

Konfigurieren von Catalyst-Switches für Microsoft NLB

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Unicast-Modus](#)

[Multicast-Modus](#)

[IGMP-Modus](#)

[IGMP-Modus - Einschränkungen](#)

[Netzwerkdiagramm](#)

[Konfigurieren](#)

[Konfiguration des Multicast-Modus](#)

[Konfiguration für IGMP-Modus](#)

[Überprüfung](#)

[Überprüfung des Multicast-Modus](#)

[IGMP-Modusüberprüfung](#)

[Fehlerbehebung](#)

Einleitung

Dieses Dokument beschreibt die Konfiguration der Cisco Catalyst Switches für die Interaktion mit dem Microsoft Network Load Balancing (NLB).

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen und werden entsprechend konfiguriert:

- Catalyst 6500 Sup2T-Switch mit Cisco IOS-Software 15.1(1)SY1
- Catalyst 4948-Switch mit Cisco IOS-Software 15.0(2)SG7
- Microsoft Windows Server

 Anmerkung: Die Befehle, um diese Funktionen auf anderen Cisco Plattformen zu aktivieren, finden Sie im entsprechenden Konfigurationsleitfaden.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Hintergrundinformationen

Die NLB-Technologie kann verwendet werden, um Client-Anforderungen auf eine Reihe von Servern zu verteilen. Um sicherzustellen, dass die Clients stets ein akzeptables Leistungsniveau aufweisen, bietet Microsoft Windows NLB die Möglichkeit, zusätzliche Server hinzuzufügen, sodass Sie zustandslose Anwendungen wie IIS-basierte Webserver bei zunehmender Client-Auslastung skalieren können. Darüber hinaus werden Ausfallzeiten reduziert, die durch fehlerhafte Server verursacht werden.

Microsoft Windows NLB ist eine Clustering-Technologie, die als Teil aller Betriebssysteme der Windows 2000 Server- und Windows 2003 Server-Familie angeboten wird. Es stellt eine einzige virtuelle IP-Adresse für alle Clients als Ziel-IP-Adresse für das gesamte Cluster bereit.

Sie können den NLB so konfigurieren, dass er in einem der folgenden drei Modi funktioniert:

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

Unicast-Modus

Hier einige Hinweise zur Verwendung von NLB im Unicast-Modus:

- Im Unicast-Modus ersetzt NLB die tatsächliche MAC-Adresse (Media Access Control) jedes Servers im Cluster durch eine gemeinsame NLB-MAC-Adresse. Wenn alle Server im Cluster über dieselbe MAC-Adresse verfügen, werden alle an diese Adresse weitergeleiteten Pakete an alle Mitglieder im Cluster gesendet. Der NLB erstellt eine fiktive MAC-Adresse und weist sie jedem Server im NLB-Cluster zu. Die NLB weist jedem NLB-Server eine andere fiktive MAC-Adresse zu, die auf der Host-ID des Mitglieds basiert. Diese Adresse wird im Ethernet-Frame-Header angezeigt.
- Die MAC-Adresse wird im ARP-Header (Address Resolution Protocol) und nicht im Ethernet-Header verwendet. Der Switch verwendet die MAC-Adresse im Ethernet-Header und nicht den ARP-Header. Dies führt zu einem Problem, wenn ein Paket an den NLB-Cluster gesendet wird, dessen Ziel-MAC-Adresse die MAC-Adresse des Clusters 00-bf-ac-10-00-01 ist. Der Switch zeigt die Content Addressable Memory (CAM)-Tabelle für die MAC-Adresse 00-bf-ac-10-00-01 an, und da kein Port bei der NLB-Cluster-MAC registriert ist, address 00-bf-ac-10-00-01: Der Frame wird an alle Switch-Ports geliefert. Dies führt zu Unicast-

Flooding. Um Flooding zu vermeiden, empfiehlt Cisco die Verwendung eines dedizierten VLAN für den NLB, damit das Flooding eingeschränkt wird.

