Configurer des VLAN privés isolés sur des commutateurs Catalyst

Table des matières

Introduction

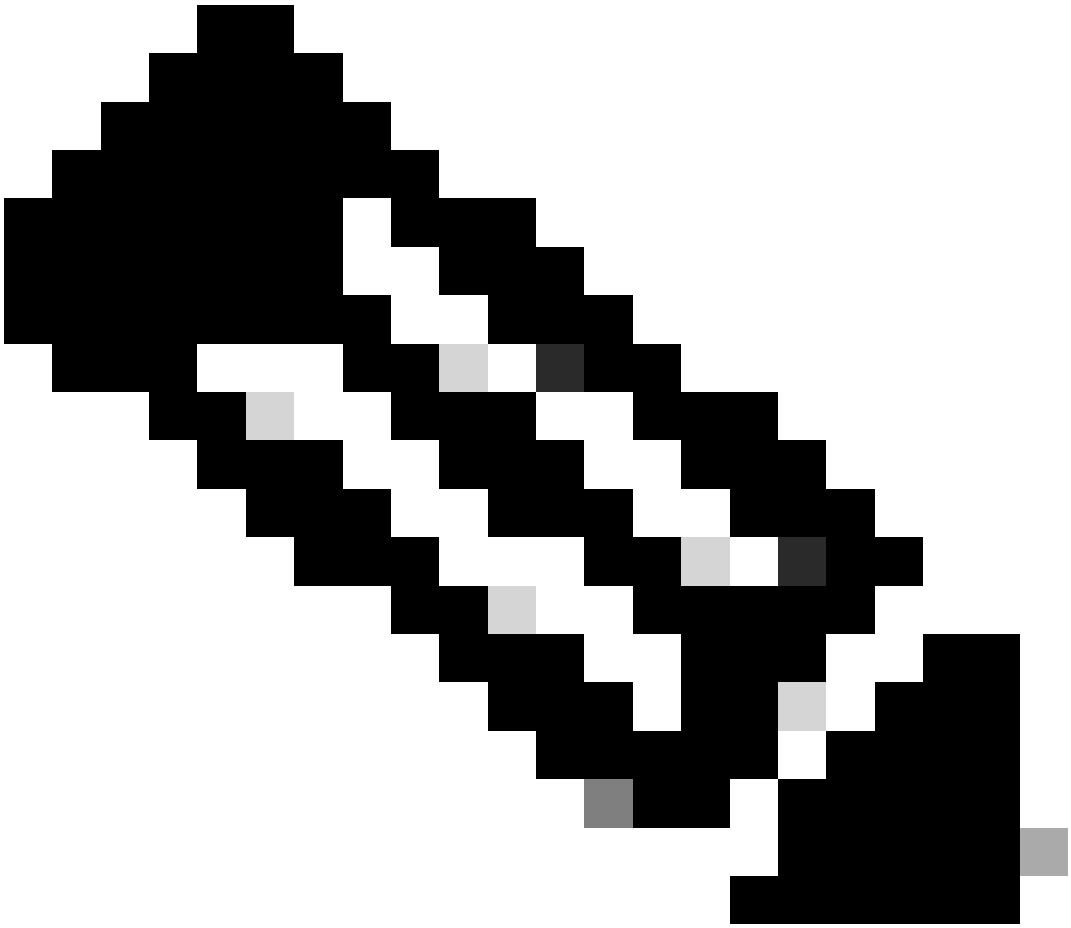
Ce document décrit la procédure pour configurer des PVLAN isolés sur des commutateurs Cisco Catalyst avec le logiciel Catalyst OS (CatOS) ou Cisco IOS®.

Conditions préalables

Exigences

Ce document suppose que vous avez un réseau qui existe déjà et pouvez établir la connectivité parmi les différents ports pour les ajouter à un PVLAN. Si vous avez plusieurs commutateurs, assurez-vous que l'agrégation entre les commutateurs fonctionne correctement et autorise les PVLAN sur l'agrégation.

Les PVLAN ne sont pas pris en charge par tous les commutateurs et toutes les versions logicielles.



Remarque : certains commutateurs (comme indiqué dans la matrice de prise en charge des commutateurs Catalyst pour VLAN privé) prennent actuellement en charge uniquement la fonctionnalité Périphérie PVLAN. Le terme « ports protégés » se rapporte également à cette fonctionnalité. Les ports d'extrémité PVLAN ont une restriction qui empêche la communication avec d'autres ports protégés sur le même commutateur. Les ports protégés sur des commutateurs distincts, cependant, peuvent communiquer les uns avec les autres. Ne confondez pas cette fonctionnalité avec les configurations normales PVLAN indiquées dans ce document. Pour plus d'informations sur les ports protégés,

---

consultez la section Configuration de la sécurité des ports du document Configuration du contrôle de trafic de port.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Commutateur Catalyst 4003 avec le module Supervisor Engine 2 qui exécute la version 6.3(5) de CatOS
- Commutateur Catalyst 4006 avec le module Supervisor Engine 3 qui exécute la version 12.1(12c)EW1 du logiciel Cisco IOS

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Dans certaines situations, vous devez empêcher la connectivité de la couche 2 (L2) entre les équipements d'extrémité sur un commutateur sans placer les périphériques dans différents sous-réseaux d'IP. Cette configuration empêche la perte d'adresses IP. Les VLAN privés (PVLAN) permettent l'isolation à la couche 2 de périphériques du même sous-réseau IP. Vous pouvez restreindre certains ports sur le commutateur pour atteindre seulement les ports spécifiques qui ont une passerelle par défaut, un serveur de secours ou un Cisco LocalDirector attaché.

Ce document décrit la procédure pour configurer des PVLAN isolés sur des commutateurs Cisco Catalyst avec Catalyst OS (CatOS) ou le logiciel Cisco IOS.

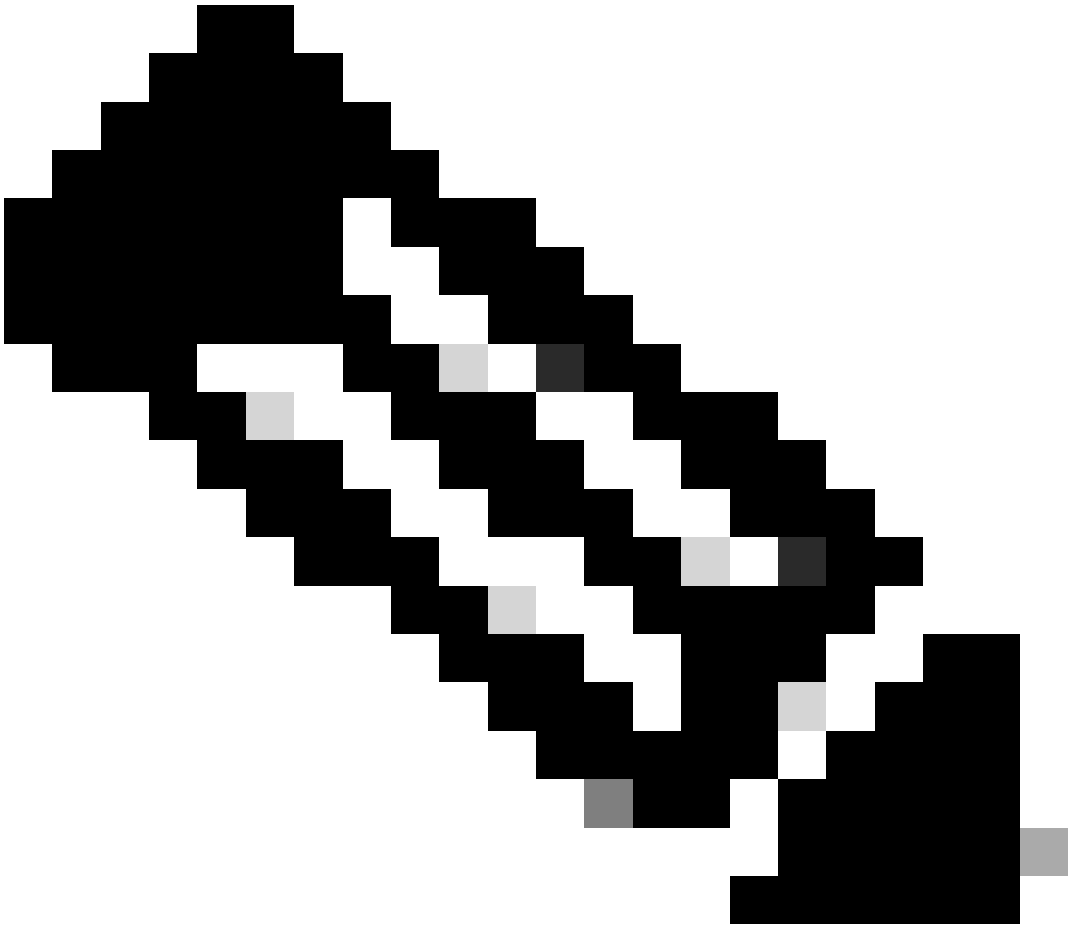
Un PVLAN est un VLAN avec la configuration pour l'isolation de la couche 2 d'autres ports dans le même domaine de diffusion ou sous-réseau. Vous pouvez attribuer un ensemble de ports spécifique dans un PVLAN et contrôler de ce fait l'accès parmi les ports à la couche 2. Vous pouvez configurer des PVLAN et des VLAN normaux sur le même commutateur.

Il existe trois types de ports PVLAN : les ports proches, les ports isolés et les ports communautaires.

- Un port proche communique avec tous autres ports PVLAN. Le port proche est le port que vous utilisez typiquement pour communiquer avec des routeurs externes, LocalDirectors, des périphériques d'administration de réseau, des serveurs de secours, des postes de travail

d'administration et d'autres périphériques. Sur certains commutateurs, le port allant au module de routage (par exemple, la carte de fonctionnalité de commutateur multicouche [MSFC]) doit être proche.

