Configurer des VLAN privés isolés sur les commutateurs Catalyst

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
  - Conventions
- Informations générales
  - Règles et restrictions
- Configurer
  - Exemple 1 : PVLAN isolé sur un commutateur Cisco IOS XE
  - Diagramme du réseau
  - Étape 1 : configuration du mode transparent VTP
  - Étape 2 : configuration des réseaux locaux virtuels principaux et isolés
  - Étape 3 : configuration des ports hôtes isolés
  - Étape 4. Configuration du port de proximité
  - Configuration de couche 3
    - Méthode 1 : Configuration de l'interface SVI du VLAN principal
    - Méthode 2 : Connexion du modem routeur à un port proche
  - Vérification
  - Exemple 2 : PVLAN sur plusieurs commutateurs Cisco IOS XE
  - Diagramme du réseau
  - Vérification
- Informations connexes

Introduction

Ce document décrit comment configurer des VLAN privés isolés (PVLAN), sur des commutateurs de la gamme Cisco Catalyst 9000 qui exécutent le logiciel Cisco IOS XE.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration VLAN
- Solutions de liaisons 802.1Q
- Interface de ligne de commande (CLI) de base de Cisco IOS XE

Composants utilisés

Ce document est basé sur ces versions logicielles et matérielles ; cependant, PVLAN n'est pas limité à ces versions. Validez la prise en charge PVLAN, la syntaxe des commandes et les restrictions pour la plate-forme spécifique et la version Cisco IOS XE avant le déploiement :

- Commutateurs de la gamme Cisco Catalyst 9300 qui exécutent le logiciel Cisco IOS XE versions 17.X et 26.X

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 couche 2 entre les périphériques finaux sur un commutateur sans placer les périphériques dans des sous-réseaux IP différents. Les PVLAN assurent l’isolation de couche 2 entre les ports qui appartiennent au même sous-réseau IP. Cette conception est utile lorsque les hôtes doivent atteindre une passerelle par défaut, un pare-feu, un équilibreur de charge ou un service partagé, mais ne doivent pas communiquer directement avec d'autres hôtes isolés du même VLAN et permet également de préserver les sous-réseaux IP.

Un PVLAN sépare un domaine de diffusion de couche 2 en un VLAN principal et un ou plusieurs VLAN secondaires. Vous pouvez affecter un ensemble spécifique de ports dans un PVLAN et contrôler ainsi l'accès entre les ports au niveau de la couche 2. Vous pouvez configurer des PVLAN et des VLAN normaux sur le même commutateur.

Il existe trois types de ports PVLAN : promiscuité, isolement et communauté.

Types de ports PVLAN

Type de port	Description	Diffusion, monodiffusion inconnue et comportement de multidiffusion
Promiscueux	Communique avec tous les ports du domaine PVLAN associé. Ce port se connecte généralement à une passerelle par défaut, un pare-feu, un routeur, un équilibreur de charge ou un service partagé.	Un port proche peut recevoir du trafic provenant de ports isolés et de ports de communauté. Le trafic de diffusion, de monodiffusion inconnue et de multidiffusion provenant d'un port proche peut être transféré vers les ports VLAN secondaires associés. Le trafic de diffusion provenant des ports VLAN secondaires peut être transféré au port proche.
Isolé	Ne communique qu'avec des ports proches. Il ne communique pas avec d'autres ports isolés dans le même PVLAN.	Le trafic de diffusion, de monodiffusion inconnue et de multidiffusion provenant d'un port isolé est transféré uniquement vers les ports proches associés. Il n'est pas transmis à d'autres ports isolés ou à des ports de communauté. Le trafic de diffusion en provenance d'autres ports isolés n'est pas reçu par un port isolé.
Communauté	Communique avec les ports de la même communauté et avec les ports proches.	Le trafic de diffusion, de monodiffusion inconnue et de multidiffusion provenant d'un port de communauté est transféré vers d'autres ports du même VLAN de communauté et vers les ports proches associés. Il n'est pas transmis aux ports isolés ou aux ports d'autres VLAN de communauté.

Types de VLAN PVLAN

Type de VLAN	Description
VLAN principal	Transporte le trafic des ports proches et le mappe aux VLAN secondaires.
VLAN isolé	VLAN secondaire utilisé pour l’isolation des hôtes. Les ports isolés de ce VLAN ne peuvent pas communiquer entre eux au niveau de la couche 2.

