

CatalystスイッチによるVLAN間ルーティングの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[関連製品](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[コンフィギュレーション](#)

[推奨事項](#)

[確認](#)

[Catalyst 3850](#)

[Catalyst 4500-A](#)

[Catalyst 4500-B](#)

[トラブルシューティング](#)

[関連情報](#)

はじめに

このドキュメントでは、Cisco CatalystシリーズスイッチでVLAN間ルーティングを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- VLAN 作成の知識
- トランクリンクの作成方法に関する知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco IOS® XEソフトウェアリリース16.12.7が稼働するCatalyst 3850

- Cisco IOS®ソフトウェアリリース03.09.00Eが稼働するCatalyst 4500

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

表記法

表記法の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

関連製品

この設定は、次のバージョンのハードウェアとソフトウェアにも使用できます。

- Catalyst 3000/9000スイッチ以降
- アクセスレイヤスイッチとして使用される任意のCatalystスイッチモデル

背景説明

VLAN間ルーティングを実装することで、組織はVLANセグメンテーションの利点を維持しながら、ネットワークの異なる部分の間で必要な通信を可能にすることができます。これは、異なる部門やサービスが安全かつ効率的にやり取りする必要がある複雑なネットワーク環境で特に役立ちます。Catalyst 3850シリーズスイッチにインターVLANルーティングの設定例を設定し、Catalyst 3850に直接接続するレイヤ2(L2)スイッチとして機能するCatalyst 4500シリーズスイッチのペアを使用します。Catalyst 3850スイッチには、インターネット宛てのすべてのトラフィックに対するデフォルトルートがあります。ネクストホップはCiscoルータですが、ファイアウォールなどのインターネットゲートウェイを指定することもできます。

LANでは、VLANはデバイスを個別のコリジョンドメインとレイヤ3(L3)サブネットに分割します。同じVLAN内のデバイスは、ルーティングを必要とせずに直接通信できる。ただし、異なるVLANのデバイス間の通信にはルーティングデバイスが必要です。

レイヤ2(L2)スイッチには、VLAN間の通信を容易にするためにL3ルーティングデバイスが必要です。このルーティングデバイスは、スイッチに対して外部に配置することも、同じシャーシ内の別のモジュールに統合することもできます。Catalyst 3000/9000などの最新のスイッチは、ルーティング機能をスイッチ内に直接組み込んでいます。これらのスイッチは、パケットを受信し、別のVLANに属していることを識別して、宛先VLAN上の適切なポートに転送できます。