- Un port isolé est complètement séparé de la couche 2 d'autres ports dans le même PVLAN. Cette séparation inclut des diffusions, et la seule exception est le port proche. Un accord de confidentialité au niveau de la couche 2 se produit avec le bloc du trafic sortant vers tous les ports isolés. Le trafic qui provient d'un port isolé transmet uniquement à tous les ports proches.
- Les ports de communauté peuvent communiquer les uns avec les autres et avec les ports proches. Ces ports ont l'isolation de la couche 2 de tous autres ports dans d'autres communautés, ou les ports d'isolement dans le PVLAN. Les diffusions se propagent seulement entre les ports associés de la communauté et le port proche.



Remarque : ce document ne couvre pas la configuration VLAN de la communauté.

Règles et limitations

Cette section fournit quelques règles et limitations que vous devez observer quand vous implémentez des PVLAN.

- Les PVLAN ne peuvent pas inclure les VLAN 1 ou 1002-1005.
- Vous devez définir le mode de Protocole de jonction VLAN (VTP) à `transparent`.
- Vous pouvez seulement spécifier un VLAN isolé comme VLAN principal.
- Vous pouvez seulement désigner un VLAN comme PVLAN si ce VLAN n'a aucune affectation actuelle des ports d'accès. Supprimez tous les ports dans ce VLAN avant de transformer le VLAN en PVLAN.
- Ne configurez pas les ports PVLAN comme EtherChannels.
- En raison des limitations matérielles, les modules commutateurs Fast Ethernet de Catalyst 6500/6000 restreignent la configuration d'un port VLAN isolé ou de communauté quand un port du même circuit intégré d'entrée à application spécifique COIL (ASIC) est un des éléments suivants :
    - Une agrégation
    - Une destination de Switched Port Analyzer (SPAN)
    - Un port PVLAN proche

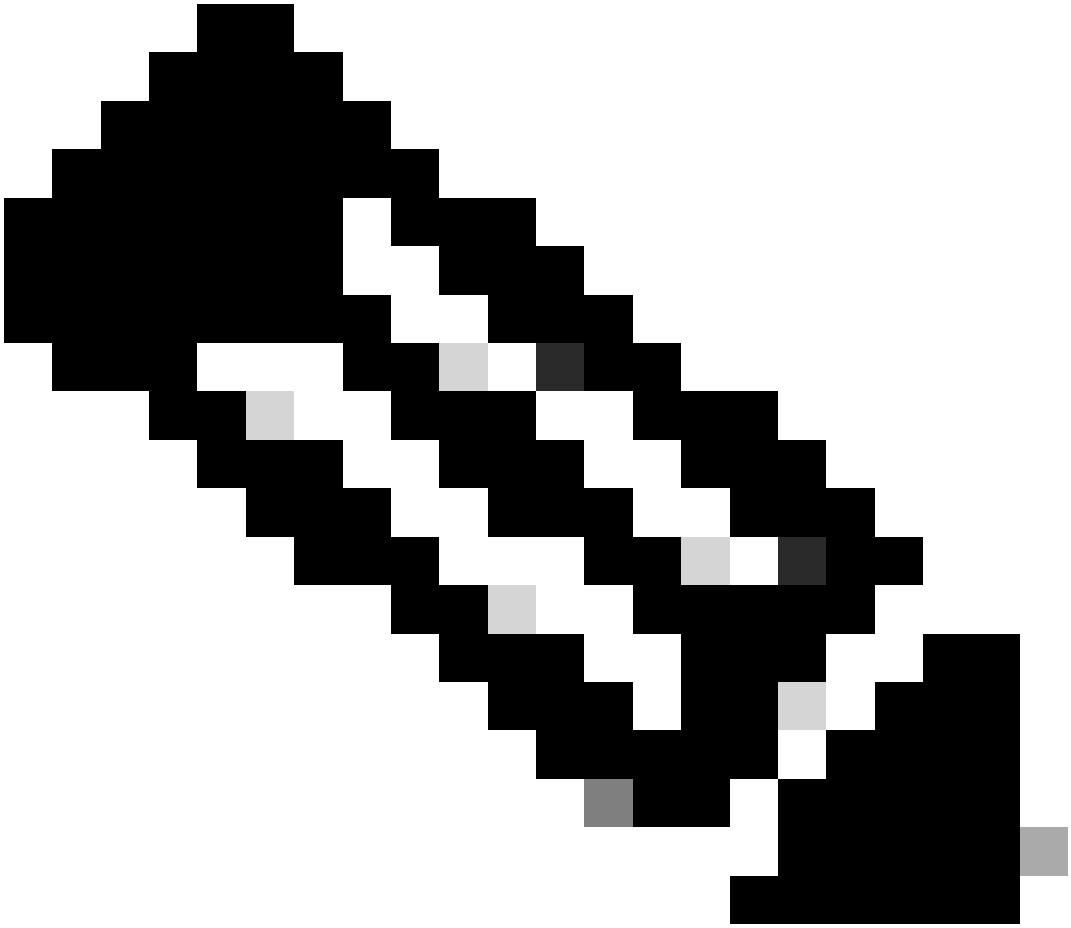
  Cette table indique la plage de ports appartenant au même ASIC sur des modules FastEthernet Catalyst 6500/6000 :

module	Ports par ASIC
WS-X6224-100FX-MT, WS-X6248-RJ-45, WS-X6248-TEL	Ports 1-12, 13-24, 25-36, 37-48
WS-X6024-10FL-MT	Ports 1-12, 13-24
WS-X6548-RJ-45, WS-X6548-RJ-21	Ports 1-48

La commande show pvlan capability (CatOS) indique également si vous pouvez transformer un port en port PVLAN. Il n'existe pas de commande équivalente dans le logiciel Cisco IOS.

- Si vous supprimez un VLAN que vous utilisez dans la configuration PVLAN, les ports qui s'associent au VLAN deviennent inactifs.
- Configurez les interfaces VLAN de la couche 3 (L3) seulement pour les VLAN principaux. Les interfaces VLAN pour les VLAN isolés et de communauté sont inactives, tandis que le VLAN a une configuration de VLAN isolé ou de communauté.
- Vous pouvez prolonger des PVLAN à travers des commutateurs en utilisant des agrégations. Les ports de jonction portent le trafic des VLAN réguliers et également des VLAN principaux, isolés et de communauté. Cisco recommande l'utilisation de ports de

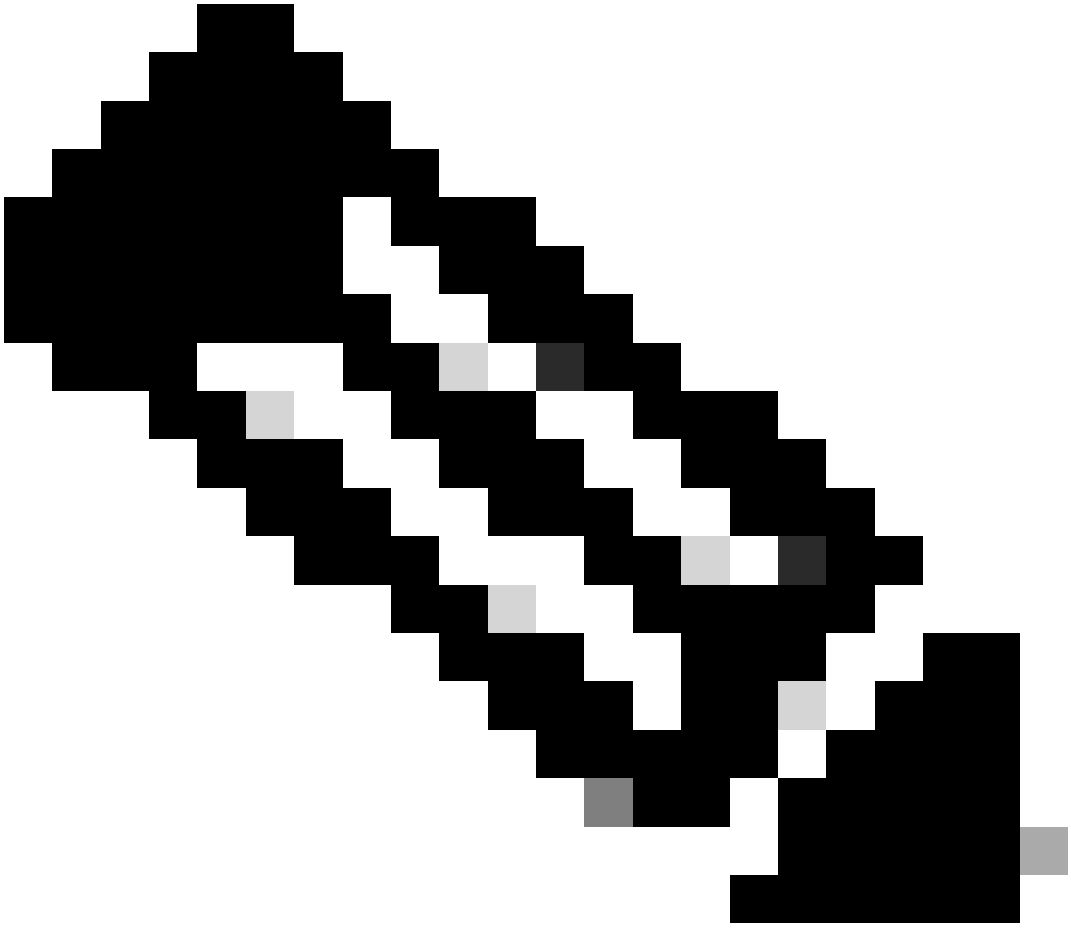
jonction standard si les deux commutateurs qui subissent l'agrégation prennent en charge les PVLAN.



