

# 對Catalyst 9000交換機上的NLB部署進行IGMP故障排除

## 目錄

[簡介](#)

[必要條件](#)

[背景資訊](#)

[設定](#)

[疑難排解](#)

[相關資訊](#)

## 簡介

本檔案介紹Catalyst 9000系列交換器上的IGMP功能在Microsoft網路負載平衡器(NLB)部署中的行為方式。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- Microsoft NLB操作模式
- IGMP多點傳送

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

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

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 ( 預設 ) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 背景資訊

NLB是一種適用於所有Windows 2000 Server和Windows 2003 Server系列系統的群集技術。它為所

有客戶機提供單個虛擬IP地址作為整個群集的目標IP地址。

NLB可用於在一組伺服器之間分發客戶端請求。為確保客戶端體驗可接受的效能級別，NLB提供了在客戶端負載增加時新增更多伺服器以擴展無狀態應用程式（如基於IIS的Web伺服器）的功能。此外，它還減少了因伺服器故障導致的停機時間。

可以將NLB配置為在以下三種模式之一中工作：

- 單播模式
- 組播模式
- 網際網路群組管理協定(IGMP)模式

---

提示：單播模式和組播模式部署具有文檔適用於Microsoft網路負載均衡的[Catalyst交換機配置示例中描述的相同配置和驗證](#)

---

本檔案將重點介紹網際網路群組管理通訊協定(IGMP)模式。

## 最佳實踐

Catalyst 9000系列交換器偵聽IGMP封包的第3層標頭，以便填充Snooping表。由於必須使用靜態組播MAC在交換機上配置NLB的方式，IGMP監聽表未填充，並且目標VLAN中會發生泛洪。換句話說，當NLB伺服器處於IGMP模式時，Catalyst 9000中的IGMP監聽不會自動包含組播泛洪（Catalyst 9000中的轉發基於組播IP，而不是基於組播MAC地址）。

---

注意：在Catalyst 9000上，NLB的所有三種模式都會發生泛洪。鑑於封包的目的地必須是其預設閘道，使用者VLAN中不會發生泛濫。只有在報頭重新寫入目標VLAN後，才會發生泛洪。

---

因此，請考慮以下成功部署的最佳實踐：

- 使用專用VLAN僅將泛洪限制到NLB群集。
- 使用靜態MAC條目來限制NLB VLAN中發生泛洪的埠。

## IGMP模式

在此模式中，NLB群集的虛擬MAC位於Internet編號指派機構(IANA)範圍內，它以0100.5exx.xxxx開頭。其IGMP Snooping 交換機上配置的功能不會在MAC地址表中程式設計群集的虛擬組播MAC地址。由於缺少此動態程式設計，交換機從NLB集群接收的組播流量將泛洪到同一VLAN的所有埠成員。思科錯誤ID [CSCvw18989](#)。

對於NLB伺服器與使用者位於不同VLAN的拓撲，由於群集的虛擬IP地址使用組播MAC地址，因此無法在本地子網外訪問。為了解決此問題，您必須在集群VLAN中具有第3層介面的每台裝置上配置靜態ARP條目。

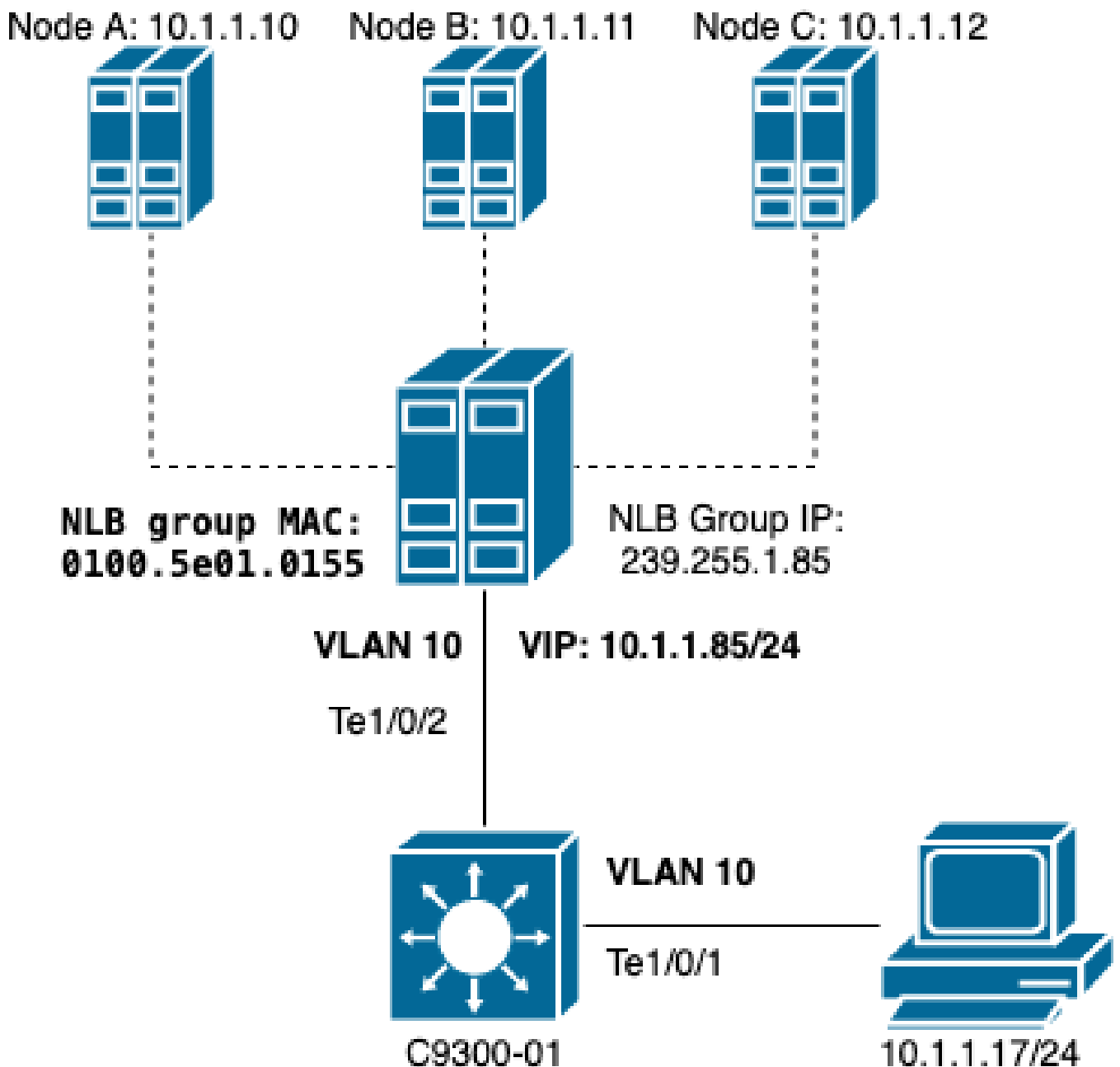
Catalyst 9000系列交換器中的IGMP窺探功能不使用多點傳送MAC位址進行轉送。它們使用組播IP地址，這就是它無法像其他舊版平台（如Catalyst 6000系列）那樣在MAC表中自動程式設計組播MAC地址的原因。所有新平台都使用組播IP地址轉發方法，以避免在舊版交換機上發現重疊地址問題。

