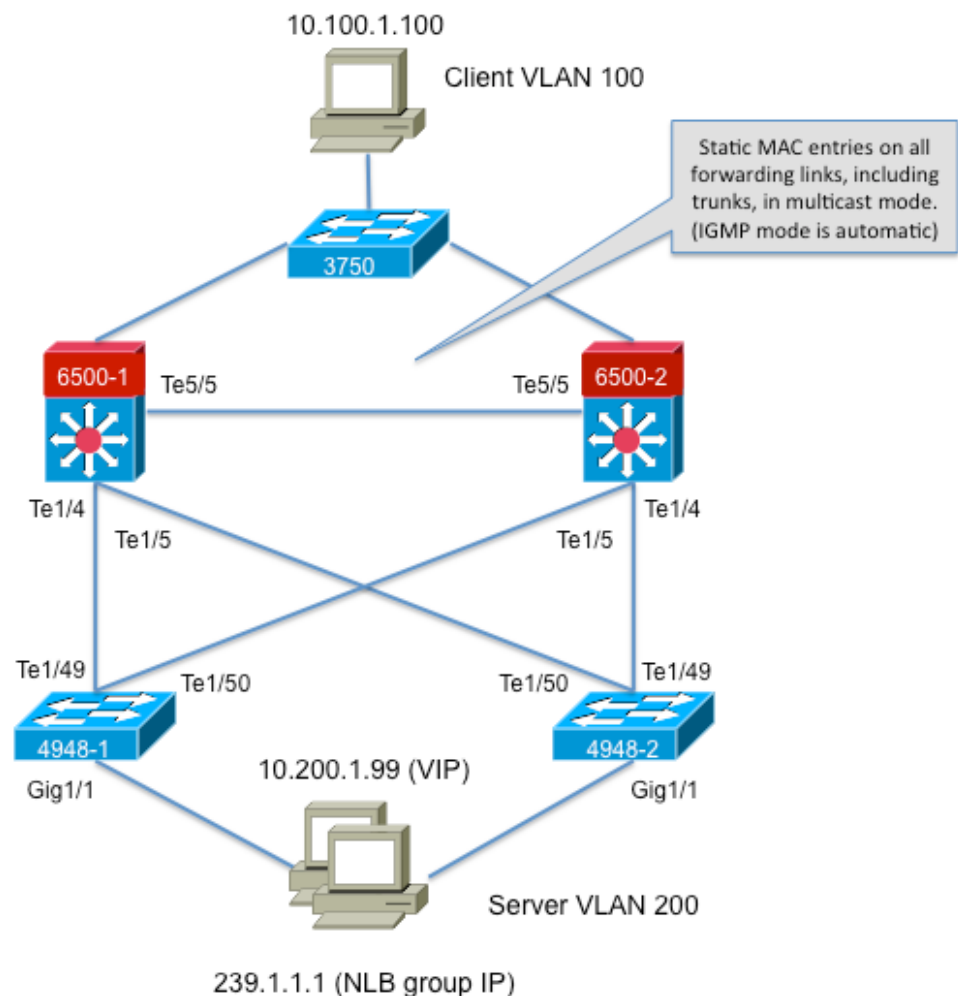
Opmerking: zoals bijgehouden door Cisco bug ID [CSCsw72680](#) kunt u geen PIM gebruiken op de NLB VLAN Switch Virtual Interface (SVI) met bepaalde versies van code. Bekijk de bug details voor de code releases die dit probleem aanpakken of gebruik de IGMP snooping querier functie.



Opmerking: Zoals bijgehouden door Cisco bug ID [CSCsy62709](#) pakketten worden gedupliceerd voor al het verkeer dat wordt gerouteerd naar de NLB servers in IGMP-modus. Bekijk de bug details voor de betreffende code versies.

 **Opmerking:** vanwege een hardwarebeperking die wordt gevolgd door Cisco bug ID [CSCug49149](#) kan NLB-verkeer niet via een gedistribueerd Etherchannel op dezelfde 6708-lijnkaart worden verzonden wanneer de switch in de PFC3B- of PFC3C-modus wordt uitgevoerd. Het poortkanaal moet bekabeld zijn, zodat alle lidkoppelingen op dezelfde doorstuurengine zitten.