Remarque : vous devez entrer manuellement la même configuration PVLAN sur chaque commutateur concerné, car le protocole VTP en mode transparent ne propage pas ces informations.

Configurer

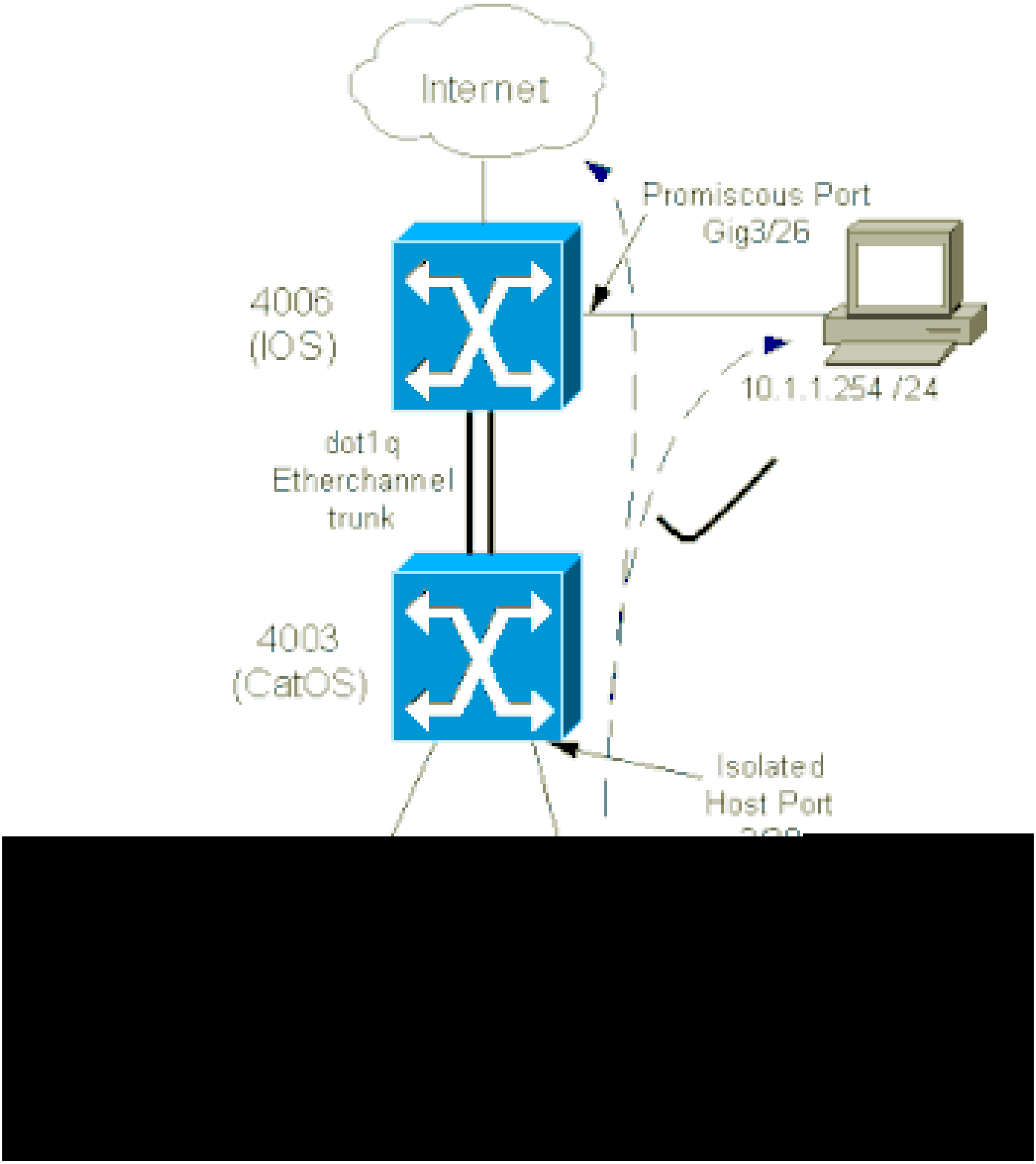
Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.



Remarque : utilisez l'outil Command Lookup Tool pour obtenir plus d'informations sur les commandes utilisées dans ce document. Seuls les utilisateurs enregistrés peuvent accéder aux informations et aux outils internes de Cisco.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Dans ce scénario, les périphériques dans le VLAN isolé (101) ont une restriction de communication au niveau de la couche 2 les uns avec les autres. Cependant, les périphériques peuvent se connecter à Internet. En outre, le port Gig 3/26 sur le 4006 a la désignation de promiscuité. Cette configuration facultative permet à un périphérique sur Gigabit Ethernet 3/26 de se connecter à tous les périphériques du VLAN isolé. Cette configuration permet également, par exemple, de sauvegarder des données de tous les périphériques hôtes PVLAN vers une station de travail de gestion. Les ports proches peuvent aussi être utilisés pour la connexion à un routeur externe, à LocalDirector, à un périphérique d'administration de réseau et à d'autres périphériques.

Configuration des VLAN principaux et isolés

Effectuez ces étapes pour créer le VLAN principal et le VLAN secondaire, et pour relier les différents ports à ces VLAN. Les étapes comprennent des exemples pour CatOS et le logiciel Cisco IOS®. Émettez le jeu de commandes approprié pour le système d'exploitation installé.

1. Créez le PVLAN principal.

    - CatOS

      <#root>

      ```
      Switch_CatOS> (enable)

      set vlan primary_vlan_id
      pvlan-type primary name primary_vlan


       !--- Note: This command must be on one line.

      VTP advertisements transmitting temporarily stopped,
      and will resume after the command finishes.
      Vlan 100 configuration successful
      ```

    - Logiciel Cisco IOS

      <#root>

      ```
      Switch_IOS(config)#

      vlan primary_vlan_id

      Switch_IOS(config-vlan)#

      private-vlan primary

      Switch_IOS(config-vlan)#

      name primary-vlan

      Switch_IOS(config-vlan)#

      exit
      ```

2. Créez le(s) VLAN isolé(s).

    - CatOS

      <#root>

      ```
      Switch_CatOS> (enable)
      ```

```
set vlan secondary_vlan_id
pvlan-type isolated name isolated_pvlan

 !--- Note: This command must be on one line.

VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 101 configuration successful
```

- Logiciel Cisco IOS

```
<#root>

Switch_IOS(config)#

vlan secondary_vlan_id

Switch_IOS(config-vlan)#

private-vlan isolated

Switch_IOS(config-vlan)#

name isolated_pvlan

Switch_IOS(config-vlan)#

exit
```

3. Reliez le(s) VLAN isolé(s) au VLAN principal.

- CatOS

```
<#root>

Switch_CatOS> (enable)

set pvlan primary_vlan_id secondary_vlan_id

Vlan 101 configuration successful
Successfully set association between 100 and 101.
```

- Logiciel Cisco IOS

```
<#root>

Switch_IOS(config)#

vlan primary_vlan_id
```

```
Switch_IOS(config-vlan)#
private-vlan association secondary_vlan_id
Switch_IOS(config-vlan)#
exit
```

4. Vérifiez la configuration de VLAN privé.

- CatOS

<#root>

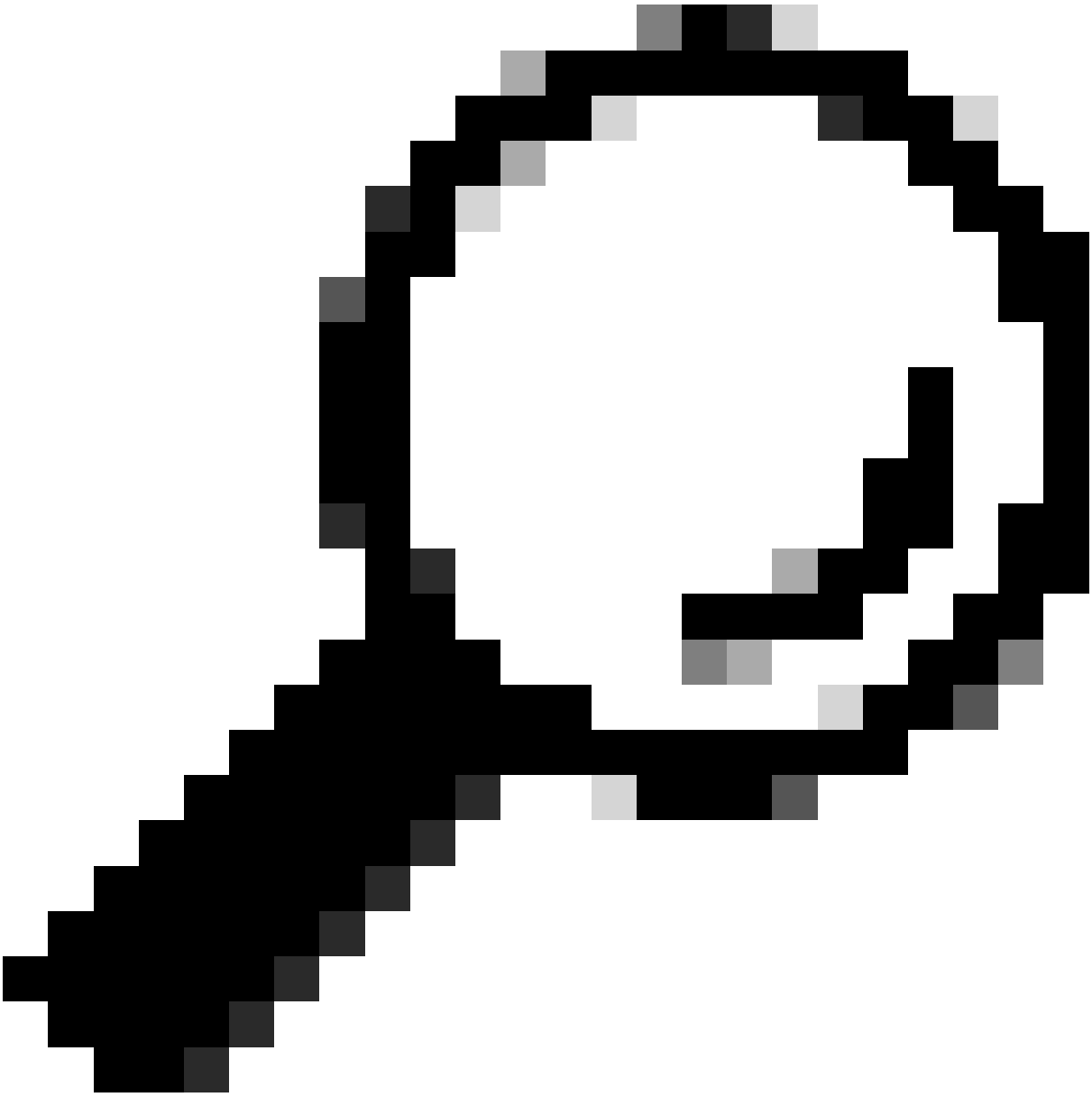
```
Switch_CatOS> (enable)
show pvlan
Primary Secondary Secondary-Type   Ports
------- --------- ---------------- ------------
100     101       isolated
```

