Konfigurieren isolierter privater VLANs auf Catalyst-Switches

Inhalt

Einleitung

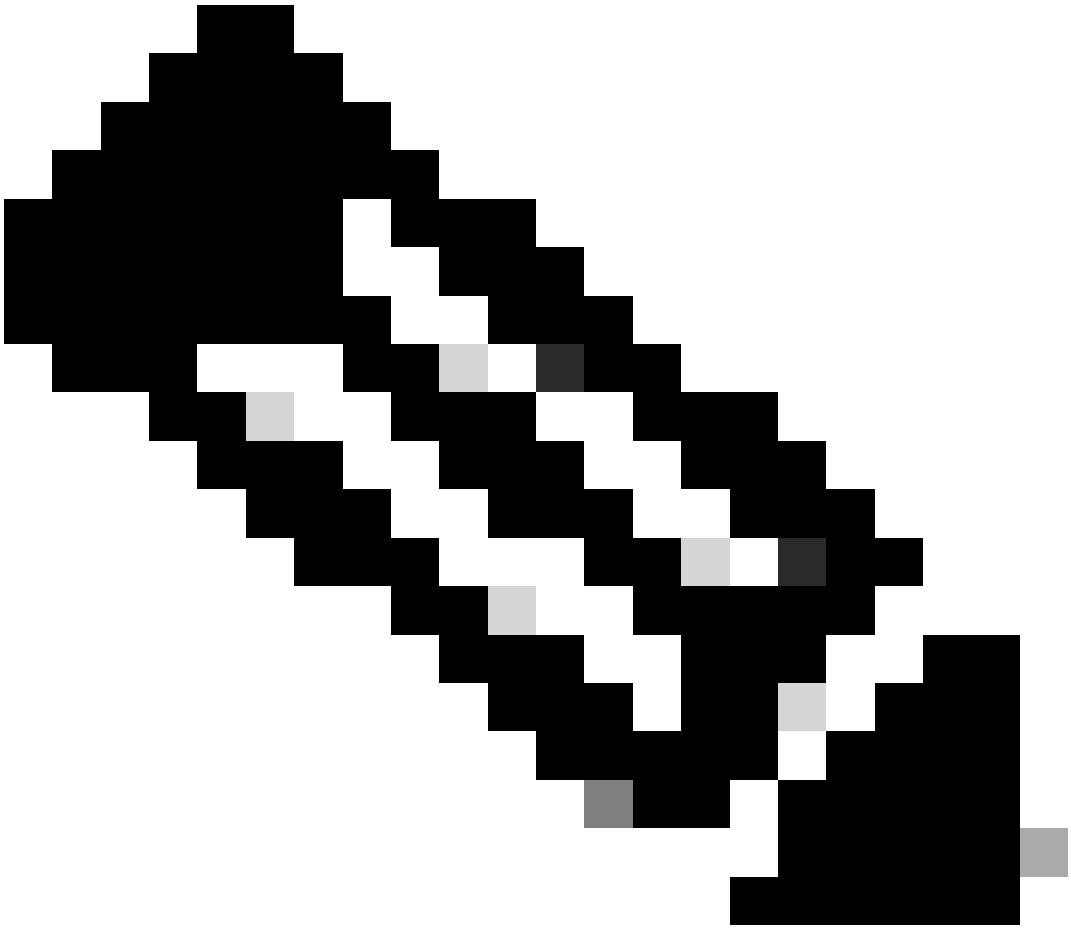
In diesem Dokument wird das Verfahren zum Konfigurieren isolierter PVLANs auf Cisco Catalyst Switches mit Catalyst OS (CatOS) oder Cisco IOS® Software beschrieben.

Voraussetzungen

Anforderungen

In diesem Dokument wird davon ausgegangen, dass bereits ein Netzwerk vorhanden ist, das die Verbindung zwischen den verschiedenen Ports herstellen und so zu einem PVLAN hinzufügen kann. Wenn Sie über mehrere Switches verfügen, stellen Sie sicher, dass der Trunk zwischen den Switches ordnungsgemäß funktioniert und die PVLANs auf dem Trunk zulässt.

Nicht alle Switches und Softwareversionen unterstützen PVLANs.



Hinweis: Einige Switches (wie in der Unterstützungsmatrix für Private VLAN Catalyst Switches angegeben) unterstützen derzeit nur die PVLAN Edge-Funktion. Der Begriff "geschützte Ports" bezieht sich ebenfalls auf diese Funktion. PVLAN Edge-Ports verfügen über eine Einschränkung, die die Kommunikation mit anderen geschützten Ports auf demselben Switch verhindert. Geschützte Ports auf separaten Switches können jedoch miteinander kommunizieren. Verwechseln Sie diese Funktion nicht mit den in diesem Dokument gezeigten normalen PVLAN-Konfigurationen. Weitere Informationen zu geschützten Ports finden Sie im Abschnitt Konfigurieren der Port-Sicherheit im Dokument Konfigurieren der Port-basierten Datenverkehrskontrolle.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Catalyst 4003-Switch mit Supervisor Engine 2-Modul mit CatOS-Version 6.3(5)
- Catalyst 4006-Switch mit Supervisor Engine 3-Modul für Cisco IOS Software, Version 12.1(12c)EW1

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Hintergrundinformationen

In einigen Situationen müssen Sie die Layer-2-Konnektivität (L2) zwischen Endgeräten auf einem Switch verhindern, ohne die Geräte in verschiedenen IP-Subnetzen zu platzieren. Diese Konfiguration verhindert die Verschwendung von IP-Adressen. Private VLANs (PVLANs) ermöglichen die Isolierung von Geräten im selben IP-Subnetz auf Layer 2. Sie können festlegen, dass bestimmte Ports am Switch nur bestimmte Ports erreichen, die über ein Standard-Gateway, einen Backup-Server oder Cisco LocalDirector verfügen.

In diesem Dokument wird das Verfahren zum Konfigurieren isolierter PVLANs auf Cisco Catalyst Switches mit Catalyst OS (CatOS) oder Cisco IOS Software beschrieben.

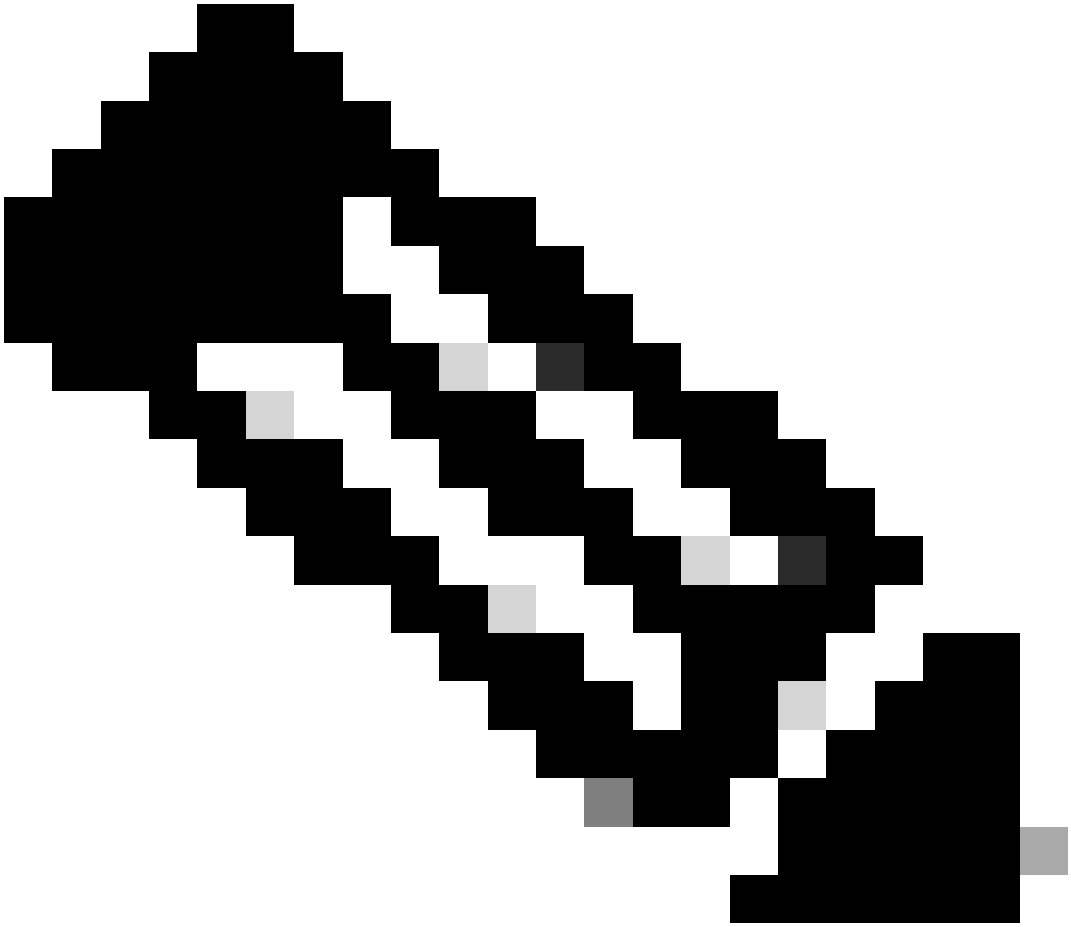
Ein PVLAN ist ein VLAN mit Konfiguration für die Layer-2-Isolierung von anderen Ports innerhalb derselben Broadcast-Domäne oder desselben Subnetzes. Sie können innerhalb eines PVLAN einen bestimmten Portsatz zuweisen und so den Zugriff auf die Ports auf Layer 2 steuern. Sie können PVLANs und normale VLANs auf demselben Switch konfigurieren.

