Configurazione delle VLAN private isolate sugli switch Catalyst

Sommario

Introduzione

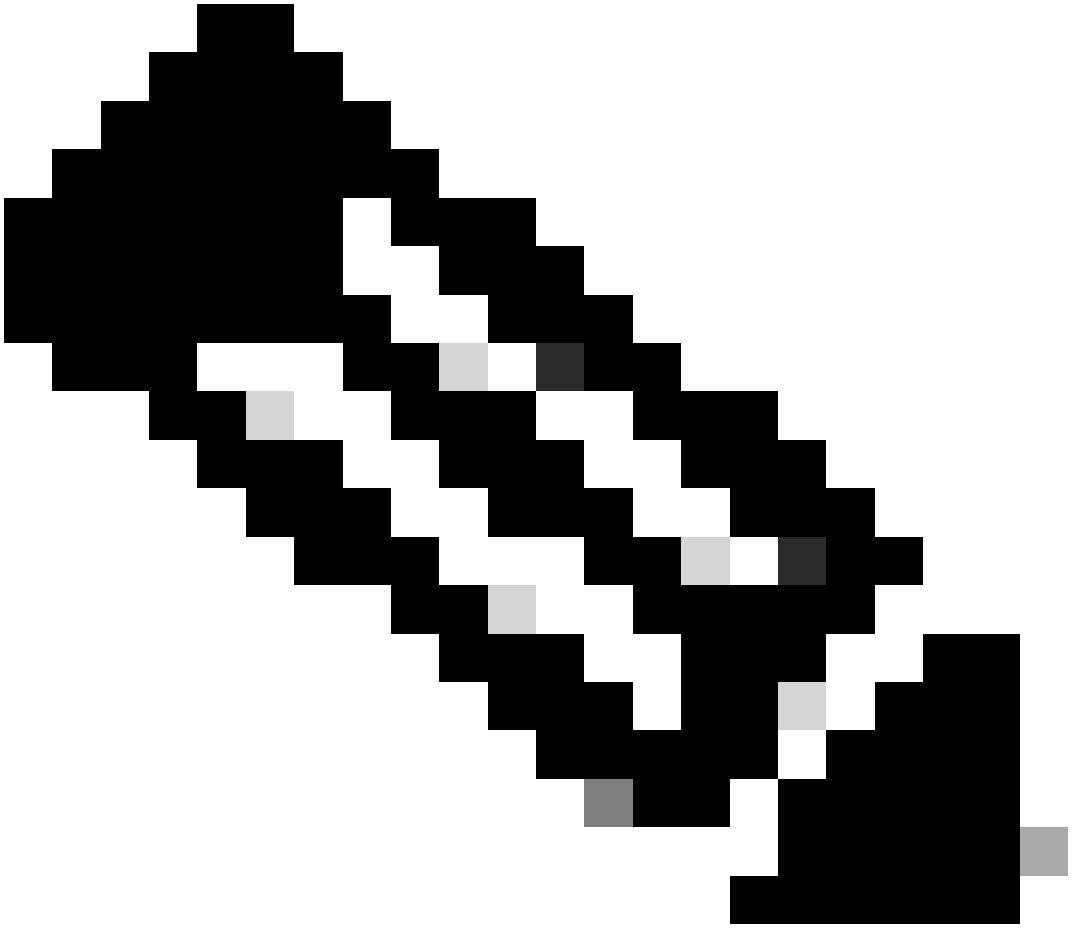
In questo documento viene descritta la procedura per configurare le PVLAN isolate sui dispositivi Cisco Catalyst Switch con Catalyst OS (CatOS) o con Cisco IOS® Software.

Prerequisiti

Requisiti

in questo documento si presume che la rete esista già e che si sia in grado di stabilire la connettività tra le varie porte per l'aggiunta di una VLAN privata (PVLAN). Se si hanno più switch, verificare che il trunk tra gli switch funzioni correttamente e autorizzi le PVLAN sul trunk.

Non tutti gli switch e le versioni software supportano le PVLAN.



> Nota: alcuni switch (come specificato nella matrice di supporto degli switch Catalyst VLAN privati) supportano solo la funzione PVLAN Edge. Anche il termine porte protette si riferisce a questa funzione. Le porte PVLAN Edge hanno una restrizione che impedisce la comunicazione con altre porte protette sullo stesso switch. Le porte protette su switch separati, tuttavia, possono comunicare tra loro. Non confondere questa funzione con le normali configurazioni PVLAN mostrate in questo documento. Per ulteriori informazioni sulle porte protette, fare riferimento alla sezione Configurazione della sicurezza delle porte nel documento Configurazione del controllo del traffico basato sulle porte.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Switch Catalyst 4003 con modulo Supervisor Engine 2 con CatOS versione 6.3(5)
- Switch Catalyst 4006 con modulo Supervisor Engine 3 con software Cisco IOS versione 12.1(12c)EW1

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

In alcune situazioni, è necessario impedire la connettività di layer 2 (L2) tra i dispositivi terminali di uno switch senza posizionare i dispositivi in diverse subnet IP. Questa configurazione impedisce lo spreco di indirizzi IP. Le PVLAN consentono di isolare al layer 2 i dispositivi della stessa subnet IP. È possibile limitare alcune porte dello switch in modo che raggiungano solo porte specifiche a cui è collegato un gateway predefinito, un server di backup o un Cisco LocalDirector.

In questo documento viene descritta la procedura per configurare le PVLAN isolate sugli switch Cisco Catalyst con il software Catalyst OS (CatOS) o Cisco IOS.

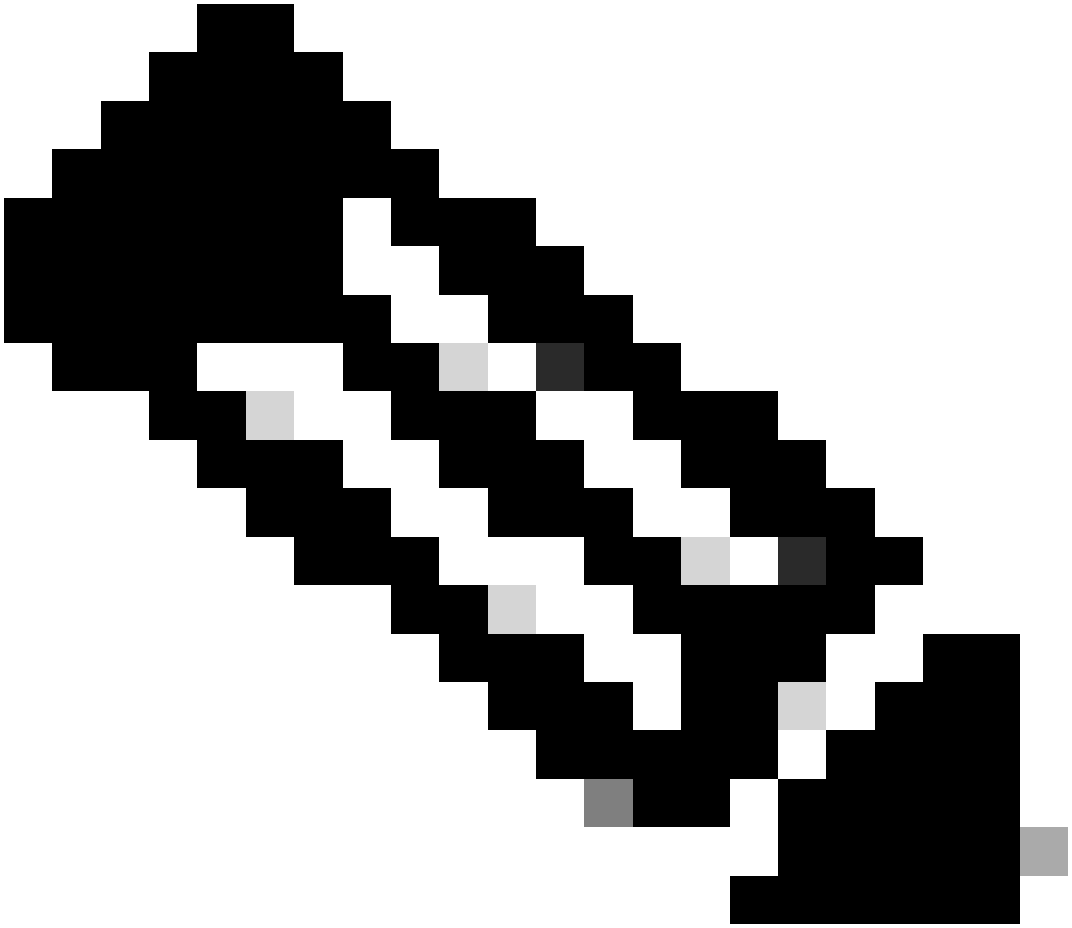
Una PVLAN è una VLAN con configurazione per l'isolamento di layer 2 da altre porte all'interno dello stesso dominio di broadcast o subnet. È possibile assegnare un set di porte specifico all'interno di una PVLAN e quindi controllare l'accesso tra le porte sul layer 2. È possibile configurare le PVLAN e le VLAN normali sullo stesso switch.