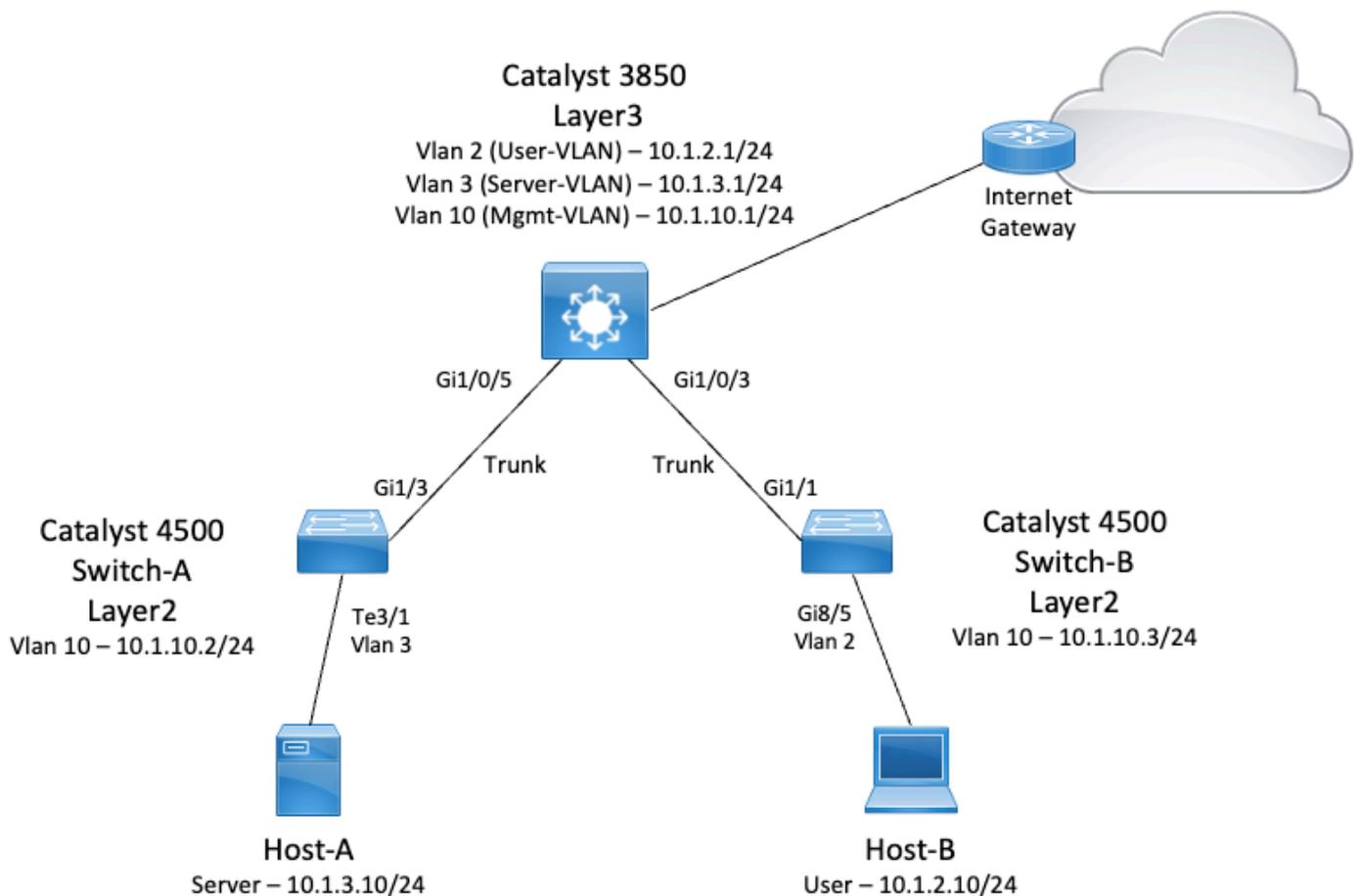
一般的なLAN設計では、デバイスのグループまたは機能に基づいてネットワークをセグメント化します。たとえば、エンジニアリングVLANにはエンジニアリング部門に関連するデバイスのみが含まれ、財務VLANには財務関連のデバイスのみが含まれます。ルーティングを有効にすると、異なるVLANのデバイスが同じブロードキャストドメイン内になくても通信できるようになります。このVLAN設計には、管理者がアクセスリストを使用してVLAN間の通信を制限できるという利点もあります。たとえば、アクセスリストを使用して、エンジニアリングVLAN内のデバイスが財務VLAN内のデバイスにアクセスするのを防ぐことができます。

設定

このセクションでは、このドキュメントで説明するVLAN間ルーティングの設定に必要な情報を提供します。

 注：ここで使用されているコマンドの詳細を調べるには、[Cisco Support Tools](#)を使用してください。このようなツールやその他の内部情報にアクセスできるのは、登録されたシスコのユーザだけです。

ネットワーク図



この図では、Catalyst 3850スイッチが異なるVLAN間でVLAN間ルーティング機能を提供します。Catalyst 3850スイッチは、IPルーティングをディセーブルにすることで、L2デバイスとして動作できます。スイッチをL3デバイスとして機能させてVLAN間ルーティングを提供するには、ip routingがグローバルに有効になっていることを確認します。

コンフィギュレーション

次の3つのVLANは、この設定のために定義されました。

- VLAN 2 : ユーザVLAN

- VLAN 3 : サーバVLAN
- VLAN 10:Mgmt-VLAN

各サーバおよびホストデバイスのデフォルトゲートウェイは、Catalyst 3850上の対応するVLANインターフェイスのIPアドレスに設定されている必要があります。たとえば、サーバのデフォルトゲートウェイは10.1.3.1です。アクセスレイヤスイッチ(Catalyst 4500)は、トランクリンクを介してCatalyst 3850に接続されます。