Es gibt drei Arten von PVLAN-Ports: Promiscuous, Isolated und Community.

- Ein Port des Typs Promiscuous kommuniziert mit allen anderen PVLAN-Ports. Der Promiscuous-Port wird normalerweise für die Kommunikation mit externen Routern, LocalDirectors, Netzwerkmanagementgeräten, Backup-Servern, administrativen Workstations und anderen Geräten verwendet. Bei einigen Switches muss der Port zum Routing-Modul (z. B. Multilayer Switch Feature Card [MSFC]) Promiscuous sein.
- Ein isolierter Port ist auf Layer 2 vollständig von anderen Ports im selben PVLAN getrennt. Diese Trennung umfasst Broadcasts, und die einzige Ausnahme ist der Promiscuous-Port. Eine Datenschutzgewährung auf Layer-2-Ebene erfolgt mit der Blockierung des

ausgehenden Datenverkehrs an alle isolierten Ports. Datenverkehr von einem isolierten Port wird nur an alle Promiscuous-Ports weitergeleitet.

- Community-Ports können untereinander und mit den Promiscuous-Ports kommunizieren. Diese Ports sind auf Layer 2 von allen anderen Ports in anderen Communitys oder von isolierten Ports im PVLAN isoliert. Broadcasts werden nur zwischen verbundenen Community-Ports und dem Promiscuous-Port weitergeleitet.



Hinweis: In diesem Dokument wird die VLAN-Konfiguration der Community nicht behandelt.

Regeln und Einschränkungen

In diesem Abschnitt finden Sie einige Regeln und Einschränkungen, die Sie beachten müssen, wenn Sie PVLANs implementieren.

- PVLANs können die VLANs 1 oder 1002-1005 nicht enthalten.

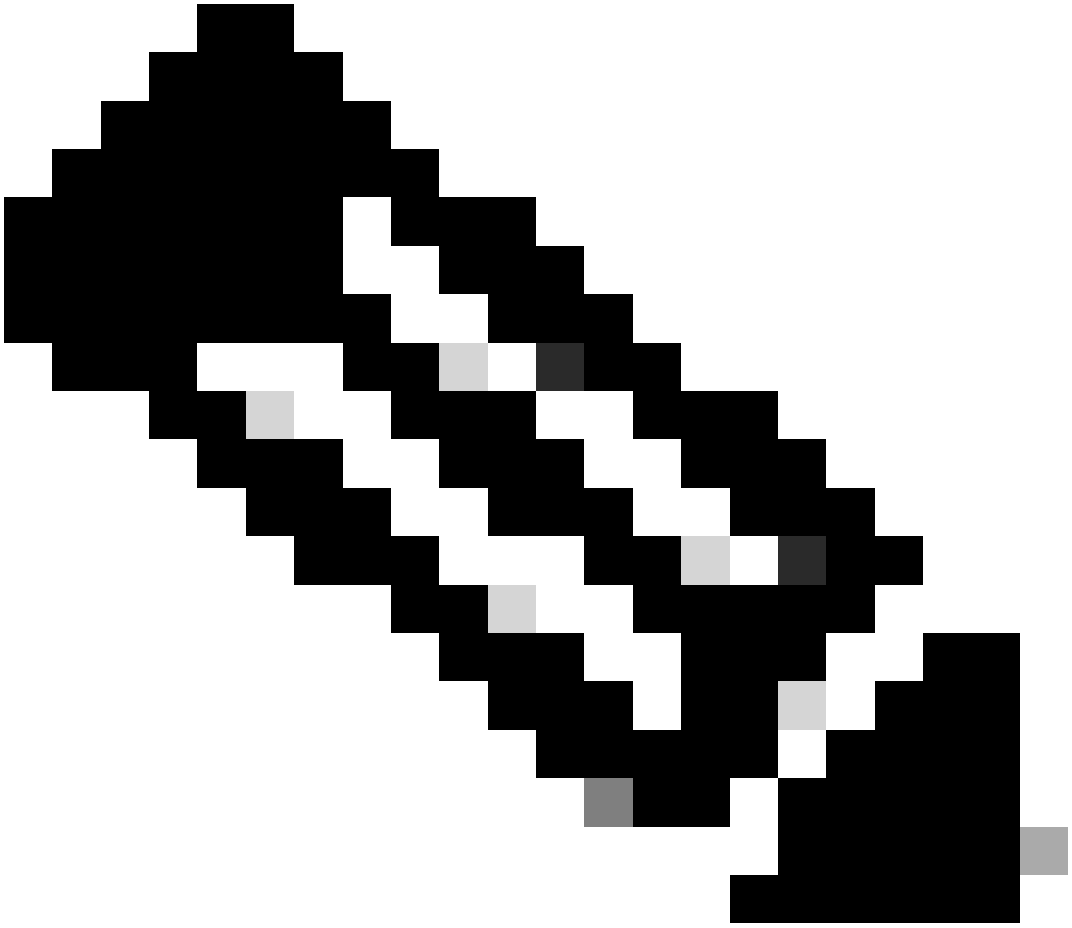
- Sie müssen den VTP-Modus (VLAN Trunk Protocol) auf `transparent` einstellen.
- Sie können nur ein isoliertes VLAN pro primärem VLAN angeben.
- Sie können ein VLAN nur dann als PVLAN festlegen, wenn diesem VLAN derzeit keine Zuweisungen von Zugriffsports zugewiesen sind. Entfernen Sie alle Ports in diesem VLAN, bevor Sie das VLAN zu einem PVLAN machen.
- Konfigurieren Sie PVLAN-Ports nicht als EtherChannels.
- Aufgrund von Hardwarebeschränkungen schränken die Catalyst 6500/6000 Fast Ethernet-Switch-Module die Konfiguration eines isolierten oder Community-VLAN-Ports ein, wenn ein Port innerhalb desselben COIL Application-Specific Integrated Circuits (ASIC) einer der folgenden ist:
    - Ein Stamm
    - Ein SPAN-Ziel (Switched Port Analyzer)
    - Ein Promiscuous PVLAN-Port

  Diese Tabelle zeigt den Portbereich an, der zum gleichen ASIC der Catalyst 6500/6000 FastEthernet-Module gehört:

Modul	Ports nach 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

Der Befehl show pvlan ability (CatOS) gibt auch an, ob Sie einen Port zu einem PVLAN-Port machen können. In der Cisco IOS Software gibt es keinen entsprechenden Befehl.

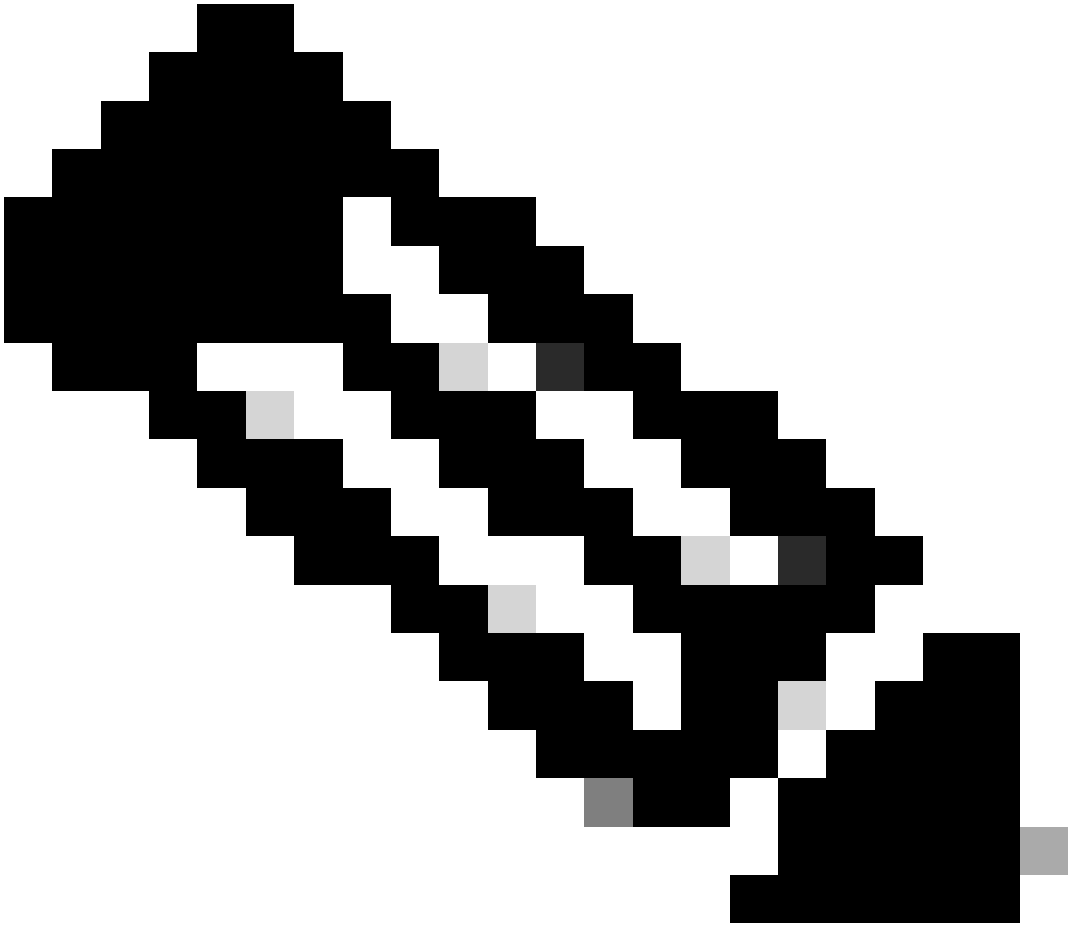
- Wenn Sie ein VLAN löschen, das Sie in der PVLAN-Konfiguration verwenden, werden die Ports, die dem VLAN zugeordnet sind, inaktiv.
- Konfigurieren Sie Layer 3 (L3)-VLAN-Schnittstellen nur für die primären VLANs. VLAN-Schnittstellen für isolierte und Community-VLANs sind inaktiv, während das VLAN über eine isolierte oder Community-VLAN-Konfiguration verfügt.
- Sie können PVLANs mithilfe von Trunks auch auf andere Switches ausdehnen. Trunk-Ports leiten den Datenverkehr von regulären VLANs sowie von primären, isolierten und Community-VLANs weiter. Cisco empfiehlt die Verwendung von Standard-Trunk-Ports, wenn beide Switches, die einem Trunking unterzogen werden, PVLANs unterstützen.



