Catalyst 스위치에서 격리 프라이빗 VLAN 구성

목차

소개

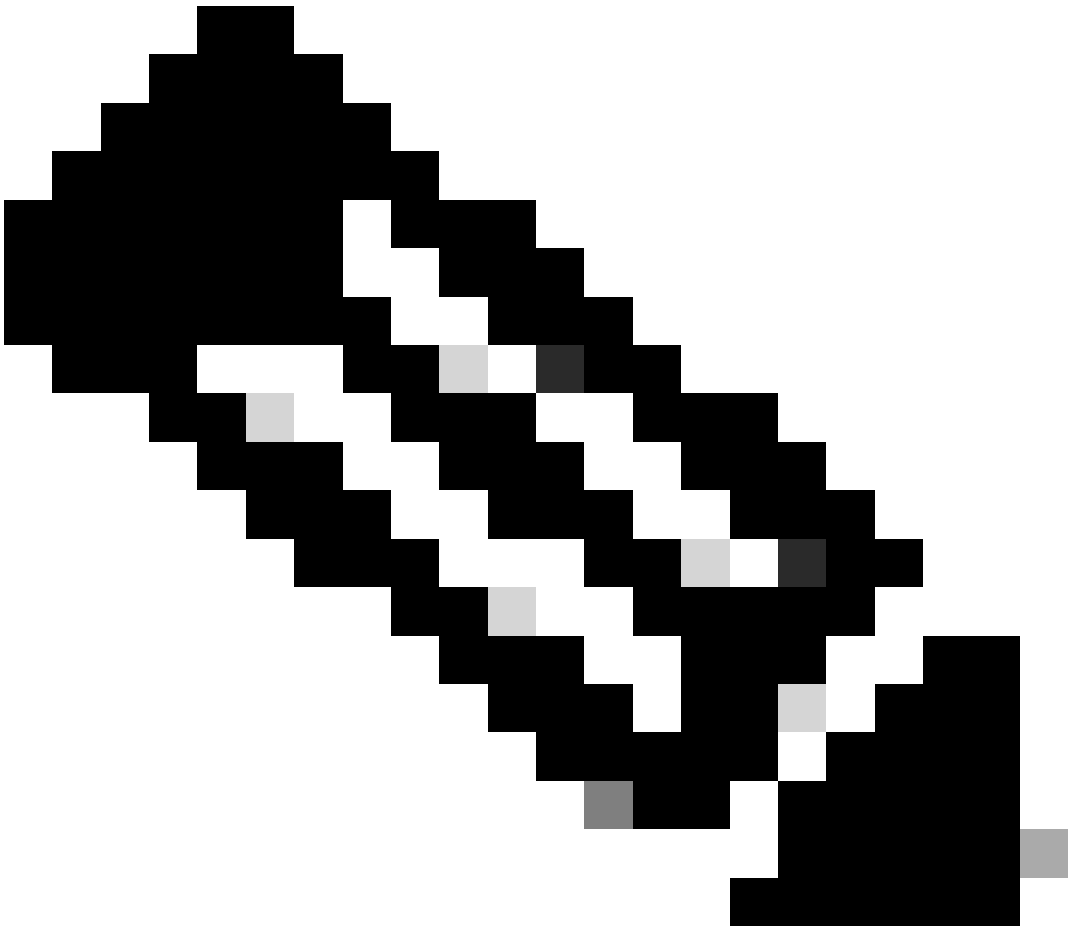
이 문서에서는 Catalyst OS(CatOS) 또는 Cisco IOS® Software를 사용하여 Cisco Catalyst 스위치에서 격리 PVLAN을 구성하는 절차에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에서는 네트워크가 이미 있으며 PVLAN에 추가하기 위해 다양한 포트 간에 연결을 설정할 수 있다고 가정합니다. 여러 스위치가 있는 경우 스위치 간 트렁크가 제대로 작동하고 트렁크의 PVLAN을 허용하는지 확인합니다.

모든 스위치와 소프트웨어 버전이 PVLAN을 지원하는 것은 아닙니다.



참고: 일부 스위치(Private VLAN Catalyst Switch Support Matrix에 지정되어 있음)는 현재 PVLAN Edge 기능만 지원합니다. "보호되는 포트"라는 용어는 이 기능을 나타내기도 합니다. PVLAN 에지 포트에는 제한이 있어 동일한 스위치의 다른 보호 포트와의 통신이 금지됩니다. 그러나 별도의 스위치에 있는 보호 포트는 서로 통신할 수 있습니다. 이 기능을 이 문서에 나와 있는 일반적인 PVLAN 컨피그레이션과 혼동하지 마십시오. 보호된 포트에 대한 자세한 내용은 포트 기반 트래픽 제어 구성 문서의 포트 보안 구성 섹션을 참조하십시오.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Catalyst 4003 스위치와 CatOS 버전 6.3(5)을 실행하는 Supervisor Engine 2 모듈
- Cisco IOS Software 릴리스 12.1(12c)EW1을 실행하는 Supervisor Engine 3 모듈이 포함된 Catalyst 4006 스위치

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

배경 정보

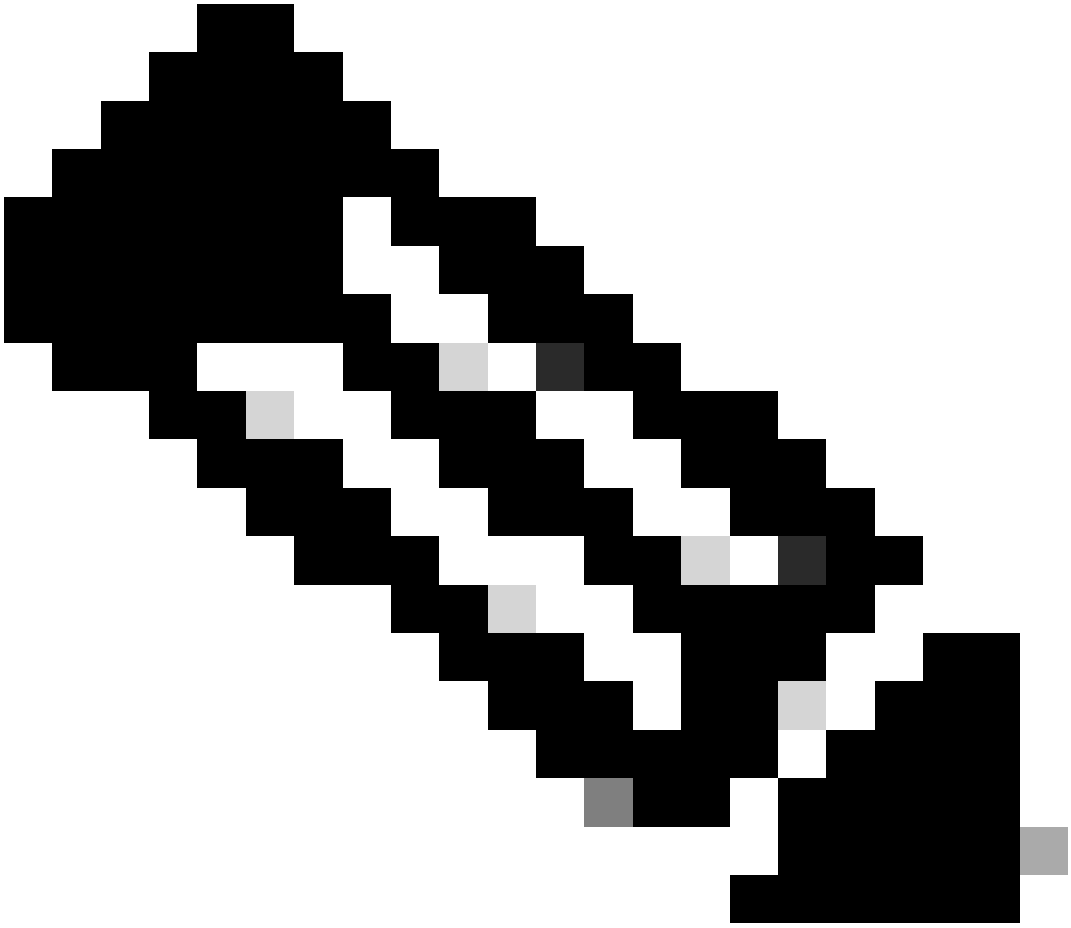
경우에 따라 다른 IP 서브넷에 디바이스를 배치하지 않고 스위치에서 엔드 디바이스 간 레이어 2(L2) 연결을 방지해야 합니다. 이렇게 설정하면 IP 주소가 낭비되는 것을 방지할 수 있습니다. PVLAN(Private VLAN)은 동일한 IP 서브넷에 있는 디바이스의 레이어 2에서 격리를 허용합니다. 스위치의 일부 포트는 기본 게이트웨이, 백업 서버 또는 Cisco LocalDirector가 연결된 특정 포트에만 연결되도록 제한할 수 있습니다.