Remarque : Les PVLAN contrôlent le transfert de couche 2 au sein du même domaine VLAN principal. Les ports isolés restent dans le même sous-réseau IP que le VLAN principal, mais le trafic de couche 2 entre les hôtes isolés est bloqué. Cela inclut le trafic de diffusion, tel que le protocole ARP (Address Resolution Protocol), entre des hôtes isolés. Les hôtes isolés peuvent toujours résoudre et atteindre la passerelle par défaut ou d'autres services connectés via un port proche associé.

Règles et restrictions

Cette section fournit quelques règles et limitations que vous devez surveiller lorsque vous mettez en oeuvre des PVLAN.

- Les PVLAN ne peuvent pas inclure les VLAN 1 ou 1002-1005.
- Les PVLAN sont pris en charge en mode transparent pour VTP 1, 2 et 3. Les VLAN privés sont également pris en charge en mode serveur avec VTP 3.
- Configurez les interfaces VLAN de couche 3 (SVI) uniquement pour les VLAN principaux.
- Vous ne pouvez désigner un VLAN en tant que PVLAN que si ce VLAN n'a pas d'affectation de port d'accès actuel. Supprimez tous les ports de ce VLAN avant de le transformer en PVLAN.

Remarque : Pour connaître les restrictions PVLAN détaillées, notamment les limitations spécifiques à la plate-forme et la prise en charge d'EtherChannel avec les modes trunk PVLAN, reportez-vous aux restrictions de VLAN privé dans le Guide de configuration VLAN de Cisco IOS XE pour la plate-forme Catalyst cible : Gamme Catalyst 9500, Restrictions pour VLAN privés et gamme Catalyst 9300, Restrictions pour VLAN privés

Configurer

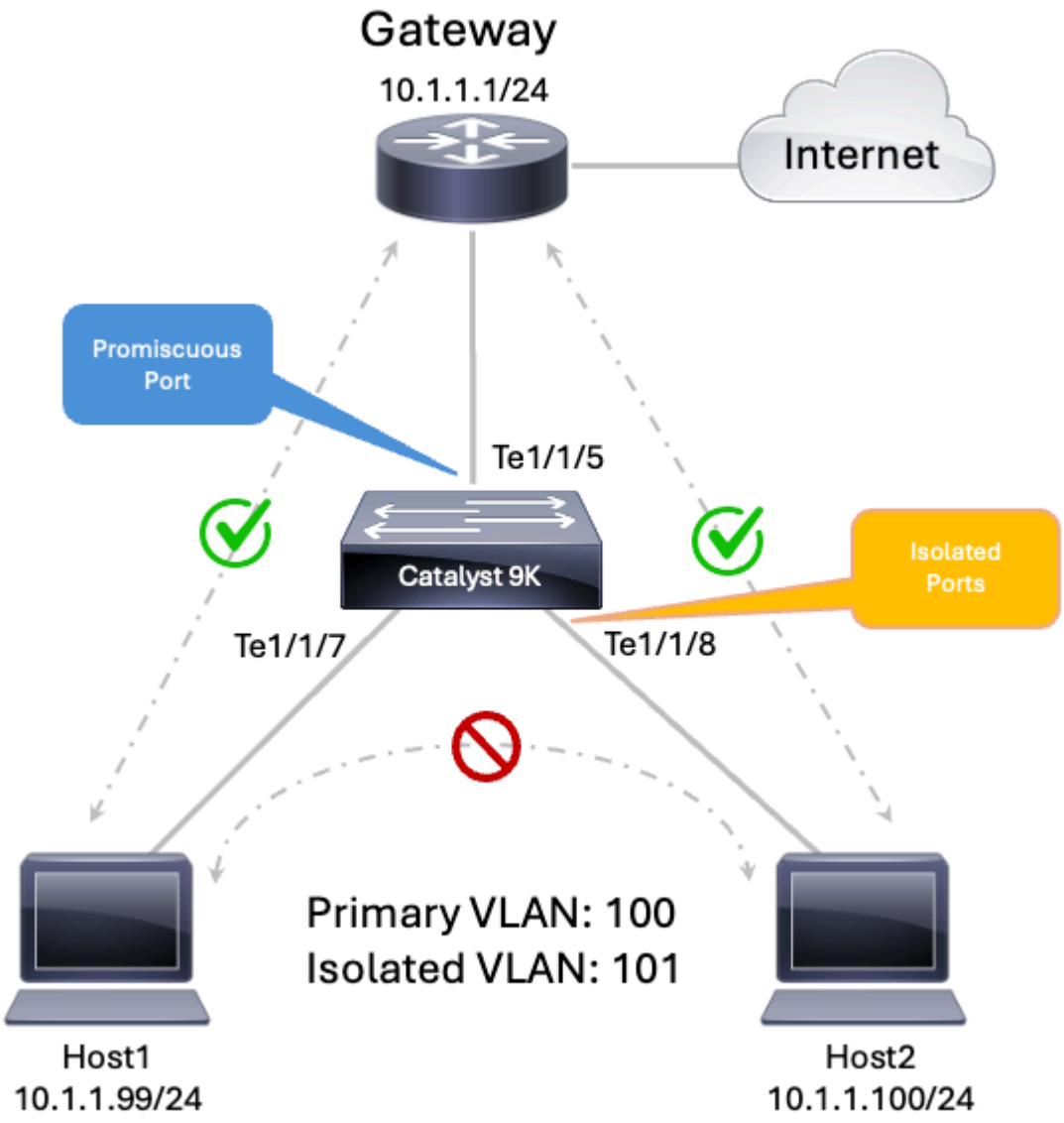
Exemple 1 : PVLAN isolé sur un commutateur Cisco IOS XE