Hinweis: Sie müssen auf jedem Switch mit Beteiligung manuell dieselbe PVLAN-Konfiguration eingeben, da diese Informationen vom VTP im transparenten Modus nicht weitergegeben werden.

Konfigurieren

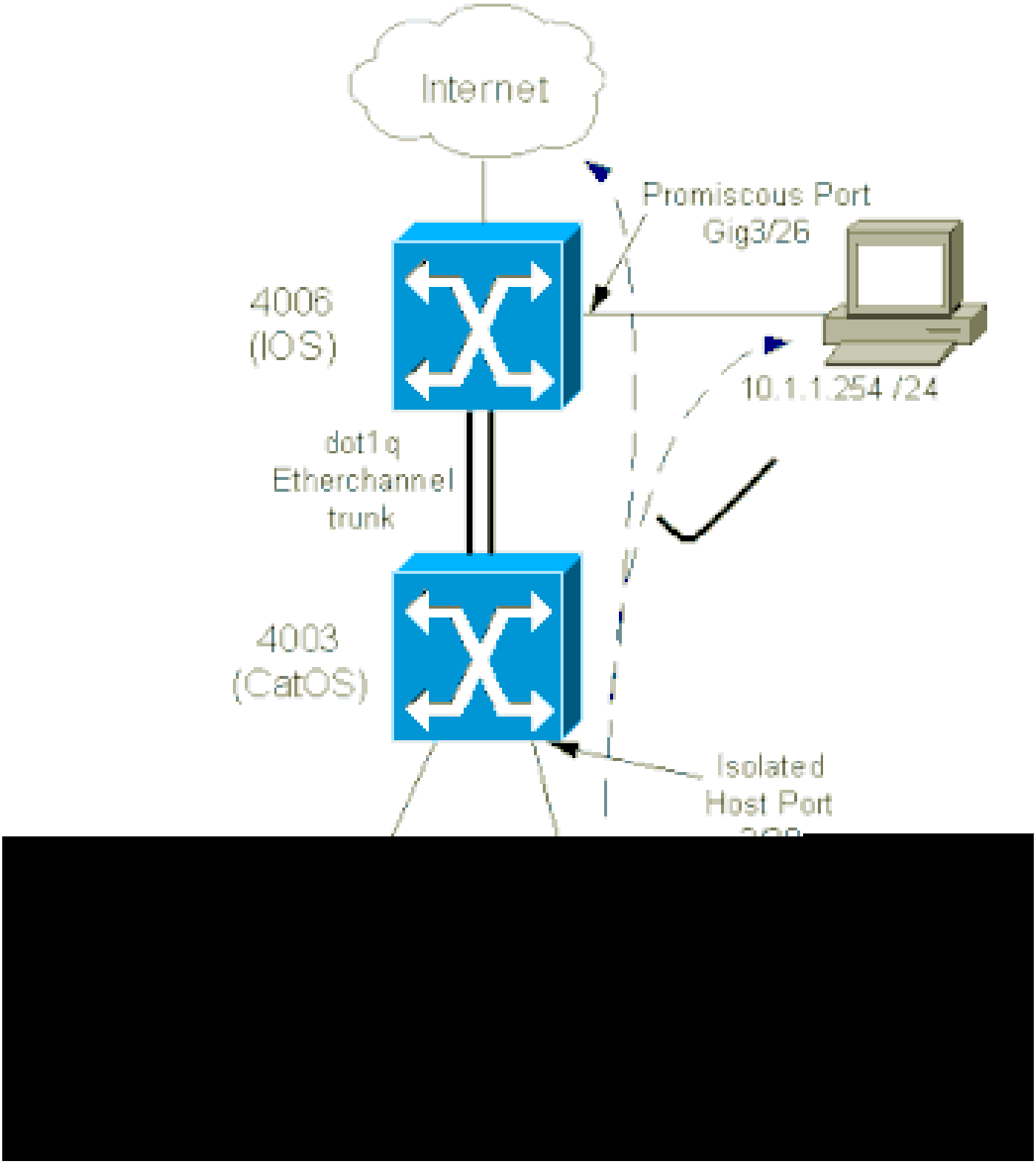
In diesem Abschnitt erfahren Sie, wie Sie die in diesem Dokument beschriebenen Funktionen konfigurieren können.



Hinweis: Verwenden Sie das Tool zur Befehlssuche, um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten. Nur registrierte Benutzer können auf interne Tools und Informationen von Cisco zugreifen.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



In diesem Szenario haben die Geräte im isolierten VLAN (101) eine Beschränkung der Kommunikation auf Layer 2 untereinander. Die Geräte können jedoch eine Verbindung mit dem Internet herstellen. Port Gig 3/26 auf dem 4006 ist darüber hinaus mit der Promiscuous-Bezeichnung versehen. Mit dieser optionalen Konfiguration kann ein Gerät auf GigabitEthernet 3/26 mit allen Geräten im isolierten VLAN verbunden werden. Diese Konfiguration ermöglicht beispielsweise auch die Sicherung der Daten aller PVLAN-Hostgeräte auf einer Administrations-Workstation. Zu den weiteren Verwendungsmöglichkeiten für Promiscuous-Ports gehören Verbindungen zu einem externen Router, LocalDirector, Netzwerkmanagementgeräten und

anderen Geräten.

Konfigurieren der primären und isolierten VLANs

Führen Sie diese Schritte aus, um die primären und sekundären VLANs zu erstellen und die verschiedenen Ports an diese VLANs zu binden. Die Schritte umfassen Beispiele für CatOS und Cisco IOS® Software. Geben Sie den entsprechenden Befehlssatz für die Betriebssysteminstallation ein.

1. Erstellen Sie das primäre PVLAN.

    - 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
      ```

    - Cisco IOS Software

      <#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. Erstellen Sie die isolierten VLANs.