注意：乙太網組播MAC地址有一些重疊。相同的MAC地址被分配給32個不同的組播組。如果乙太網段上的一個使用者訂購組播組225.1.1.1，而另一個使用者訂購230.1.1.1，則兩個使用者都接收兩個組播流 ( MAC地址相同01-00-5e-01-01-01 )。在LAN網段上設計組播網路時，需要專門監視並設計此重疊以避免問題。

## 設定

同一VLAN中的來源和目的地

網路圖表



本節介紹當群集和使用者位於同一個VLAN中時，如何配置NLB。

1. 檢驗是否已建立NLB VLAN。由於泛洪，建議為NLB流量設定專用VLAN。

```
<#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. C為必須獲取此NLB流量的埠配置靜態MAC地址條目。此命令必須包括通往NLB VLAN中的NLB集群路徑中的所有中繼埠或接入埠。在圖中，只有一個通過Tengig1/0/2通往NLB的路徑。

```
<#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
```

---

注意：靜態MAC地址條目中可根據需要有任何數量的對映埠。此埠對映可減少NLB VLAN內的預期泛洪。在本例中，靜態MAC條目可以避免向NLB集群的流量從Te1/0/3泛洪出去。

---

## 不同VLAN中的源和目標

### 網路圖表



```
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. 為NLB群集伺服器的虛擬IP地址配置靜態ARP條目。必須在集群VLAN中具有交換機虛擬介面 (SVI)的所有第3層裝置上配置靜態ARP。靜態ARP的目的是允許交換機具有向NLB VLAN傳送路由資料包所需的重寫資訊。

```
<#root>
```

```
C9300-01(config)#
```

```
arp 10.1.1.85 0100.5e01.0155 arpa
```

3. 檢驗在接入層建立的使用者VLAN及其預設網關。您必須在雙方上設定預設閘道。( NLB群集和使用者 )。

```
<#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
```

---

注意：在重寫MAC報頭後路由的任何資料包，其目標MAC未在輸出SVI中獲知，然後資料包會在相應的VLAN中泛洪。為了緩解泛洪，您需要為NLB伺服器建立網關和單獨的VLAN。如果不希望為NLB流量配置專用VLAN，則可以為必須接收NLB流量的埠配置靜態MAC地址條目，即mac address-table static 0100.5exx.xxxx vlan #interface interface\_name

---

## 疑難排解

1. 驗證是否已將靜態MAC地址配置為需要將流量轉發到NLB的所有目標埠。

```
<#root>
C9300-01#
show mac address multicast
Vlan Mac Address Type Ports
---- -
10 0100.5e01.0155 USER Te1/0/2
```

2. 對於NLB群集與客戶端位於不同子網的部署，請驗證是否存在靜態ARP條目將NLB伺服器的虛擬IP與其組播MAC地址進行對映。

```
<#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
```





5.在具有EPC的輸入連線埠和具有SPAN的輸出連線埠上擷取封包擷取，並檢查交換器是否正在轉送資料。

```
<#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
```

---

提示：在第2層入口或出口方向轉發資料包時，嵌入式資料包捕獲(EPC)功能是可靠的。但是，如果流量由交換機路由然後轉發到出口埠，則EPC不可靠。若要在第3層路由發生後擷取輸出中的封包，請使用交換器連線埠分析器(SPAN)功能。

---

```
<#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
```

## 相關資訊

- [適用於Microsoft網路負載平衡的Catalyst交換器組態範例](#)
- [思科技術支援與下載](#)

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。