インターネットトラフィックの場合、Catalyst 3850には、インターネットゲートウェイとして機能するCiscoルータを指すデフォルトルートがあります。その結果、Catalyst 3850のルーティングテーブルにルートがないトラフィックは、処理のためにCiscoルータに転送されます。

推奨事項

- 802.1QトランクのネイティブVLANが、トランクリンクの両端で必ず同じになるようにします。ネイティブVLANが異なると、ネイティブVLAN上のトラフィックが正しく送信されず、ネットワークで接続の問題が発生する可能性があります。
- 次の図に示すように、管理VLANを他のVLANから分離します。この分離により、ユーザVLANまたはサーバVLANでのブロードキャストまたはパケットストームがスイッチ管理に影響を及ぼさなくなります。
- VLAN 1 は管理用に使用しないでください。CatalystスイッチのすべてのポートはデフォルトでVLAN 1に設定され、未設定のポートはVLAN 1に配置されます。管理にVLAN 1を使用すると、潜在的な問題が発生する可能性があります。
- デフォルトゲートウェイポートへの接続には、レイヤ3(ルーテッド)ポートを使用します。この例では、Ciscoルータを、インターネットゲートウェイルータに接続するファイアウォールに置き換えることができます。
- この例では、インターネットに到達するためのCiscoルータへのスタティックデフォルトルートをCatalyst 3850に設定します。この設定は、インターネットへのルートが1つしかない場合に最適です。Catalyst 3850が到達可能なサブネットに対して、ゲートウェイルータ上にスタティックルート(集約されていることが望ましい)を設定していることを確認します。この設定ではルーティングプロトコルを使用しないため、この手順は重要です。
- ネットワークに2台のL3スイッチがある場合は、両方の3850スイッチにアクセスレイヤスイッチを接続し、スイッチ間でホットスタンバイルータプロトコル(HSRP)を実行してネットワークの冗長性を確保できます。
- アップリンクポートに追加の帯域幅が必要な場合は、EtherChannelを設定できます。これにより、リンク障害時にリンクの冗長性も提供されます。

次に、このトポロジで使用されるスイッチの実行コンフィギュレーションを示します。

 注:インターネットゲートウェイルータの設定は関連がないので、このドキュメントでは説明しません。

- Catalyst 3850
- Catalyst 4500-A

- Catalyst 4500-B

Catalyst 3850

```
<#root>
```

```
SW_3850#
```

```
show running-config
```

```
Building configuration...
```

```
Current configuration : 11543 bytes
```

```
!
```

```
! Last configuration change at 12:16:54 UTC Tue Nov 15 2022
```

```
!
```

```
version 16.12
```

```
no service pad
```

```
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
```

```
service internal
```

```
service call-home
```

```
no platform punt-keepalive disable-kernel-core
```

```
!
```

```
hostname SW_3850
```

```
!
```

```
!--- IP routing enabled for Inter-VLAN routing.
```

```
ip routing
```

```
!
```

```
!
```

```
no ip domain lookup
```

```
!
```

```
!
```

```
login on-success log
```

```
!
```

```
!
```

```
!
```

```
vtp mode off
```

```
!
```

```
!--- Output suppressed.
```

```
!--- Configure IEEE 802.1q trunks.
```

```
!--- Issue the switchport mode trunk command to force the switch port to trunk mode.
```

```
!
```

```
interface GigabitEthernet1/0/1
```

```
shutdown
```

```
!
```

```
interface GigabitEthernet1/0/2
```

```
shutdown
```

```
!
```

```
interface GigabitEthernet1/0/3 description To_Switch-B switchport mode trunk
```

```
!  
interface GigabitEthernet1/0/4  
no switchport no ip address shutdown  
!  
interface GigabitEthernet1/0/5  
  
description To_Switch-A  
  
switchport mode trunk  
  
!  
interface GigabitEthernet1/0/6  
no switchport  
no ip address  
shutdown  
!  
interface Vlan1  
no ip address  
shutdown  
!  
!--- This Switch Virtual Interface (SVI) is the default gateway for Users.  
!  
interface Vlan2  
  
description User-SVI  
  
ip address 10.1.2.1 255.255.255.0  
  
!  
!--- This SVI is the default gateway for Servers VLAN.  
!  
interface Vlan3  
  
description Server-SVI  
  
ip address 10.1.3.1 255.255.255.0  
  
!  
!--- This SVI is the default gateway for other L2 switches management interface.  
!  
interface Vlan10  
  
description Management-SVI
```

```
ip address 10.1.10.1 255.255.255.0

!  
!--- This route statement allows the 3850 to send Internet traffic to the Cisco router.  
  
ip route 0.0.0.0 0.0.0.0 10.1.1.2  
  
ip forward-protocol nd  
ip http server  
ip http authentication local  
ip http secure-server  
!  
!  
!  
line con 0  
line vty 5 15  
!  
end
```