    - 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
```

- Cisco IOS Software

<#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. Binden Sie die isolierten VLANs/VLANs an das primäre VLAN.

- CatOS

<#root>

```
Switch_CatOS> (enable)

set pvlan primary_vlan_id secondary_vlan_id

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

- Cisco IOS Software

```
<#root>

Switch_IOS(config)#

vlan primary_vlan_id

Switch_IOS(config-vlan)#

private-vlan association secondary_vlan_id

Switch_IOS(config-vlan)#

exit
```

4. Überprüfen der privaten VLAN-Konfiguration

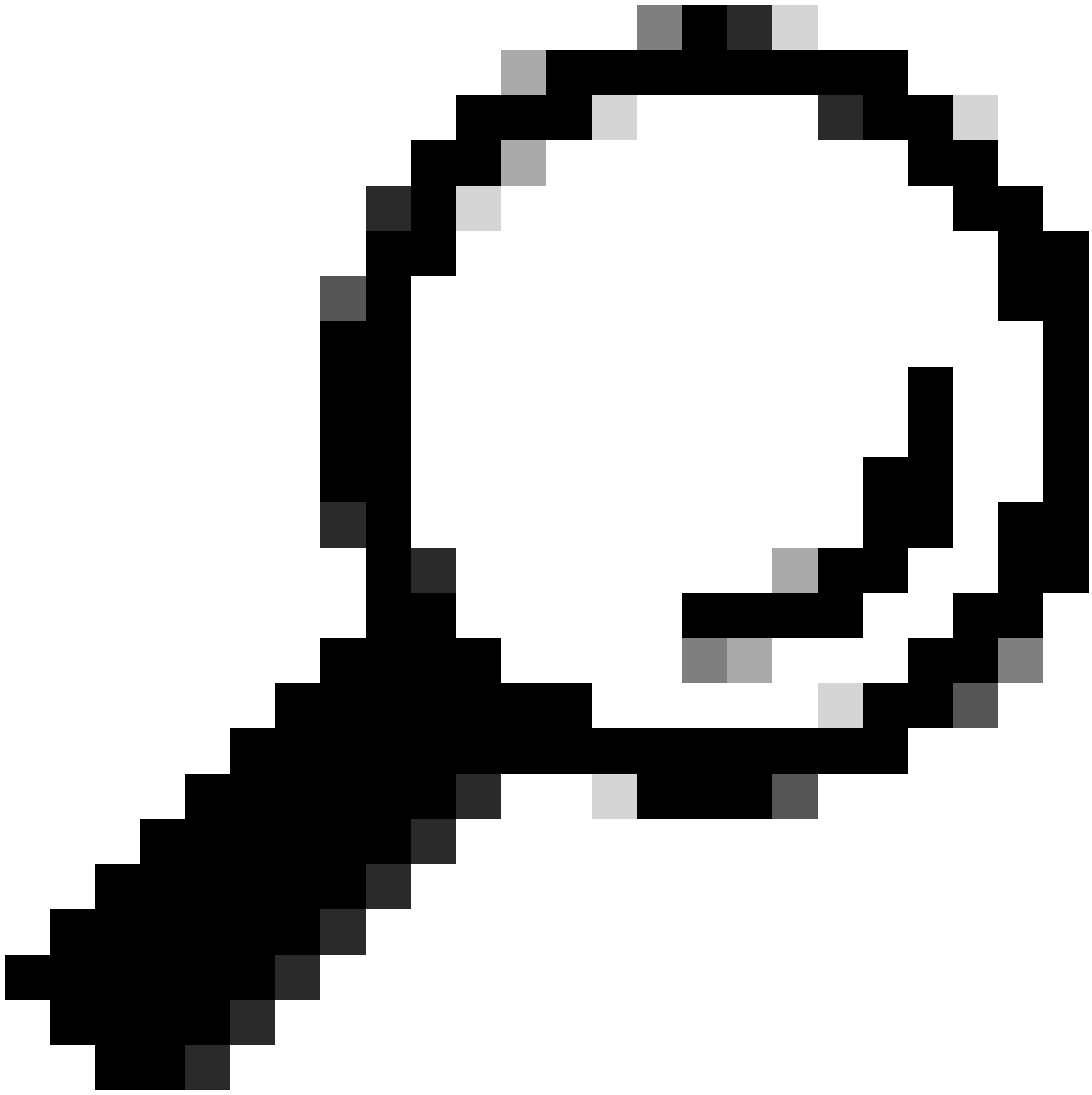
- CatOS

```
<#root>

Switch_CatOS> (enable)

show pvlan

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

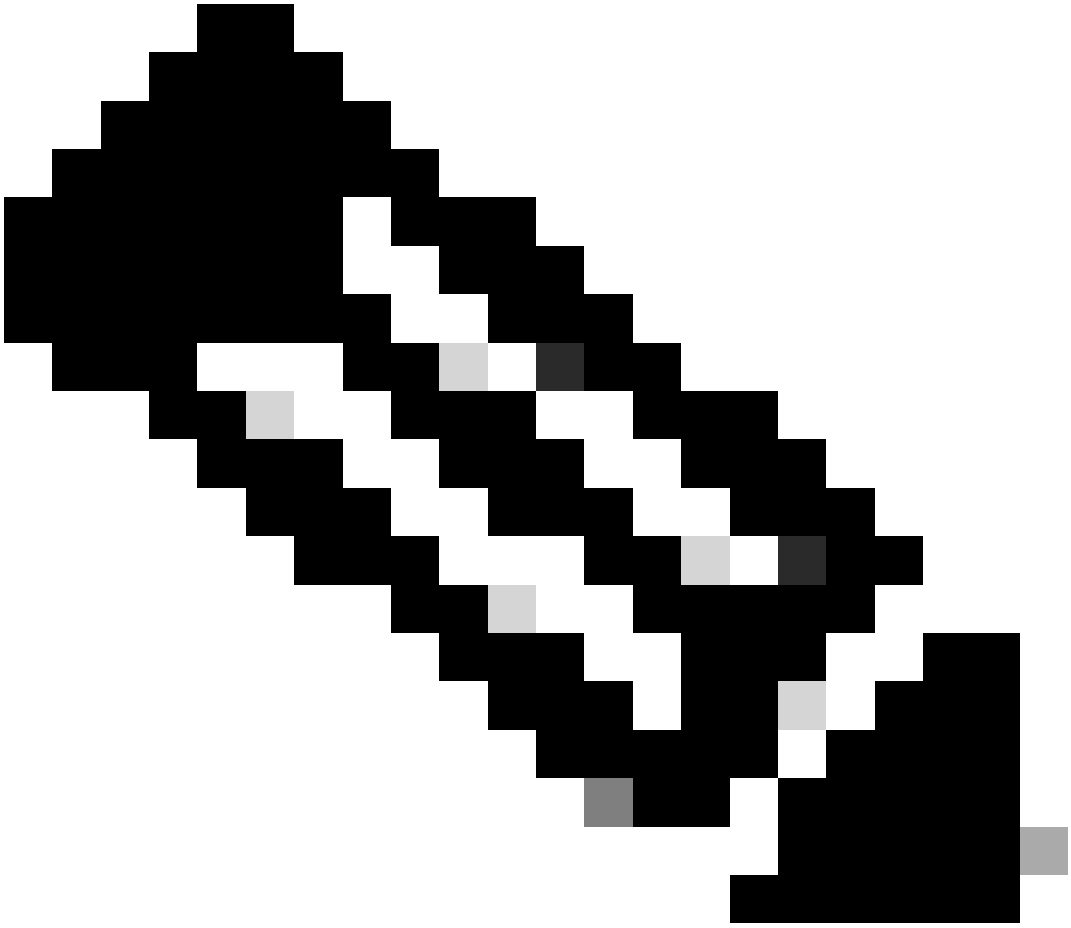
- Cisco IOS Software

```
<#root>

Switch_IOS#

show vlan private-vlan

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

Zuweisen von Ports zu den PVLANs



Tipp: Führen Sie vor der Implementierung dieses Verfahrens den show PVLAN capability mod/port Befehl (für CatOS) aus, um zu bestimmen, ob ein Port ein PVLAN-Port werden kann.



Hinweis: Führen Sie vor Schritt 1 dieses Verfahrens den Befehl switchport im Schnittstellenkonfigurationsmodus aus, um den Port als Layer-2-Switched-Schnittstelle zu konfigurieren.

- Konfigurieren Sie die Host-Ports auf allen entsprechenden Switches.

  - **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

Cisco IOS Software

<#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
```

- Konfigurieren Sie den Promiscuous-Port an einem der Switches.

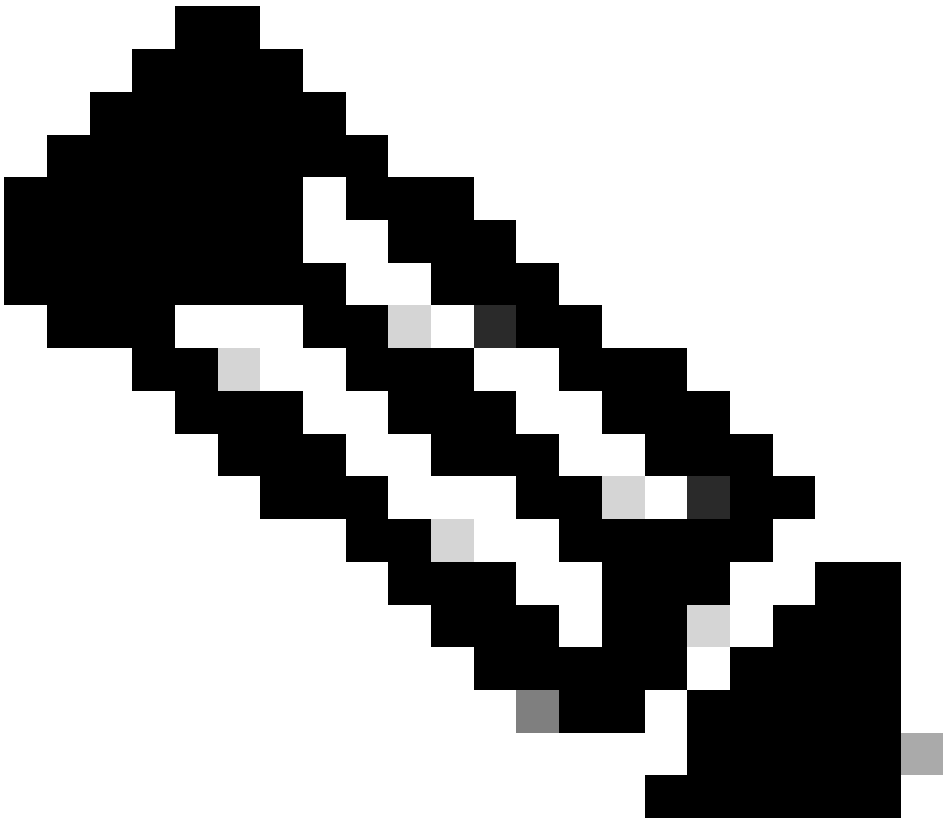
  - **CatOS**