- Logiciel Cisco IOS

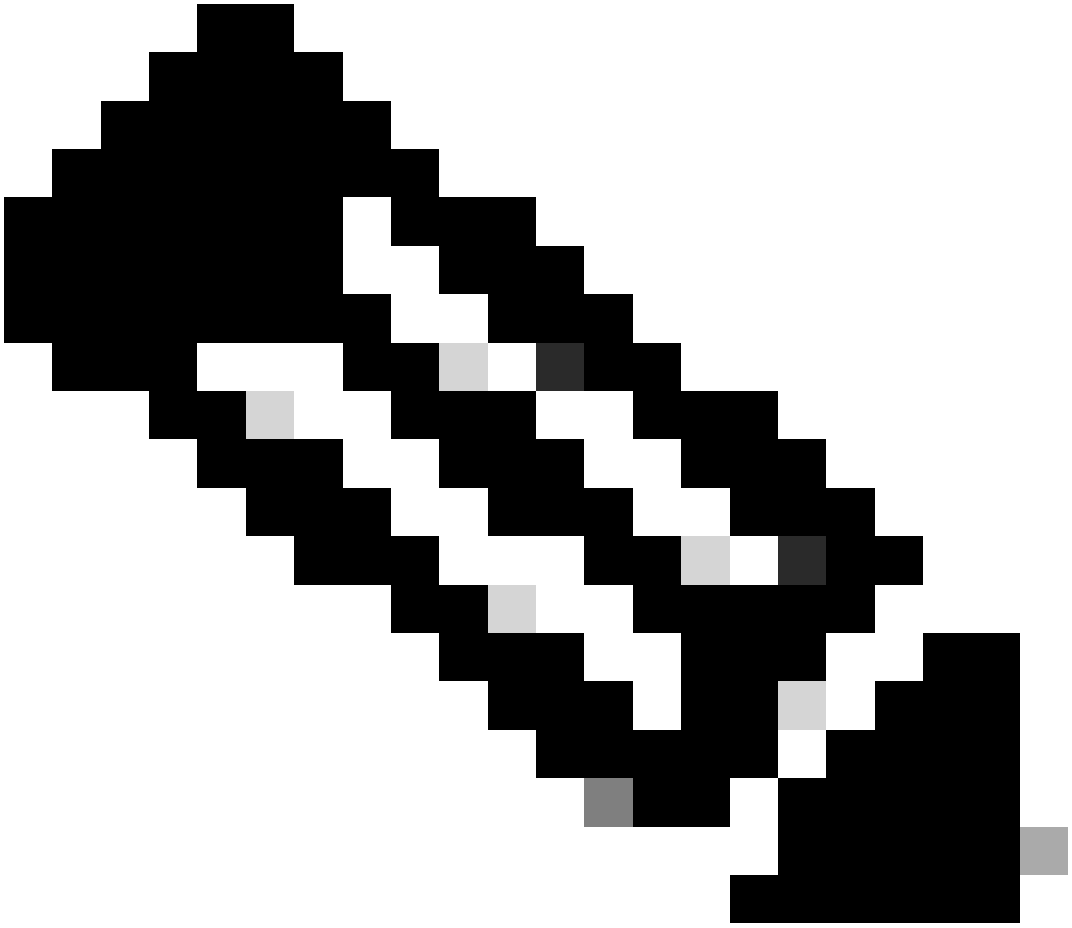
<#root>

```
Switch_IOS#
show vlan private-vlan
Primary  Secondary  Type              Ports
------- --------- ----------------- -------
100     101       isolated
```

Attribution de ports aux PVLAN



Conseil : avant d'implémenter cette procédure, exécutez la commandeshow PVLAN capability mod/port (pour CatOS) pour déterminer si un port peut devenir un port PVLAN.



Remarque : avant d'effectuer l'étape 1 de cette procédure, exécutez la commande switchport en mode de configuration d'interface pour configurer le port en tant qu'interface commutée de couche 2.

-

Configurez les ports hôte sur tous les commutateurs appropriés.

  - **CatOS**

<#root>

Switch_CatOS> (enable)

set pvlan primary_vlan_id secondary_vlan_id mod/port

!--- Note: This command must be on one line.

Successfully set the following ports to Private Vlan 100,101: 2/20

Logiciel Cisco IOS

<#root>

Switch_IOS(config)#

interface gigabitEthernet mod/port

Switch_IOS(config-if)#

switchport private-vlan host
primary_vlan_id secondary_vlan_id

!--- Note: This command must be on one line.

Switch_IOS(config-if)#

switchport mode private-vlan host

```
Switch_IOS(config-if)#
```

```
exit
```

- Configurez le port proche sur un des commutateurs.

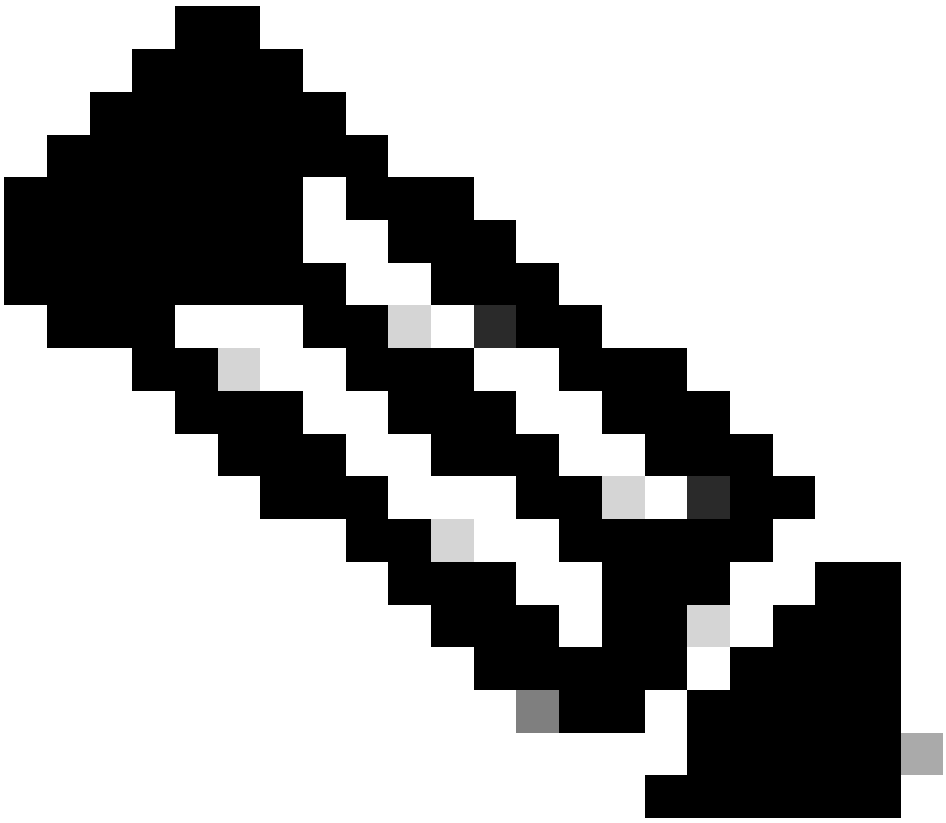
  - **CatOS**

```
<#root>
```

```
Switch_CatOS> (enable)
```

```
set pvlan mapping primary_vlan_id secondary_vlan_id mod/port
```

```
!--- Note: This command must be on one line.
Successfully set mapping between 100 and 101 on 3/26
```



Remarque : pour Catalyst 6500/6000 lorsque le Supervisor Engine exécute CatOS comme logiciel système, le port MSFC sur le Supervisor Engine (15/1 ou 16/1) doit être proche si vous souhaitez commuter la couche 3 entre les VLAN.

•

Logiciel Cisco IOS

<#root>

```
Switch_IOS(config)#


interface interface_type mod/port


Switch_IOS(config-if)#


switchport private-vlan
mapping primary_vlan_id secondary_vlan_id


 !--- Note: This command must be on one line.

Switch_IOS(config-if)#


switchport mode private-vlan promiscuous


Switch_IOS(config-if)#


end
```

Configuration de la couche 3

Cette section facultative décrit les étapes de configuration pour permettre le routage du trafic PVLAN en entrée. Si vous devez seulement activer la connectivité de la couche 2, vous pouvez omettre cette phase.

- Configurez l'interface VLAN de la même manière que lorsque vous configurez le routage normal de la couche 3.

Cette configuration implique :

- Configuration d'une adresse IP

- Activation de l'interface avec la commande **no shutdown**

- Vérification que le VLAN existe dans la base de données VLAN

Consultez l'assistance technique VLAN/VTP pour des exemples de configuration.