Sono disponibili tre tipi di porte PVLAN: promiscue, isolate e di comunità.

1. Una porta promiscua comunica con tutte le altre porte PVLAN. La porta promiscua è la porta che in genere viene utilizzata per comunicare con router esterni, director locali, dispositivi di gestione di rete, server di backup, workstation amministrative e altri dispositivi. Su alcuni switch, la porta del modulo di routing (ad esempio, Multilayer Switch Feature Card [MSFC]) deve essere promiscua.
2. Una porta isolata ha una separazione completa di layer 2 dalle altre porte nell'ambito della stessa PVLAN. Questa separazione include le trasmissioni, e l'unica eccezione è la porta promiscua. Una concessione di privacy al livello 2 si verifica con il blocco del traffico in uscita verso tutte le porte isolate. Il traffico proveniente da una porta isolata viene inoltrato solo a

tutte le porte promiscue.

3. I porti della comunità possono comunicare tra loro e con i porti promiscui. Queste porte presentano un'isolamento di layer 2 da tutte le altre porte di altre community o porte isolate nella PVLAN. Le trasmissioni si propagano solo tra le porte della community associate e la porta promiscua.



Nota: questo documento non descrive la configurazione della VLAN della community.

Regole e limitazioni

In questa sezione vengono descritte alcune regole e limitazioni da tenere in considerazione quando si implementano le PVLAN.

- Le PVLAN non possono includere le VLAN 1 o 1002-1005.
- È necessario impostare la modalità VLAN Trunk Protocol (VTP) su `transparent`.

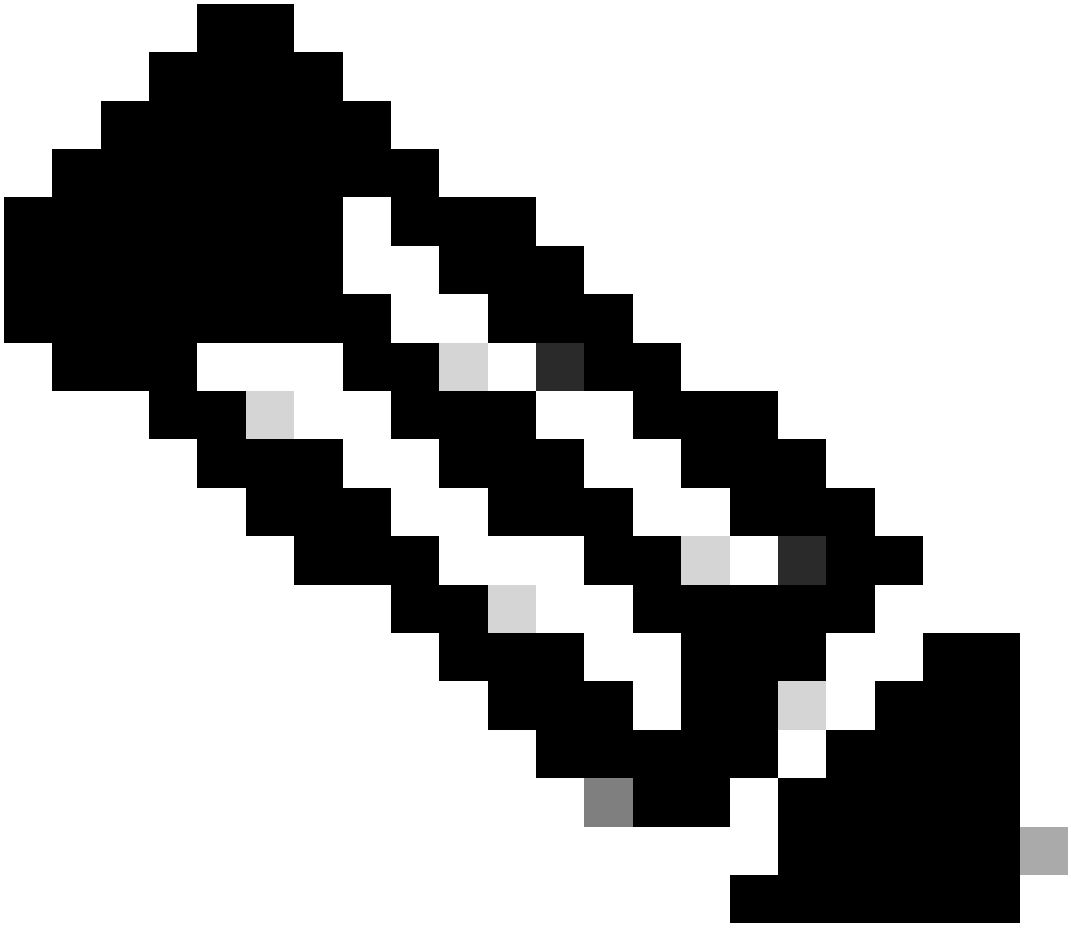
- È possibile specificare solo una VLAN isolata per VLAN primaria.
- È possibile designare una VLAN come PVLAN solo se a tale VLAN non è assegnata alcuna porta di accesso. Rimuovere le porte dalla VLAN prima di configurare la VLAN come PVLAN.
- Non configurare le porte PVLAN come EtherChannel.
- A causa dei limiti hardware, i moduli Fast Ethernet dello switch Catalyst 6500/6000 limitano la configurazione di una porta VLAN isolata o di una porta di comunità quando una porta dello stesso circuito integrato specifico dell'applicazione COIL (ASIC) è una di queste:
    - Un bagagliaio
    - Una destinazione SPAN (Switched Port Analyzer)
    - Una porta PVLAN promiscua

Nella tabella seguente viene indicato l'intervallo di porte che appartengono allo stesso ASIC sui moduli Fast Ethernet di Catalyst 6500/6000:

Modulo	Porte di ASIC
WS-X624-100FX-MT, WS-X6248-RJ-45, WS-X6248-TEL	Porte 1-12, 13-24, 25-36, 37-48
WS-X6024-10FL-MT	Porte 1-12, 13-24
WS-X6548-RJ-45, WS-X6548-RJ-21	Porte 1-48

Il comando show pvlan capabilities (CatOS) indica anche se è possibile configurare una porta come porta PVLAN. Non sono disponibili comandi equivalenti nel software Cisco IOS.

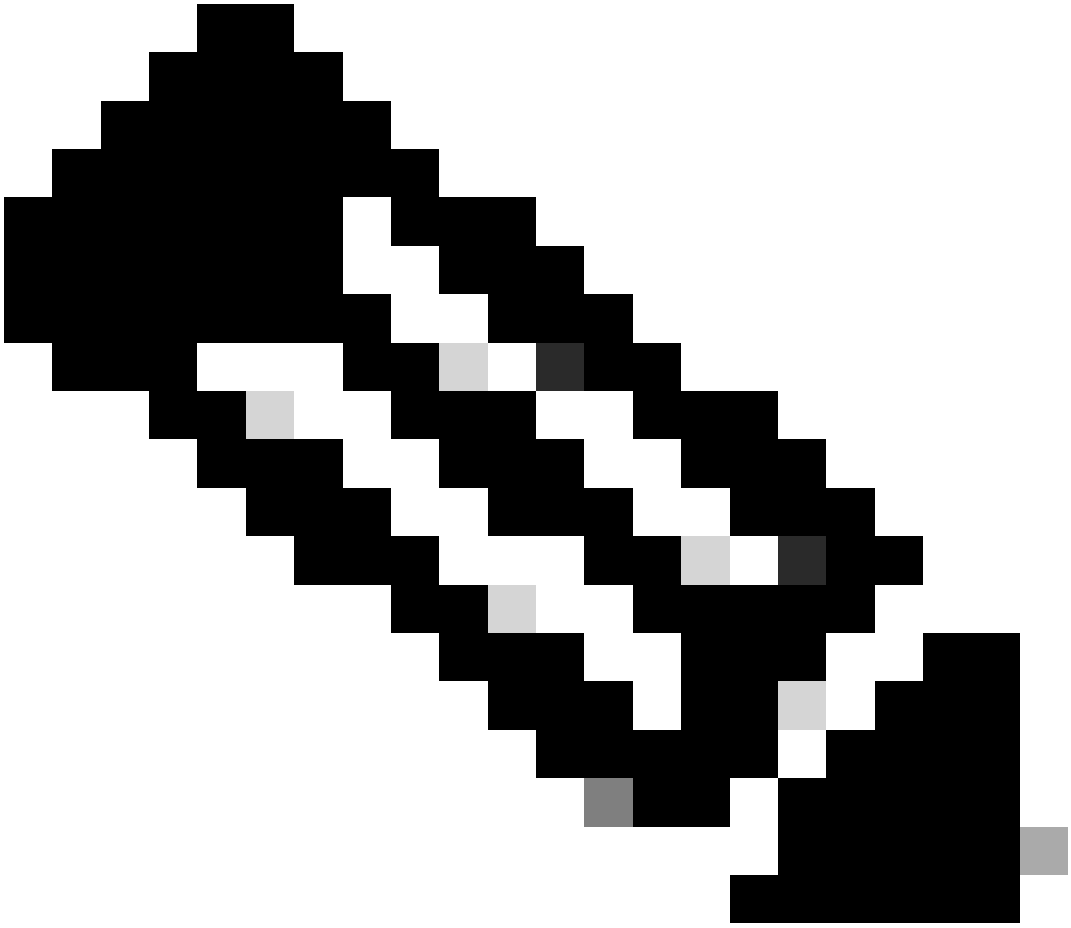
- Se si elimina una VLAN utilizzata nella configurazione PVLAN, le porte associate alla VLAN diventano inattive.
- Configurare le interfacce VLAN di layer 3 (L3) solo per le VLAN primarie. Le interfacce VLAN per le VLAN isolate e di comunità sono inattive mentre la VLAN è configurata come VLAN isolata o di comunità.
- È possibile estendere le PVLAN sugli switch con l'uso di trunk. Le porte trunk trasportano il traffico proveniente dalle VLAN normali e anche dalle VLAN principali, isolate e di comunità. Cisco consiglia di utilizzare le porte trunk standard se entrambi gli switch con trunking supportano le PVLAN.