```
<#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
```



Hinweis: Wenn auf der Supervisor Engine als Systemsoftware CatOS ausgeführt wird, muss der MSFC-Port auf der Supervisor Engine (15/1 oder 16/1) für Catalyst 6500/6000 Promiscuous sein, wenn Sie zwischen den VLANs Layer 3 wechseln möchten.

•

Cisco IOS Software

<#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
```

Layer-3-Konfiguration

In diesem optionalen Abschnitt werden die Konfigurationsschritte beschrieben, um die Route des PVLAN-Eingangsdatenverkehrs zuzulassen. Wenn Sie nur die Layer-2-Anbindung aktivieren müssen, können Sie diese Phase auslassen.

- Konfigurieren Sie die VLAN-Schnittstelle auf die gleiche Weise, die Sie für normales Layer-3-Routing konfigurieren.

  Diese Konfiguration umfasst:

- Konfiguration einer IP-Adresse

- Aktivieren der Schnittstelle mit dem Befehl **no shutdown**

- Überprüfen, ob das VLAN in der VLAN-Datenbank vorhanden ist

Konfigurationsbeispiele finden Sie unter Technischer VLAN-/VTP-Support.

- Ordnen Sie die sekundären VLANs zu, die Sie mit dem primären VLAN routen möchten.

<#root>

Switch_IOS(config)#

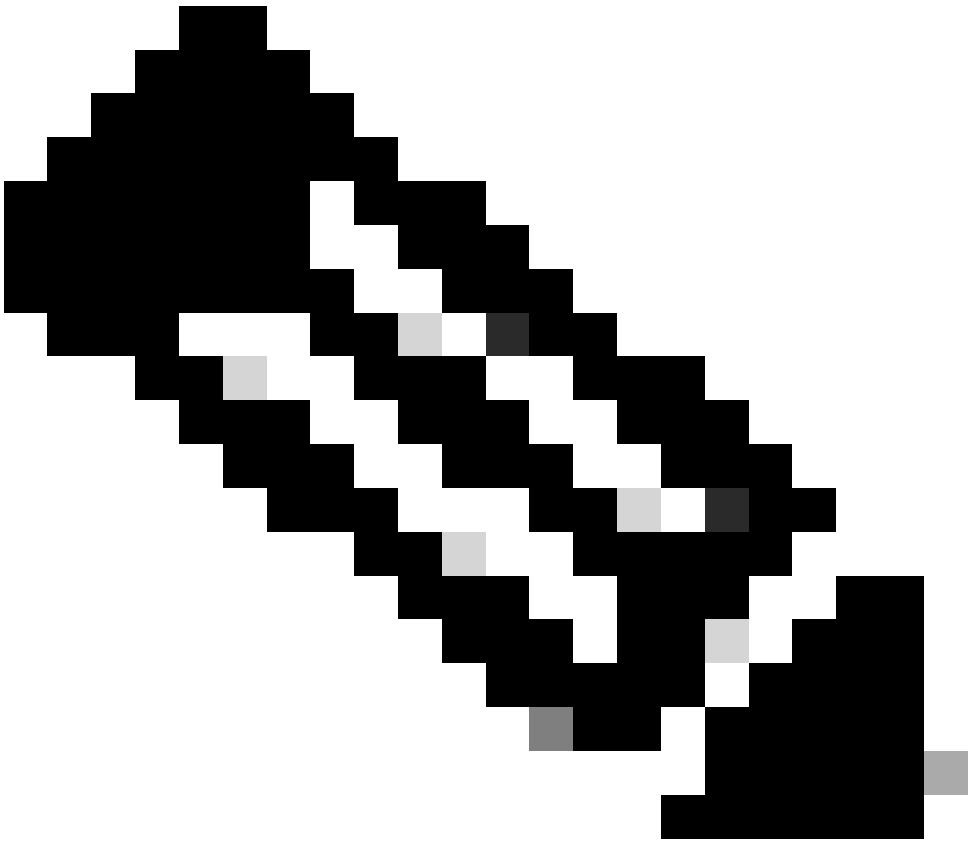
interface vlan primary_vlan_id

Switch_IOS(config-if)#

private-vlan mapping secondary_vlan_list

Switch_IOS(config-if)#

end



Hinweis: Konfigurieren Sie Layer 3-VLAN-Schnittstellen nur für primäre VLANs. VLAN-Schnittstellen für isolierte und Community-VLANs sind mit einer isolierten oder Community-VLAN-Konfiguration inaktiv.

•

Führen Sie den Befehl **show interfaces private-vlan mapping (**Cisco IOS Software) oder **show pvlan mapping (**CatOS) aus, um die Zuordnung zu überprüfen.

•

Wenn Sie die Liste der sekundären VLANs nach der Konfiguration der Zuordnung ändern müssen, verwenden Sie das Schlüsselwort **add** oder **remove**.

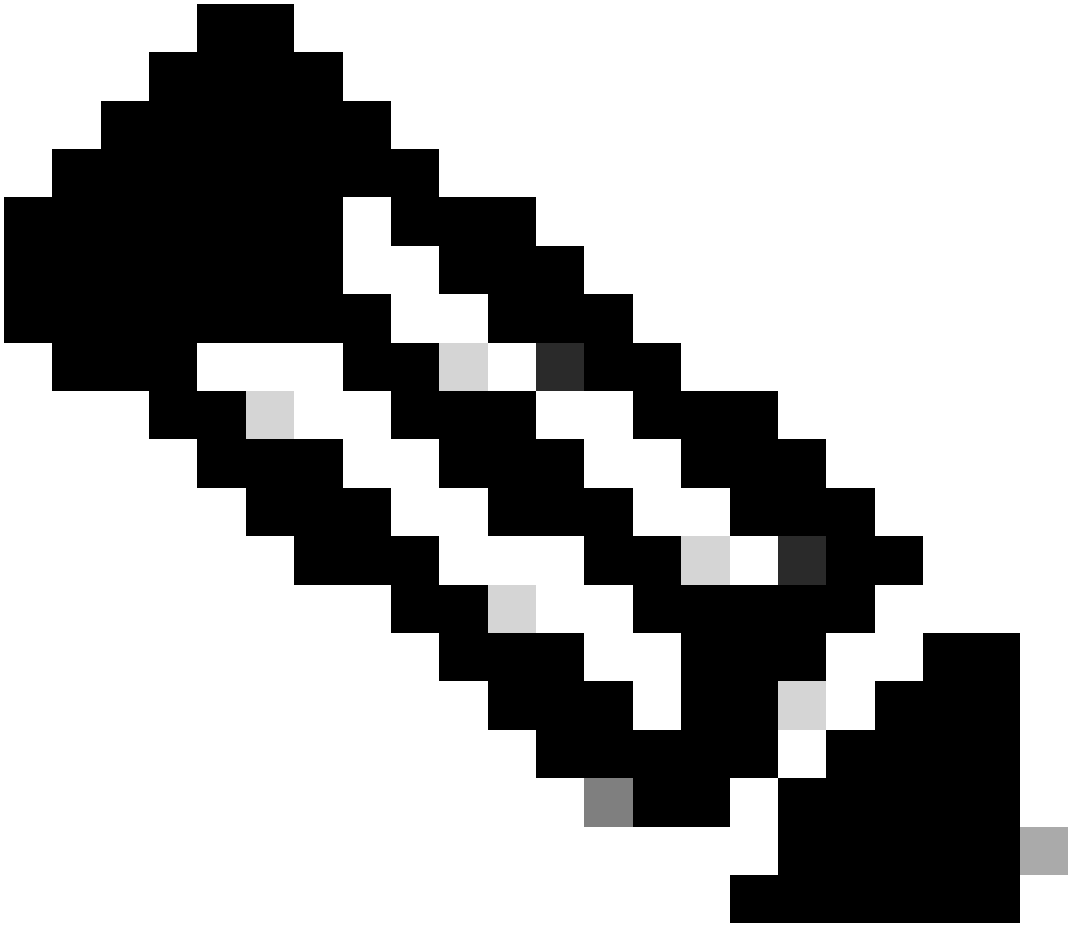
<#root>

Switch_IOS(config-if)#

private-vlan mapping add secondary_vlan_list

or
Switch_IOS(config-if)#

private-vlan mapping remove secondary_vlan_list



Hinweis: Bei Catalyst 6500/6000-Switches mit MSFC muss der Port von der Supervisor Engine zur Routing-Engine (z. B. Port 15/1 oder 16/1) promiskuitiv sein.

