

Configuration des commutateurs Catalyst pour Microsoft NLB

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Mode Unicast](#)

[Mode Multicast](#)

[Mode IGMP](#)

[Cavasses du mode IGMP](#)

[Diagramme du réseau](#)

[Configuration](#)

[Configuration pour le mode multidiffusion](#)

[Configuration pour le mode IGMP](#)

[Vérification](#)

[Vérification du mode multidiffusion](#)

[Vérification du mode IGMP](#)

[Dépannage](#)

Introduction

Ce document décrit la méthode de configuration de commutateurs Cisco Catalyst afin qu'ils interagissent avec l'équilibrage de charge réseau (NLB) Microsoft.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations contenues dans ce document sont basées et configurées sur les versions logicielles et matérielles suivantes :

- Commutateur Catalyst 6500 Sup2T exécutant le logiciel Cisco IOS 15.1(1)SY1
- Commutateur Catalyst 4948 exécutant le logiciel Cisco IOS 15.0(2)SG7
- Serveurs Microsoft Windows

Note: Consultez le guide de configuration approprié pour connaître les commandes utilisées

afin d'activer ces fonctionnalités sur d'autres plates-formes Cisco.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

La technologie NLB peut être utilisée afin de distribuer les requêtes des clients sur un ensemble de serveurs. Afin de s'assurer que les clients bénéficient toujours de niveaux de performances acceptables, Microsoft Windows NLB permet d'ajouter des serveurs supplémentaires afin que vous puissiez étendre les applications sans état, telles que les serveurs Web basés sur IIS, à mesure que la charge client augmente. En outre, il réduit les temps d'arrêt causés par les serveurs qui ne fonctionnent pas correctement.

Microsoft Windows NLB est une technologie de mise en grappe qui fait partie de tous les systèmes d'exploitation Windows 2000 Server et Windows 2003 Server. Il fournit une adresse IP virtuelle unique pour tous les clients en tant qu'adresse IP de destination pour l'ensemble du cluster.

Vous pouvez configurer NLB pour fonctionner dans l'un des trois modes suivants :

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

Mode Unicast

Voici quelques notes sur l'utilisation de NLB en mode monodiffusion :

- En mode monodiffusion, NLB remplace l'adresse MAC (Media Access Control) réelle de chaque serveur du cluster par une adresse MAC NLB commune. Lorsque tous les serveurs du cluster ont la même adresse MAC, tous les paquets qui sont transférés à cette adresse sont envoyés à tous les membres du cluster. La NLB crée une adresse MAC fictive et l'attribue à chaque serveur du cluster NLB. Le NLB attribue à chaque serveur NLB une adresse MAC fictive différente, en fonction de l'ID d'hôte du membre. Cette adresse s'affiche dans l'en-tête de trame Ethernet.
- L'adresse MAC est utilisée dans l'en-tête ARP (Address Resolution Protocol), et non dans l'en-tête Ethernet. Le commutateur utilise l'adresse MAC contenue dans l'en-tête Ethernet et non celle de l'en-tête ARP. Cela entraîne un problème lorsqu'un paquet est envoyé au cluster NLB avec l'adresse MAC de destination comme adresse MAC de cluster 00-bf-ac-10-00-01. Le commutateur affiche la table Content Addressable Memory (CAM) pour l'adresse MAC 00-bf-ac-10-00-01 et comme aucun port n'est enregistré avec l'adresse MAC de cluster NLB 00-bf-ac-10-00-01, la trame est remise à tous les ports du commutateur. Ceci introduit *l'inondation de monodiffusion*. Afin d'éviter les inondations, Cisco vous recommande d'utiliser un VLAN dédié pour NLB afin que l'inondation soit limitée.