이 문서에서는 Catalyst OS(CatOS) 또는 Cisco IOS Software를 사용하여 Cisco Catalyst 스위치에서 격리 PVLAN을 구성하는 절차에 대해 설명합니다.

PVLAN은 동일한 브로드캐스트 도메인 또는 서브넷 내의 다른 포트와의 레이어 2 격리를 위한 컨피그레이션을 포함하는 VLAN입니다. PVLAN 내에서 특정 포트 집합을 할당하여 레이어 2의 포트 간 액세스를 제어할 수 있습니다. 동일한 스위치에서 PVLAN과 일반 VLAN을 구성할 수 있습니다.

PVLAN 포트에는 프로미스큐어스(promiscuous), 격리(isolated) 및 커뮤니티(community)의 세 가지 유형이 있습니다.

- 프로미스큐어스 포트는 다른 모든 PVLAN 포트와 통신합니다. 프로미스큐어스 포트는 외부 라우터, LocalDirectors, 네트워크 관리 디바이스, 백업 서버, 관리 워크스테이션 및 기타 디바이스와 통신하는 데 일반적으로 사용하는 포트입니다. 일부 스위치에서 경로 모듈(예: MSFC(Multilayer Switch Feature Card))에 대한 포트는 프로미스큐어스여야 합니다.
- 격리된 포트는 동일한 PVLAN 내의 다른 포트와 완전한 레이어 2 분리를 갖습니다. 이러한 분리에는 브로드캐스트가 포함되며, 유일한 예외는 프로미스큐어스 포트입니다. 레이어 2 레벨의 프라이버시 부여는 모든 격리된 포트에 대한 발신 트래픽 차단과 함께 발생합니다. 격리된 포트에서 오는 트래픽은 모든 프로미스큐어스 포트에만 전달됩니다.
- 커뮤니티 포트는 서로 및 프로미스큐어스 포트와 통신할 수 있습니다. 이러한 포트는 다른 커뮤니티의 다른 모든 포트 또는 PVLAN 내의 격리된 포트와 레이어 2 격리됩니다. 브로드캐스트는 연결된 커뮤니티 포트와 프로미스큐어스 포트 간에만 전파됩니다.



참고: 이 문서에서는 커뮤니티 VLAN 컨피그레이션을 다루지 않습니다.

규칙 및 제한 사항

이 섹션에서는 PVLAN을 구현할 때 확인해야 하는 몇 가지 규칙 및 제한 사항을 제공합니다.

- PVLAN에는 VLAN 1 또는 1002-1005를 포함할 수 없습니다.
- VTP(VLAN Trunk Protocol) 모드를 투명으로 설정해야 합니다.
- 기본 VLAN당 격리 VLAN을 하나만 지정할 수 있습니다.
- VLAN에 현재 액세스 포트 할당이 없는 경우에만 VLAN을 PVLAN으로 지정할 수 있습니다. VLAN을 PVLAN으로 만들기 전에 해당 VLAN의 모든 포트를 제거합니다.
- PVLAN 포트를 EtherChannel로 구성하지 마십시오.
- 하드웨어 제한으로 인해, Catalyst 6500/6000 고속 이더넷 스위치 모듈은 동일한 COIL

ASIC(application-specific integrated circuit) 내의 한 포트가 다음 중 하나인 경우 격리 또는 커뮤니티 VLAN 포트의 구성을 제한합니다.

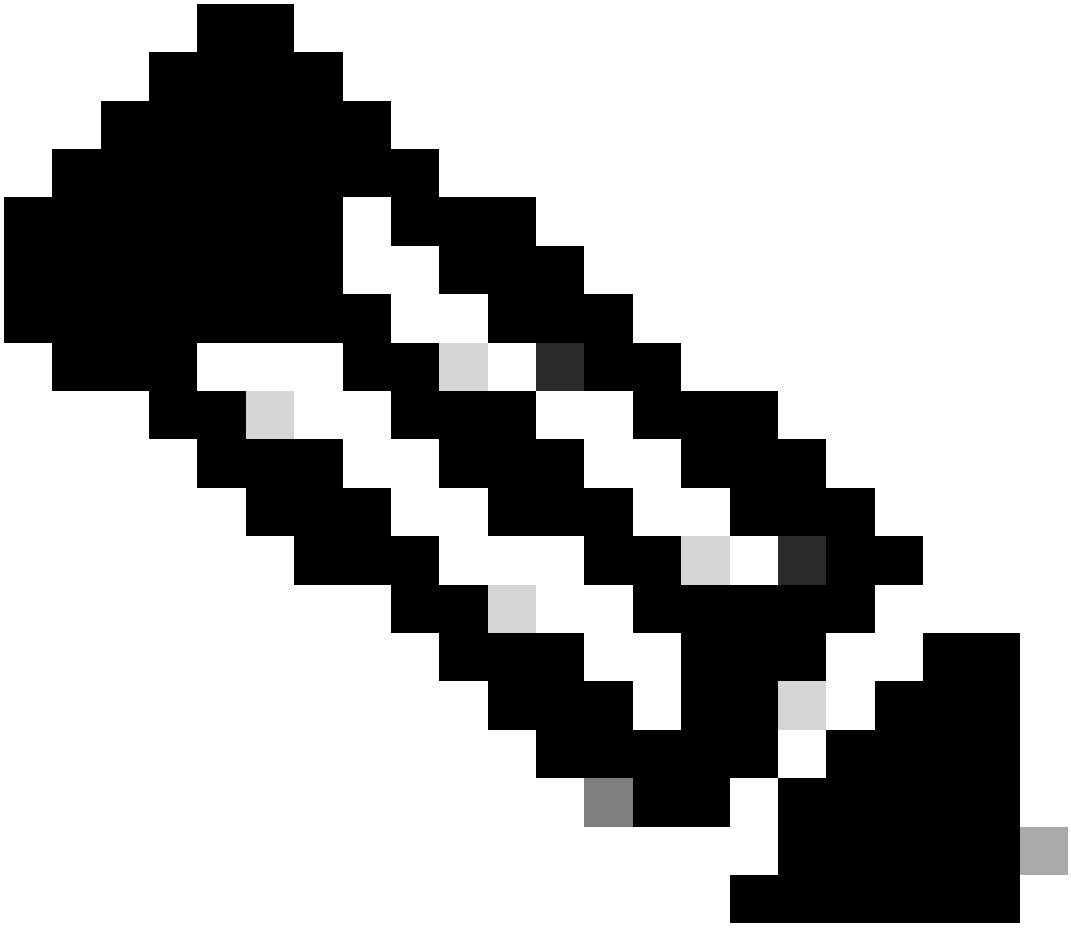
- 트렁크
- SPAN(Switched Port Analyzer) 대상
- 무차별 PVLAN 포트

이 표는 Catalyst 6500/6000 FastEthernet 모듈의 동일한 ASIC에 속하는 포트 범위를 나타냅니다.

모듈	ASIC별 포트
WS-X6224-100FX-MT, WS-X6248-RJ-45, WS-X6248-TEL	포트 1-12, 13-24, 25-36, 37-48
WS-X6024-10FL-MT	포트 1-12, 13-24
WS-X6548-RJ-45, WS-X6548-RJ-21	포트 1-48

CatOS(show pvlan capability command)는 포트를 PVLAN 포트로 설정할 수 있는지도 나타냅니다. Cisco IOS Software에는 이에 상응하는 명령이 없습니다.