- L’hôte 1 se connecte à TenGigabitEthernet1/1/7.
- L’hôte 2 se connecte à TenGigabitEthernet1/1/8.
- Un pare-feu, routeur ou service partagé se connecte à TenGigabitEthernet1/1/5.
- Le VLAN 100 est le VLAN principal.

- Le VLAN 101 est le VLAN isolé.
- Les hôtes isolés utilisent 10.1.1.1 comme passerelle par défaut.

Hôte	Commutateur	Interface	Rôle VLAN	Adresse IP
Hôte1	9300-2	Te1/1/7	Isolé, VLAN 101	10.1.1.99/24
Hôte2	9300-2	Te1/1/8	Isolé, VLAN 101	10.1.1.100/24
Passerelle	9300-2	Te1/1/5	Promiscueux	10.1.1.1/24

Diagramme du réseau



Topologie PVLAN

Étape 1 : configuration du mode transparent VTP

<#root>

9300-2#

configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
9300-2(config)#

vtp mode transparent

Setting device to VTP Transparent mode for VLANS.
9300-2(config)#

end

Étape 2 : configuration des réseaux locaux virtuels principaux et isolés

<#root>

9300-2#

configure terminal

Enter configuration commands, one per line. End with CNTL/Z. 9300-2(config)#

vlan 100

9300-2(config-vlan)#

name PVLAN_PRIMARY_100

9300-2(config-vlan)#

private-vlan primary

9300-2(config-vlan)#

private-vlan association 101

9300-2(config-vlan)#

exit

```
 9300-2(config)# 9300-2(config)#

vlan 101

 9300-2(config-vlan)#

name PVLAN_ISOLATED_101

 9300-2(config-vlan)#

private-vlan isolated

 9300-2(config-vlan)#

exit

 9300-2(config)#

end
```



Remarque : La commande private-vlan association <vlan-id> est utilisée pour lier le VLAN isolé au VLAN principal.

Étape 3 : configuration des ports hôtes isolés

<#root>

9300-2#

```
configure terminal

 Enter configuration commands, one per line. End with CNTL/Z. 9300-2(config)#

interface TenGigabitEthernet1/1/7

 9300-2(config-if)#

description Isolated Host 1

 9300-2(config-if)#

switchport

 9300-2(config-if)#
```

```
switchport mode private-vlan host

 9300-2(config-if)#

switchport private-vlan host-association 100 101

 9300-2(config-if)#

spanning-tree portfast

 9300-2(config-if)#

exit

 9300-2(config)# 9300-2(config)#

interface TenGigabitEthernet1/1/8

 9300-2(config-if)#

description Isolated Host 2

 9300-2(config-if)#

switchport

 9300-2(config-if)#

switchport mode private-vlan host

 9300-2(config-if)#

switchport private-vlan host-association 100 101

 9300-2(config-if)#

spanning-tree portfast

 9300-2(config-if)#

exit

 9300-2(config)#

end
```

Étape 4. Configuration du port de proximité

```
<#root>

9300-2#

configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
9300-2(config)#

interface TenGigabitEthernet1/1/5

9300-2(config-if)#

description Firewall Router or Shared Service

9300-2(config-if)#

switchport

9300-2(config-if)#

switchport mode private-vlan promiscuous

9300-2(config-if)#

switchport private-vlan mapping 100 101

9300-2(config-if)#

exit

9300-2(config)#

end
```

Configuration de couche 3

Les PVLAN assurent l’isolation de la couche 2 au sein du même sous-réseau IP. La connectivité de couche 3 est toujours nécessaire lorsque des hôtes isolés doivent atteindre des réseaux en dehors du sous-réseau local, tels qu'Internet, des services de data center ou des réseaux routés en amont.