- Mappez les VLAN secondaires que vous souhaitez acheminer avec le VLAN principal.

<#root>

Switch_IOS(config)#

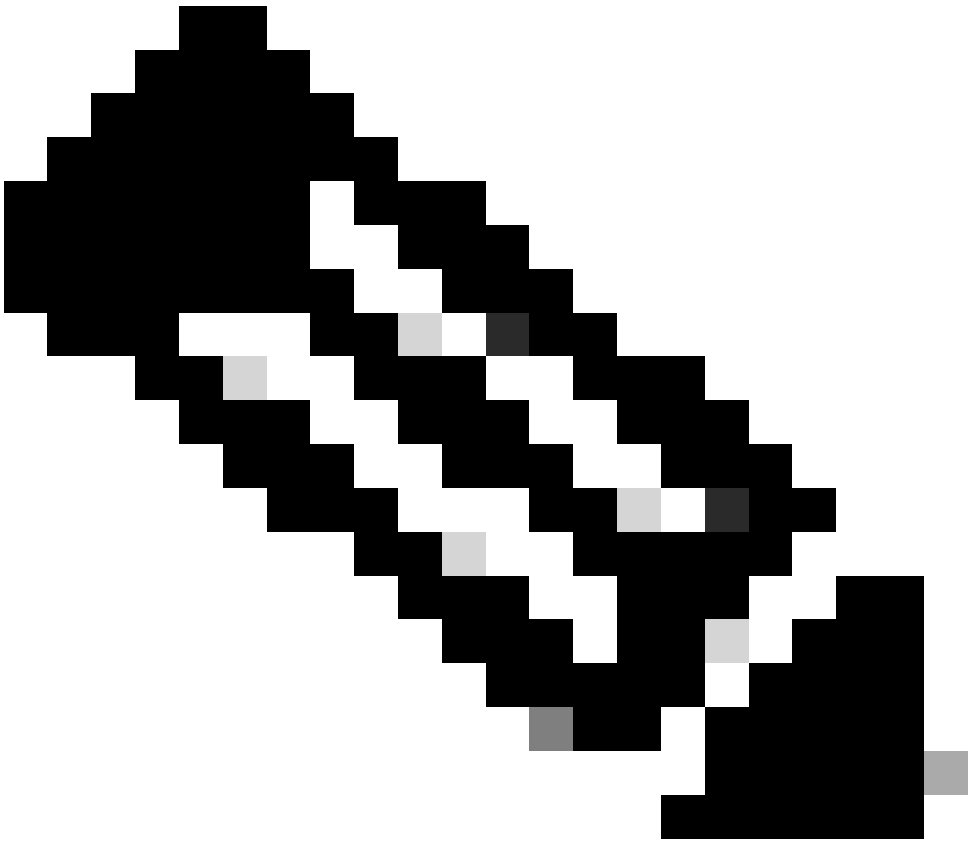
interface vlan primary_vlan_id

Switch_IOS(config-if)#

private-vlan mapping secondary_vlan_list

Switch_IOS(config-if)#

end



Remarque : configurez les interfaces VLAN de couche 3 uniquement pour les VLAN principaux. Les interfaces VLAN pour les VLAN isolés et de communauté sont inactives avec une configuration de VLAN isolé ou de communauté.

•

Émettez la commande **show interfaces private-vlan mapping (logiciel Cisco IOS) ou show pvlan mapping (CatOS) pour vérifier le mappage.**

•

Si vous devez modifier la liste de VLAN secondaire après la configuration du mappage, utilisez le mot clé **ajouter ou supprimer.**

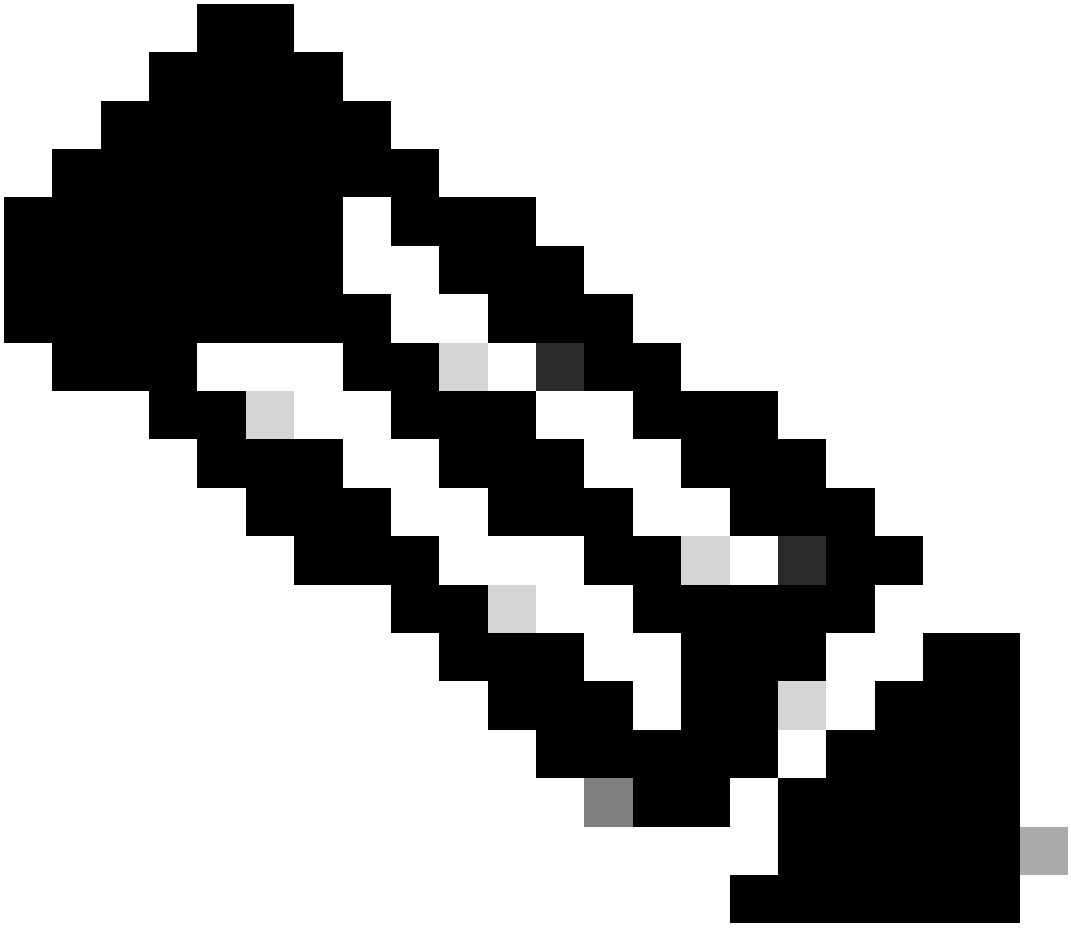
<#root>

Switch_IOS(config-if)#

private-vlan mapping add secondary_vlan_list

or
Switch_IOS(config-if)#

private-vlan mapping remove secondary_vlan_list



Remarque : pour les commutateurs Catalyst 6500/6000 avec MSFC, assurez-vous que le port du Supervisor Engine au moteur de routage (par exemple, le port 15/1 ou 16/1) est proche.

<#root>

```
cat6000> (enable)
```

set pvlan mapping primary_vlan secondary_vlan 15/1

```
Successfully set mapping between 100 and 101 on 15/1
```

Émettez la commande **show pvlan mapping** pour vérifier le mappage.

```
<#root>

cat6000> (enable)

show pvlan mapping

Port Primary Secondary
---- ------- ---------
15/1  100      101
```

Configurations

Ce document utilise les configurations suivantes :

- Couche d'accès (Catalyst 4003 : CatOS)
- Core (Catalyst 4006 : logiciel Cisco IOS)

Couche d'accès (Catalyst 4003 : CatOS)

```
<#root>

Access_Layer> (enable)
```

```
show config

 This command shows non-default configurations only.
 Use 'show config all' to show both default and non-default configurations.
 .............


!--- Output suppressed.


 #system
 set system name  Access_Layer
 !
 #frame distribution method
 set port channel all distribution mac both
 !
 #vtp
 set vtp domain Cisco
 set vtp mode transparent
 set vlan 1 name default type ethernet mtu 1500 said 100001 state active
 set vlan 100 name primary_for_101 type ethernet pvlan-type primary mtu 1500
 said 100100 state active

!--- This is the primary VLAN 100.
!--- Note: This command must be on one line.

 set vlan 101 name isolated_under_100 type ethernet pvlan-type isolated mtu
 1500 said 100101 state active

!--- This is the isolated VLAN 101.
!--- Note: This command must be on one line.

 set vlan 1002 name fddi-default type fddi mtu 1500 said 101002 state active


!--- Output suppressed.


 #module 1 : 0-port Switching Supervisor
 !
 #module 2 : 24-port 10/100/1000 Ethernet


set pvlan 100 101 2/20


!--- Port 2/20 is the PVLAN host port in primary VLAN 100, isolated
!--- VLAN 101.

 set trunk 2/3  desirable dot1q 1-1005
 set trunk 2/4  desirable dot1q 1-1005
 set trunk 2/20 off dot1q 1-1005

!--- Trunking is automatically disabled on PVLAN host ports.

 set spantree portfast    2/20 enable

!--- PortFast is automatically enabled on PVLAN host ports.

 set spantree portvlancost 2/1  cost 3


!--- Output suppressed.
```

```
 set spantree portvlancost 2/24 cost 3
 set port channel 2/20 mode off

!--- Port channeling is automatically disabled on PVLAN !--- host ports.

 set port channel 2/3-4 mode desirable silent
 !
 #module 3 : 34-port 10/100/1000 Ethernet
 end
```

Core (Catalyst 4006 : logiciel Cisco IOS)