Nota: è necessario immettere manualmente la stessa configurazione PVLAN su ciascuno switch coinvolto, in quanto il VTP in modalità trasparente non propaga queste informazioni.

Configurazione

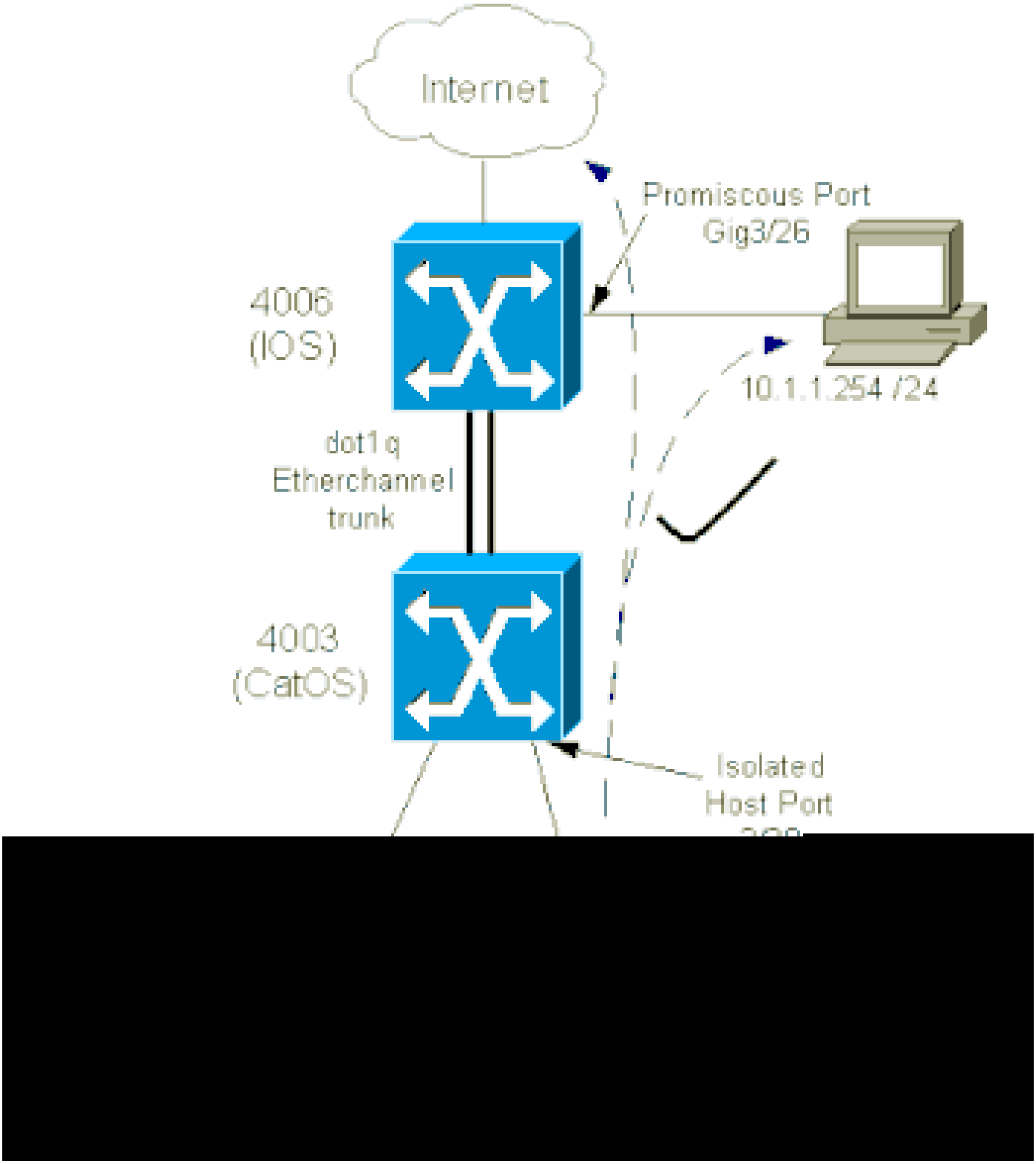
In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.



Nota: per ulteriori informazioni sui comandi menzionati in questo documento, usare lo strumento di ricerca dei comandi. Solo gli utenti registrati possono accedere agli strumenti e alle informazioni interni di Cisco.

Esempio di rete

Il documento usa la seguente configurazione di rete:



In questo scenario, i dispositivi nella VLAN isolata (101) hanno una restrizione alla comunicazione tra dispositivi sul layer 2. Tuttavia, le periferiche possono connettersi a Internet. Inoltre, il port Gig 3/26 sul 4006 ha la designazione promiscua. Questa configurazione opzionale consente la connessione di un dispositivo su Gigabit Ethernet 3/26 a tutti i dispositivi della VLAN isolata. Questa configurazione consente, ad esempio, di eseguire il backup dei dati da tutti i dispositivi host PVLAN a una workstation di amministrazione. Le porte promiscue possono inoltre essere utilizzate per il collegamento a un router esterno, a LocalDirector, a un dispositivo di gestione di rete e ad altri dispositivi.

Configurazione delle VLAN primarie e isolate

Per creare le VLAN primaria e secondaria e associare le diverse porte a queste VLAN, attenersi alla seguente procedura. I passaggi includono esempi sia per il software CatOS che per il software Cisco IOS®. Utilizzare il set di comandi appropriato per l'installazione del sistema operativo.

1. Creare la PVLAN primaria.

    - 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
      ```

    - Software Cisco IOS

      <#root>

      ```
      Switch_IOS(config)#
      vlan primary_vlan_id
      Switch_IOS(config-vlan)#
      private-vlan primary
      Switch_IOS(config-vlan)#
      name primary-vlan
      Switch_IOS(config-vlan)#
      exit
      ```

2. Creare la VLAN o le VLAN isolate.

    - 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
```

- Software Cisco IOS

```
<#root>

Switch_IOS(config)#

vlan secondary_vlan_id

Switch_IOS(config-vlan)#

private-vlan isolated

Switch_IOS(config-vlan)#

name isolated_pvlan

Switch_IOS(config-vlan)#

exit
```

3. Associare le VLAN/VLAN isolate alla VLAN primaria.

- CatOS

```
<#root>

Switch_CatOS> (enable)