Il existe deux méthodes courantes pour fournir une connectivité de couche 3 aux hôtes PVLAN isolés :

1. Configurez l'interface virtuelle commutée (SVI) du VLAN principal sur le commutateur.
2. Connectez la passerelle par défaut directement à un port proche.



Remarque : Choisissez une méthode de passerelle de couche 3 pour un sous-réseau PVLAN. Utilisez l'interface SVI du VLAN principal sur le commutateur ou une passerelle externe connectée à un port proche.

Méthode 1 : Configuration de l'interface SVI du VLAN principal

Utilisez cette méthode lorsque le commutateur Cisco IOS XE fournit la passerelle par défaut pour les hôtes isolés.

Dans une conception PVLAN, l'interface SVI de couche 3 doit être configurée uniquement pour le VLAN principal. Le VLAN isolé est un VLAN secondaire et ne fournit pas de service de passerelle de couche 3.

Dans cet exemple :

- Le VLAN 100 est le VLAN principal.
- Le VLAN 101 est le VLAN secondaire isolé.
- interface Vlan100 fournit la passerelle par défaut.
- Les hôtes du VLAN 101 isolé utilisent 10.1.1.1/24 as comme passerelle par défaut.

<#root>

9300-2#

configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
9300-2(config)#

interface Vlan100

9300-2(config-if)#

description Primary PVLAN Gateway

9300-2(config-if)#

```
ip address 10.1.1.1 255.255.255.0

9300-2(config-if)#

private-vlan mapping 101

9300-2(config-if)#

no shutdown

9300-2(config-if)#

exit

9300-2(config)#

end
```

Points clés

- Configurez l'interface SVI uniquement pour le VLAN principal.
- Mappez le VLAN secondaire isolé à l'interface SVI du VLAN principal avec la commande private-vlan mapping.
- Ne configurez pas le VLAN isolé en tant que SVI pour le service de passerelle :
- Les hôtes isolés restent dans le même sous-réseau IP que l'interface SVI du VLAN principal.
- Les hôtes isolés peuvent atteindre l'interface SVI du VLAN principal.
- Les hôtes isolés ne peuvent pas communiquer directement avec d’autres hôtes isolés au niveau de la couche 2.



Remarque : Configurez l'interface SVI 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.

Méthode 2 : Connexion du modem routeur à un port proche

Utilisez cette méthode lorsqu'un périphérique externe fournit la passerelle par défaut pour les hôtes isolés. Le périphérique externe peut être un routeur, un pare-feu ou un autre périphérique de passerelle de couche 3.

Dans cette conception, le commutateur Cisco IOS XE n'a pas besoin d'une interface SVI pour le sous-réseau PVLAN. Au lieu de cela, la passerelle externe se connecte à un port proche. Le port

proche mappe le VLAN principal au VLAN secondaire isolé, ce qui permet aux hôtes isolés d'atteindre la passerelle externe.

Dans cet exemple :

- Le VLAN 100 est le VLAN principal.
- Le VLAN 101 est le VLAN secondaire isolé.
- La passerelle externe se connecte à TenGigabitEthernet1/1/5.
- L'adresse IP de la passerelle externe est 10.1.1.1/24.
- Les hôtes isolés utilisent 10.1.1.1 comme passerelle par défaut.

```
<#root>

9300-2#

configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
9300-2(config)#

interface TenGigabitEthernet1/1/5

9300-2(config-if)#

description Firewall Router or Shared Service

9300-2(config-if)#

switchport

9300-2(config-if)#

switchport mode private-vlan promiscuous

9300-2(config-if)#

switchport private-vlan mapping 100 101

9300-2(config-if)#

exit

9300-2(config)#

end
```

Points clés

- Aucune interface SVI n'est requise sur le commutateur pour le sous-réseau PVLAN lorsque la passerelle se connecte directement à un port proche.
- L'interface de passerelle externe doit utiliser une adresse IP dans le même sous-réseau que les hôtes isolés.
- Le port proche doit mapper le VLAN principal au VLAN isolé.
- Les hôtes isolés peuvent atteindre la passerelle externe via le port proche.
- Les hôtes isolés ne peuvent toujours pas communiquer directement entre eux.

Vérification

Vérifiez l'association PVLAN avec la commande show vlan private-vlan :

<#root>

9300-2#

show vlan private-vlan

```
Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
100     101       isolated

Te1/1/5, Te1/1/7, Te1/1/8
```



Remarque : Dans la sortie show vlan private-vlan, la colonne Type identifie le type de VLAN secondaire, tel que isolé ou communauté. Il n'identifie pas le rôle opérationnel de chaque interface répertoriée dans la colonne Ports. La colonne Ports répertorie les interfaces associées à la paire de VLAN principal et secondaire, y compris les ports hôtes isolés et les ports proches mappés à ce VLAN secondaire.