Netwerkdigram



Configureren

In dit gedeelte wordt beschreven hoe u NLB configureert voor de platforms uit de Cisco Catalyst 6500- en 4948-reeks die in de Multicast- of IGMP-modus worden uitgevoerd.

Configuratie voor multicast-modus

In dit gedeelte wordt beschreven hoe u NLB configureert voor de platforms uit de Cisco Catalyst 6500- en 4948-reeks die in de Multicast-modus worden uitgevoerd:

<#root>

6500-1#

show running-config

Building configuration...

```
!  
hostname 6500-1  
!  
boot system flash disk0:s2t54-adventerprisek9-mz.SPA.151-1.SY1  
!  
interface TenGigabitEthernet1/4  
switchport  
switchport trunk allowed vlan 1,100,200  
switchport mode trunk  
!  
interface TenGigabitEthernet1/5  
switchport  
switchport trunk allowed vlan 1,100,200  
switchport mode trunk  
!  
interface Vlan100  
  
ip address 10.100.1.1 255.255.255.0  
  
!  
!  
interface Vlan200  
  
ip address 10.200.1.1 255.255.255.0  
  
!  
!  
arp 10.100.1.88 0300.5e01.0101 ARPA  
  
!  
!  
mac address-table static 0300.5e01.0101 vlan 200 interface TenGigabitEthernet1/4  
  
TenGigabitEthernet1/5 TenGigabitEthernet5/5  
  
!
```

Hier zijn enkele belangrijke opmerkingen over deze configuratie:

- De interface Vlan100 ip address value configureert het VLAN van de gebruiker.
- De interface Vlan200 ip address value configureert het NLB-cluster VLAN. Het is belangrijk dat u de standaardgateway van de Microsoft Server op dit adres configureert.

- De EARP 10.100.1.88 0300.5e01.0101 ARPA omvat alle L3-interfaces in het VLAN en is het virtuele IP-adres van de NLB-clusterservers.
- Met de statische 0300.5e01.0101 vlan 200-interface voor de emac-adrestabel wordt een statische MAC-invoer naar poorttoewijzing in de switch voor het multicast virtual MAC-adres gemaakt.

 **Opmerking:** zorg ervoor dat u de Multicast-modus op het NLB-cluster gebruikt. Cisco raadt u aan geen multicast MAC-adressen te gebruiken die beginnen met 01 omdat bekend is dat ze een conflict hebben met de IGMP-setup.

<#root>

4948-1#

show running-config

```
Building configuration...
!
hostname 4948-1
!
boot system bootflash:cat4500-entservices-mz.150-2.SG7
!
interface GigabitEthernet1/1
switchport access vlan 200
!
interface TenGigabitEthernet1/49
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,100,200
switchport mode trunk
!
interface TenGigabitEthernet1/50
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,100,200
switchport mode trunk
!
mac address-table static 0300.5e01.0101 vlan 200 interface Gi1/1 Te1/49 Te1/50

!
!
end
```

 **Opmerking:** de statische mac-adrestabel 0300.5e01.0101 vlan 200 maakt een statische invoer in de switch voor het multicast virtual MAC-adres. Het is belangrijk om te onthouden dat alle trunk-interfaces die NLB-verkeer tussen de switches vervoeren, moeten worden toegevoegd. Zodra een statisch MAC-adres is gedefinieerd, is overstroming beperkt. Als u een interface vergeet op te nemen, breekt het NLB-cluster.

Configuratie voor IGMP-modus

In dit gedeelte wordt beschreven hoe u NLB configureert voor de platforms uit de Cisco Catalyst 6500- en 4948-reeks die in de IGMP-modus worden uitgevoerd

<#root>

6500-1#

show running-config

Building configuration...

!

hostname 6500-1

!

boot system flash disk0:s2t54-adventerprisek9-mz.SPA.151-1.SY1

!

ip igmp snooping querier

!

vlan configuration 1,100

no ip igmp snooping querier

!

vlan configuration 200

ip igmp snooping querier address 10.200.1.1

!

interface TenGigabitEthernet1/4

switchport

switchport trunk allowed vlan 1,100,200

switchport mode trunk

!

interface TenGigabitEthernet1/5

switchport

switchport trunk allowed vlan 1,100,200

switchport mode trunk

!

interface Vlan100

ip address 10.100.1.1 255.255.255.0

!