set pvlan primary_vlan_id secondary_vlan_id

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

- Software Cisco IOS

```
<#root>

Switch_IOS(config)#
```

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

4. Verificare la configurazione della VLAN privata.

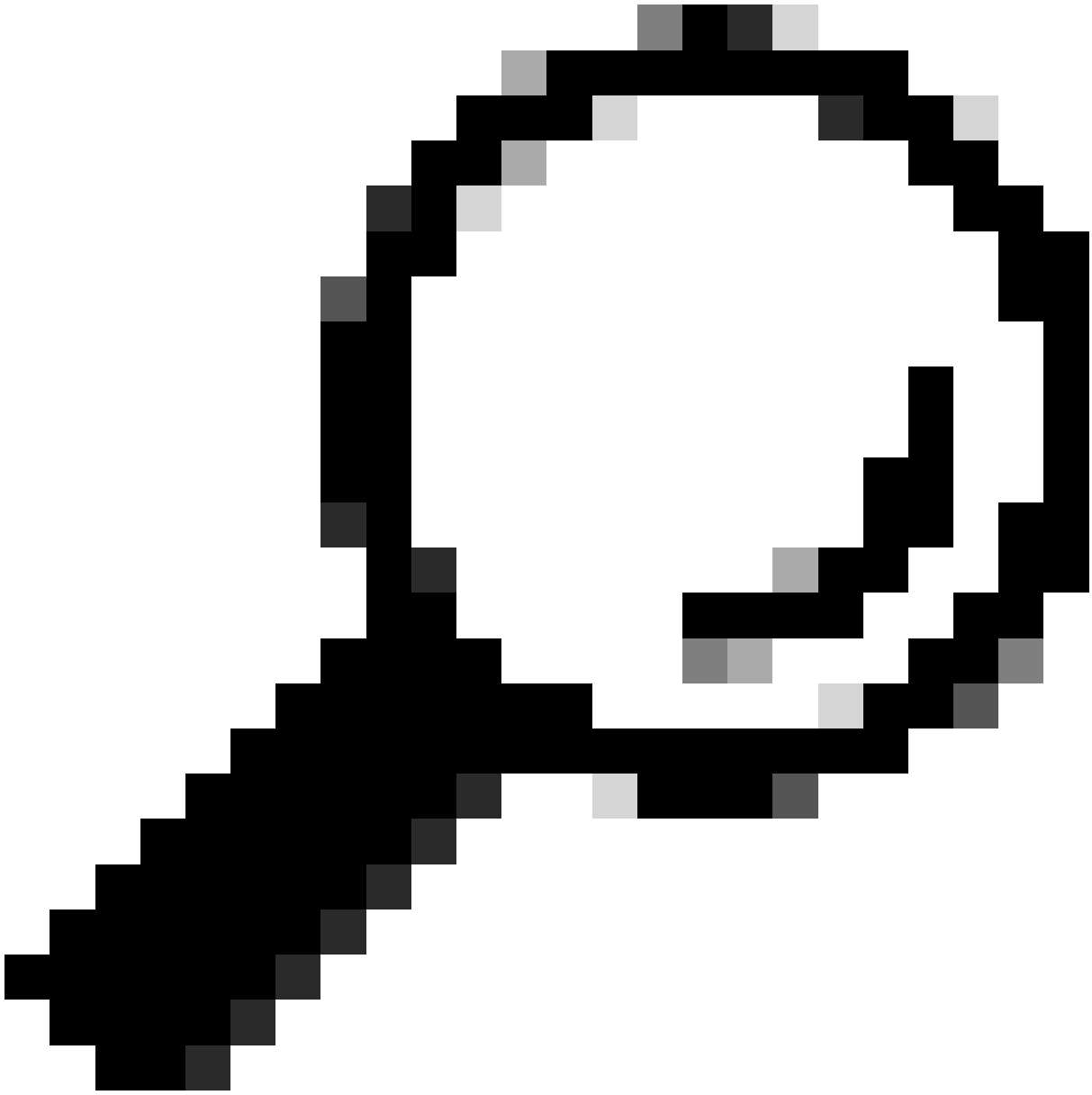
- CatOS

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

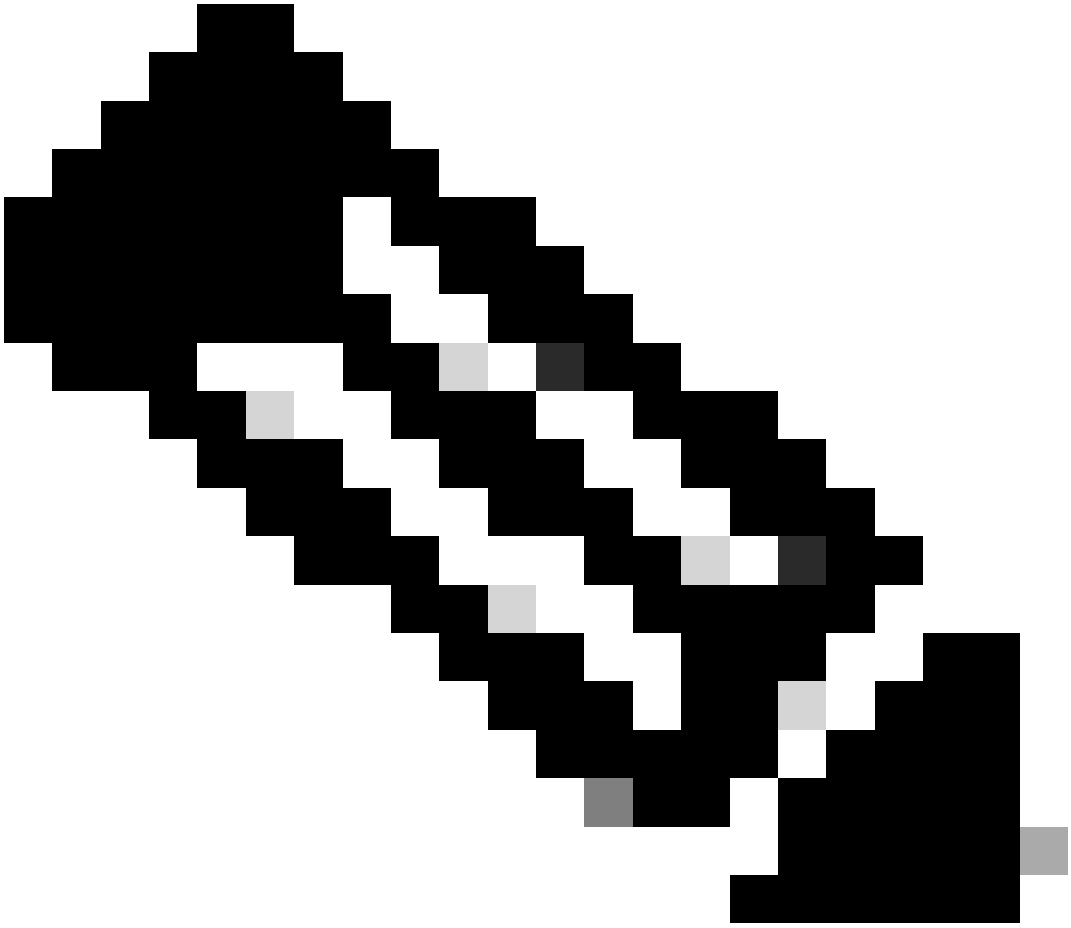
- Software Cisco IOS

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

Assegnazione delle porte alle PVLAN



Suggerimento: prima di implementare questa procedura, usare il comando (per CatOS) per determinare se una porta può diventare una porta PVLAN.show PVLAN capability mod/port



Nota: prima di eseguire il passo 1 di questa procedura, usare il comando switchport in modalità di configurazione interfaccia per configurare la porta come interfaccia a commutazione di layer 2.

- Configurare le porte host su tutti gli switch.
  - 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
```

- Software Cisco IOS

<#root>

```
Switch_IOS(config)#

interface gigabitEthernet mod/port

Switch_IOS(config-if)#

switchport private-vlan host
primary_vlan_id secondary_vlan_id

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

Switch_IOS(config-if)#

switchport mode private-vlan host

Switch_IOS(config-if)#

exit
```

- Configurare la porta promiscua su uno degli switch.
  - CatOS

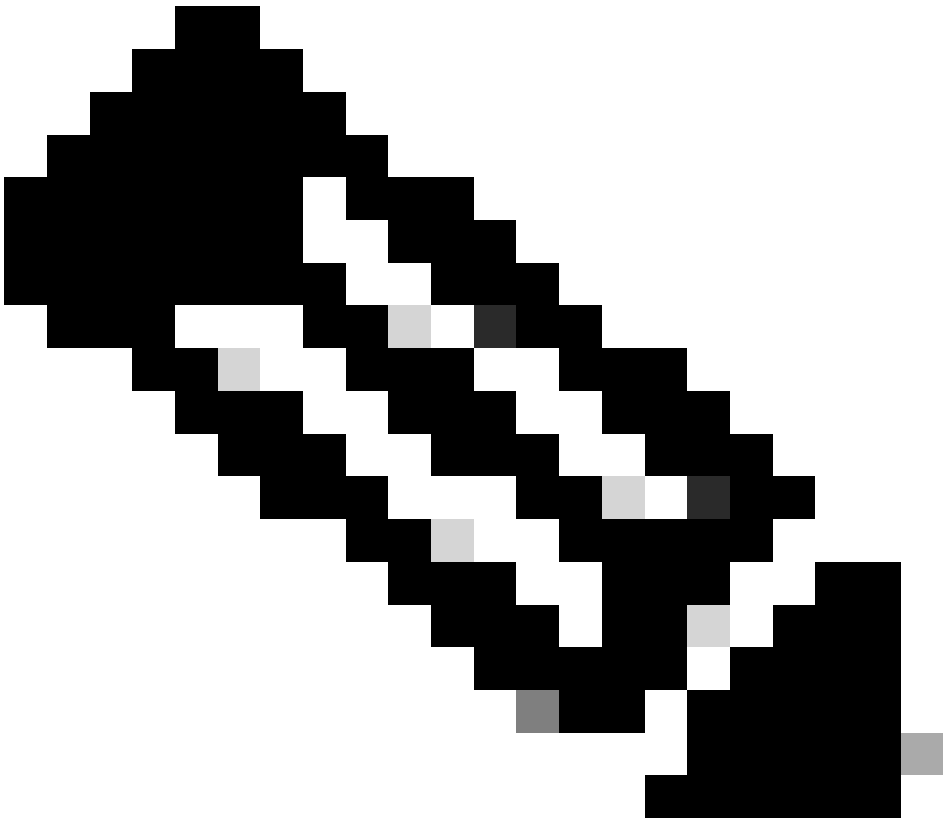
<#root>