<#root>

cat6000> (enable)

set pvlan mapping primary_vlan secondary_vlan 15/1

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

Geben Sie den Befehl **show pvlan mapping** aus, um die Zuordnung zu überprüfen.

```
<#root>

cat6000> (enable)

show pvlan mapping

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

Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

- Access-Layer (Catalyst 4003: CatOS)
- Core (Catalyst 4006: Cisco IOS Software)

Access-Layer (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: Cisco IOS Software)

<#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.
```

Private VLANs können auf zwei Arten über mehrere Switches hinweg genutzt werden. In diesem Abschnitt werden folgende Methoden behandelt:

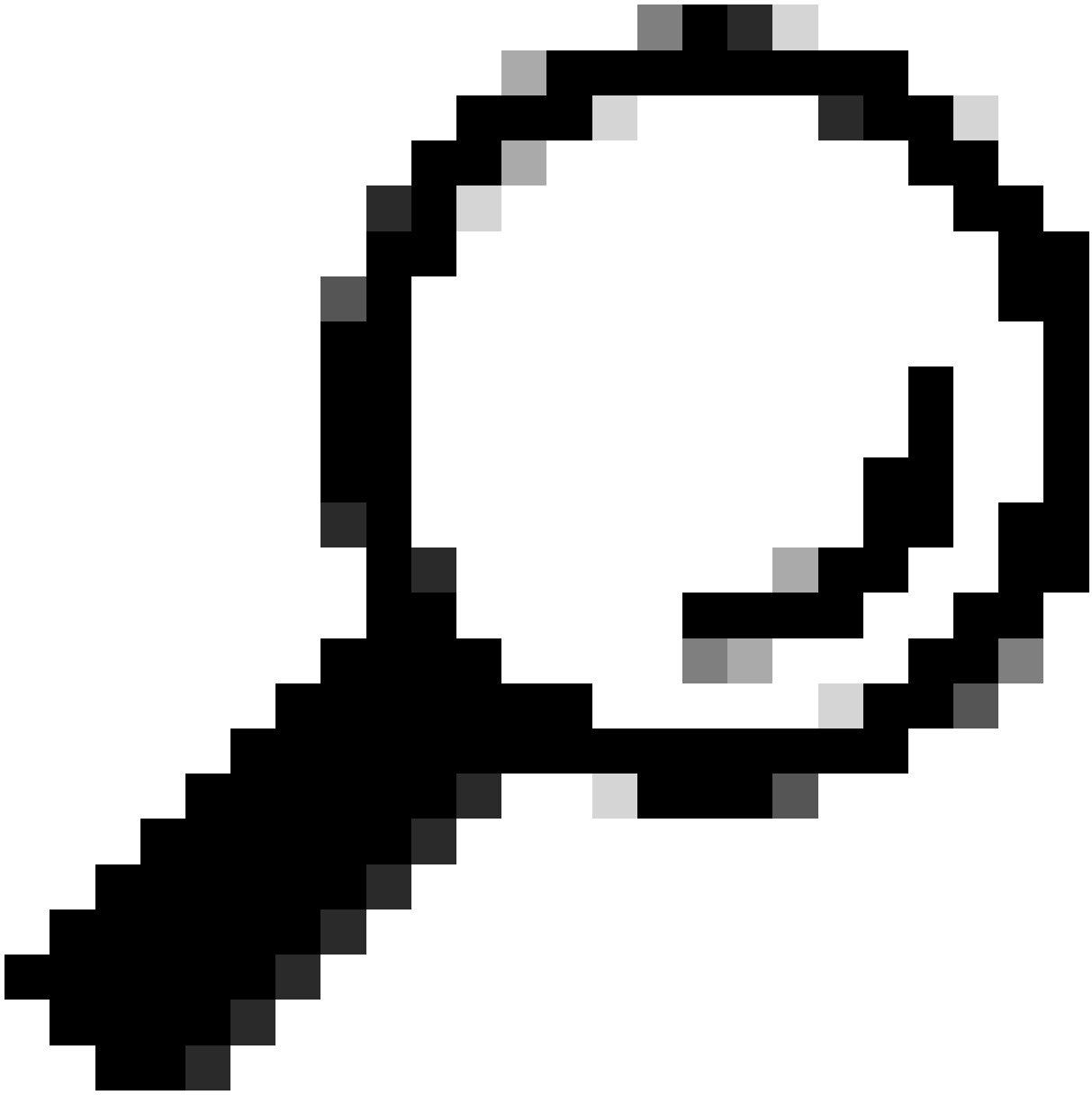
- Reguläre Trunks
- Private VLAN-Trunks

Reguläre Trunks

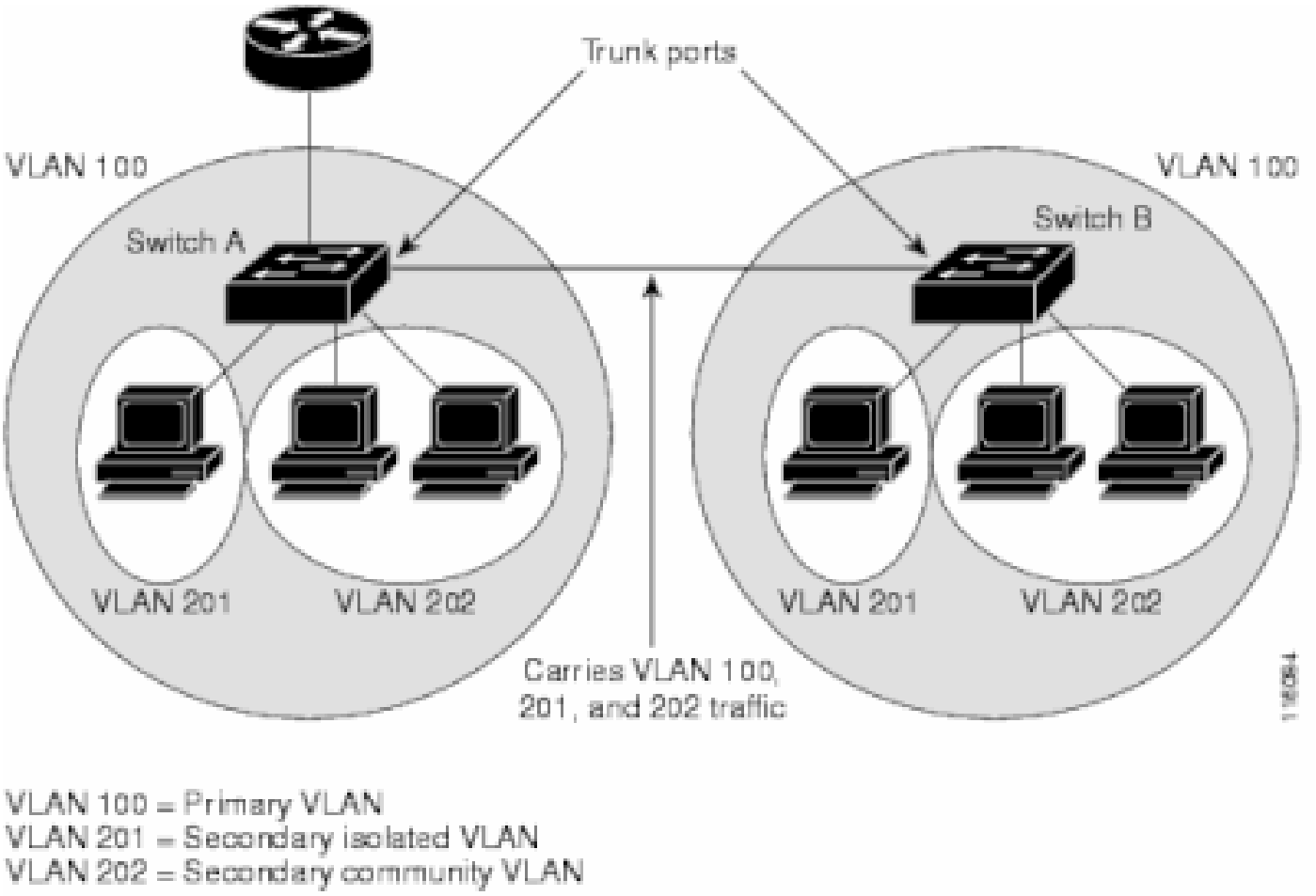
Wie bei regulären VLANs können sich PVLANs über mehrere Switches erstrecken. Ein Trunk-Port verbindet das primäre VLAN und die sekundären VLANs mit einem benachbarten Switch. Der Trunk-Port verarbeitet das private VLAN wie jedes andere VLAN. Eine Funktion von PVLANs, die mehrere Switches umfassen, ist, dass der Datenverkehr von einem isolierten Port eines Switches keinen isolierten Port eines anderen Switches erreicht.

Konfigurieren Sie PVLANs auf allen zwischengeschalteten Geräten, einschließlich Geräten ohne PVLAN-Ports, um die Sicherheit Ihrer PVLAN-Konfiguration zu gewährleisten und eine anderweitige Verwendung der als PVLANs konfigurierten VLANs zu vermeiden.