Vérifiez l'état opérationnel du port hôte à l'aide de la commande show interface <id-interface> switchport, dans ce scénario TenGigabitEthernet1/1/7 et TenGigabitEthernet1/1/8 :

<#root>

9300-2#

show interface TenGigabitEthernet1/1/7 switchport

Name: Te1/1/7

Switchport: Enabled

Administrative Mode: private-vlan host

Operational Mode: private-vlan host

Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: 100 (PVLAN_PRIMARY_100) 101 (PVLAN_ISOLATED_101)
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none

Operational private-vlan: 100 (PVLAN_PRIMARY_100) 101 (PVLAN_ISOLATED_101)

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

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Vepa Enabled: false
App Interface: false
Appliance trust: none

9300-2#

show interface TenGigabitEthernet1/1/8 switchport

Name: Te1/1/8

Switchport: Enabled

Administrative Mode: private-vlan host

Operational Mode: private-vlan host

Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)

```
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: 100 (PVLAN_PRIMARY_100) 101 (PVLAN_ISOLATED_101)
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none

Operational private-vlan: 100 (PVLAN_PRIMARY_100) 101 (PVLAN_ISOLATED_101)



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

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Vepa Enabled: false
App Interface: false
Appliance trust: none
```

Vérifiez l'état opérationnel du port de proximité, dans ce cas TenGigabitEthernet1/1/5 :

<#root>

9300-2#

show interface TenGigabitEthernet1/1/5 switchport

Name: Te1/1/5

Switchport: Enabled

Administrative Mode: private-vlan promiscuous

Operational Mode: private-vlan promiscuous

```
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: 100 (PVLAN_PRIMARY_100) 101 (PVLAN_ISOLATED_101)
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
```

```
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none

Operational private-vlan: 100 (PVLAN_PRIMARY_100) 101 (PVLAN_ISOLATED_101)


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

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Vepa Enabled: false
App Interface: false
Appliance trust: none
```

Vérifiez à présent que les hôtes isolés peuvent atteindre la passerelle 10.1.1.1/24 mais ne peuvent pas envoyer de requête ping entre 10.1.1.99/24 et 10.1.1.100/24

Comportement du trafic

Source	Destination	Résultat attendu
Hôte 1	Hôte 2	Échecs
Hôte 2	Hôte 1	Échecs
Hôte 1	Passerelle par défaut	Réussit
Hôte 2	Passerelle par défaut	Réussit
Port De Promiscuité	Hôtes isolés	Réussit

Résultats du trafic
<#root> Host1# **ping 10.1.1.1**

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms

Host1#
ping 10.1.1.99


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.99, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

Host1#
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)

Host2#
ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms

Host2#
ping 10.1.1.99

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.99, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

Host2#
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 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Lors de la vérification de la table d’adresses MAC, vous pouvez observer deux entrées BLOCKED. Ces entrées sont attendues pour les hôtes PVLAN isolés. Ils représentent la règle d'isolation de couche 2 dans le VLAN secondaire, le commutateur empêche ces adresses MAC d'être utilisées pour le transfert direct isolé vers isolé.

Les adresses MAC d'hôte isolées apparaissent deux fois, car le transfert PVLAN utilise à la fois le VLAN principal et le contexte VLAN secondaire :

- Dans le VLAN secondaire 101, l'adresse MAC est bloquée pour le transfert direct de VLAN isolé.
- Dans le VLAN principal 100, l'adresse MAC est disponible pour le transfert PVLAN via le chemin proche.

<#root>

9300-2#

show mac address-table dynamic

```
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    000c.000c.000c    DYNAMIC     Te1/1/3
   1    f87a.41a8.c1b5    DYNAMIC     Te1/1/1
   1    f87a.41a8.c1ba    DYNAMIC     Te1/1/6
   1    f87a.41a8.c1d1    DYNAMIC     Te1/1/6
```

101 000a.000a.000a BLOCKED Te1/1/7 101 000b.000b.000b BLOCKED Te1/1/8 100 000a.000a.000a DYNAMIC pv Te1

```
Total Mac Addresses for this criterion: 9
```