interface Vlan200

ip address 10.200.1.1 255.255.255.0

!

```
arp 10.100.1.99 0100.5e01.0101 ARPA
```

```
!  
end
```

Hier zijn enkele belangrijke opmerkingen over deze configuratie:

- De IIP IgMP snooping querier maakt de snooping querier-functie mogelijk.
- Het IP igmp snooping querier-adres 10.200.1.1 configureert de snooping querier voor het NLB VLAN.
- De VLAN-gebruikersinterface is VLAN100.
- De NLB cluster VLAN-interface is VLAN200. Het is belangrijk dat u de standaardgateway van de Microsoft Server op dit adres configureert (IP-adres 10.200.1.1 255.255.255.0).
- De EARP 10.100.1.99 0100.5e01.0101 ARPA is het virtuele IP-adres van de NLB-clusterservers. De statische ARP moet op alle L3-interfaces in het VLAN staan.

```
<#root>
```

```
4948-1#
```

```
show running-config
```

```
Building configuration...  
!  
hostname 4948-1  
!  
boot system bootflash:cat4500-entservices-mz.150-2.SG7  
!  
interface GigabitEthernet1/1  
switchport access vlan 200  
!  
interface TenGigabitEthernet1/49  
switchport trunk encapsulation dot1q  
switchport trunk allowed vlan 1,100,200  
switchport mode trunk  
!  
interface TenGigabitEthernet1/50  
switchport trunk encapsulation dot1q  
switchport trunk allowed vlan 1,100,200  
switchport mode trunk  
!  
end
```

 **Opmerking:** Het is niet nodig om statische items te configureren, omdat IGMP-snooping dit dynamisch doet in deze modus. Er is ook geen speciale configuratie voor deze modus vereist op de downstream Layer 2 (L2)-switches.

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

 Opmerking: de [Output Interpreter Tool](#) ([alleen geregistreerde](#) klanten) (OIT) ondersteunt bepaalde show-opdrachten. Gebruik de OIT om een analyse te bekijken van de output van de opdracht show.

Verificatie van multicast-modus

Voer de opdracht ip arp in om de ARP-cache te bekijken:

```
<#root>
```

```
6500-1#
```

```
sh ip arp
```

```
Protocol Address Age (min) Hardware Addr Type Interface
Internet
```

```
10.100.1.99 - 0300.5e01.0101 ARPA
```

Voer de statische opdracht mac-adrestabel weergeven in om een specifieke statische en dynamische MAC-adrestabel of de statische en dynamische MAC-adrestabel op een specifieke interface of VLAN te bekijken:

```
<#root>
```

```
6500-1#
```

```
show mac address-table static add 0300.5e01.0101
```

```
vlan mac address      type  learn age      ports
----+-----+-----+-----+-----
200  0300.5e01.0101  static No      -      Te1/4 Te1/5 Te5/5
```

```
<#root>
```

```
4948-1#
```

```
show mac address-table static add 0300.5e01.0101
```

Multicast Entries

vlan	mac address	type	ports
200	0300.5e01.0101	static	Gi1/1,Te1/49,Te1/50

Verificatie IGMP-modus

Voer de opdracht ip arp in om de ARP-cache te bekijken:

```
<#root>
6500-1#
show ip arp
```

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	10.100.1.99	-	0100.5e01.0101	ARPA	

Voer de show-ip igmp-snooping-router in om de routerpoort te bekijken die is geprogrammeerd door de query's die zijn ontvangen van de upstream-snooping-querier:

```
<#root>
4948-1#
show ip igmp snooping mrouter
```

Vlan	ports
200	Te1/49(dynamic)

Voer de show mac address-table multicast igmp-snooping in om het dynamisch toegevoegde MAC-adres te bekijken dat wordt geleerd van IGMP-snooping en de lidpoorten:

```
<#root>
4948-1#
show mac address-table multicast igmp-snooping
```

Multicast Entries			
vlan	mac address	type	ports

```

-----+-----+-----+-----
200      0100.5e01.0101  igmp   Gi1/1,Te1/49

```

Voer de groepen voor het snuffelen van ip igmp in om de poortlijst te bekijken van clusterleden die lid zijn geworden van de multicast-groep:

```
<#root>
```

```
4948-1#
```

```
show ip igmp snooping groups
```

```

Vlan      Group      Version      Port List
-----
200       239.1.1.1    v2           Gi1/1

```

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

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.