Trunk-Ports leiten den Datenverkehr von regulären VLANs sowie von primären, isolierten und Community-VLANs weiter.



Tipp: Cisco empfiehlt die Verwendung von Standard-Trunk-Ports, wenn beide Switches, die Trunking durchlaufen, PVLANs unterstützen.



Manuelle Konfiguration von PVLANs auf allen Switches im Layer-2-Netzwerk

Da VTP PVLANs nicht unterstützt, müssen Sie die PVLANs manuell auf allen Switches im Layer-2-Netzwerk konfigurieren. Wenn Sie die primäre und sekundäre VLAN-Zuordnung auf einigen Switches im Netzwerk nicht konfigurieren, werden die Layer-2-Datenbanken auf diesen Switches nicht zusammengeführt. Diese Situation kann zu einer unnötigen Überflutung des PVLAN-Datenverkehrs auf diesen Switches führen.

Private VLAN-Trunks

Ein PVLAN-Trunk-Port kann mehrere sekundäre und Nicht-PVLANs enthalten. Pakete werden über sekundäre oder reguläre VLAN-Tags auf den PVLAN-Trunk-Ports empfangen und übertragen.

Nur IEEE 802.1q-Kapselung wird unterstützt. Mit isolierten Trunk-Ports können Sie den Datenverkehr für alle sekundären Ports über einen Trunk kombinieren. Promiscuous-Trunk-Ports ermöglichen die Kombination der in dieser Topologie erforderlichen mehreren Promiscuous-Ports in einem einzelnen Trunk-Port, der mehrere primäre VLANs überträgt.

Verwenden Sie isolierte private VLAN-Trunk-Ports, wenn Sie davon ausgehen, dass private VLAN-isolierte Host-Ports mehrere VLANs übertragen, entweder normale VLANs oder mehrere private VLAN-Domänen. Dies ist für den Anschluss eines Downstream-Switches nützlich, der keine privaten VLANs unterstützt.

Private VLAN Promiscuous Trunks werden in Situationen verwendet, in denen normalerweise ein Private VLAN Promiscuous Host-Port verwendet wird, aber mehrere VLANs (normale VLANs oder mehrere Private VLAN-Domänen) übertragen werden müssen. Dies ist für die Verbindung mit einem Upstream-Router nützlich, der keine privaten VLANs unterstützt.

Zusätzliche Informationen

Weitere Informationen finden Sie unter Private VLAN Trunks (Private VLAN-Trunks).

Informationen zum Konfigurieren einer Schnittstelle als PVLAN-Trunk-Port finden Sie unter Configuring a Layer 2 Interface as a PVLAN Trunk Port (Konfigurieren einer Layer-2-Schnittstelle als PVLAN-Trunk-Port).

Informationen zum Konfigurieren einer Schnittstelle als Promiscuous-Trunk-Port finden Sie unter Konfigurieren einer Layer-2-Schnittstelle als Promiscuous-Trunk-Port .

Überprüfung

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

CatOS

- **show pvlan**: Zeigt die PVLAN-Konfiguration an. Überprüfen Sie, ob die isolierten und primären VLANs miteinander verknüpft sind. Überprüfen Sie außerdem, ob alle Host-Ports angezeigt werden.

- **show pvlan mapping (**PVLAN-Zuordnung anzeigen): Zeigt die PVLAN-Zuordnung mit Konfiguration an Promiscuous-Ports an.

Cisco IOS Software

- **show vlan private-vlan**: Zeigt PVLAN-Informationen an, darunter auch die Ports, die eine Verbindung herstellen.

- **show interfaceMode/portsSwitchPort**: Zeigt schnittstellenspezifische Informationen an. Überprüfen Sie, ob der Betriebsmodus und die PVLAN-Einstellungen richtig sind.

- **show interfaces private-vlan mapping**: Zeigt die von Ihnen konfigurierte PVLAN-Zuordnung an.

Prüfverfahren

Führen Sie diese Schritte aus:

-

Überprüfen Sie die PVLAN-Konfiguration der Switches.

Überprüfen Sie, ob die primären und sekundären PVLANs einander zugeordnet sind. Überprüfen Sie auch, ob die erforderlichen Ports vorhanden sind.

<#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
```

-

Überprüfen Sie die korrekte Konfiguration des Promiscuous-Ports.

Diese Ausgabe zeigt an, dass der Port-Betriebsmodus **Promiscuous** ist und dass die Betriebs-VLANs 100 und 101 sind.

<#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

•

Initiieren Sie ein ICMP-Ping-Paket (Internet Control Message Protocol) vom Host-Port zum Promiscuous-Port.

Bedenken Sie, dass sich beide Geräte im gleichen primären VLAN befinden und daher im gleichen Subnetz sein müssen.

<#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.

•

Initiieren Sie einen ICMP-Ping zwischen Host-Ports.

In diesem Beispiel versucht host_port_2 (10.1.1.99), einen Ping an > host_port (10.1.1.100) zu senden. Dieser Ping schlägt fehl. Ein Ping von einem anderen Host-Port an den Promiscuous-Port ist jedoch weiterhin erfolgreich.

<#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.
```

Fehlerbehebung

PVLAN-Fehlerbehebung

Dieser Abschnitt behandelt einige häufige Probleme, die bei PVLAN-Konfigurationen auftreten.

Problem 1

Die folgende Fehlermeldung wird angezeigt: `%PM-SP-3-ERR_INCOMP_PORT: <mod/port> ist auf inaktiv gesetzt, da <mod/port> ein Trunk-Port ist`.

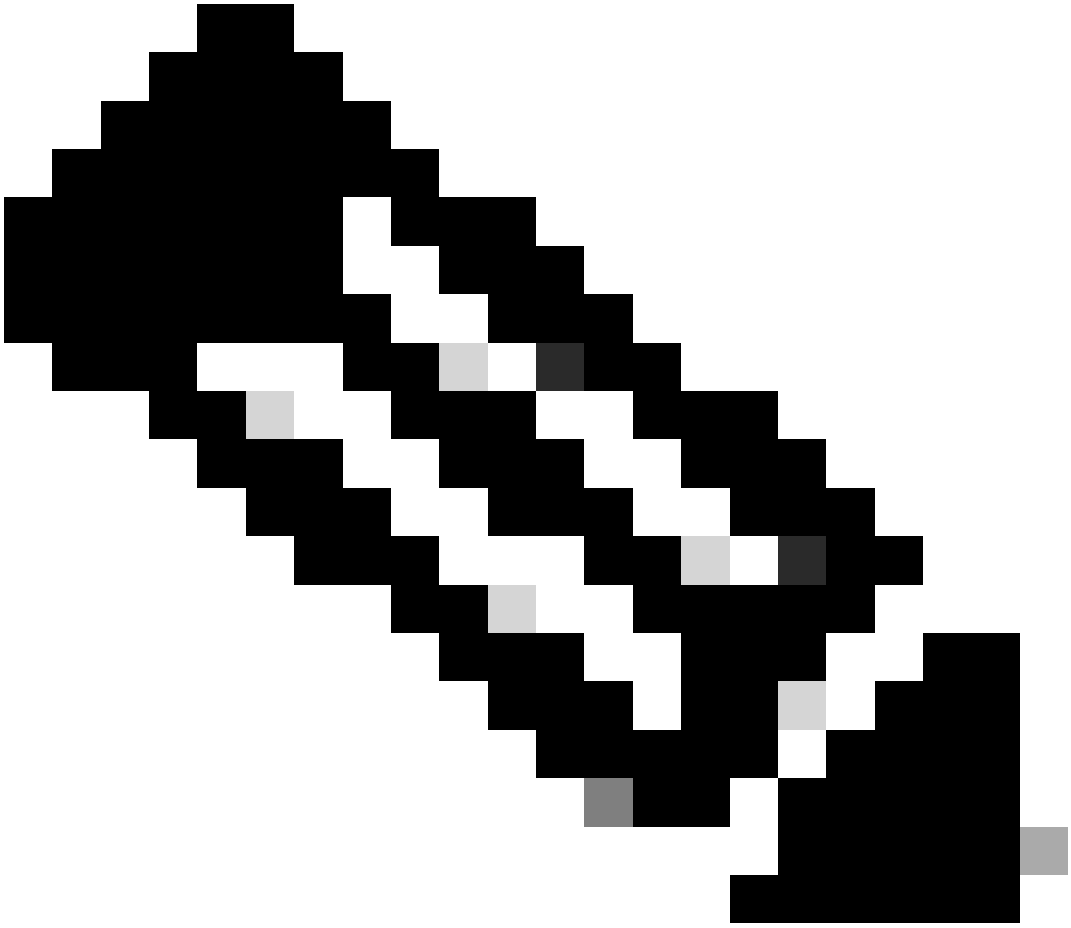
Diese Fehlermeldung kann aus mehreren Gründen angezeigt werden, wie hier beschrieben.