 注：この例では、vtp mode offコマンドを使用して、VLAN Trunk Protocol(VTP)がすべてのスイッチでオフに設定されています。

<#root>

SW_3850(config)#

vtp mode off

Setting device to VTP Off mode for VLANs.

SW_3850(config)#

vlan 2

SW_3850(config-vlan)#

name User_VLAN

SW_3850(config-vlan)#

exit

SW_3850(config)#

vlan 3

SW_3850(config-vlan)#

name Server_VLAN

SW_3850(config-vlan)#

exit

SW_3850(config)#

vlan 10

```
SW_3850(config-vlan)#  
name Mgmt_VLAN  
SW_3850(config-vlan)#  
exit  
SW_3850(config)#  
end
```

Catalyst 4500-A

```
<#root>  
Switch-A#  
show running-config  
Building configuration...  
Current configuration : 15360 bytes  
!  
! Last configuration change at 01:06:17 UTC Wed Nov 16 2022  
!  
version 15.2  
no service pad  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
service internal  
service compress-config  
!  
hostname Switch-A  
!  
no ip domain-lookup  
no ip dhcp snooping information option  
!  
!  
login block-for 60 attempts 3 within 60  
login delay 1  
login quiet-mode access-class testblock  
login on-failure log  
login on-success log  
vtp mode off  
!  
!  
spanning-tree mode pvst  
spanning-tree extend system-id  
!  
!  
vlan 3 name Server-VLAN ! vlan 10 name Mgmt-VLAN  
!
```

!--- Output suppressed

```
!  
interface GigabitEthernet1/1  
shutdown  
!  
interface GigabitEthernet1/2  
shutdown  
!  
interface GigabitEthernet1/3 switchport mode trunk  
!  
!--- Configure Server (Host-A) to be the on the access VLAN 3.  
!  
interface TenGigabitEthernet3/1 switchport access vlan 3 switchport mode access  
!  
interface TenGigabitEthernet3/2  
shutdown  
!  
interface TenGigabitEthernet3/3  
!  
interface TenGigabitEthernet3/4  
!
```

!--- Output suppressed.

!--- IP address on VLAN 10 manages this switch.

```
!  
interface Vlan1  
no ip address  
!  
interface Vlan10 ip address 10.1.10.2 255.255.255.0  
!  
ip forward-protocol nd  
ip http server  
ip http banner  
ip http authentication local  
!
```

!--- Configure the default gateway so that the switch is reachable from other !--- VLANs/subnets. The gateway points to the VLAN 10 interface on the 3850

```
ip default-gateway 10.1.10.1  
ip forward-protocol nd  
ip http server  
ip http banner  
ip http authentication local  
!  
!  
line con 0  
stopbits 1  
line vty 0 4  
logging synchronous  
transport input all  
line vty 5 15  
logging synchronous
```

```
transport input all
!  
end
```