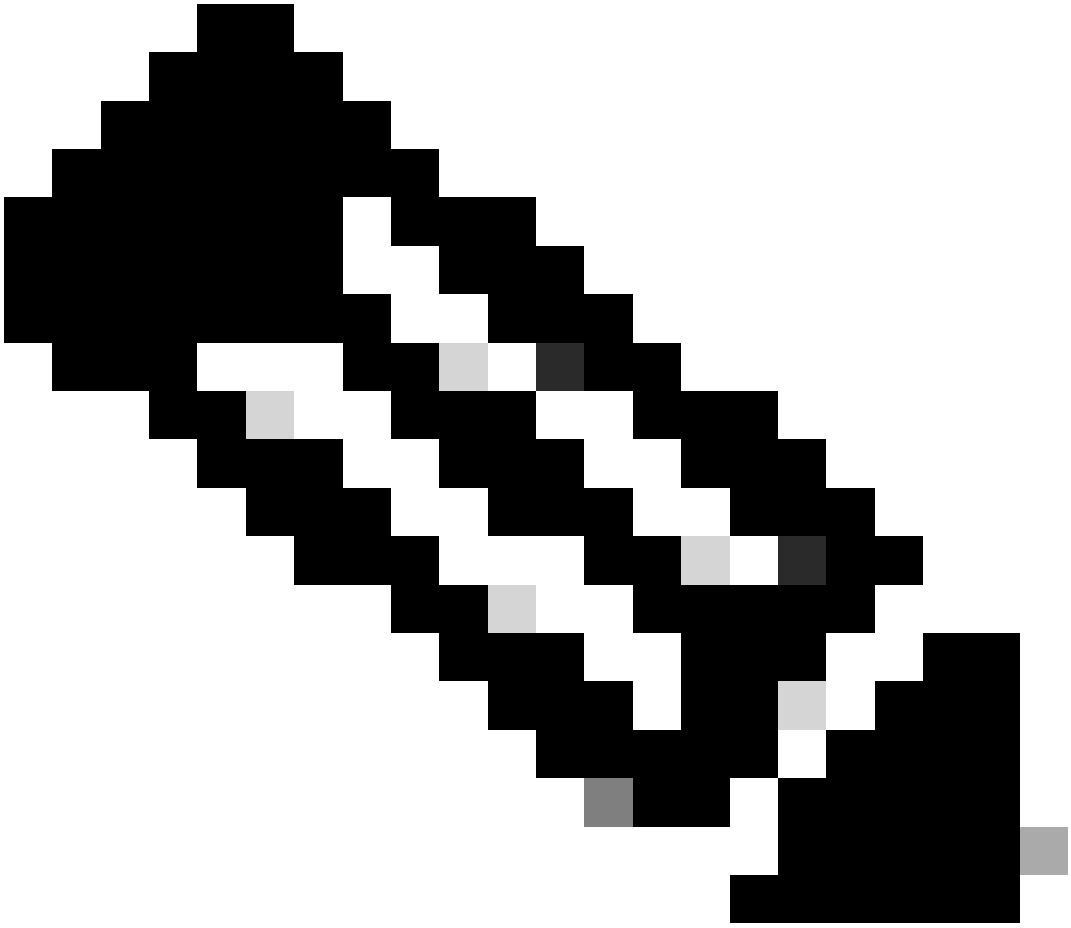
- PVLAN 컨피그레이션에서 사용하는 VLAN을 삭제하면 해당 VLAN과 연결된 포트가 비활성화됩니다.
- 기본 VLAN에 대해서만 레이어 3(L3) VLAN 인터페이스를 구성합니다. 격리 및 커뮤니티 VLAN에 대한 VLAN 인터페이스는 비활성 상태이며, VLAN에는 격리 또는 커뮤니티 VLAN 컨피그레이션이 있습니다.
- 트렁크를 사용하여 스위치 간에 PVLAN을 확장할 수 있습니다. 트렁크 포트는 일반 VLAN과 기본, 격리 및 커뮤니티 VLAN의 트래픽을 전달합니다. 트렁킹을 받는 두 스위치가 모두 PVLAN을 지원하는 경우에는 표준 트렁크 포트를 사용하는 것이 좋습니다.



참고: 투명 모드의 VTP는 이 정보를 전파하지 않으므로 관여가 있는 모든 스위치에서 동일한 PVLAN 컨피그레이션을 수동으로 입력해야 합니다.

구성

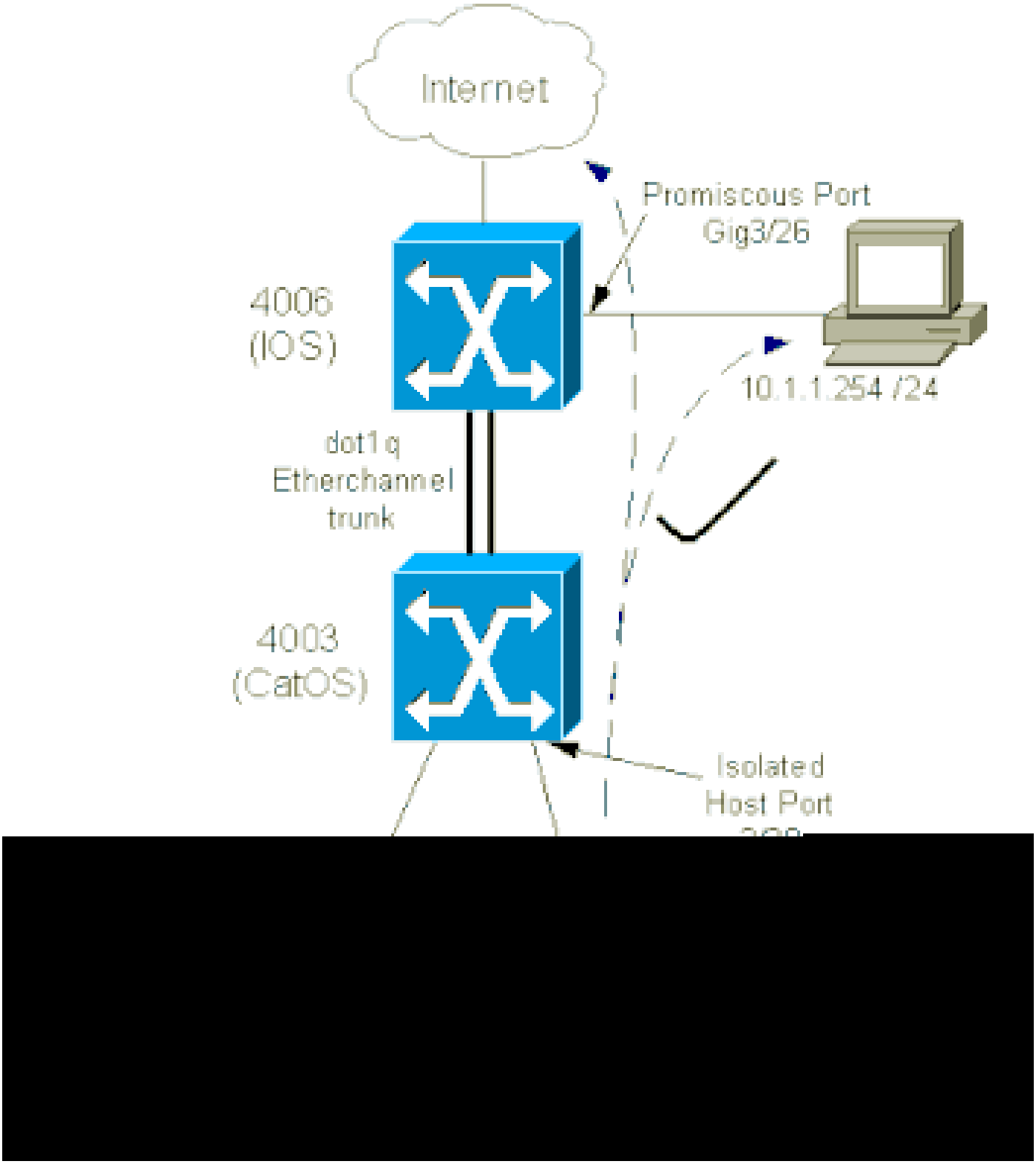
이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.



참고: 이 문서에서 사용되는 명령에 대한 자세한 내용을 보려면 명령 조회 도구를 사용하십시오. 등록된 사용자만 내부 Cisco 툴 및 정보에 액세스할 수 있습니다.

네트워크 다이어그램

이 문서에서는 이 네트워크 설정을 사용합니다.



이 시나리오에서 격리 VLAN(101)의 디바이스는 레이어 2에서 서로 통신하는 데 제한이 있습니다. 그러나 디바이스는 인터넷에 연결할 수 있습니다. 또한 4006의 포트 Gig 3/26은 프로미스큐어스(promiscuous)로 지정됩니다. 이 선택적 컨피그레이션을 통해 GigabitEthernet 3/26의 디바이스를 격리된 VLAN의 모든 디바이스에 연결할 수 있습니다. 이 컨피그레이션에서는 예를 들어 모든 PVLAN 호스트 디바이스에서 관리 워크스테이션으로 데이터를 백업할 수도 있습니다. 프로미스큐어스 포트에 대한 기타 용도로는 외부 라우터, LocalDirector, 네트워크 관리 디바이스 및 기타 디바이스에 대한 연결이 있습니다.

기본 및 격리 VLAN 구성

기본 및 보조 VLAN을 생성하고 다양한 포트를 이러한 VLAN에 바인딩하려면 다음 단계를 수행합니다. 이 단계에는 CatOS 및 Cisco IOS® Software의 예가 포함됩니다. OS 설치에 적합한 명령 세트를 실행합니다.

1. 기본 PVLAN을 생성합니다.

   - 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. 격리된 VLAN 또는 VLAN을 생성합니다.

   - 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. 격리된 VLAN/VLAN을 기본 VLAN에 바인딩합니다.

- 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. 프라이빗 VLAN 컨피그레이션을 확인합니다.