Multicast-Modus

Hier einige Hinweise zur Verwendung von NLB im Multicast-Modus:

- Im Multicast-Modus klickt der Systemadministrator in der Microsoft NLB-Konfigurationsbenutzeroberfläche auf die Schaltfläche Multicast. Bei dieser Auswahl werden die Cluster-Mitglieder angewiesen, auf die ARPs für ihre virtuelle Adresse mithilfe einer Multicast-MAC-Adresse wie 0300.5e01.0101 zu reagieren.
- Der ARP-Prozess wird für Multicast-MAC-Adressen nicht abgeschlossen (dadurch wird RFC 1812 unterbrochen). Eine statische MAC-Adresse ist erforderlich, um den Cluster außerhalb des lokalen Subnetzes zu erreichen.
- Die virtuelle IP-Adresse lautet 10.100.1.99, und die Multicast-MAC-Adresse lautet 0300.5e01.0101. Geben Sie diesen Befehl ein, um die ARP-Tabelle statisch zu füllen:

<#root>

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

- Da die eingehenden Pakete eine Unicast-Ziel-IP-Adresse und eine Multicast-Ziel-MAC-Adresse aufweisen, ignoriert das Cisco Gerät diesen Eintrag und überflutet alle clustergebundenen Pakete. Um dieses Flooding zu vermeiden, fügen Sie wie unten beschrieben einen statischen MAC-Adresstableneintrag ein, um clustergebundene Pakete in der Hardware zu vermitteln.

<#root>

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

 Anmerkung: Wenn Sie eine MAC-Adresse mehreren Ports statisch zuordnen, wird sie nur von der Software auf dem Cisco Catalyst Switch der Serie 4500 unterstützt. Außerdem kann die Verwendung dieser Konfiguration auf dem Catalyst Switch der Serie 4500 zu einer hohen CPU-Auslastung führen. Um dieses Problem zu vermeiden, können Sie den NLB zu einem bestimmten VLAN isolieren, nur die statischen ARP-Einträge hinzufügen und das Flooding auf diesem VLAN zulassen.

 Anmerkung: Bei Cisco Catalyst Switches der Serien 6000/6500 müssen Sie den Parameter disable-snooping hinzufügen, um den Datenverkehr auf die angegebenen Ports zu beschränken. Wenn Sie eine statische Verbindung konfigurieren, geben Sie das

 Schlüsselwort `disable-snooping` ein, um zu verhindern, dass Multicast-Datenverkehr, der an die statisch konfigurierte Multicast-MAC-Adresse adressiert ist, auch an andere Ports im selben VLAN gesendet wird. (Dieser Befehl ist auf anderen Plattformen nicht erforderlich.)

IGMP-Modus

Hier einige Hinweise zur Verwendung von NLB im IGMP-Modus:

- Die Verwendung von NLB im IGMP-Modus erfordert den geringsten manuellen Konfigurationsaufwand. Die virtuelle MAC-Adresse liegt im Bereich der Internet Assigned Numbers Authority (IANA) und beginnt bei 0100.5exx.xxxx. Da die MAC-Adresse nun den IANA-Spezifikationen entspricht, können die Cisco Switches die MAC-Adresse mithilfe von IGMP-Snooping dynamisch programmieren. Damit entfällt die Notwendigkeit, die MAC-Adresse manuell auf die im Multicast-Modus erforderlichen Port-Maps zu programmieren, um eine Überflutung des VLANs zu verhindern.
- IGMP-Snooping programmiert die virtuelle MAC-Adresse für Sie, sobald der Switch einen Mitgliedsbericht von einem Mitglied im Cluster erhält. Für das NLB-VLAN muss ein Router-Port programmiert werden, entweder mit Protocol Independent Multicast (PIM) oder mit der IGMP Querier-Funktion.
- Da die virtuelle IP-Adresse eine Multicast-MAC-Adresse verwendet, ist sie außerhalb des lokalen Subnetzes nicht erreichbar. Um dieses Problem zu beheben, müssen Sie auf jedem Gerät mit einer Layer 3 (L3)-Schnittstelle im Cluster-VLAN einen statischen ARP-Eintrag konfigurieren. Dies geschieht auf die gleiche Weise wie im Multicast-Modus. Wenn die virtuelle IP-Adresse beispielsweise 10.100.1.99 und die Multicast-MAC-Adresse 0100.5e01.0101 lautet, verwenden Sie den folgenden Befehl, um die ARP-Tabelle statisch zu füllen:

```
<#root>
```

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

IGMP-Modus - Einschränkungen

Beachten Sie bei der Verwendung von NLB im IGMP-Modus die folgenden wichtigen Hinweise:

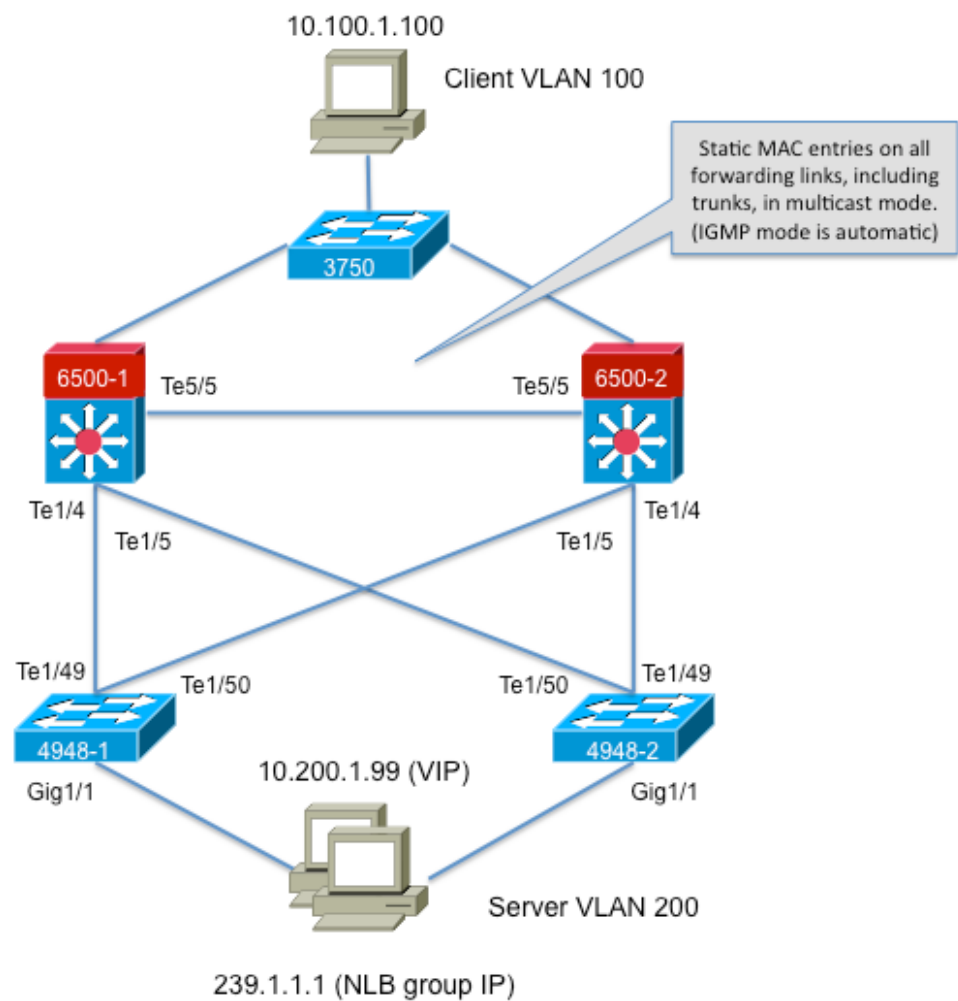
 Anmerkung: Wie von der Cisco Bug-ID [CSCsw72680](#) verfolgt, können Sie PIM auf der NLB VLANSwitch Virtual Interface (SVI) mit bestimmten Codeversionen nicht verwenden. Zeigen Sie die Fehlerdetails für die Code-Releases an, die dieses Problem beheben, oder verwenden Sie die IGMP Snooping Querier-Funktion.

 Anmerkung: [CSCsy62709](#)-Pakete werden für den gesamten Datenverkehr dupliziert, der im

 IGMP-Modus an die NLB-Server weitergeleitet wird. Die Fehlerdetails für die betroffenen Codeversionen werden angezeigt.

 Anmerkung: Aufgrund einer Hardwarebeschränkung, die von der Cisco NUG-ID [CSCug49149](#) verfolgt wird, kann der NLB-Datenverkehr nicht über einen verteilten Etherchannel auf derselben 6708-Linecard gesendet werden, wenn der Switch im PFC3B- oder PFC3C-Modus ausgeführt wird. Der Port-Channel muss verkabelt werden, damit sich alle zugehörigen Links in derselben Weiterleitungs-Engine befinden.

Netzwerkdiagramm



Konfigurieren

In diesem Abschnitt wird beschrieben, wie Sie den NLB für die Plattformen der Cisco Catalyst Serien 6500 und 4948 konfigurieren, die im Multicast- oder IGMP-Modus ausgeführt werden.