```
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
```



Nota: per Catalyst 6500/6000 quando Supervisor Engine esegue CatOS come software di sistema, la porta MSFC sul Supervisor Engine (15/1 o 16/1) deve essere promiscua se si desidera collegare lo switch di layer 3 alle VLAN.

- Software Cisco IOS

<#root>

```
Switch_IOS(config)#

interface interface_type mod/port

Switch_IOS(config-if)#

switchport private-vlan
mapping primary_vlan_id secondary_vlan_id


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

Switch_IOS(config-if)#

switchport mode private-vlan promiscuous
```

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

Configurazione livello 3

In questa sezione opzionale vengono descritti i passaggi della configurazione per consentire il routing del traffico in entrata tramite PVLAN. Se è necessario abilitare solo la connettività di layer 2, è possibile omettere questa fase.

1. Configurare l'interfaccia VLAN nello stesso modo in cui si configura il normale routing di layer 3.

   Questa configurazione comporta:

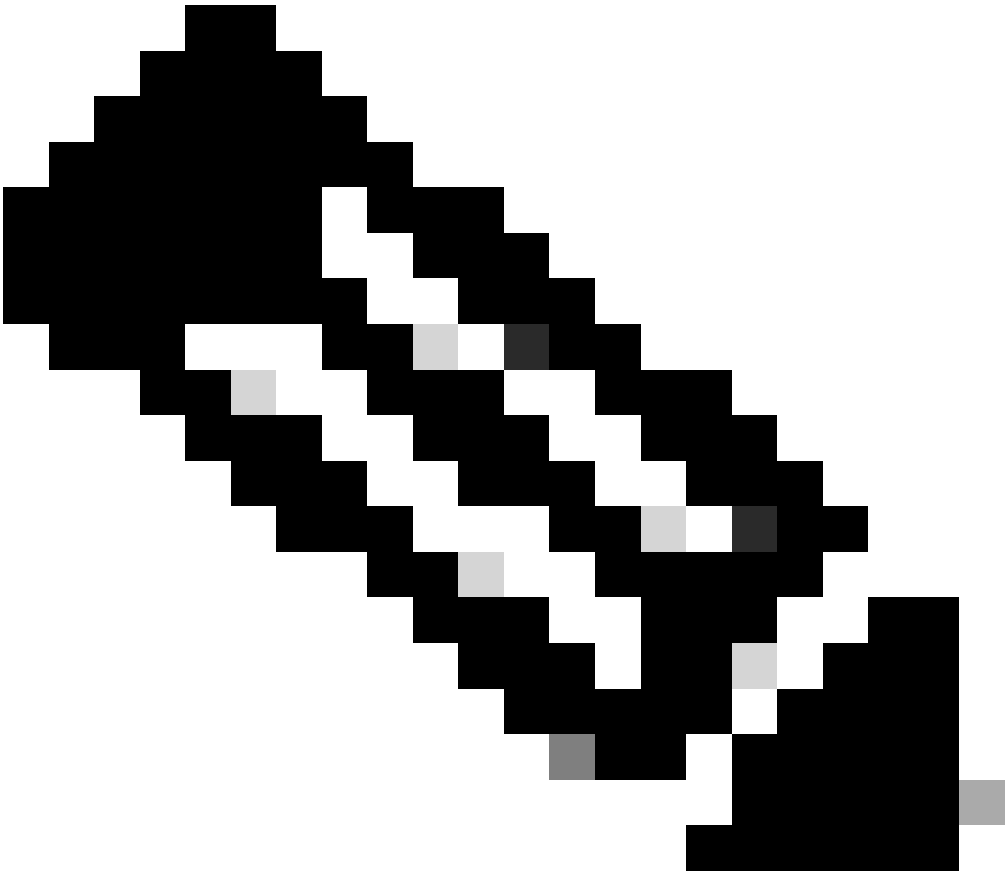
   - Configurazione di un indirizzo IP
   - Attivazione dell'interfaccia con il comando no shutdown
   - Verifica dell'esistenza della VLAN nel database VLAN

   Per esempi sulla configurazione, fare riferimento al supporto tecnico VLAN/VTP.

2. Mappare le VLAN secondarie che si desidera indirizzare con la VLAN primaria.

```
<#root>
Switch_IOS(config)#
interface vlan primary_vlan_id
Switch_IOS(config-if)#
private-vlan mapping secondary_vlan_list

Switch_IOS(config-if)#
end
```



Nota: configurare le interfacce VLAN di layer 3 solo per le VLAN primarie. Le interfacce VLAN per VLAN isolate e di comunità sono inattive con una configurazione VLAN isolata o di comunità.

3. Per verificare il mapping, usare il comando show interfaces private-vlan mapping (software Cisco IOS) o show pvlan mapping (CatOS).
4. Per modificare l'elenco delle VLAN secondarie dopo la configurazione della mappatura, usare la parola chiave add o remove.

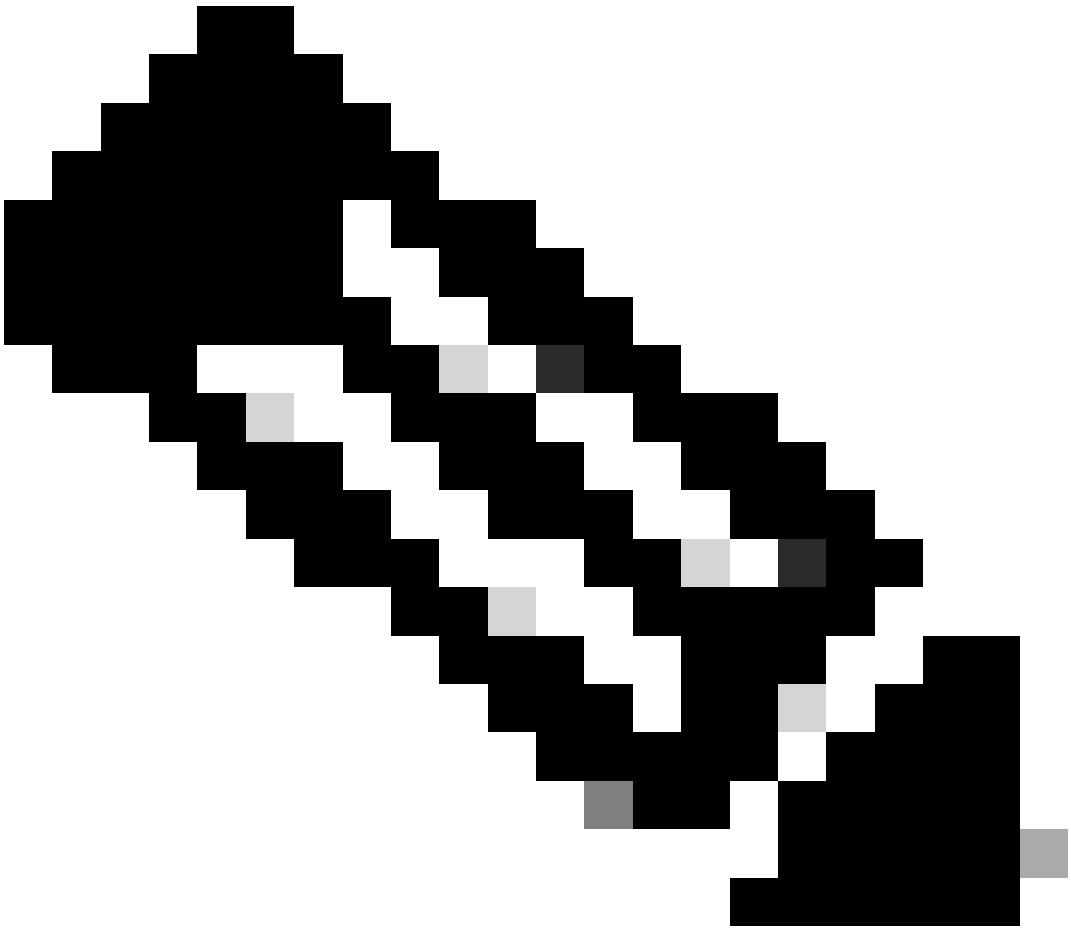
<#root>

```
Switch_IOS(config-if)#

private-vlan mapping add secondary_vlan_list

or
Switch_IOS(config-if)#

private-vlan mapping remove secondary_vlan_list
```



Nota: per gli switch Catalyst 6500/6000 con MSFC, verificare che la porta dal Supervisor Engine al motore di routing (ad esempio, la porta 15/1 o 16/1) sia promiscua.

<#root>

```
cat6000> (enable)

set pvlan mapping primary_vlan secondary_vlan 15/1

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

Per verificare il mapping, usare il comando show pvlan mapping.