- CatOS

<#root>

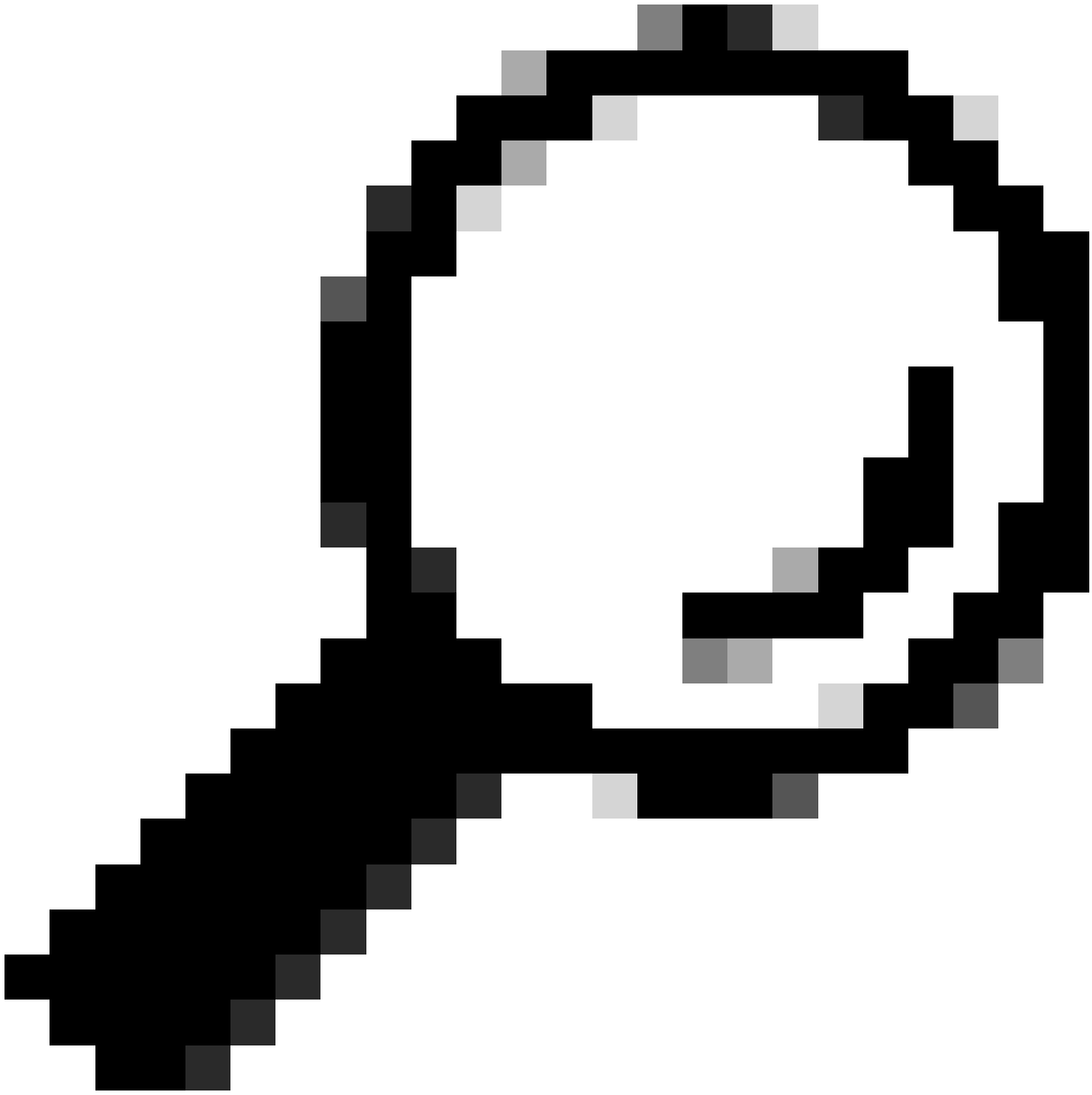
```
Switch_CatOS> (enable)
show pvlan
Primary Secondary Secondary-Type   Ports
------- --------- ---------------- ------------
100     101       isolated
```

- Cisco IOS Software

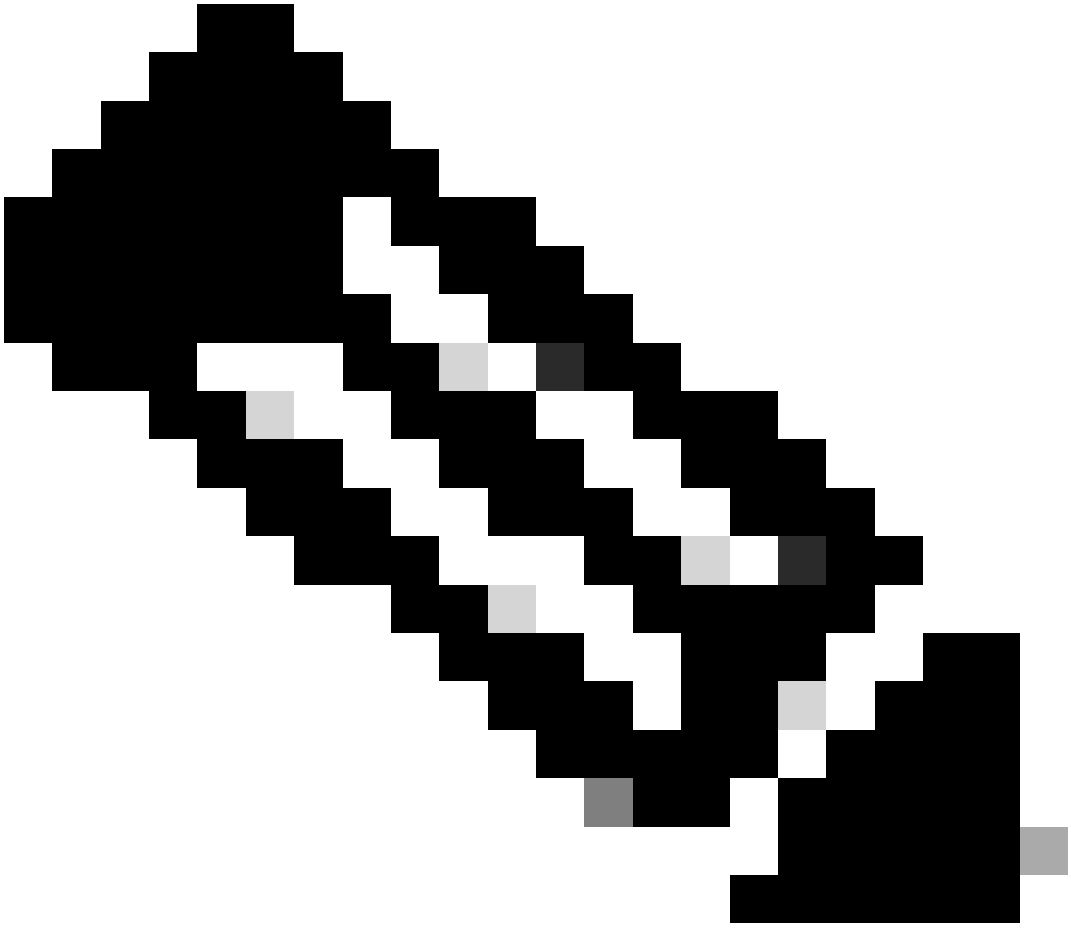
<#root>

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

PVLAN에 포트 할당



팁: 이 절차를 구현하기 전에 show PVLAN capability mod/port 명령(CatOS용)을 실행하여 포트가 PVLAN 포트가 될 수 있는지 확인합니다.



참고: 이 절차의 1단계를 수행하기 전에 인터페이스 컨피그레이션 모드에서 switchport 명령을 실행하여 포트를 레이어 2 스위치드 인터페이스로 구성합니다.

-

해당되는 모든 스위치에서 호스트 포트를 구성합니다.

  - **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
```

- 스위치 중 하나에서 프로미스큐어스 포트를 구성합니다.

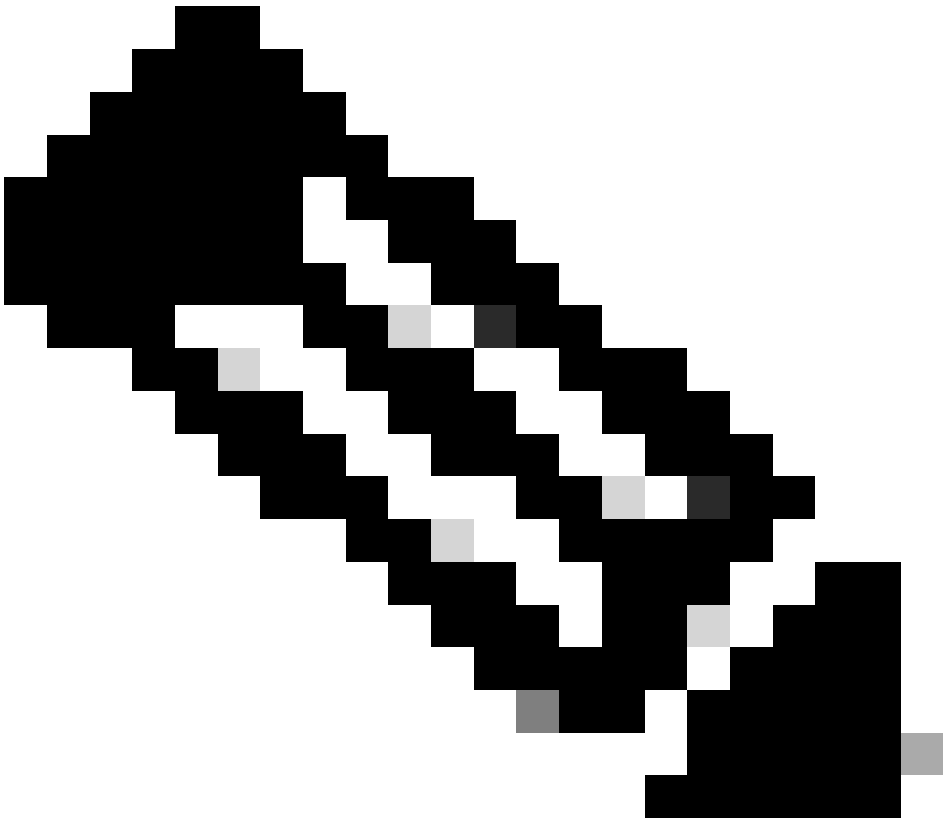
  - **CatOS**