<#root>

Core#

show running-config

```
 Building configuration...


!--- Output suppressed.

 !
 hostname Core
 !
 vtp domain Cisco
 vtp mode transparent

!--- VTP mode is transparent, as PVLANs require.

 ip subnet-zero
 !
 vlan 2-4,6,10-11,20-22,26,28
 !
 vlan 100
  name primary_for_101
   private-vlan primary
   private-vlan association 101
 !
 vlan 101
  name isolated_under_100
   private-vlan isolated
 !
 interface Port-channel1

!--- This is the port channel for interface GigabitEthernet3/1
!--- and interface GigabitEthernet3/2.

  switchport
  switchport trunk encapsulation dot1q
  switchport mode dynamic desirable
 !
 interface GigabitEthernet1/1
 !
 interface GigabitEthernet1/2
 !
```

```
 interface GigabitEthernet3/1

!--- This is the trunk to the Access_Layer switch.

  switchport trunk encapsulation dot1q
  switchport mode dynamic desirable
  channel-group 1 mode desirable
 !
 interface GigabitEthernet3/2

!--- This is the trunk to the Access_Layer switch.

  switchport trunk encapsulation dot1q
  switchport mode dynamic desirable
  channel-group 1 mode desirable
 !
 interface GigabitEthernet3/3
 !

!--- There is an omission of the interface configuration
!--- that you do not use.

 !
 interface GigabitEthernet3/26


  switchport private-vlan mapping 100 101
  switchport mode private-vlan promiscuous


!--- Designate the port as promiscuous for PVLAN 101.

 !

!--- There is an omission of the interface configuration
!--- that you do not use.

 !

!--- Output suppressed.

 interface Vlan25

!--- This is the connection to the Internet.

  ip address 10.25.1.1 255.255.255.0
 !
 interface Vlan100

!--- This is the Layer 3 interface for the primary VLAN.

  ip address 10.1.1.1 255.255.255.0
  private-vlan mapping 101

!--- Map VLAN 101 to the VLAN interface of the primary VLAN (100).
!--- Ingress traffic for devices in isolated VLAN 101 routes
!--- via interface VLAN 100.
```

Des VLAN privés peuvent être amenés à travers plusieurs commutateurs de deux manières. Cette section explique les deux méthodes :

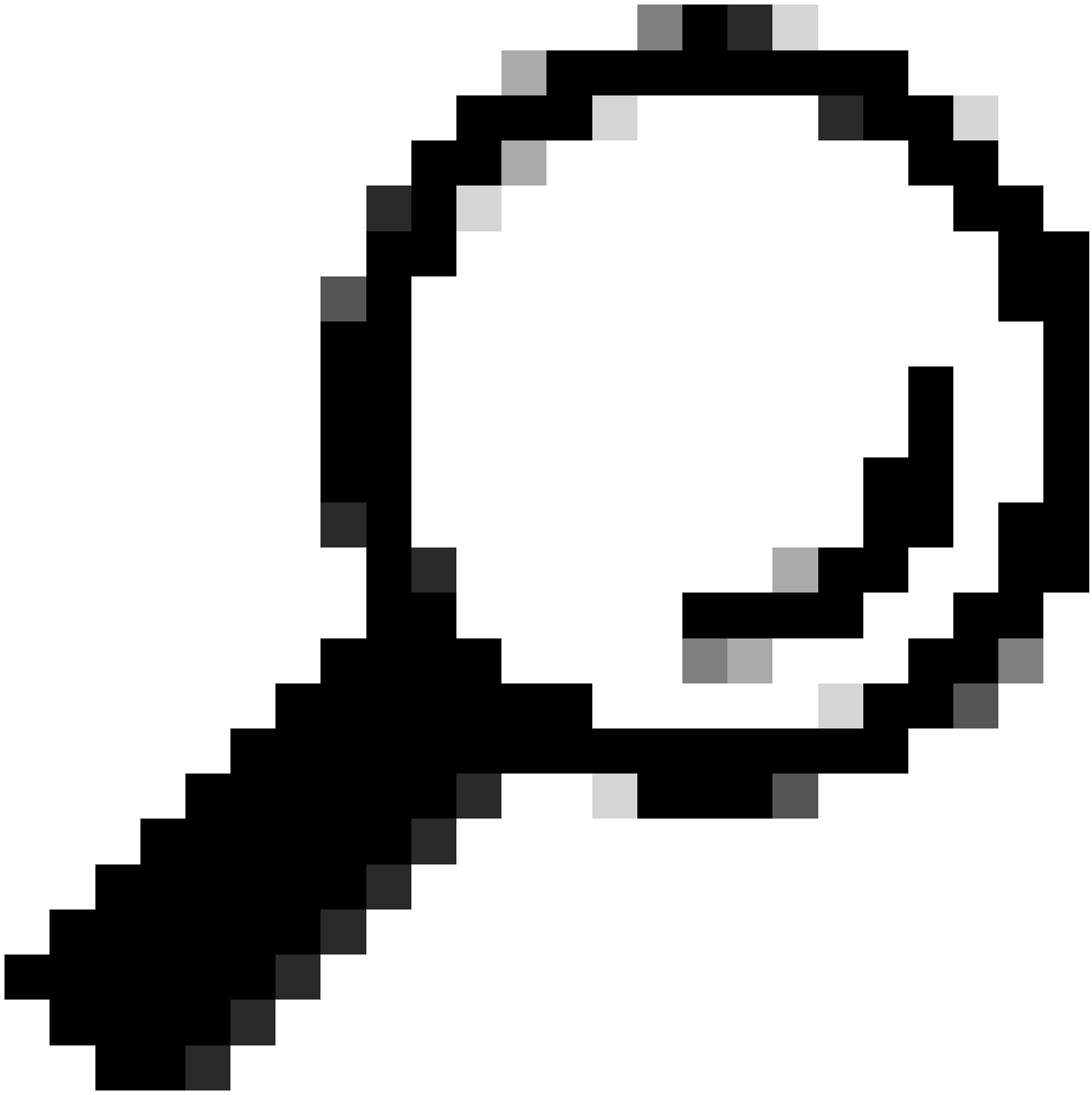
- Agrégations régulières
- Agrégations de VLAN privé

Agrégations régulières

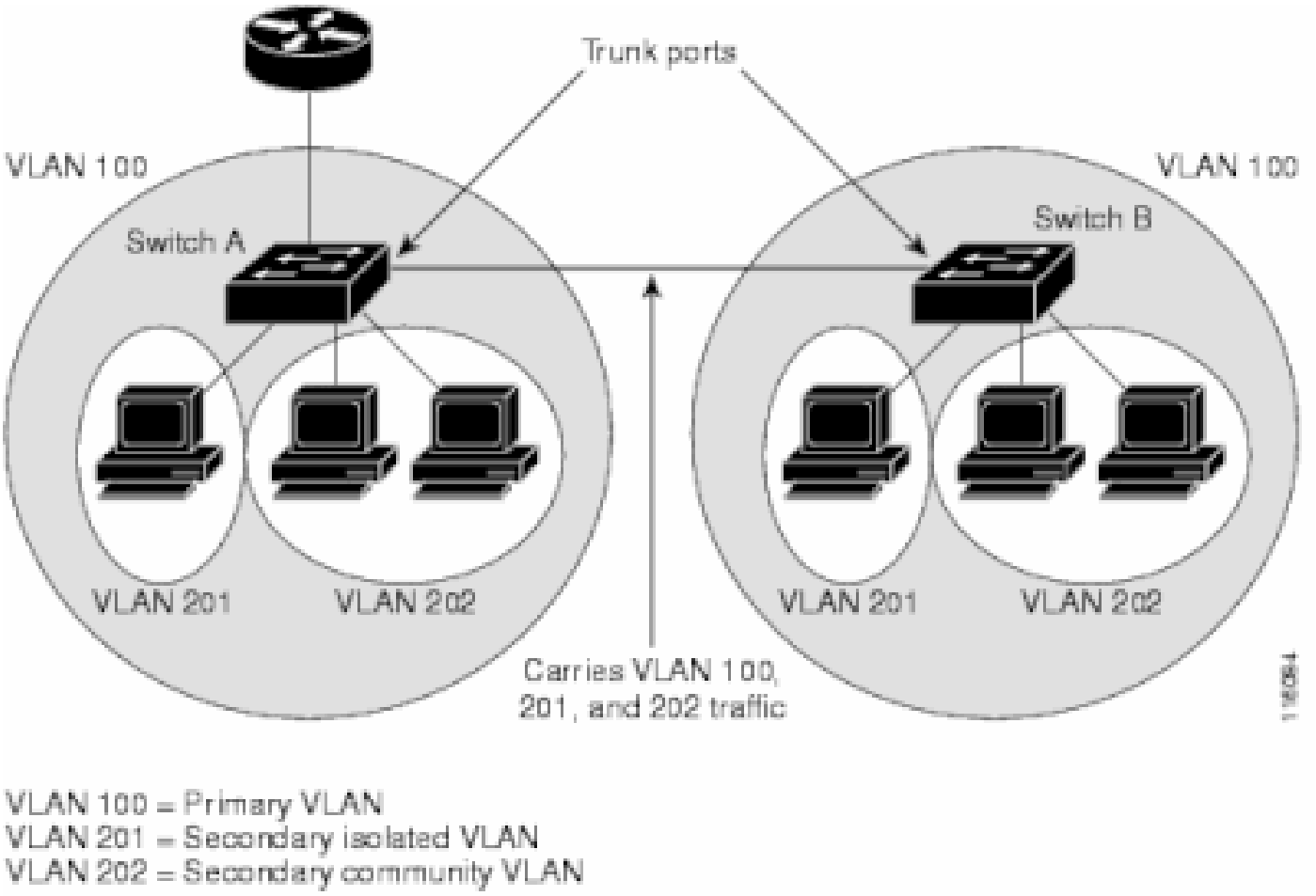
Comme les VLAN réguliers, les PVLAN peuvent s'étendre sur plusieurs commutateurs. Un port de jonction porte le VLAN principal et les VLAN secondaires à un commutateur voisin. Le port de jonction traite le VLAN privé comme n'importe quel autre VLAN. Une des fonctionnalité des PVLAN sur plusieurs commutateurs est le fait que le trafic d'un port isolé dans un commutateur n'atteint pas un port isolé sur un autre commutateur.