Mode Multicast

Voici quelques notes sur l'utilisation de NLB en mode multidiffusion :

- En mode Multicast, l'administrateur système clique sur le bouton Multicast dans l'interface utilisateur graphique de configuration de Microsoft NLB. Ce choix demande aux membres du cluster de répondre aux ARP pour leur adresse virtuelle en utilisant une adresse MAC de multidiffusion, telle que 0300.5e01.0101.
- Le processus ARP n'est pas terminé pour les adresses MAC de multidiffusion (ce qui casse la RFC 1812). Une adresse MAC statique est requise pour atteindre le cluster en dehors du sous-réseau local.
- L'adresse IP virtuelle est 10.100.1.99 et l'adresse MAC de multidiffusion est 0300.5e01.0101. Entrez cette commande afin de remplir la table ARP de manière statique :

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

- Puisque les paquets entrants ont une adresse IP de destination de monodiffusion et une adresse MAC de destination de multidiffusion, le périphérique Cisco ignore cette entrée et la monodiffusion inonde chaque paquet lié au cluster. Afin d'éviter cette inondation, insérez une entrée statique **mac-address-table** comme indiqué ci-dessous afin de commuter les paquets liés au cluster dans le matériel.

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

Note: Lorsque vous mappez de manière statique une adresse MAC à plusieurs ports, elle est uniquement prise en charge par le logiciel sur le commutateur de la gamme Cisco Catalyst 4500. En outre, l'utilisation de cette configuration sur le commutateur de la gamme Catalyst 4500 peut entraîner une utilisation élevée du CPU. Afin d'éviter ce problème, vous pouvez isoler la NLB vers un VLAN spécifique, ajouter uniquement les entrées ARP statiques et autoriser l'inondation sur ce VLAN.

Note: Pour les commutateurs de la gamme Cisco Catalyst 6000/6500, vous devez ajouter le paramètre disable-snooping pour limiter le trafic aux ports spécifiés uniquement. Lorsque vous configurez une connexion statique, entrez le mot clé disable-snooping pour empêcher que le trafic multicast adressé à l'adresse MAC multicast configurée de manière statique ne soit également envoyé à d'autres ports du même VLAN. (Cette commande n'est pas requise sur d'autres plates-formes).

Mode IGMP

Voici quelques notes sur l'utilisation de NLB en mode IGMP :

- L'utilisation de NLB en mode IGMP nécessite le moins de configuration manuelle. L'adresse MAC virtuelle fait partie de la plage IANA (Internet Assigned Numbers Authority) et commence par **0100.5exx.xxxx**. L'adresse MAC étant désormais conforme aux spécifications IANA, les commutateurs Cisco peuvent programmer dynamiquement l'adresse MAC à l'aide de la

surveillance IGMP. Cela supprime la nécessité de programmer manuellement l'adresse MAC sur les cartes de port requises en mode multidiffusion afin d'empêcher la propagation vers le VLAN.

- La surveillance IGMP programme l'adresse MAC virtuelle pour vous une fois que le commutateur reçoit un rapport d'appartenance d'un membre du cluster. Un port Mrouter doit également être programmé pour le VLAN NLB avec l'utilisation de la fonction PIM (Protocol Independent Multicast) ou de la fonction de requête IGMP.
- Puisque l'adresse IP virtuelle utilise une adresse MAC de multidiffusion, elle est inaccessible en dehors du sous-réseau local. Pour y remédier, vous devez configurer une entrée ARP statique sur chaque périphérique avec une interface de couche 3 (L3) dans le VLAN de cluster. Effectuez cette opération de la même manière qu'avec le mode multidiffusion. Par exemple, si l'adresse IP virtuelle est 10.100.1.99 et l'adresse MAC de multidiffusion est 0100.5e01.0101, utilisez cette commande afin de remplir la table ARP de manière statique :