Exemple 2 : PVLAN sur plusieurs commutateurs Cisco IOS XE

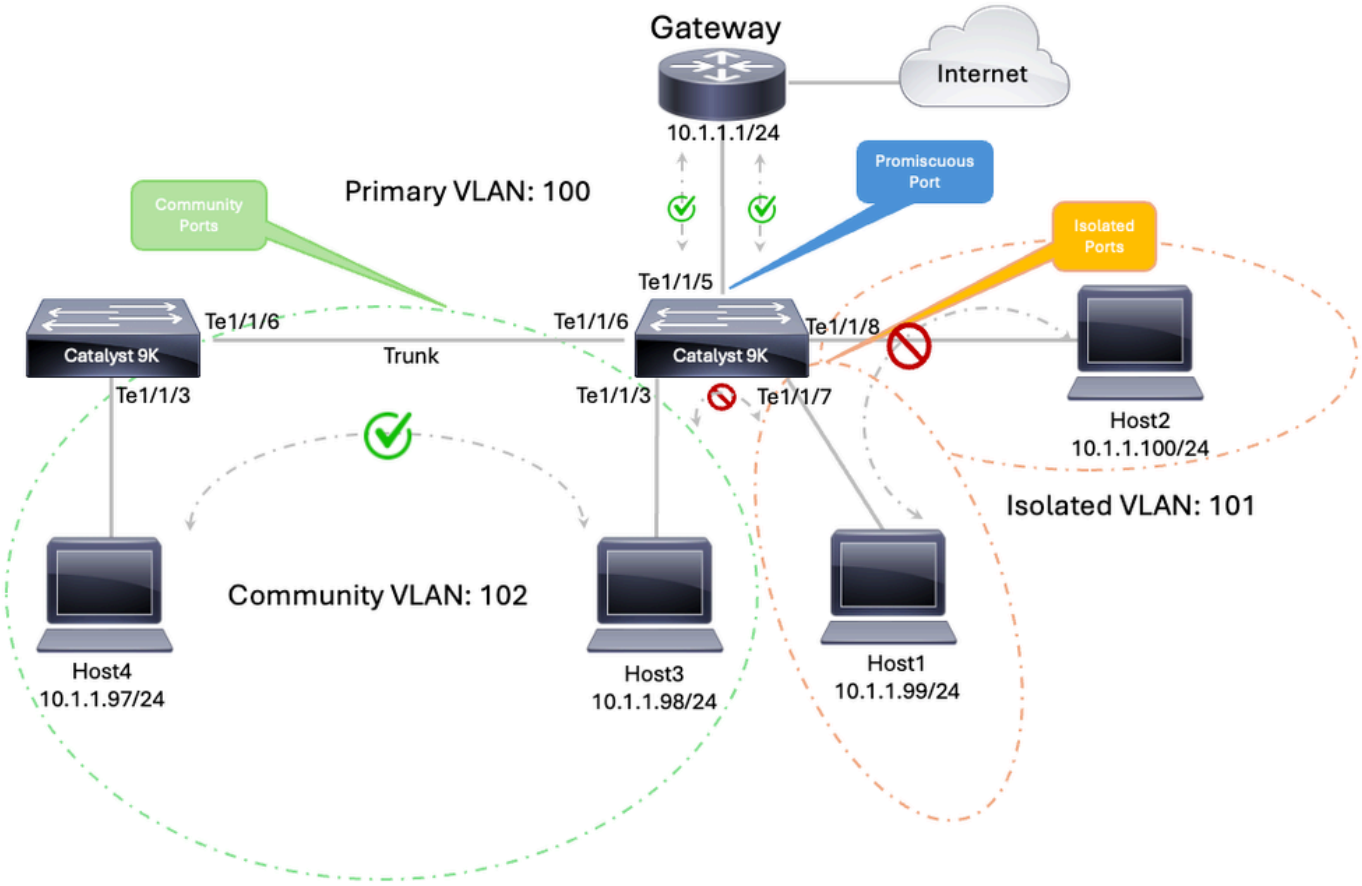
- SW1 et SW2 sont des commutateurs Catalyst 9000 Cisco IOS XE.
- Aucune interface SVI n'est configurée pour le sous-réseau PVLAN.
- Une passerelle externe fournit une connectivité de couche 3.
- L'adresse IP de la passerelle externe est 10.1.1.1/24.
- La passerelle externe se connecte à un port proche sur SW2.
- Le VLAN 100 est le VLAN principal.
- Le VLAN 101 est le VLAN secondaire isolé.
- Le VLAN 102 est le VLAN secondaire de la communauté.
- SW1 et SW2 se connectent via une agrégation 802.1Q standard.
- Les hôtes isolés ne peuvent atteindre que la passerelle proche.
- Les hôtes de communauté du VLAN 102 peuvent communiquer entre eux et avec la

passerelle proche.

- Les hôtes isolés ne peuvent pas communiquer avec les hôtes de la communauté.