Configurez les PVLAN sur tous les équipements intermédiaires, y compris les périphériques qui n'ont aucun port PVLAN, afin de maintenir la sécurité de votre configuration PVLAN et d'éviter d'autres utilisations des VLAN configurés comme PVLAN.

Les ports de jonction portent le trafic des VLAN réguliers et également des VLAN principaux, isolés et de communauté.



Conseil : Cisco recommande l'utilisation de ports d'agrégation standard si les deux commutateurs qui subissent l'agrégation prennent en charge les PVLAN.



Configuration manuelle des réseaux locaux virtuels permanents sur tous les commutateurs du réseau de couche 2

Comme le VTP ne prend pas en charge les PVLAN, vous devez manuellement configurer les PVLAN sur tous les commutateurs dans le réseau de la couche 2. Si vous ne configurez pas l'association du VLAN principal et secondaire dans certains commutateurs du réseau, les bases de données de la couche 2 dans ces commutateurs ne sont pas fusionnées. Cette situation peut avoir comme conséquence l'inondation inutile du trafic PVLAN sur ces commutateurs.

Agrégations de VLAN privé

Un trunkport PVLAN peut porter plusieurs PVLAN secondaires et non. Des paquets sont reçus et transmis avec les balises VLAN secondaires ou régulières sur les ports de jonction PVLAN.

Seule l'encapsulation 802.1Q d'IEEE est prise en charge. Les ports de jonction isolés permettent de combiner le trafic de tous les ports secondaires sur une agrégation. Les ports de jonction proche permettent de combiner les ports proches multiples requis par cette topologie dans un port de jonction unique portant plusieurs VLAN principaux.

Utilisez les ports de jonction isolés de VLAN privé quand vous prévoyez d'utiliser des ports hôte isolés de VLAN privé pour porter plusieurs VLAN, soit normaux, soit pour plusieurs domaines VLAN privés. Cela est utile pour connecter un commutateur en aval qui ne prend pas en charge les VLAN privés.

Des agrégations proches de VLAN privé sont utilisées dans les situations où un port hôte proche de VLAN privé est normalement utilisé, mais où il est nécessaire de porter plusieurs VLAN, soit normaux, soit pour plusieurs domaines VLAN privés. Cela est utile pour connecter un routeur en amont qui ne prend en charge pas les VLAN privés.

Additional Information

Consultez la section Agrégations de VLAN privé pour plus d'informations.

Afin de configurer une interface en tant que port trunk PVLAN, référez-vous à Configuration d'une interface de couche 2 en tant que port trunk PVLAN .

Afin de configurer une interface en tant que port d'agrégation proche, référez-vous à Configuration d'une interface de couche 2 en tant que port d'agrégation proche .

Vérifier

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

CatOS

- **show pvlan - Affiche la configuration PVLAN.** Vérifiez que les VLAN isolés et principaux s'associent les uns aux autres. En outre, vérifiez que tous les ports hôte apparaissent.

- **show pvlan mapping - Affiche le mappage PVLAN avec la configuration sur des ports proches.**

Logiciel Cisco IOS

- **show vlan private-vlan - Affiche les informations PVLAN, qui incluent les ports qui s'associent.**

- **show interfacemod/portswitchport** : affiche des informations spécifiques à l'interface. Vérifiez que le mode opérationnel ainsi que les paramètres opérationnels PVLAN sont corrects.

- **show interfaces private-vlan mapping - Affiche le mappage PVLAN que vous avez configuré.**

Procédure de vérification

Procédez comme suit :

•

Vérifiez la configuration PVLAN sur les commutateurs.

Vérifiez et déterminez si les VLAN principaux et secondaire s'associent/se mappent les uns aux autres. En outre, vérifiez que les ports nécessaires sont inclus.

<#root>

```
Access_Layer> (enable)
```

show pvlan

```
Primary Secondary Secondary-Type   Ports
------- --------- ---------------- ------------
 100     101       isolated         2/20

Core#
```

show vlan private-vlan

```
Primary Secondary Type              Ports
------- --------- ----------------- -----------
100     101       isolated          Gi3/26
```

•

Vérifiez que le port proche est correctement configuré.

Ce résultat indique que le mode opérationnel de port est **proche et que les VLAN opérationnels sont 100 et 101.**

<#root>

```
Core#
```

show interface gigabitEthernet 3/26 switchport

Name: Gi3/26
Switchport: Enabled
Administrative Mode: private-Vlan promiscuous

Operational Mode: private-vlan promiscuous

Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative Private VLAN Host Association: none

Administrative Private VLAN Promiscuous Mapping: 100 (primary_for_101) 101 (isolated_under_100)

Private VLAN Trunk Native VLAN: none
Administrative Private VLAN Trunk Encapsulation: dot1q
Administrative Private VLAN Trunk Normal VLANs: none
Administrative Private VLAN Trunk Private VLANs: none

Operational Private VLANs:
100 (primary_for_101) 101 (isolated_under_100)

Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

•

Lancez un paquet ping Internet Control Message Protocol (ICMP) du port hôte au port proche.

N'oubliez pas que, comme les deux périphériques sont dans le même VLAN principal, les périphériques doivent être dans le même sous-réseau.

<#root>

host_port#

show arp

```
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.1.1.100             -   0008.a390.fc80  ARPA   FastEthernet0/24

!--- The Address Resolution Protocol (ARP) table on the client indicates
!--- that no MAC addresses other than the client addresses are known.
```

host_port#

ping 10.1.1.254

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.254, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/4 ms

!--- The ping is successful. The first ping fails while the
!--- device attempts to map via ARP for the peer MAC address.
```

host_port#

show arp

```
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.1.1.100             -   0008.a390.fc80  ARPA   FastEthernet0/24
```

Internet 10.1.1.254   0   0060.834f.66f0 ARPA   FastEthernet0/24

!--- There is now a new MAC address entry for the peer.

•

Lancez un ping ICMP entre les ports hôte.

Dans cet exemple, host_port_2 (10.1.1.99) tente d'envoyer une requête ping à > host_port (10.1.1.100). Ce ping échoue. Un ping d'un autre port hôte au port proche, cependant, réussit toujours.

<#root>

```
host_port_2#
```

ping 10.1.1.100

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.100, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

!--- The ping between host ports fails, which is desirable.

host_port_2#
```

ping 10.1.1.254

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.254, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms

!--- The ping to the promiscuous port still succeeds.

host_port_2#
```

show arp

```
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.1.1.99              -   0005.7428.1c40  ARPA   Vlan1
Internet  10.1.1.254             2   0060.834f.66f0  ARPA   Vlan1