```
<#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
```



참고: 수퍼바이저 엔진이 시스템 소프트웨어로 CatOS를 실행하는 Catalyst 6500/6000의 경우, VLAN 간에 레이어 3 스위치를 사용하려는 경우 수퍼바이저 엔진의 MSFC 포트(15/1 또는 16/1)가 프로미스큐어스여야 합니다.

•

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
```

레이어 3 컨피그레이션

이 선택 사항 섹션에서는 PVLAN 인그레스 트래픽의 경로를 허용하는 컨피그레이션 단계에 대해 설명합니다. 레이어 2 연결만 활성화해야 하는 경우 이 단계를 생략할 수 있습니다.

- 일반 레이어 3 라우팅에 대해 구성하는 것과 동일한 방식으로 VLAN 인터페이스를 구성합니다.

  이 컨피그레이션에는 다음이 포함됩니다.

- IP 주소 컨피그레이션

- **no shutdown** 명령으로 인터페이스 활성화

- VLAN이 VLAN 데이터베이스에 있는지 확인

컨피그레이션 예제는 VLAN/VTP 기술 지원을 참조하십시오.

- 라우팅할 보조 VLAN을 기본 VLAN과 매핑합니다.

<#root>

Switch_IOS(config)#

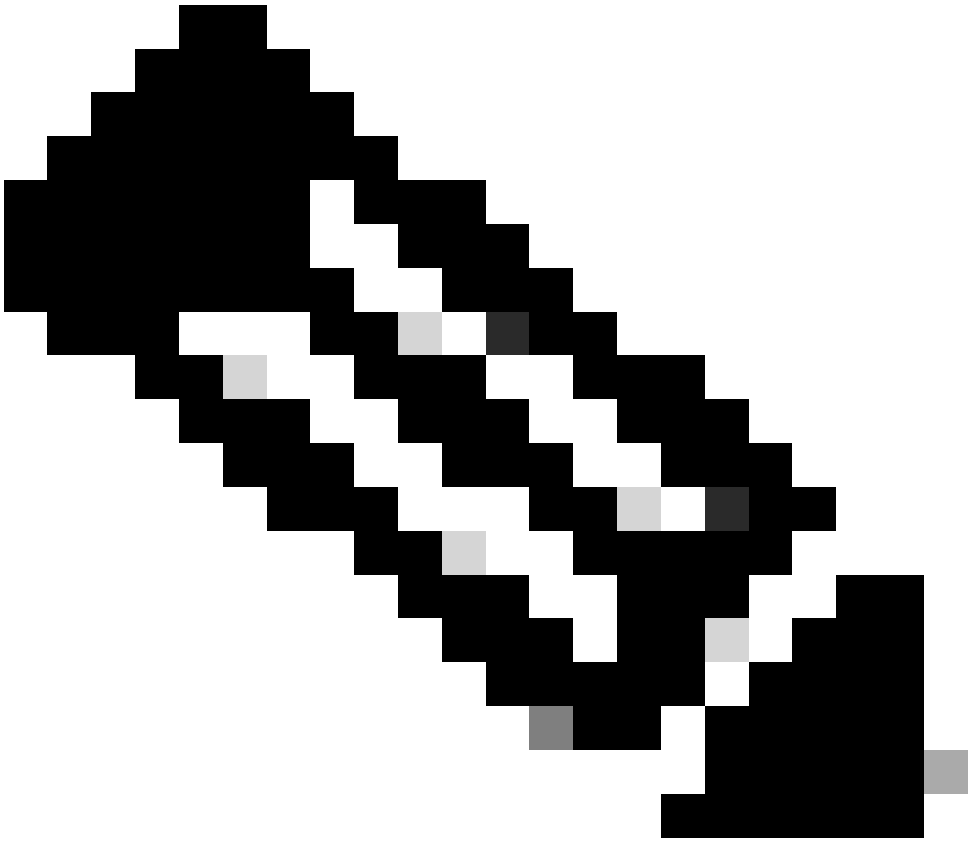
interface vlan primary_vlan_id

Switch_IOS(config-if)#

private-vlan mapping secondary_vlan_list

Switch_IOS(config-if)#

end



참고: 기본 VLAN에 대해서만 레이어 3 VLAN 인터페이스를 구성합니다. 격리 및 커뮤니티 VLAN에 대한 VLAN 인터페이스는 격리 또는 커뮤니티 VLAN 컨피그레이션으로 비활성 상태입니다.

•

매핑을 확인하기 위해 **show interfaces private-vlan mapping**(Cisco IOS Software) 또는 **show pvlan mapping**(CatOS) 명령을 실

행합니다.

-

매핑을 구성한 후 보조 VLAN 목록을 수정해야 하는 경우 add 또는 **remove** 키워드를 **사용합니다**.

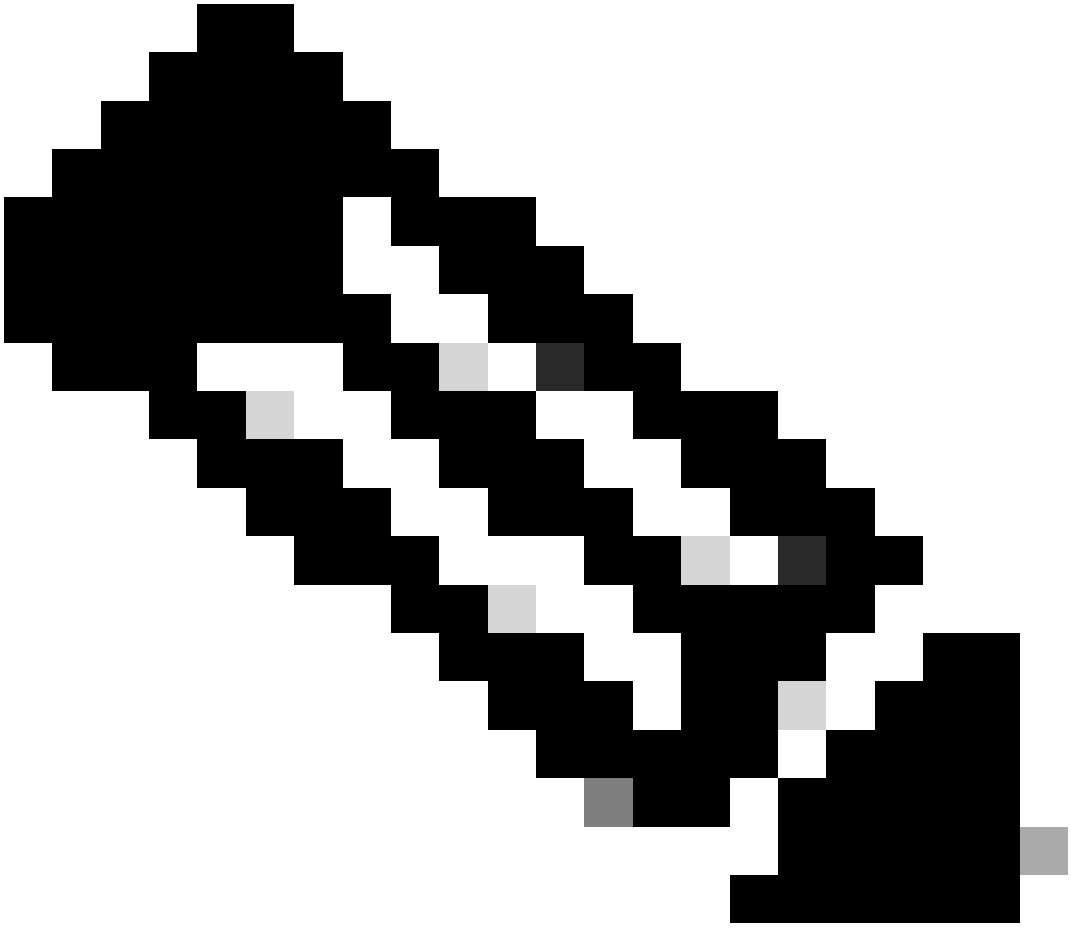
<#root>

Switch_IOS(config-if)#

private-vlan mapping add secondary_vlan_list

or
Switch_IOS(config-if)#

private-vlan mapping remove secondary_vlan_list



참고: MSFC가 포함된 Catalyst 6500/6000 스위치의 경우 수퍼바이저 엔진에서 라우팅 엔진으로의 포트(예: 포트 15/1 또는 16/1)가 프로미스큐어스인지 확인합니다.