Hôte	Commutateur	Interface	Rôle PVLAN	Association VLAN	Adresse IP	Passerelle par défaut
Hôte 3	Logiciel 1 / 9300-1	TenGigabitEthernet1/1/3	hôte communautaire	VLAN principal 100, VLAN de communauté 102	10.1.1.97/24	10.1.1.1
Hôte4	SW2/9300-2	TenGigabitEthernet1/1/3	hôte communautaire	VLAN principal 100, VLAN de communauté 102	10.1.1.98/24	10.1.1.1
Hôte1	SW2/9300-2	TenGigabitEthernet1/1/7	Hôte isolé	VLAN principal 100, VLAN isolé 101	10.1.1.99/24	10.1.1.1
Hôte2	SW2/9300-2	TenGigabitEthernet1/1/8	Hôte isolé	VLAN principal 100, VLAN isolé 101	10.1.1.100/24	10.1.1.1
Passerelle externe	SW2/9300-2	TenGigabitEthernet1/1/5	Promiscuité (périphérique faisant face à la passerelle)	VLAN principal 100 mappé aux VLAN 101 et 102	10.1.1.1/24	Sans objet

Diagramme du réseau



PVLAN sur les commutateurs

VLAN et plan d'interface

Périphérique	Interface	Rôle
SW1	TenGigabitEthernet1/1/3	Hôte de la communauté, VLAN 102
SW1	TenGigabitEthernet1/1/6	Liaison vers SW2
SW2	TenGigabitEthernet1/1/3	Hôte de la communauté, VLAN 102
SW2	TenGigabitEthernet1/1/7	Hôte isolé, VLAN 101
SW2	TenGigabitEthernet1/1/8	Hôte isolé, VLAN 101
SW2	TenGigabitEthernet1/1/6	Liaison vers SW1

Périphérique	Interface	Rôle
SW2	TenGigabitEthernet1/1/5	Port de proximité vers la passerelle externe 10.1.1.1/24

Remarque : Les VLAN privés peuvent être pris sur plusieurs commutateurs avec ces méthodes : ports d'agrégation standard, ports d'agrégation de VLAN privés isolés ou ports d'agrégation de VLAN privés proches. Pour plus d'informations, reportez-vous au guide de documentation Private VLAN Across Multiple Switches.

SW1 - 9300-1 - Configuration en cours	Comm2 - 9300-2 -
<#root> 9300-1# **show running-config** Building configuration... Current configuration : 17988 bytes ! ! Last configuration change at 17:39:58 UTC Tue Aug 11 2026 ! version 26.1 service timestamps debug datetime msec service timestamps log datetime msec ! hostname 9300-1 ! ! **vtp mode transparent** ! ! ! **vlan 100 name PVLAN_PRIMARY_100 private-vlan primary private-vlan association 101,102** ! **vlan 101 name PVLAN_ISOLATED_101 private-vlan isolated** ! **vlan 102 name PVLAN_COMMUNITY_102 private-vlan community** ! ! **interface TenGigabitEthernet1/1/3** description Community Host VLAN 102 **switchport private-vlan host-association 100 102 switchport mode private-vlan host** spanning-tree portfast !	<#root> 9300-2# **show running-confi** Building configura Current configurat ! ! Last configurati ! version 17.12 service timestamps service timestamps ! hostname 9300-2 ! ! **vtp mode transpare** ! ! ! **vlan 100 name PVLA** ! **vlan 101 name PVLA** ! **vlan 102 name PVLA** ! ! **interface TenGigab** description Commu **switchport privat** spanning-tree por

```
interface TenGigabitEthernet1/1/6
 description Trunk to SW2
 switchport trunk allowed vlan 100-102
 switchport mode trunk
!
!
end
```

```
!
interface TenGigab
 description Exter
 switchport privat
!
interface TenGigab
 description Trunk
 switchport trunk a
 switchport mode t
!
interface TenGigab
 description Isola
 switchport privat
 switchport mode p
 spanning-tree por
!
interface TenGigab
 description Isola
 switchport privat
 switchport mode p
 spanning-tree por
!
!
end
```

Remarque : Dans cet exemple, comme les deux commutateurs utilisent VTP en mode transparent, les PVLAN doivent être configurés manuellement sur chaque commutateur.

Remarque : Les VLAN privés sont pris en charge en mode transparent pour VTP 1, 2 et 3. Les VLAN privés sont également pris en charge en mode serveur avec VTP 3.