Konfiguration des Multicast-Modus

In diesem Abschnitt wird beschrieben, wie Sie den NLB für die Cisco Catalyst-Plattformen der Serien 6500 und 4948 konfigurieren, die im Multicast-Modus ausgeführt werden:

```
<#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 einige wichtige Hinweise zu dieser Konfiguration:

- Die Schnittstelle Vlan100 ip addressValue konfiguriert das Benutzer-VLAN.
- Die Schnittstelle Vlan200 ip addressValue konfiguriert das NLB-Cluster-VLAN. Es ist wichtig, dass Sie das Standard-Gateway des Microsoft-Servers für diese Adresse konfigurieren.
- Thearp 10.100.1.88 0300.5e01.0101 ARPAenthält alle L3-Schnittstellen im VLAN und ist die virtuelle IP-Adresse der NLB-Cluster-Server.
- Die statische MAC-Adresstabelle 0300.5e01.0101 VLAN 200 erstellt für die virtuelle Multicast-MAC-Adresse eine statische MAC-Eintrag-zu-Port-Zuordnung im Switch.



Anmerkung: Stellen Sie sicher, dass Sie den Multicast-Modus auf dem NLB-Cluster verwenden. Cisco empfiehlt, keine Multicast-MAC-Adressen zu verwenden, die mit 01 beginnen, da bekannt ist, dass sie einen Konflikt mit der IGMP-Einrichtung haben.

<#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
```



Anmerkung: Die statische MAC-Adresstabelle 0300.5e01.0101 VLAN 200 erstellt einen statischen Eintrag im Switch für die virtuelle Multicast-MAC-Adresse. Denken Sie daran, dass alle Trunk-Schnittstellen, die NLB-Datenverkehr zwischen den Switches übertragen, hinzugefügt werden müssen. Sobald eine statische MAC-Adresse definiert ist, wird das

 Flooding eingeschränkt. Wenn Sie eine Schnittstelle vergessen haben, wird der NLB-Cluster unterbrochen.

Konfiguration für IGMP-Modus

In diesem Abschnitt wird die Konfiguration des NLB für die Plattformen der Cisco Catalyst Serien 6500 und 4948 beschrieben, die im IGMP-Modus ausgeführt werden.

```
<#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 einige wichtige Hinweise zu dieser Konfiguration:

- Der eip igmp snooping querier aktiviert die Funktion snooping querier.
- Die Snooping-Abfragenummer 10.200.1.1 konfiguriert die Snooping-Abfragenummer für das NLB-VLAN.
- Das Benutzer-VLAN ist die Schnittstelle Vlan100.
- Das NLB-Cluster-VLAN ist die Schnittstelle Vlan200. Es ist wichtig, dass Sie das Standard-Gateway des Microsoft Servers für diese Adresse konfigurieren (IP-Adresse 10.200.1.1 255.255.255.0).
- Thearp 10.100.1.99 0100.5e01.0101 ARPA ist die virtuelle IP-Adresse der NLB-Cluster-Server. Das statische ARP muss sich an allen L3-Schnittstellen im VLAN befinden.

```
<#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

```

 Anmerkung: Es müssen keine statischen Einträge konfiguriert werden, da IGMP-Snooping dies in diesem Modus dynamisch durchführt. Außerdem ist für diesen Modus keine spezielle Konfiguration auf den Downstream-Layer-2-Switches (L2) erforderlich.

Überprüfung

Nutzen Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

 Anmerkung: Das Output Interpreter-Tool (OIT) (nur registrierte Kunden) unterstützt bestimmte show-Befehle. Verwenden Sie das OIT, um eine Analyse der show-Befehlsausgabe anzuzeigen.

Überprüfung des Multicast-Modus

Geben Sie den Befehl `show ip arp` ein, um den ARP-Cache anzuzeigen:

```
<#root>
```

```
6500-1#
```

```
sh ip arp
```

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

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

Geben Sie den Befehl `show mac address-table static` ein, um einen bestimmten statischen und dynamischen Eintrag einer MAC-Adresstabelle oder die statischen und dynamischen Einträge der MAC-Adresstabelle auf einer bestimmten Schnittstelle oder einem VLAN anzuzeigen:

```
<#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

IGMP-Modusüberprüfung

Geben Sie den Befehl show ip arp ein, um den ARP-Cache anzuzeigen:

<#root>

6500-1#

show ip arp

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet					

10.100.1.99 - 0100.5e01.0101 ARPA

Geben Sie den Befehl show ip igmp snooping mrouterin ein, um den Mrouter-Port anzuzeigen, der durch die Abfragen vom Upstream-Snooping-Abfrager programmiert wurde:

<#root>

4948-1#

show ip igmp snooping mrouter

Vlan	ports
200	Te1/49(dynamic)

Geben Sie show mac address-table multicast igmp-snooping ein, um die dynamisch hinzugefügte MAC-Adresse anzuzeigen, die vom IGMP-Snooping und den Mitglieds-Ports empfangen wird:

<#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

Geben Sie die show ip igmp snooping-Gruppen ein, um die Portliste der Cluster-Mitglieder anzuzeigen, die der Multicast-Gruppe beigetreten sind:

<#root>

4948-1#

show ip igmp snooping groups

Vlan	Group	Version	Port List
200	239.1.1.1	v2	Gi1/1

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.