Catalyst 4500-B

```
<#root>
```

```
Switch-B#
```

```
show running-config
```

```
Building configuration...
```

```
Current configuration : 6841 bytes
```

```
!  
! Last configuration change at 10:44:33 UTC Tue Nov 15 2022  
!  
version 15.2  
no service pad  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
service compress-config  
!  
hostname Switch-B  
!  
boot-start-marker  
boot system bootflash:cat4500es8-universal.SPA.03.11.06.E.152-7.E6.bin  
boot-end-marker  
!  
!  
vrf definition mgmtVrf  
!  
  address-family ipv4  
  exit-address-family  
!  
  address-family ipv6  
  exit-address-family  
!  
!  
no aaa new-model  
hw-module module 7 mode 1  
!  
!  
!  
!  
!  
!  
!  
!  
vtp mode off  
!  
!  
! spanning-tree mode pvst spanning-tree extend system-id !
```

```
vlan 2
name User-VLAN
!
vlan 10 name
Mgmt-VLAN

!
!

interface GigabitEthernet1/1 switchport mode trunk

!
interface GigabitEthernet1/2
!
interface GigabitEthernet1/3
shutdown
!
interface GigabitEthernet1/4
shutdown
!

!--- Output suppressed.
!--- Configure User (Host-B) in VLAN 2.

!

interface GigabitEthernet8/5 switchport access vlan 2 switchport mode access

!

!--- Configure the management IP address in VLAN 10.
!
interface Vlan1
no ip address
!

interface Vlan10 ip address 10.1.10.3 255.255.255.0

!

!--- Define the default route so that the switch is reachable.
!

ip default-gateway 10.1.10.1

ip forward-protocol nd
ip http server
ip http banner
ip http authentication local
!
!
line con 0
stopbits 1
line vty 0 4
login
transport input none
!
!
end
```

確認

次に、デバイスのステータスを確認し、設定が正しく動作していることを確認するために使用できる、重要なコマンドのリストを示します。

`show vtp status` : このコマンドは、スイッチ上のVLANランキングプロトコル(VTP)のステータスを表示します。VTPバージョン、ドメイン名、モード(サーバ、クライアント、またはトランスペアレント)、および既存のVLANの数に関する情報を提供します。これは、VTP設定を確認し、ネットワーク全体でVLAN情報の一貫性を確保する場合に便利です。

`show interfaces trunk` : このコマンドは、スイッチのトランクポートのステータスを示します。また、トランクとして設定されているインターフェイス、カプセル化のタイプ(802.1Qなど)、および各トランクで許可されているVLANに関する詳細を提供します。これは、VLAN接続の問題のトラブルシューティングと適切なトランク設定を行うために不可欠です。

`show ip route` : このコマンドは、スイッチのIPルーティングテーブルを表示します。直接接続されたネットワーク、スタティックルート、ダイナミックルーティングプロトコルを通じて学習されたルートを含む、すべての既知のルートが一覧表示されます。これは、ルーティングパスを確認し、スイッチが必要なすべてのネットワークに到達できることを確認するために重要です。

`show ip cef` : このコマンドはCisco Express Forwarding(CEF)の出力を表示します。ネクストホップアドレスや関連するインターフェイスなど、CEFエントリに関する情報を提供します。これは、転送に関する問題のトラブルシューティングや、効率的なパケット処理の確保に役立ちます。



注：[Cisco CLIアナライザ](#)ツールは、統合TACツールと知識を使用するこのスマートSSHクライアントを使用して、シスコがサポートするソフトウェアのトラブルシューティングと全体的な健全性のチェックを行うのに役立ちます。

 注:CLIコマンドの詳細については、特定のスイッチングプラットフォームの『コマンドリファレンスガイド』を参照してください。

 注：このようなツールやその他の内部情報にアクセスできるのは、登録ユーザのCiscoだけです。

Catalyst 3850

<#root>

SW_3850#

H - NHRP, G - NHRP registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PFR

Gateway of last resort is 10.100.100.2 to network 0.0.0.0

```
s* 0.0.0.0/0 [1/0] via 10.100.100.2
```

10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks

```
C 10.1.2.0/24 is directly connected, Vlan2
L 10.1.2.1/32 is directly connected, Vlan2
C 10.1.3.0/24 is directly connected, Vlan3
L 10.1.3.1/32 is directly connected, Vlan3
C 10.1.10.0/24 is directly connected, Vlan10
L 10.1.10.1/32 is directly connected, Vlan10
C 10.100.100.0/24 is directly connected, GigabitEthernet1/0/2
L 10.100.100.1/32 is directly connected, GigabitEthernet1/0/2
```