Vérification

SW1 - 9300-1 - État	SW2 -
<#root>	<#root

9300-1#

show vlan private-vlan

```
Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
100     101       isolated
100
```

102

community Te1/1/3

9300-1#

show interfaces trunk

```
Port           Mode             Encapsulation  Status        Native vlan
Te1/1/6        on               802.1q         trunking      1

Port           Vlans allowed on trunk
```

Te1/1/6 100-102

```
Port           Vlans allowed and active in management domain
```

Te1/1/6 100-102

```
Port           Vlans in spanning tree forwarding state and not pruned
```

Te1/1/6 100-102

9300-1#

show interface TenGigabitEthernet1/1/3 switchport

Name: Te1/1/3

Switchport: Enabled

Administrative Mode: private-vlan host

Operational Mode: private-vlan host

```
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: 100 (PVLAN_PRIMARY_100) 102 (PVLAN_COMMUNITY_102)
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
```

9300-2#

show vl

Primary

100

Te1/1/5

100

Te1/1/3

9300-2#

show in

Port

Te1/1/6

Port

Te1/1/6

Port

Te1/1/6

Port

Te1/1/6

9300-2#

show in

Name: T

Switchp

Adminis

Operati

Adminis
Operati
Negotia
Access
Trunkin
Adminis
Voice V
Adminis
Adminis
Adminis
Adminis
Adminis
Adminis
Adminis

Operational private-vlan: 100 (PVLAN_PRIMARY_100) 102 (PVLAN_COMMUNITY_102)

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

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Vepa Enabled: false
App Interface: false
Appliance trust: none

Operati

Trunkir
Pruning
Capture
Capture

Protect
Unknown
Unknown
Vepa En
App Int
Applian

9300-2#

show in

Name: T

Switchp

Adminis

Operati

Adminis
Operati
Negotia
Access
Trunkir
Adminis
Voice V
Adminis
Adminis
Adminis
Adminis
Adminis
Adminis
Adminis
Adminis

Operati

Trunkir
Pruning
Capture
Capture

Protect
Unknown
Unknown
Vepa En
App Int
Applian

9300-2#

show in

Name: T

Switchp

```
Admini

Operati

Admini
Operati
Negotia
Access
Trunkin
Admini
Voice V
Admini
Admini
Admini
Admini
Admini
Admini
Admini
Admini

Operati


Trunkin
Pruning
Capture
Capture

Protect
Unknown
Unknown
Vepa En
App Int
Appliar

9300-2#

show in

Name: T

Switchp

Admini

Operati

Admini
Operati
Negotia
Access
Trunkin
Admini
Voice V
Admini
Admini
Admini
Admini
Admini
Admini
Admini
Admini

Operati
```

	Trunkin Pruning Capture Capture Protect Unknown Unknown Vepa En App Int Appliar

Comportement du trafic

Source	Destination	Résultat attendu
Hôte isolé SW2 sur Te1/1/7	Hôte isolé SW2 sur Te1/1/8	Échecs
Hôte isolé SW2 sur Te1/1/7	Hôte de la communauté SW1 sur Te1/1/3	Échecs
Hôte isolé SW2 sur Te1/1/7	Passerelle externe 10.1.1.1	Réussit
Hôte de la communauté SW1 sur Te1/1/3	Hôte de la communauté SW2 sur Te1/1/3	Réussit
Hôte de la communauté SW1 sur Te1/1/3	Passerelle externe 10.1.1.1	Réussit
Hôte de la communauté SW2 sur Te1/1/3	Hôte isolé SW2 sur Te1/1/7	Échecs

<#root> Host4# **ping 10.1.1.1**

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Host4#
```

ping 10.1.1.98

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.98, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Host4#
```

ping 8.8.8.8

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Host4#
```

ping 10.1.1.99

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.99, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Host4#
```

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)

Host3#
```

ping 10.1.1.1

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Host3#
```

ping 10.1.1.97

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.97, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Host3#
```

ping 8.8.8.8

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Host3#
```

ping 10.1.1.99

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.99, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Host3#
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)

Host1#
ping 10.1.1.1


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Host1#
ping 8.8.8.8


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Host1#
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)
Host1#
ping 10.1.1.97


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.97, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Host1#
ping 10.1.1.98

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.98, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

Host2#
ping 10.1.1.1


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Host2#

ping 8.8.8.8


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Host2#

ping 10.1.1.99

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.99, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Host2#

ping 10.1.1.97

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.97, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Host2#

ping 10.1.1.98

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.98, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```



Remarque : L'accessibilité à Internet dépend du routage en amont et de la conception NAT. Elle est fournie uniquement pour indiquer que la passerelle externe fournit une connectivité routée.

Informations connexes

- Configuration des VLAN privés
- Guides de configuration des commutateurs Cisco Catalyst 9300
- 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.