!--- The ARP table includes only an entry for this port and
!--- the promiscuous port.
```

Dépannage

Dépannage des PVLAN

Cette section aborde quelques problèmes courants qui se posent avec des configurations PVLAN.

Problème 1

Vous obtenez ce message d'erreur : `%PM-SP-3-ERR_INCOMP_PORT : <mod/port> est défini sur inactive parce que <mod/port> est un port agrégé`.

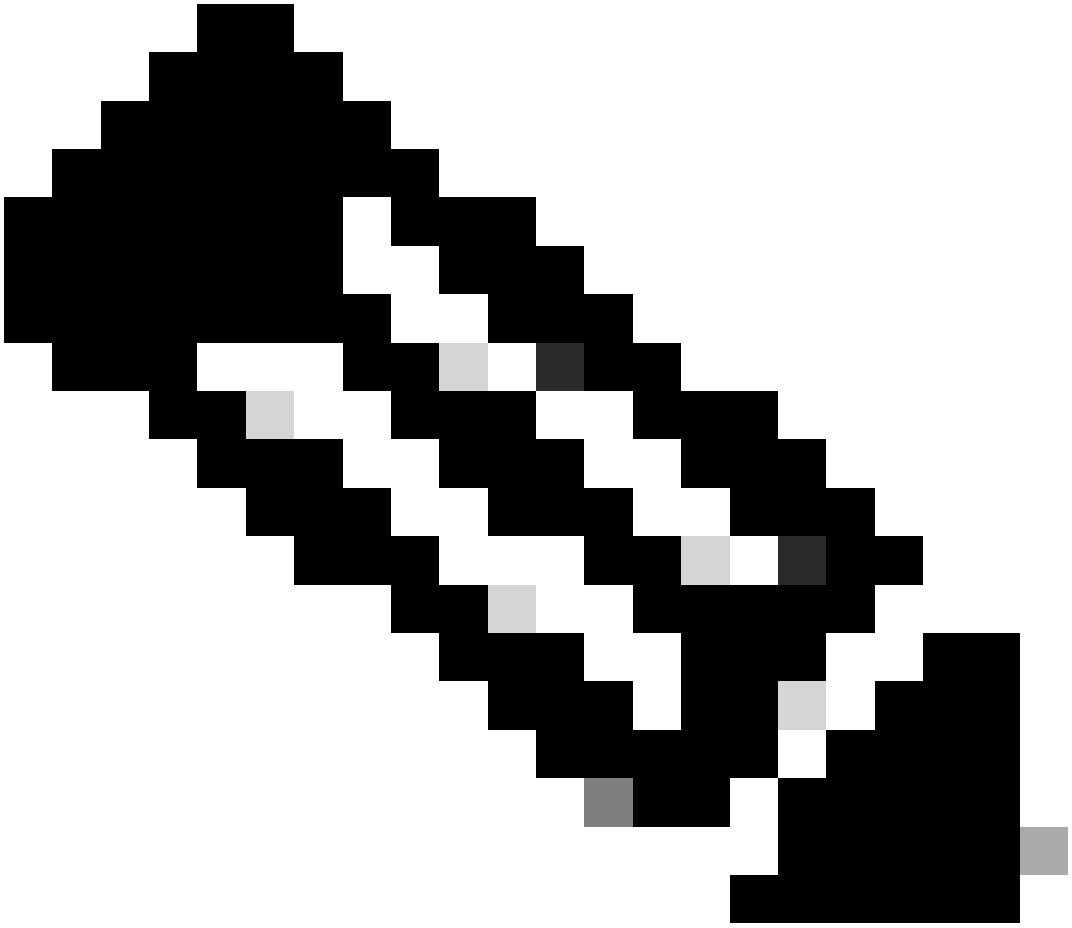
Ce message d'erreur peut être affiché pour plusieurs raisons, comme expliqué ici.

Explication - 1 : en raison de limitations matérielles, les modules 10/100 Mbits/s Catalyst 6500/6000 limitent la configuration d'un port VLAN isolé ou de communauté lorsqu'un port du même ASIC COIL est une agrégation, une destination SPAN ou un port PVLAN proche. (La BOBINE ASIC contrôle 12 ports sur la plupart des modules et 48 ports sur le module Catalyst 6548.) La table à la section Règles et limitations de ce document fournit une répartition de la restriction de port sur les modules 10/100-Mbps Catalyst 6500/6000.

Procédure de résolution - 1 : si le PVLAN n'est pas pris en charge sur ce port, sélectionnez un port sur un autre ASIC sur le module ou sur un autre module. Afin de réactiver les ports, supprimez la configuration de VLAN isolé ou de communauté et émettez la commande **shutdown et no shutdown.**

Explication - 2 : si les ports sont configurés manuellement ou par défaut en mode *dynamic desirable* ou *dynamic auto*.

Procédure de résolution - 2 : configurez les ports en mode d'accès à l'aide de la commande **switchport mode access**. Afin de réactiver les ports, émettez la commande **shutdown et la commande no shutdown.**



Remarque : dans le logiciel Cisco IOS version 12.2(17a)SX et versions ultérieures, la restriction de 12 ports ne s'applique pas aux modules de commutation Ethernet WS-X6548-RJ-45, WS-X6548-RJ-21 et WS-X6524-100FX-MM.

Problème 2

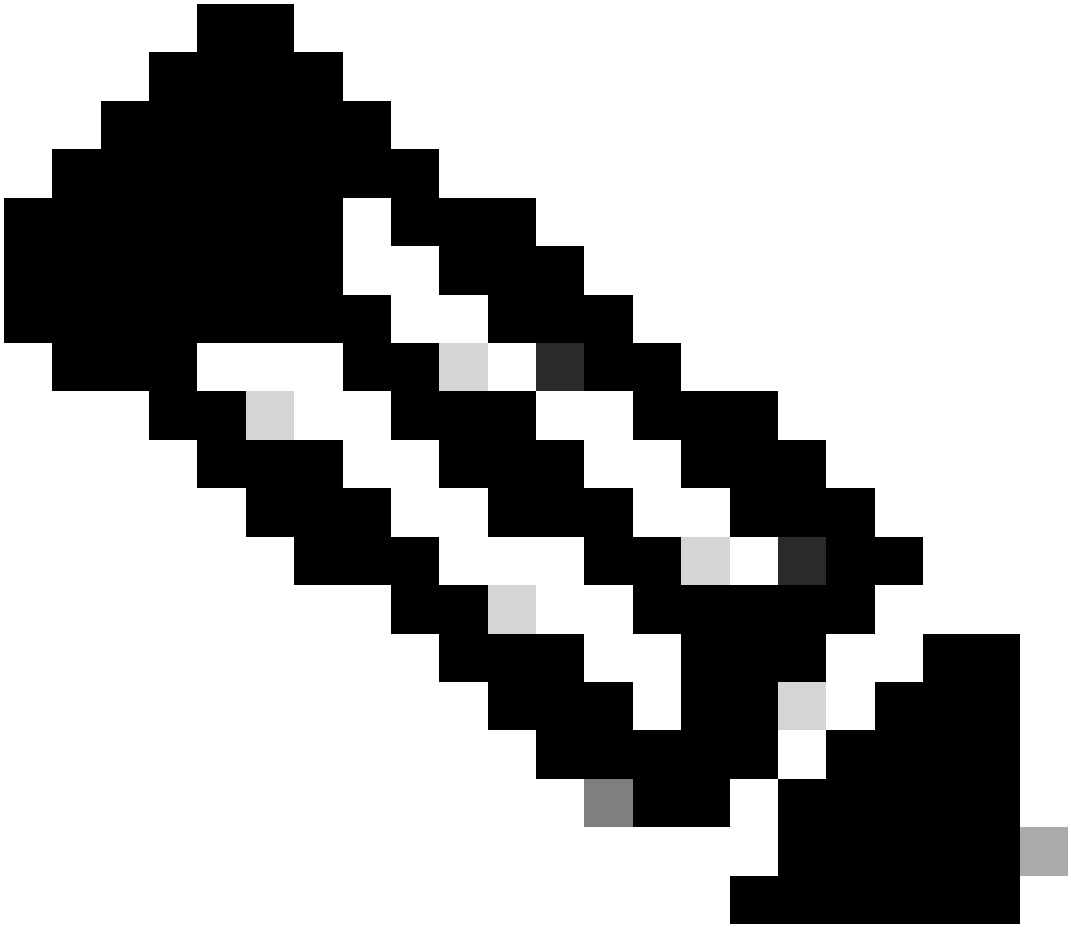
Pendant la configuration PVLAN, vous rencontrez *un de ces messages :*

```
Cannot add a private vlan mapping to a port with another Private port in
the same ASIC.
Failed to set mapping between <vlan> and <vlan> on <mod/port>
```

```
Port with another Promiscuous port in the same ASIC cannot be made
Private port.
Failed to add ports to association.
```

Explication : en raison de limitations matérielles, les modules 10/100 Mbits/s Catalyst 6500/6000 limitent la configuration d'un port VLAN isolé ou de communauté lorsqu'un port du même ASIC COIL est une agrégation, une destination SPAN ou un port PVLAN proche. (La BOBINE ASIC contrôle 12 ports sur la plupart des modules et 48 ports sur le module Catalyst 6548.) La table à la section Règles et limitations de ce document fournit une répartition de la restriction de port sur les modules 10/100-Mbps Catalyst 6500/6000.

Procédure de résolution : Exécutez la commande **show pvlan capability** (CatOS), qui indique si un port peut devenir un port PVLAN. S'il n'y a aucune prise en charge de PVLAN sur ce port, choisissez un port sur un autre ASIC du module ou sur un autre module.



Remarque : dans le logiciel Cisco IOS version 12.2(17a)SX et versions ultérieures, la restriction de 12 ports ne s'applique pas aux modules de commutation Ethernet WS-X6548-RJ-45, WS-X6548-RJ-21 et WS-X6524-100FX-MM.

Problème 3

Vous ne pouvez pas configurer de PVLAN sur certaines plates-formes.

Résolution : vérifiez que la plate-forme prend en charge les PVLAN. Consultez la section Matrice de prise en charge des commutateurs Catalyst de VLAN privés pour déterminer si votre plate-forme et votre version de logiciel prennent en charge les PVLAN avant de commencer la configuration.

Problème 4

Sur un Catalyst 6500/6000 MSFC, vous ne pouvez pas exécuter de commande ping sur un périphérique qui se connecte au port isolé sur le commutateur.

Résolution : sur le Supervisor Engine, vérifiez que le port vers le MSFC (15/1 ou 16/1) est proche.

```
<#root>

cat6000> (enable)

set pvlan mapping primary_vlan secondary_vlan 15/1

Successfully set mapping between 100 and 101 on 15/1
```

En outre, configurez l'interface VLAN sur le MSFC comme spécifié à la section Configuration de la couche 3 de ce document.

Problème 5

Avec le problème de la commande **no shutdown, vous ne pouvez pas activer l'interface VLAN pour les VLAN isolés ou de communauté.**

Résolution : en raison de la nature des PVLAN, vous ne pouvez pas activer l'interface VLAN pour les VLAN isolés ou de communauté. Vous pouvez seulement activer l'interface VLAN qui appartient au VLAN principal.

Problème 6

Sur des périphériques Catalyst 6500/6000 avec MSFC/MSFC2, les entrées ARP apprises sur des interfaces PVLAN de la couche 3 ne vieillissent pas.

Résolution : les entrées ARP apprises sur les interfaces VLAN privées de couche 3 sont des entrées ARP rémanentes et ne vieillissent pas. La connexion de nouveau matériel avec la même adresse IP génère un message, et il n'y a aucune création d'entrée ARP. Par conséquent, vous devez supprimer manuellement les entrées ARP de port PVLAN si une adresse MAC change. Afin d'ajouter ou de supprimer des entrées ARP PVLAN manuellement, émettez ces commandes :

```
<#root>

Router(config)#

no arp 10.1.3.30

IP ARP:Deleting Sticky ARP entry 10.1.3.30
Router(config)#

arp 10.1.3.30 0000.5403.2356 arpa

IP ARP:Overwriting Sticky ARP entry 10.1.3.30, hw:00d0.bb09.266e by
hw:0000.5403.2356
```

Vous pouvez aussi émettre la commande **no ip sticky-arp dans le logiciel Cisco IOS version 12.1(11b)E et ultérieures.**

Informations connexes

- **Commutateurs de la gamme Cisco Catalyst 2955 - Notification de retrait**
- **Réseaux sécurisés avec PVLAN et VACL**

- **Prise en charge de la technologie de commutation LAN**
- **Assistance technique de Cisco et téléchargements**

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.