Catalyst 4500-A

```
<#root>
```

```
Switch-A#
```

```
show vtp status
```

```
VTP Version capable      : 1 to 3
VTP version running     : 2
VTP Domain Name         : cisco.com
VTP Pruning Mode        : Disabled
VTP Traps Generation    : Disabled
Device ID               : 6400.f13e.dc40
Configuration last modified by 10.1.10.2 at 0-0-00 00:00:00
```

```
Feature VLAN:
```

```
-----
```

```
VTP Operating Mode : Off
```

```
Maximum VLANs supported locally : 1005
Number of existing VLANs       : 32
Configuration Revision         : 0
MD5 digest                    : 0x0B 0x61 0x4F 0x9B 0xCD 0x1B 0x37 0x55
                               0xAB 0x0C 0xC1 0x4B 0xF8 0xDE 0x33 0xB3
```

```
<#root>
```

```
Switch-A#
```

```
show interfaces trunk
```

```
Port      Mode          Encapsulation  Status        Native vlan
Gi1/3 on 802.1q trunking 1
```

Port Vlans allowed on trunk

Gi1/3 1-4094

Port Vlans allowed and active in management domain

Gi1/3 1,3,10

Port Vlans in spanning tree forwarding state and not pruned

Gi1/3 1,3,10

Catalyst 4500-B

<#root>

Switch-B#

show vtp status

```
VTP Version capable      : 1 to 3
VTP version running     : 1
VTP Domain Name         :
VTP Pruning Mode        : Disabled
VTP Traps Generation    : Disabled
Device ID                : 6c20.5606.3540
Configuration last modified by 10.1.10.3 at 11-15-22 10:42:29
```

Feature VLAN:

VTP Operating Mode : Off

```
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 7
Configuration Revision          : 0
MD5 digest                      : 0xEC 0xB4 0x8D 0x46 0x94 0x95 0xE0 0x8F
                                0xEE 0x1E 0xC7 0x9F 0x26 0x88 0x49 0x9F
```

<#root>

Switch-B#

show interfaces trunk

```
Port      Mode           Encapsulation  Status        Native vlan
Gi1/1 on 802.1q trunking 1
```

Port Vlans allowed on trunk

Gi1/1 1-4094

Port Vlans allowed and active in management domain

Gi1/1 1-2,10

Port Vlans in spanning tree forwarding state and not pruned

Gi1/1 1-2,10

トラブルシューティング

1. 同じVLAN内でのpingの問題

- 同じVLAN内のデバイスにpingできない場合は、送信元ポートと宛先ポートのVLAN割り当てをチェックして、それらが同じVLANにあることを確認します。
- VLAN割り当てを確認するには、show interface statusコマンドを使用します。
- show mac address-tableコマンドを使用して、L2スイッチが適切なVLANの各デバイスのMACアドレスを学習していることを確認します。

2. 異なるスイッチ間でのPingの問題

- 送信元と宛先が異なるスイッチにある場合は、トランクが正しく設定されていることを確認します。show interfaces trunkコマンドを使用して、設定を確認します。
- トランクリンクの両側でネイティブVLANが一致していること、および送信元デバイスと宛先デバイスの間でサブネットマスクが一致していることを確認します。

3. 異なるVLAN間でのpingの問題

- 異なるVLANのデバイスにpingできない場合は、それぞれのデフォルトゲートウェイにpingできることを確認します（ステップ1を参照）。
- デバイスのデフォルトゲートウェイが正しいVLANインターフェイスのIPアドレスを指していること、およびサブネットマスクが一致していることを確認します。

4. インターネット接続の問題

- インターネットに到達できない場合は、Catalyst 3850のデフォルトルートが正しいIPアドレスを指していること、およびサブネットアドレスがインターネットゲートウェイルータと一致していることを確認します。
- L3スイッチ（このシナリオでは3850）からインターネットゲートウェイにpingできることを確認します。
- これを確認するには、show ip cef <prefix>コマンドを使用して、正しいインターフェイスを指しているかどうかを確認します。
- インターネットゲートウェイルータにインターネットと内部ネットワークの両方へのルートがあることを確認します。

関連情報

- [外部ルータを使用した VLAN 間ルーティングの設定](#)
- [Catalyst スイッチによるイーサネット VLAN の構築](#)

- [シスコのテクニカルサポートとダウンロード](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。