<#root>

cat6000> (enable)

set pvlan mapping primary_vlan secondary_vlan 15/1

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

명령 show pvlan **mapping** 명령을 실행하여 매핑을 확인합니다.

```
<#root>

cat6000> (enable)

show pvlan mapping

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

설정

이 문서에서는 다음 설정을 사용합니다.

- Access_Layer(Catalyst 4003: CatOS)
- 코어(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
```

코어(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.
```

여러 스위치의 프라이빗 VLAN

프라이빗 VLAN은 두 가지 방법으로 여러 스위치에서 사용할 수 있습니다. 이 섹션에서는 다음 방법에 대해 설명합니다.

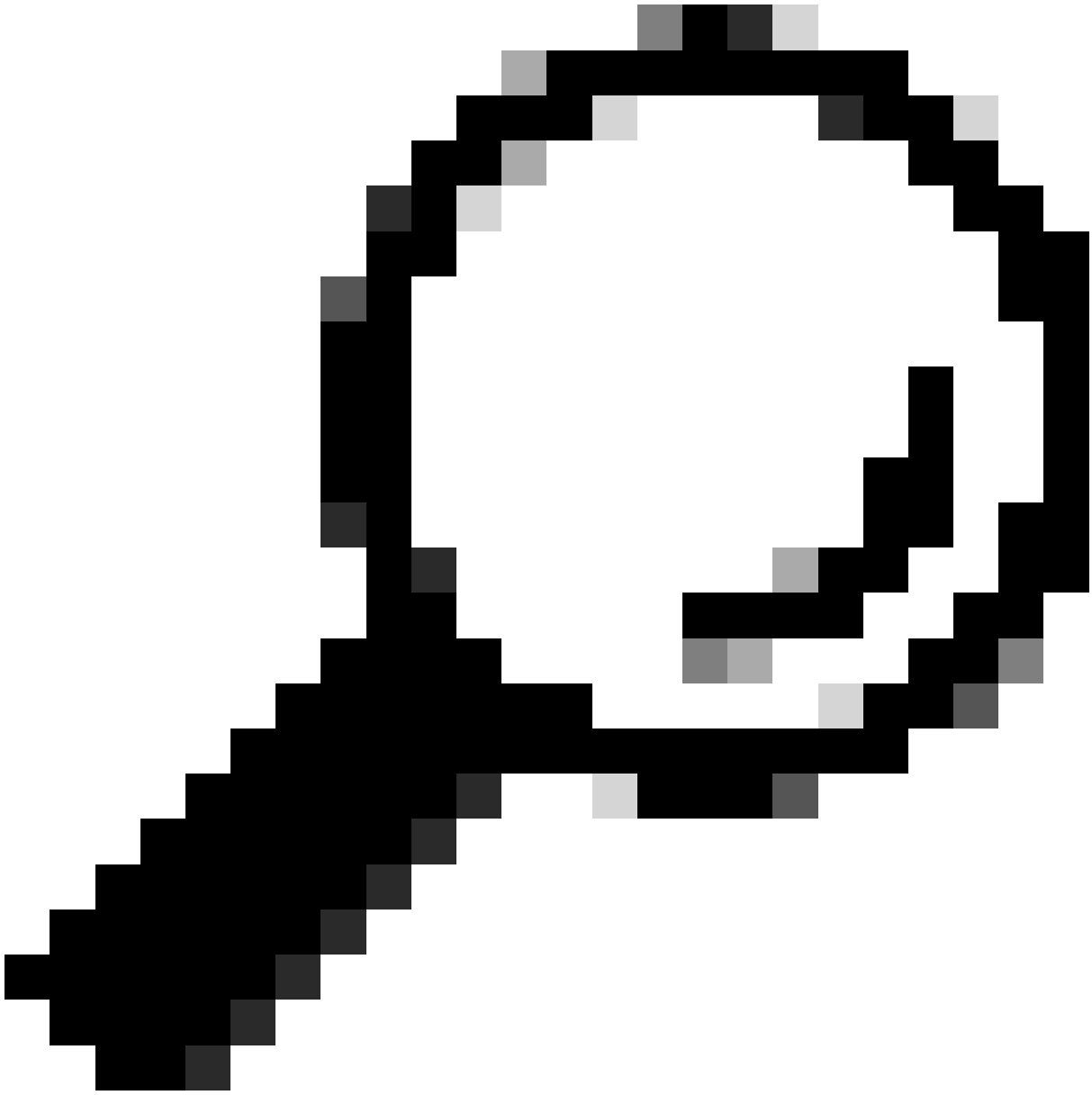
- 일반 트렁크
- 프라이빗 VLAN 트렁크

일반 트렁크

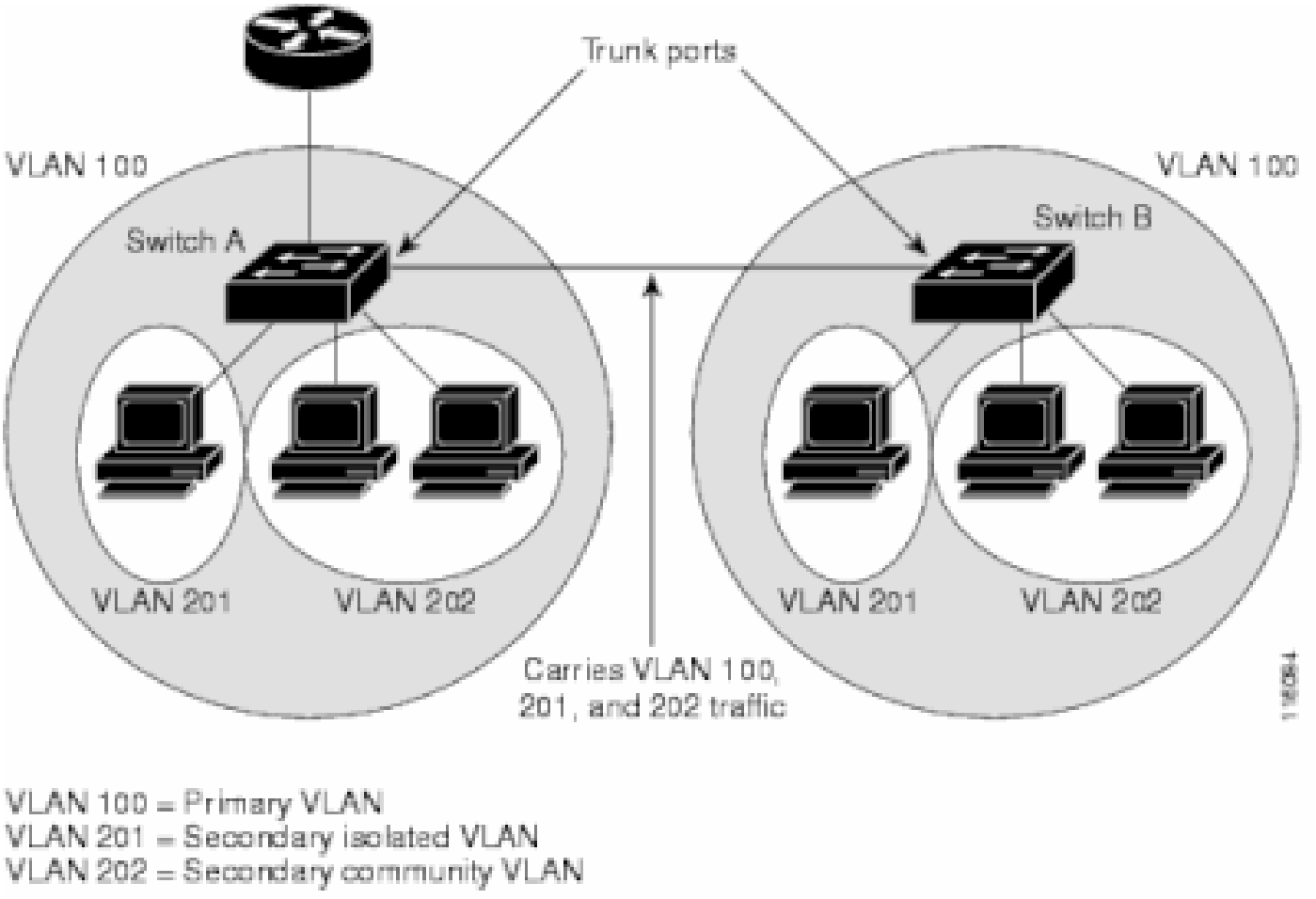
일반 VLAN과 마찬가지로 PVLAN은 여러 스위치에 걸쳐 있을 수 있습니다. 트렁크 포트는 기본 VLAN 및 보조 VLAN을 인접 스위치로 전송합니다. 트렁크 포트는 프라이빗 VLAN을 다른 VLAN과 동일하게 처리합니다. 여러 스위치 간 PVLAN의 특징은 한 스위치의 격리된 포트에서 보낸 트래픽이 다른 스위치의 격리된 포트에 도달하지 않는다는 것입니다.

PVLAN 컨피그레이션의 보안을 유지하고 PVLAN으로 구성된 VLAN의 다른 사용을 방지하기 위해 PVLAN 포트가 없는 디바이스를 포함하는 모든 중간 디바이스에서 PVLAN을 구성합니다.

트렁크 포트는 일반 VLAN과 기본, 격리 및 커뮤니티 VLAN의 트래픽을 전달합니다.



팁: Cisco는 트렁킹을 받는 두 스위치가 모두 PVLAN을 지원하는 경우 표준 트렁크 포트를 사용할 것을 권장합니다.



레이어 2 네트워크의 모든 스위치에 *PVLAN* 수동 구성

VTP는 PVLAN을 지원하지 않으므로 레이어 2 네트워크의 모든 스위치에 PVLAN을 수동으로 구성해야 합니다. 네트워크의 일부 스위치에서 기본 및 보조 VLAN 연결을 구성하지 않으면 이러한 스위치의 레이어 2 데이터베이스가 병합되지 않습니다. 이러한 상황에서는 해당 스위치에서 PVLAN 트래픽이 불필요하게 플러딩될 수 있습니다.

프라이빗 VLAN 트렁크

PVLAN 트렁크 포트는 여러 보조 및 비 PVLAN을 전달할 수 있습니다. 패킷은 PVLAN 트렁크 포트의 보조 또는 일반 VLAN 태그와 함께 수신 및 전송됩니다.

IEEE 802.1q 캡슐화만 지원됩니다. 격리된 트렁크 포트를 사용하면 트렁크를 통해 모든 보조 포트에 대한 트래픽을 결합할 수 있습니다. 프로미스큐어스 트렁크 포트를 사용하면 이 토폴로지에 필요한 여러 프로미스큐어스 포트를 여러 기본 VLAN을 전송하는 단일 트렁크 포트에 결합할 수 있습니다.

여러 VLAN(일반 VLAN 또는 여러 프라이빗 VLAN 도메인)을 전달하기 위해 프라이빗 VLAN 격리 호스트 포트를 사용할 것으로 예상할 경우 격리 프라이빗 VLAN 트렁크 포트를 사용합니다. 이렇게 하면 프라이빗 VLAN을 지원하지 않는 다운스트림 스위치를 연결하는 데 유용합니다.

프라이빗 VLAN 프로미스큐어스 트렁크는 프라이빗 VLAN 프로미스큐어스 호스트 포트가 일반적으로 사용되지만 여러 VLAN(일반 VLAN 또는 여러 프라이빗 VLAN 도메인)을 전달해야 하는 경우에 사용됩니다. 이렇게 하면 프라이빗 VLAN을 지원하지 않는 업스트림 라우터를 연결하는 데 유용합니다.

추가 정보

자세한 내용은 프라이빗 VLAN 트렁크를 참조하십시오.

인터페이스를 PVLAN 트렁크 포트로 구성하려면 레이어 2 인터페이스를 PVLAN 트렁크 포트로 구성을 참조하십시오.

인터페이스를 프로미스큐어스 트렁크 포트로 구성하려면 레이어 2 인터페이스를 프로미스큐어스 트렁크 포트로 구성을 참조하십시오.

다음을 확인합니다.

설정이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

CatOS

- **show pvlan** - PVLAN 컨피그레이션을 표시합니다. 격리 VLAN과 기본 VLAN이 서로 연결되는지 확인합니다. 또한 호스트 포트가 표시되는지 확인합니다.

- **show pvlan mapping** - 프로미스큐어스 포트의 컨피그레이션과 함께 PVLAN 매핑을 표시합니다.

Cisco IOS Software

- **show vlan private-vlan** - 연결된 포트를 포함하는 PVLAN 정보를 표시합니다.

- **show interface/portswitchport** - 인터페이스별 정보를 표시합니다. 작동 모드 및 작동 PVLAN 설정이 올바른지 확인합니다.

- **show interfaces private-vlan mapping** - 구성한 PVLAN 매핑을 표시합니다.

확인 절차

다음 단계를 완료하십시오.

•

스위치에서 PVLAN 컨피그레이션을 확인합니다.

기본 및 보조 PVLAN이 서로 연결/매핑되는지 여부를 확인합니다. 또한 필요한 포트가 포함되어 있는지 확인합니다.

<#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
```