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

Cavasses du mode IGMP

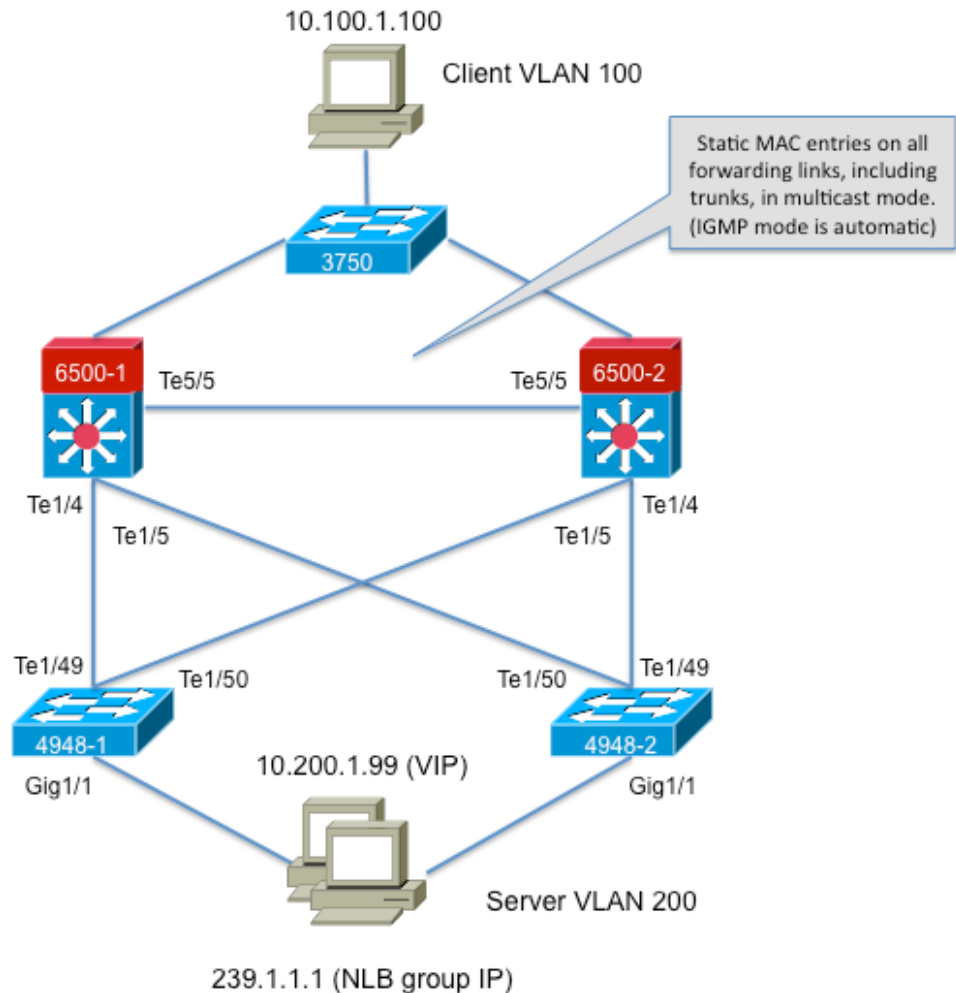
Voici quelques remarques importantes à garder à l'esprit lorsque vous utilisez NLB en mode IGMP :

Note: Comme suivi par l'ID de bogue Cisco [CSCsw72680](#), vous ne pouvez pas utiliser PIM sur l'interface virtuelle NLB VLANSwitch (SVI) avec certaines versions de code. Affichez les détails du bogue pour les versions de code qui répondent à ce problème ou utilisez la fonctionnalité de l'interrogateur IGMP Snooping.

Note: Comme suivi par l'ID de bogue Cisco [CSCsy62709](#) les paquets sont dupliqués pour tout le trafic qui est acheminé vers les serveurs NLB en mode IGMP. Affichez les détails du bogue pour les versions de code affectées.

Note: En raison d'une limitation matérielle qui est suivie par le trafic NLB Cisco n'ayant pas l'ID [CSCug49149](#) ne peut pas être envoyé via un Etherchannel distribué sur la même carte de ligne 6708 lorsque le commutateur est exécuté en mode PFC3B ou PFC3C. Le canal de port doit être câblé de sorte que toutes les liaisons membres soient sur le même moteur de transfert.

Diagramme du réseau



Configuration

Cette section décrit comment configurer NLB pour les plates-formes des gammes Cisco Catalyst 6500 et 4948 qui s'exécutent en mode Multicast ou IGMP.

Configuration pour le mode multidiffusion

Cette section décrit comment configurer NLB pour les plates-formes des gammes Cisco Catalyst 6500 et 4948 qui s'exécutent en mode multidiffusion :

```
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
!