Erläuterung - 1: Aufgrund von Hardware-Einschränkungen beschränken Catalyst 6500/6000-Module mit 10/100 Mbit/s die Konfiguration eines isolierten oder Community-VLAN-Ports, wenn ein Port innerhalb desselben COIL-ASIC ein Trunk-, SPAN- oder Promiscuous-PVLAN-Port ist. (Der COIL ASIC steuert 12 Ports an den meisten Modulen und 48 Ports am Catalyst 6548-Modul.) Die Tabelle im Abschnitt "Regeln und Einschränkungen" dieses Dokuments enthält eine Aufschlüsselung der Portbeschränkungen für die Catalyst 6500/6000-Module mit 10/100 Mbit/s.

Auflösungsverfahren - 1: Wenn an diesem Port keine Unterstützung für PVLAN vorhanden ist, wählen Sie einen Port auf einem anderen ASIC auf dem Modul oder auf einem anderen Modul aus. Um die Ports zu reaktivieren, entfernen Sie die Konfiguration des isolierten oder Community-VLAN-Ports, und geben Sie den Befehl **shutdown** und **no shutdown** ein.

Erklärung - 2: Wenn die Ports manuell oder standardmäßig für den *dynamischen erwünschten* oder *dynamischen Auto*-Modus konfiguriert sind.

Auflösungsverfahren - 2: Konfigurieren Sie die Ports mit dem Befehl **switchport mode access** als Zugriffsmodus. Um die Ports zu reaktivieren, geben Sie den Befehl **shutdown** und den Befehl **no shutdown** ein.



Hinweis: In Version 12.2(17a)SX der Cisco IOS-Software und späteren Versionen gilt die Beschränkung auf 12 Ports nicht für WS-X6548-RJ-45, WS-X6548-RJ-21 und WS-X6524-100FX-MM Ethernet-Switching Module.

Problem 2

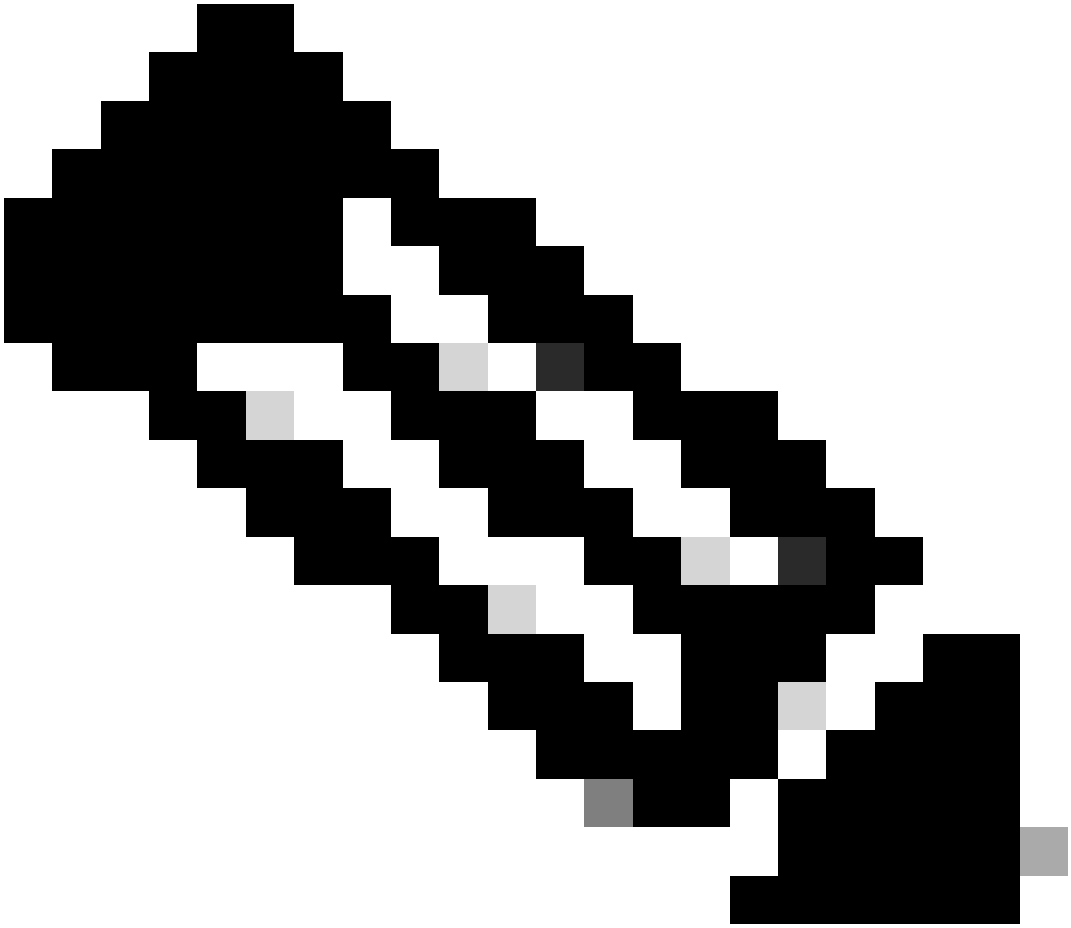
Während der PVLAN-Konfiguration wird *eine* der folgenden Meldungen angezeigt:

```
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.
```

Erläuterung: Aufgrund von Hardwarebeschränkungen schränken Catalyst 6500/6000-Module mit 10/100 Mbit/s die Konfiguration eines isolierten oder Community-VLAN-Ports ein, wenn ein Port innerhalb desselben COIL-ASIC ein Trunk-, SPAN- oder Promiscuous-PVLAN-Port ist. (Der COIL ASIC steuert 12 Ports an den meisten Modulen und 48 Ports am Catalyst 6548-Modul.) Die Tabelle im Abschnitt "Regeln und Einschränkungen" dieses Dokuments enthält eine Aufschlüsselung der Portbeschränkungen für die Catalyst 6500/6000-Module mit 10/100 Mbit/s.

Auflösungsverfahren: Geben Sie den Befehl **show pvlan ability** (CatOS) ein, der angibt, ob ein Port ein PVLAN-Port werden kann. Wenn an diesem Port kein PVLAN unterstützt wird, wählen Sie einen Port an einem anderen ASIC auf dem Modul oder einem anderen Modul aus.



Hinweis: In Version 12.2(17a)SX der Cisco IOS-Software und späteren Versionen gilt die Beschränkung auf 12 Ports nicht für WS-X6548-RJ-45, WS-X6548-RJ-21 und WS-X6524-100FX-MM Ethernet-Switching Module.

Problem 3

Auf einigen Plattformen können keine PVLANs konfiguriert werden.

Auflösung: Stellen Sie sicher, dass die Plattform PVLANs unterstützt. In der Private VLAN Catalyst Switch Support Matrix können Sie vor Beginn der Konfiguration ermitteln, ob Ihre Plattform- und Softwareversion PVLANs unterstützt.

Problem 4

Bei einer Catalyst 6500/6000 MSFC können Sie kein Gerät anpingen, das mit dem isolierten Port des Switches verbunden ist.

Auflösung: Überprüfen Sie auf der Supervisor Engine, ob der Port zur MSFC (15/1 oder 16/1) Promiscuous ist.

```
<#root>

cat6000> (enable)

set pvlan mapping primary_vlan secondary_vlan 15/1

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

Konfigurieren Sie außerdem die VLAN-Schnittstelle auf der MSFC, wie im Abschnitt zur Layer-3-Konfiguration dieses Dokuments angegeben.

Problem 5

Mit dem Befehl **no shutdown** können Sie die VLAN-Schnittstelle für isolierte VLANs oder Community-VLANs nicht aktivieren.

Auflösung: Aufgrund der Eigenschaften von PVLANs können Sie die VLAN-Schnittstelle für isolierte oder Community-VLANs nicht aktivieren. Sie können nur die VLAN-Schnittstelle aktivieren, die zum primären VLAN gehört.

Problem 6

Auf Catalyst 6500/6000-Geräten mit MSFC/MSFC2 veralten die ARP-Einträge, die auf den Layer-3-PVLAN-Schnittstellen gelernt werden, nicht.

Auflösung: ARP-Einträge, die an privaten VLAN-Schnittstellen auf Layer 3 erfasst werden, sind starre ARP-Einträge und werden nicht veraltet. Beim Anschluss neuer Geräte mit derselben IP-Adresse wird eine Meldung generiert, und es wird kein ARP-Eintrag erstellt. Daher müssen Sie PVLAN-Port-ARP-Einträge manuell entfernen, wenn sich eine MAC-Adresse ändert. Führen Sie die folgenden Befehle aus, um PVLAN ARP-Einträge manuell hinzuzufügen oder zu entfernen:

```
<#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
```

Eine weitere Option besteht darin, den Befehl **no ip sticky-arp** in Version 12.1(11b)E der Cisco IOS-Software und höher auszugeben.

Zugehörige Informationen

- **Cisco Catalyst Switches der Serie 2955 - Einstellungsbenachrichtigung**
- **Sichere Netzwerke mit PVLANs und VACLs**

- **Support für LAN-Switching-Technologie**
- **Technischer Support und Downloads von Cisco**

Informationen zu dieser Übersetzung

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