•

프로미스큐어스 포트의 올바른 컨피그레이션을 확인합니다.

이 출력은 포트 작동 모드가 **프로미스큐어스이고 작동 VLAN**이 100 및 101임을 나타냅니다.

<#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
```

•

호스트 포트에서 프로미스큐어스 포트로 ICMP(Internet Control Message Protocol) ping 패킷을 시작합니다.

두 디바이스 모두 동일한 기본 VLAN에 있으므로 디바이스는 동일한 서브넷에 있어야 합니다.

```
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.
```

•

호스트 포트 간에 ICMP ping을 시작합니다.

이 예에서 host_port_2(10.1.1.99)는 > host_port(10.1.1.100)를 ping합니다. 이 ping은 실패합니다. 그러나 다른 호스트 포트에서 프로미스큐어스 포트로의 ping은 여전히 성공합니다.

<#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.
```

문제 해결

PVLAN 문제 해결

이 섹션에서는 PVLAN 컨피그레이션에서 발생하는 몇 가지 일반적인 문제를 다룹니다.

문제 1

이 오류 메시지가 나타납니다. %PM-SP-3-ERR_INCOMP_PORT: <mod/port>이(가) 트렁크 포트이므로 <mod/port>이(가) 비활성 상태로 설정되어 있습니다.

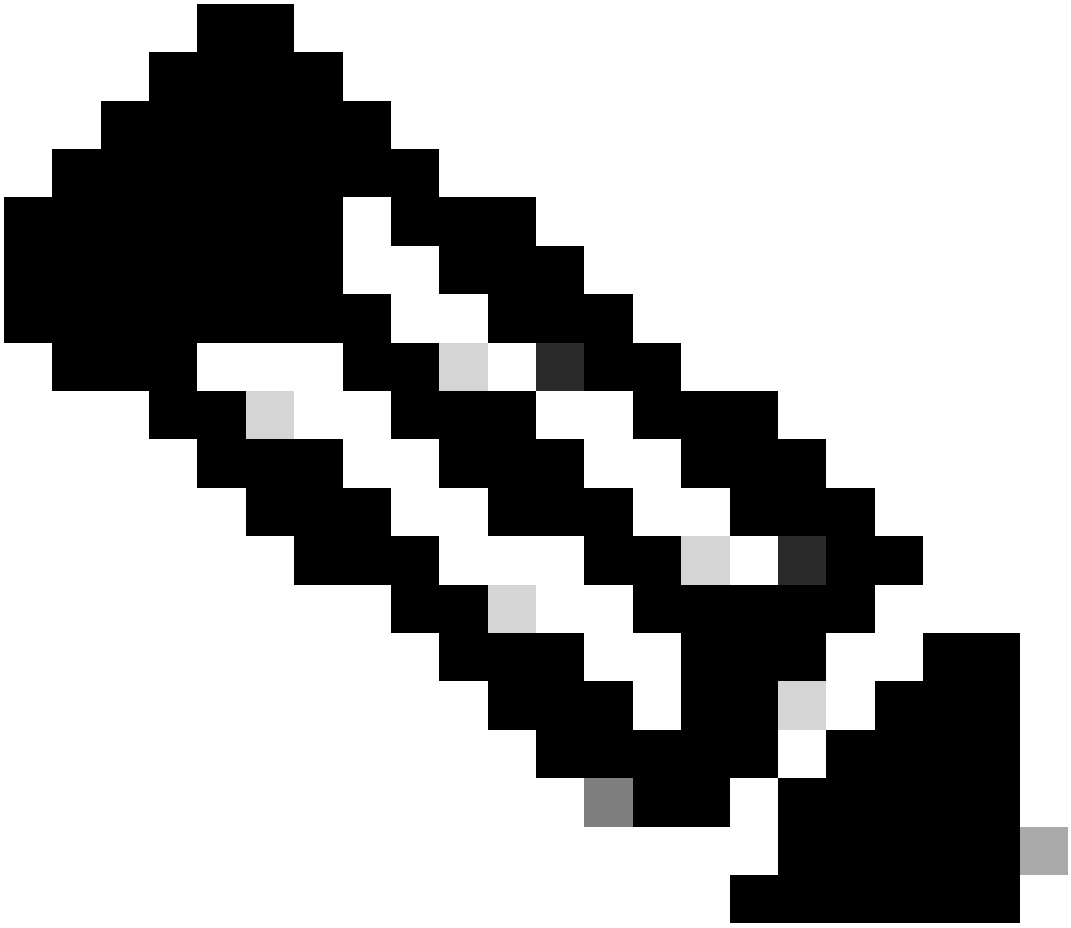
이 오류 메시지는 여기에서 설명한 것처럼 여러 가지 이유로 표시될 수 있습니다.