<#root>

```
cat6000> (enable)
```

```
show pvlan mapping

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

Configurazioni

In questo documento vengono usate le seguenti configurazioni:

- Access_Layer (Catalyst 4003: CatOS)
- Core (Catalyst 4006: software Cisco IOS)

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: software Cisco IOS)

<#root>

```
Core#

show running-config

 Building configuration...


!--- Output suppressed.

 !
 hostname Core
 !
 vtp domain Cisco
 vtp mode transparent

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

 ip subnet-zero
 !
```

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

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

  switchport
  switchport trunk encapsulation dot1q
  switchport mode dynamic desirable
 !
 interface GigabitEthernet1/1
 !
 interface GigabitEthernet1/2
 !
 interface GigabitEthernet3/1

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

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

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

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

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

 !
 interface GigabitEthernet3/26


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


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

 !

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

 !
```

```
!--- Output suppressed.

 interface Vlan25

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

  ip address 10.25.1.1 255.255.255.0
 !
 interface Vlan100

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

  ip address 10.1.1.1 255.255.255.0
  private-vlan mapping 101

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

VLAN private su più switch

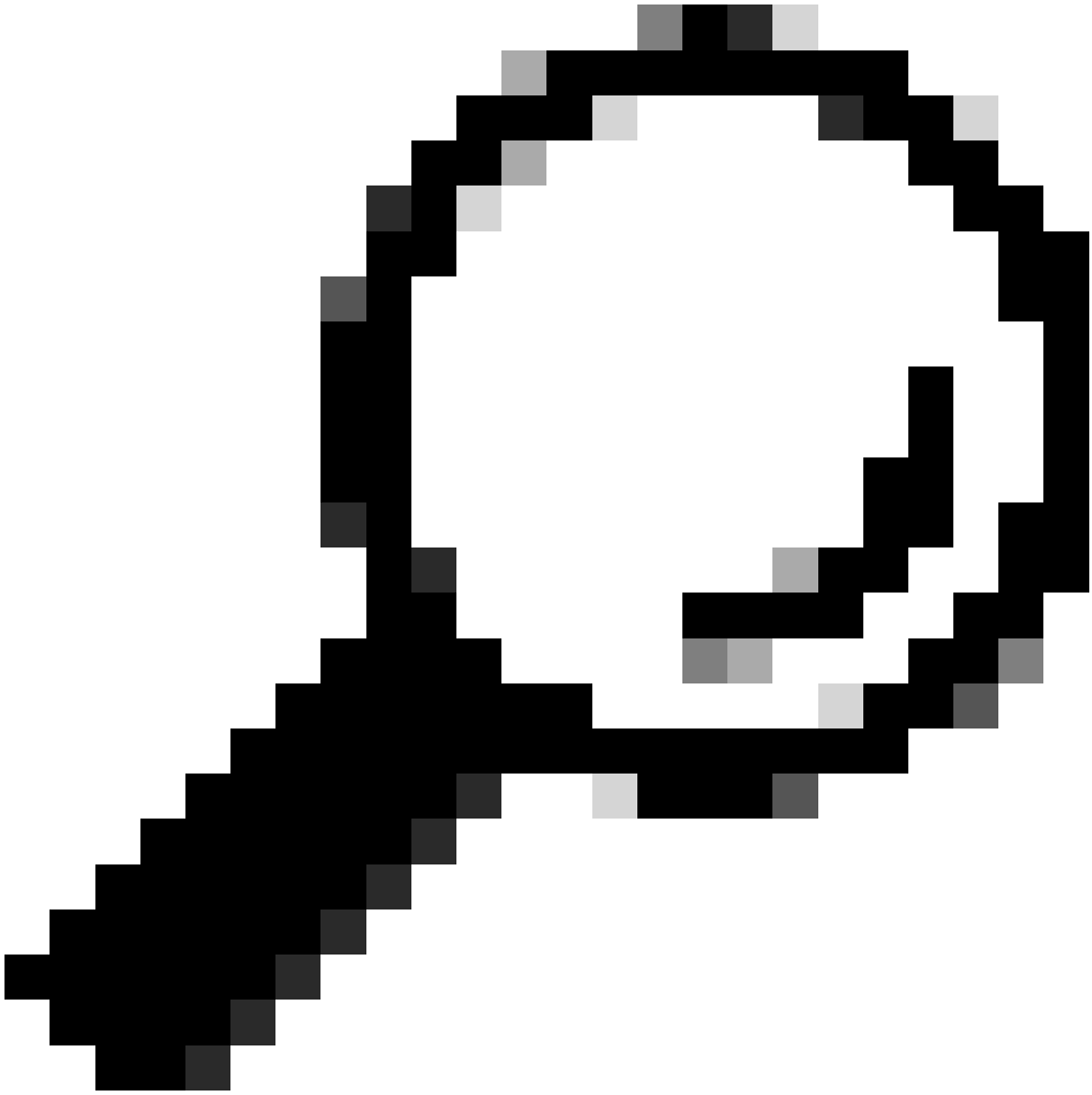
Per le VLAN private, sono disponibili due metodi per collegare più switch. In questa sezione vengono illustrati i metodi seguenti:

- Trunk regolari
- Trunk VLAN privati

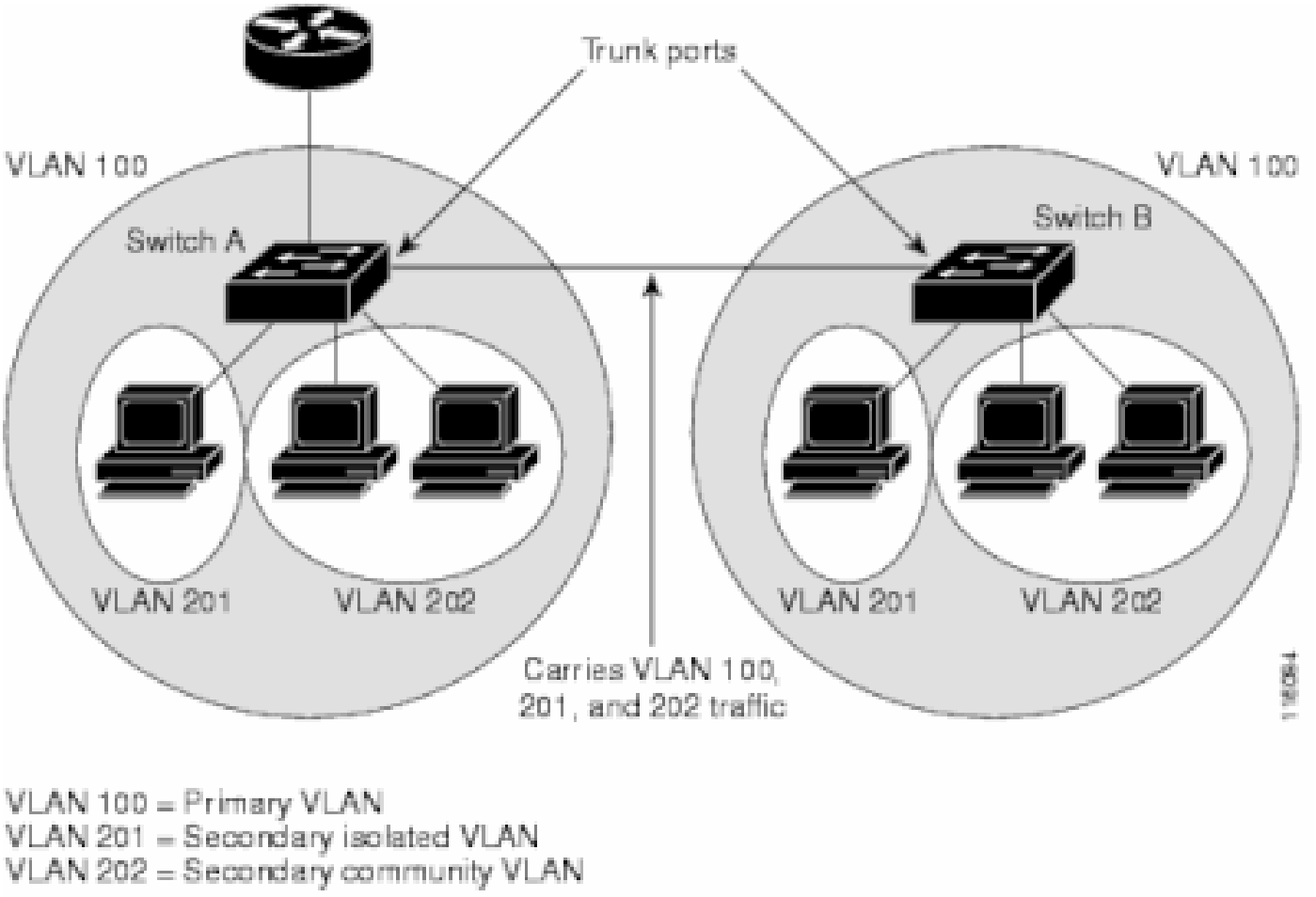
Trunk regolari

Come per le VLAN normali, le PVLAN possono estendersi su più switch. Una porta trunk trasferisce la VLAN primaria e le VLAN secondarie a uno switch adiacente. La porta trunk tratta la VLAN privata come qualsiasi altra VLAN. Una funzionalità delle PVLAN su più switch è che il traffico proveniente da una porta isolata di uno switch non raggiunge una porta isolata di un altro switch.

Configurare le PVLAN su tutti i dispositivi intermedi, compresi i dispositivi senza porte PVLAN, in modo da mantenere la sicurezza della configurazione PVLAN ed evitare altri usi delle VLAN configurate come PVLAN. Le porte trunk trasportano il traffico proveniente dalle VLAN normali e anche dalle VLAN principali, isolate e di comunità.



Suggerimento: Cisco consiglia di utilizzare le porte trunk standard se entrambi gli switch con trunking supportano le PVLAN.



Configurazione manuale delle PVLAN su tutti gli switch della rete di layer 2

Poiché il VTP non supporta le PVLAN, è necessario configurare manualmente le PVLAN su tutti gli switch della rete di layer 2. Se non si configura l'associazione della VLAN primaria e secondaria in alcuni switch della rete, i database di layer 2 in questi switch non vengono uniti. Questa situazione può causare un'inutile inondazione del traffico PVLAN su questi switch.

Trunk VLAN privati

Una porta trunkport PVLAN può trasportare più VLAN secondarie e non. I pacchetti vengono ricevuti e trasmessi con tag VLAN secondari o normali sulle porte del trunk PVLAN.

È supportato solo l'incapsulamento IEEE 802.1q. Le porte trunk isolate consentono di combinare il traffico di tutte le porte secondarie su un trunk. Le porte trunk promiscue consentono di combinare le diverse porte promiscue richieste in questa topologia in un'unica porta trunk che trasporta più VLAN primarie.

Utilizzare le porte trunk della VLAN privata isolata quando si prevede di usare le porte host isolate della VLAN privata per trasportare più VLAN, normali o per più domini di VLAN privata. Questa funzionalità risulta utile per la connessione di uno switch in downstream che non supporta VLAN private.

I trunk promiscui sulla VLAN privata vengono usati quando una porta host promiscua sulla VLAN privata è normalmente usata ma è necessaria per il trasporto di più vlan, normali o per più domini

di VLAN privata. Questa opzione permette di connettere un router upstream che non supporta VLAN private.

Ulteriori informazioni

Per ulteriori informazioni, fare riferimento a Private VLAN Trunk.

Per configurare un'interfaccia come porta trunk PVLAN, consultare il documento sulla configurazione di un'interfaccia di layer 2 come porta trunk PVLAN.

Per configurare un'interfaccia come porta trunk promiscua, fare riferimento alla configurazione di un'interfaccia di layer 2 come porta trunk promiscua.

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

CatOS

- show pvlan: visualizza la configurazione PVLAN. Verificare che le VLAN isolate e primarie siano associate. Verificare inoltre che siano visualizzate le porte host.
- show pvlan mapping: visualizza il mapping della PVLAN con la configurazione sulle porte promiscue.

Software Cisco IOS

- show vlan private-vlan: visualizza le informazioni sulla PVLAN, tra cui le porte associate.
- show interfacemod/portswitchport: visualizza le informazioni specifiche dell'interfaccia. Verificare che la modalità operativa e le impostazioni PVLAN operative siano corrette.
- show interfaces private-vlan mapping: visualizza il mapping PVLAN configurato.

Procedura di verifica

Attenersi alla seguente procedura:

1. Verificare la configurazione della PVLAN sugli switch.

   Verificare che le PVLAN primaria e secondaria siano associate/mappate l'una all'altra. Verificare inoltre l'inclusione delle porte necessarie.

   <#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
```