```

Voici des remarques importantes concernant cette configuration :

- **La valeur d'adresse ip de l'interface Vlan100** configure le VLAN utilisateur.
- **La valeur d'adresse ip de l'interface Vlan200** configure le VLAN de cluster NLB. Il est important de configurer la passerelle par défaut de Microsoft Server à cette adresse.
- **Thearp 10.100.1.88 0300.5e01.0101 ARPA** inclut toutes les interfaces L3 dans le VLAN et est l'adresse IP virtuelle des serveurs de cluster NLB.
- **La table d'adresses MAC statique 0300.5e01.0101 vlan 200** interface crée une entrée MAC statique au mappage de port dans le commutateur pour l'adresse MAC virtuelle de multidiffusion.

Note: Assurez-vous d'utiliser le mode multidiffusion sur le cluster NLB. Cisco vous recommande de ne pas utiliser d'adresses MAC multicast commençant par 01 car elles entrent en conflit avec la configuration IGMP.

```

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

```

Note: L'interface **mac address-table static 0300.5e01.0101 vlan 200** crée une entrée statique dans le commutateur pour l'adresse MAC virtuelle de multidiffusion. Il est important de se

rappeler que toutes les interfaces d'agrégation qui transportent le trafic NLB entre les commutateurs doivent être ajoutées. Une fois qu'une adresse MAC statique est définie, la propagation est limitée. Si vous oubliez d'inclure une interface, le cluster NLB se brise.

Configuration pour le mode IGMP

Cette section décrit comment configurer NLB pour les plates-formes des gammes Cisco Catalyst 6500 et 4948 qui s'exécutent en mode IGMP

```
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
```

Voici des remarques importantes concernant cette configuration :

- Cette requête **igmp snooping** active la fonctionnalité de requête snooping.
- L'adresse **10.200.1.1** du demandeur de surveillance **igmp** configure le demandeur de surveillance pour le VLAN NLB.
- Le VLAN utilisateur est l'interface **Vlan100**.
- Le VLAN de cluster NLB est l'interface **Vlan200**. Il est important de configurer la passerelle par défaut de Microsoft Server à cette adresse (**adresse IP 10.200.1.1 255.255.255.0**).
- **Thearp 10.100.1.99 0100.5e01.0101 ARPA** est l'adresse IP virtuelle des serveurs de cluster NLB. Le protocole ARP statique doit se trouver sur toutes les interfaces L3 du VLAN.

```
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

```

Note: Il n'est pas nécessaire de configurer des entrées statiques, car IGMP Snooping le fait dynamiquement dans ce mode. En outre, aucune configuration spéciale n'est requise pour ce mode sur les commutateurs de couche 2 (L2) en aval.

Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Note: L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes show. Utilisez l'OIT pour afficher une analyse de la sortie de la commande show .

Vérification du mode multidiffusion

Entrez la commande **show ip arp** afin d'afficher le cache ARP :

```

6500-1#sh ip arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 10.100.1.99 - 0300.5e01.0101 ARPA

```

Saisissez le **show mac address-table static** afin d'afficher une entrée statique et dynamique de table d'adresses MAC spécifique ou les entrées statiques et dynamiques de table d'adresses MAC sur une interface ou un VLAN spécifique :

```

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

```

```

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
```

Vérification du mode IGMP

Entrez la commande **show ip arp** afin d'afficher le cache ARP :

```
6500-1#show ip arp
```

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

Entrez la commande **show ip igmp snooping mrouter** afin d'afficher le port Mrouter qui est programmé par les requêtes reçues du demandeur de snooping en amont :

```
4948-1#show ip igmp snooping mrouter
```

```
Vlan ports
-----
```

```
200 Te1/49 (dynamic)
```

Saisissez le **show mac address-table multicast igmp-snooping** afin d'afficher l'adresse MAC ajoutée dynamiquement qui est apprise de la surveillance IGMP et des ports membres :

```
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
```

Entrez la commande **show ip igmp snooping groups** afin d'afficher la liste des ports des membres du cluster qui ont rejoint le groupe de multidiffusion :

```
4948-1#show ip igmp snooping groups
```

```
Vlan Group Version Port List
```

```
-----+-----+-----+-----
200    239.1.1.1    v2          Gi1/1
```

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.