설명 - 1: 하드웨어 제한 때문에 Catalyst 6500/6000 10/100Mbps 모듈은 동일한 COIL ASIC 내의 한 포트가 트렁크, SPAN 대상 또는 프로미스큐어스 PVLAN 포트인 경우 격리된 또는 커뮤니티 VLAN 포트의 구성을 제한합니다. (COIL ASIC는 대부분의 모듈에서 12개의 포트를 제어하고 Catalyst 6548 모듈에서 48개의 포트를 제어합니다.) 이 문서의 Rules and Limitations(규칙 및 제한) 섹션의 표에서는 Catalyst 6500/6000 10/100Mbps 모듈에 대한 포트 제한을 분석합니다.

해결 절차 - 1: 해당 포트에서 PVLAN을 지원하지 않는 경우 모듈의 다른 ASIC 또는 다른 모듈의 포트를 선택합니다. 포트를 다시 활성화하려면 격리 또는 커뮤니티 VLAN 포트 컨피그레이션을 제거하고 shutdown 명령과 no shutdown **명령을 실행합니다**.

설명 - 2: 포트가 수동으로 또는 기본적으로 동적 권장 또는 동적 자동 모드로 구성된 경우

확인 절차 - 2: switchport mode access 명령을 사용하여 포트를 **액세스 모드로** 구성합니다. 포트를 다시 활성화하려면 shutdown 명령과 no **shutdown** 명령을 **차례로** 실행합니다.



참고: Cisco IOS Software Release 12.2(17a)SX 이상 릴리스에서는 WS-X6548-RJ-45, WS-X6548-RJ-21 및 WS-X6524-100FX-MM 이더넷 스위칭 모듈에 12포트 제한이 적용되지 않습니다.

문제 2

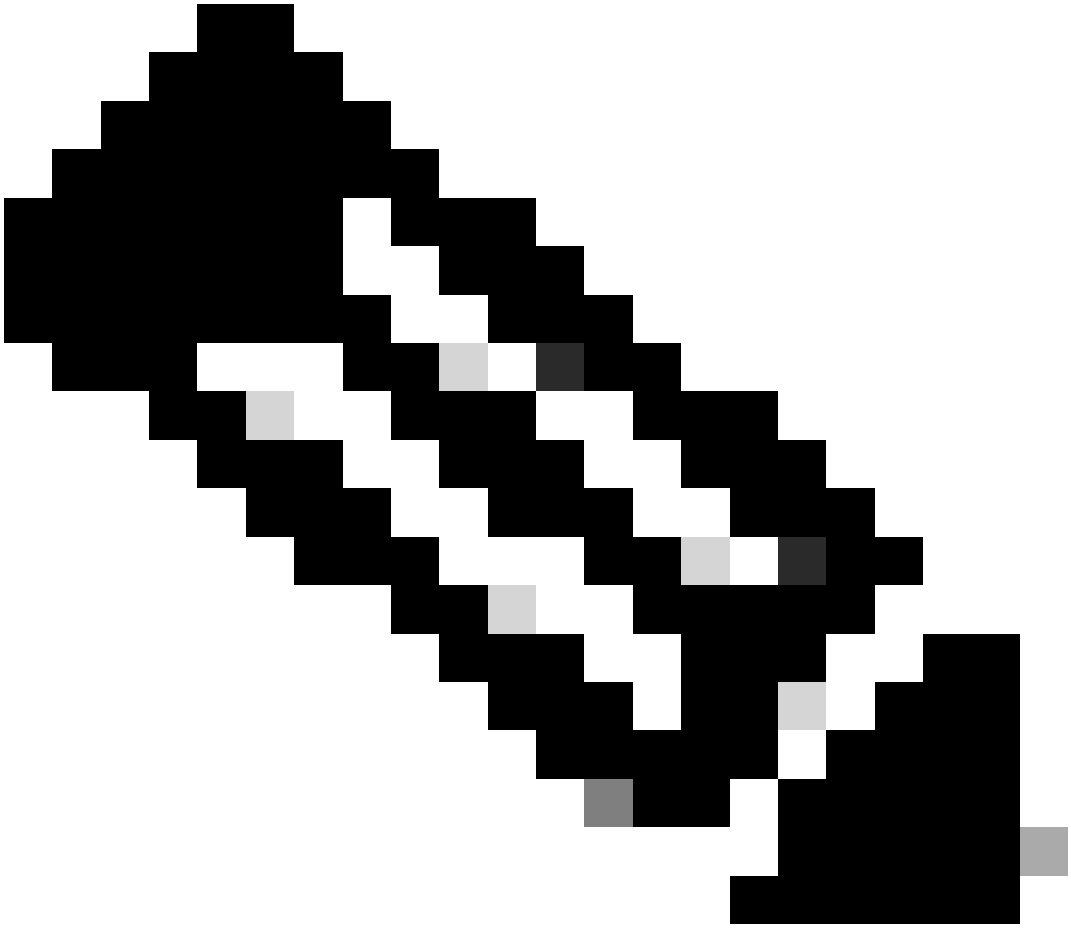
PVLAN 컨피그레이션 중에 다음 메시지 중 하나가 발생합니다.

```
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.
```

설명: 하드웨어 제한 때문에 Catalyst 6500/6000 10/100Mbps 모듈은 동일한 COIL ASIC 내의 한 포트가 트렁크, SPAN 대상 또는 프로미스큐어스 PVLAN 포트인 경우 격리된 또는 커뮤니티 VLAN 포트의 구성을 제한합니다. (COIL ASIC는 대부분의 모듈에서 12개의 포트를 제어하고 Catalyst 6548 모듈에서 48개의 포트를 제어합니다.) 이 문서의 Rules and Limitations(규칙 및 제한) 섹션의 표에서는 Catalyst 6500/6000 10/100Mbps 모듈에 대한 포트 제한을 분석합니다.

해결 절차: 포트가 **PVLAN 포트가** 될 수 있는지 여부를 나타내는 CatOS(show pvlan capability command)를 실행합니다. 특정 포트에서 PVLAN을 지원하지 않는 경우 모듈의 다른 ASIC 또는 다른 모듈의 포트를 선택합니다.



참고: Cisco IOS Software Release 12.2(17a)SX 이상 릴리스에서는 WS-X6548-RJ-45, WS-X6548-RJ-21 및 WS-X6524-100FX-MM 이더넷 스위칭 모듈에 12포트 제한이 적용되지 않습니다.

문제 3

일부 플랫폼에서는 PVLAN을 구성할 수 없습니다.

해결 방법: 플랫폼에서 PVLAN을 지원하는지 확인합니다. 구성을 시작하기 전에 플랫폼 및 소프트웨어 버전이 PVLAN을 지원하는지 확인하려면 프라이빗 VLAN Catalyst 스위치 지원 매트릭스를 참조하십시오.

문제 4

Catalyst 6500/6000 MSFC에서는 스위치의 격리된 포트에 연결하는 디바이스를 ping할 수 없습니다.

해결 방법: Supervisor Engine에서 MSFC에 대한 포트(15/1 또는 16/1)가 프로미스큐어스인지 확인합니다.

```
<#root>

cat6000> (enable)

set pvlan mapping primary_vlan secondary_vlan 15/1

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

또한 이 문서의 레이어 3 컨피그레이션 섹션에서 지정하는 대로 MSFC의 VLAN 인터페이스를 구성합니다.

문제 5

no shutdown 명령을 **사용하면 격리 또는** 커뮤니티 VLAN에 대한 VLAN 인터페이스를 활성화할 수 없습니다.

해결: PVLAN의 특성상 격리 또는 커뮤니티 VLAN에 대해서는 VLAN 인터페이스를 활성화할 수 없습니다. 기본 VLAN에 속하는 VLAN 인터페이스만 활성화할 수 있습니다.

문제 6

MSFC/MSFC2가 포함된 Catalyst 6500/6000 디바이스에서는 레이어 3 PVLAN 인터페이스에서 학습된 ARP 항목이 에이징되지 않습니다.

해상도: 레이어 3 프라이빗 VLAN 인터페이스에서 학습되는 ARP 항목은 스티커 ARP 항목이며 타임아웃되지 않습니다. 동일한 IP 주소로 새 장비를 연결하면 메시지가 생성되며 ARP 항목이 생성되지 않습니다. 따라서 MAC 주소가 변경되는 경우 PVLAN 포트 ARP 엔트리를 수동으로 제거해야 합니다. PVLAN ARP 항목을 수동으로 추가하거나 제거하려면 다음 명령을 실행합니다.

```
<#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
```

또 다른 옵션은 Cisco IOS Software Release 12.1(11b)E 이상에서 **no ip sticky**-arp 명령을 실행하는 것입니다.

관련 정보

- **Cisco Catalyst 2955 Series 스위치 - 서비스 중단 알림**
- **PVLAN 및 VACL을 사용하는 보안 네트워크**
- **LAN 스위칭 기술 지원**
- **Cisco**

기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.