2. Verificare la configurazione corretta della porta promiscua.

   Questo output indica che la modalità operativa della porta è **promiscua** e che le VLAN operative sono 100 e 101.

   <#root>

   ```
   Core#
   ```

   show interface gigabitEthernet 3/26 switchport

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

   Operational Mode: private-vlan promiscuous

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

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

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

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

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

3. Eseguire il ping Internet Control Message Protocol (ICMP) tra la porta host e la porta promiscua.

Tenere presente che, poiché entrambi i dispositivi si trovano nella stessa VLAN primaria, i dispositivi devono trovarsi nella stessa subnet.

```
<#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.
```

4. Eseguire un ping ICMP tra le porte dell'host.

Nell'esempio, `host_port_2` (10.1.1.99) tenta di eseguire il ping su `host_port` (10.1.1.100). Il ping ha esito negativo. Il ping tra un'altra porta host e la porta promiscua, tuttavia, ha ancora esito positivo.

```
<#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.
```

Risoluzione dei problemi

Risoluzione dei problemi delle PVLAN

In questa sezione vengono illustrati alcuni problemi comuni relativi alle configurazioni PVLAN.

Problema 1

Viene visualizzato il seguente messaggio di errore: "`%PM-SP-3-ERR_INCOMP_PORT: <mod/porta> è impostato su inactive perché <mod/porta> è una porta trunk.`"

Questo messaggio di errore può essere visualizzato per diversi motivi, come descritto di seguito.

Spiegazione - 1

A causa dei limiti hardware, i moduli Catalyst 6500/6000 10/100-Mbps limitano la configurazione di una porta VLAN isolata o di comunità quando una porta nello stesso ASIC COIL è un trunk, una destinazione SPAN o una porta PVLAN promiscua. (COIL ASIC controlla 12 porte sulla maggior parte dei moduli e 48 porte sul modulo Catalyst 6548). La tabella nella sezione Regole e limitazioni di questo documento fornisce una descrizione dettagliata delle limitazioni imposte alla porta sui moduli Catalyst 6500/6000 10/100-Mbps.

Procedura di risoluzione - 1

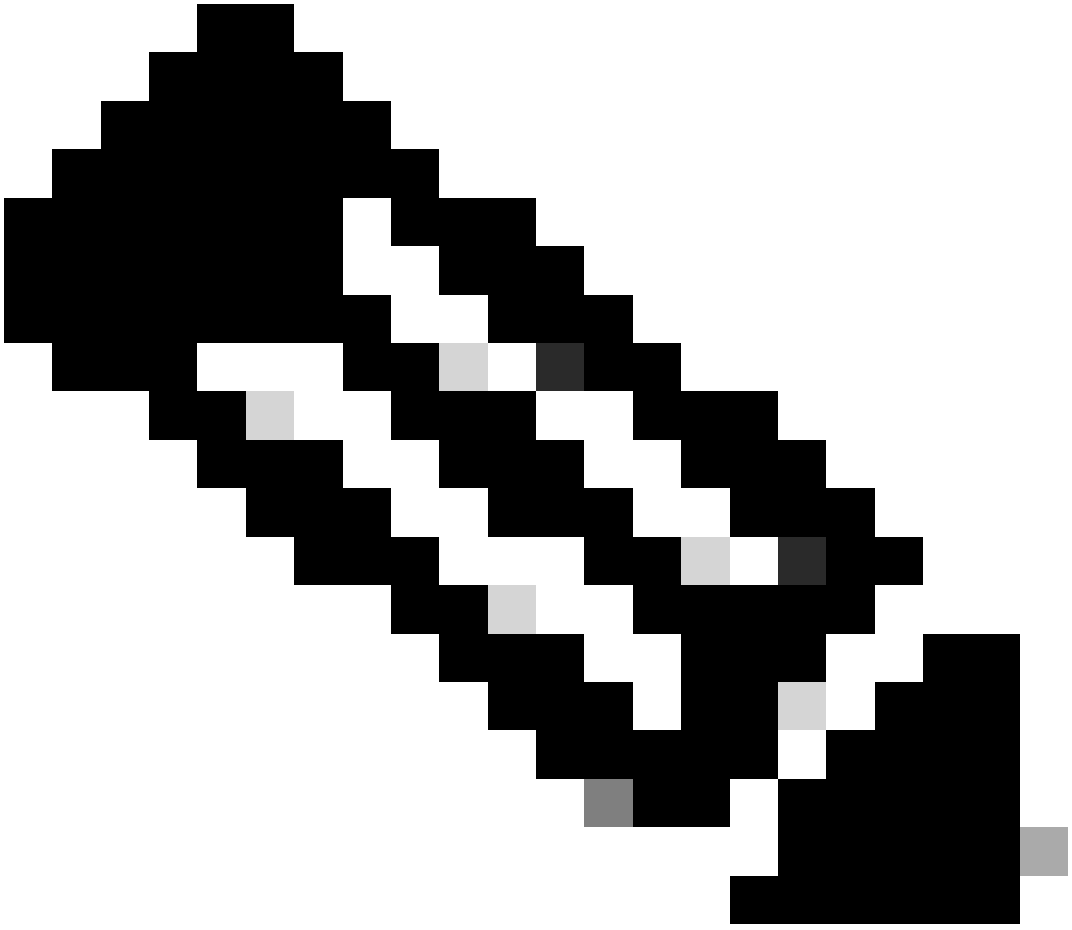
Se la PVLAN non è supportata su questa porta, selezionare una porta su un ASIC diverso sul modulo o su un modulo diverso. Per riattivare le porte, rimuovere la configurazione della porta VLAN isolata o della community e usare il comando shutdown e no shutdown.

Spiegazione - 2

Se le porte sono configurate manualmente o per impostazione predefinita in modalità automatica dinamica desiderata o dinamica.

Procedura di risoluzione - 2

Configurare le porte come modalità di accesso con il comando switchport mode access. Per riattivare le porte, usare il comando shutdown e il comando no shutdown.



Nota: nel software Cisco IOS versione 12.2(17a)SX e successive, la restrizione sulle 12 porte non si applica ai moduli di switching Ethernet WS-X6548-RJ-45, WS-X6548-RJ-21 e WS-X6524-100FX-MM.

Problema 2

Durante la configurazione della PVLAN, viene visualizzato uno dei seguenti messaggi:

```
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>
```

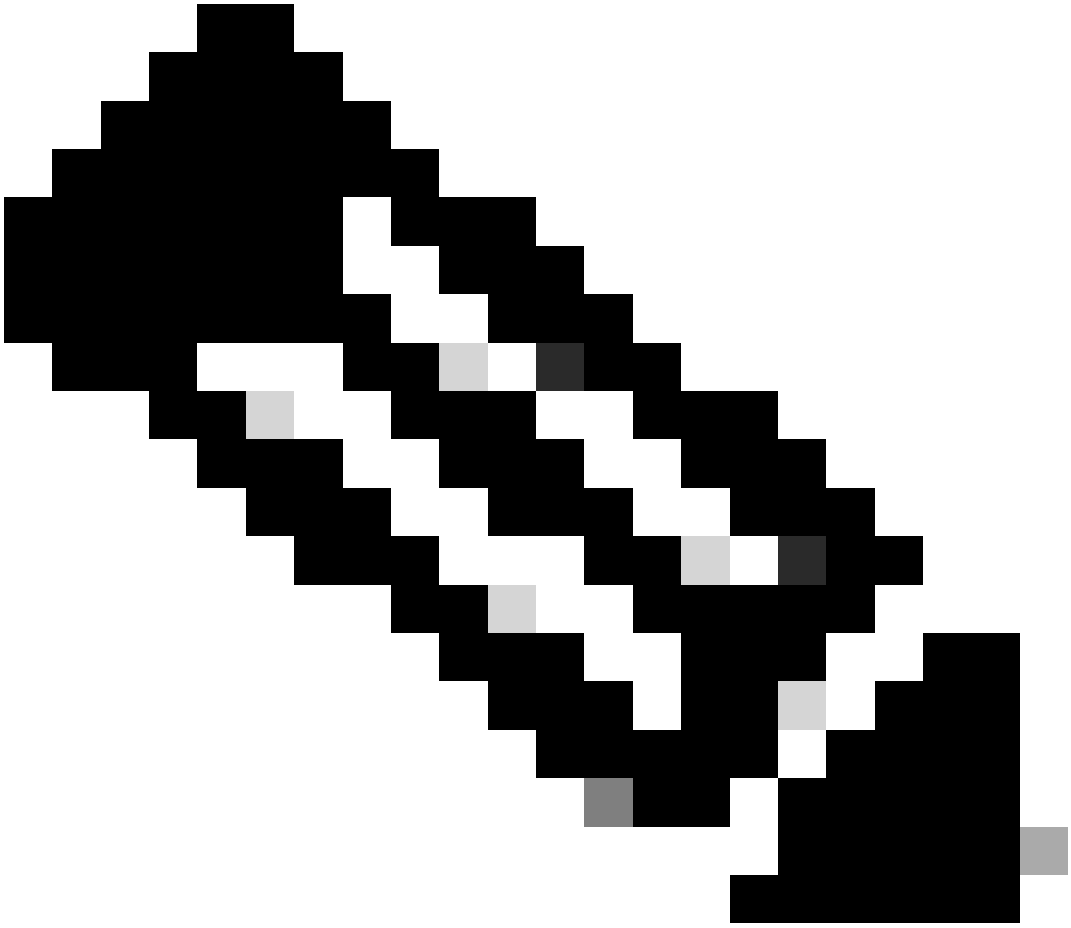
```
Port with another Promiscuous port in the same ASIC cannot be made
Private port.
Failed to add ports to association.
```

Spiegazione

A causa dei limiti hardware, i moduli Catalyst 6500/6000 10/100-Mbps limitano la configurazione di una porta VLAN isolata o di comunità quando una porta nello stesso ASIC COIL è un trunk, una destinazione SPAN o una porta PVLAN promiscua. (COIL ASIC controlla 12 porte sulla maggior parte dei moduli e 48 porte sul modulo Catalyst 6548). La tabella nella sezione Regole e limitazioni di questo documento fornisce una descrizione dettagliata delle limitazioni imposte alla porta sui moduli Catalyst 6500/6000 10/100-Mbps.

Procedura di risoluzione

Eseguire il comando show pvlan capabilities (CatOS), che indica se una porta può diventare una porta PVLAN. Se la PVLAN non è supportata su questa porta, selezionare una porta su un ASIC diverso sul modulo o su un modulo diverso.



Nota: nel software Cisco IOS versione 12.2(17a)SX e successive, la restrizione sulle 12 porte non si applica ai moduli di switching Ethernet WS-X6548-RJ-45, WS-X6548-RJ-21 e WS-X6524-100FX-MM.

Problema 3

Non è possibile configurare le PVLAN su alcune piattaforme.

Risoluzione

Verificare che la piattaforma supporti le PVLAN. Prima di iniziare la configurazione, consultare la matrice di supporto dello switch Catalyst VLAN privata per determinare se la piattaforma e la versione software supportano le PVLAN.

Problema 4

Su un modulo Catalyst 6500/6000 MSFC, non è possibile eseguire il ping di un dispositivo che si

connette alla porta isolata dello switch.

Risoluzione

Sul Supervisor Engine, verificare che la porta all'MSFC (15/1 o 16/1) sia promiscua.

<#root>

```
cat6000> (enable)
set pvlan mapping primary_vlan secondary_vlan 15/1
Successfully set mapping between 100 and 101 on 15/1
```

Inoltre, configurare l'interfaccia VLAN sull'MSFC come specificato nella sezione Configurazione di layer 3 di questo documento.

Problema 5

Con il comando no shutdown non è possibile attivare l'interfaccia VLAN per le VLAN isolate o di comunità.

Risoluzione

A causa della natura delle PVLAN, non è possibile attivare l'interfaccia VLAN per VLAN isolate o di comunità. È possibile attivare solo l'interfaccia VLAN che appartiene alla VLAN primaria.

Problema 6

Sui dispositivi Catalyst 6500/6000 con MSFC/MSFC2, le voci ARP apprese sulle interfacce PVLAN di layer 3 non scadono.

Risoluzione

Le voci ARP visualizzate sulle interfacce VLAN private di layer 3 sono voci ARP adesive e non scadono. La connessione di nuove apparecchiature con lo stesso indirizzo IP genera un messaggio e non viene creata la voce ARP. Pertanto, se l'indirizzo MAC viene modificato, è necessario rimuovere manualmente le voci ARP della porta PVLAN. Per aggiungere o rimuovere manualmente le voci ARP PVLAN, eseguire questi comandi:

<#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
```

In alternativa è possibile usare il comando no ip sticky-arp nel software Cisco IOS versione 12.1(11b)E e successive.

Informazioni correlate

- Proteggere le reti con PVLAN e VACL
- Supporto della tecnologia di switching LAN
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).