



## レイヤ 3 インターフェイスの設定

この章では、Catalyst 4500 シリーズ スイッチ上のレイヤ 3 インターフェイスについて説明します。設定上の注意事項、設定手順、および設定例についても示します。

この章の主な内容は、次のとおりです。

- 「レイヤ 3 インターフェイスについて」 (P.33-1)
- 「設定時の注意事項」 (P.33-5)
- 「論理レイヤ 3 VLAN インターフェイスの設定」 (P.33-6)
- 「レイヤ 3 インターフェイスとしての VLAN の設定」 (P.33-7)
- 「物理レイヤ 3 インターフェイスの設定」 (P.33-12)
- 「EIGRP スタブ ルーティングの設定」 (P.33-13)



(注)

この章で使用するスイッチ コマンドの構文および使用方法の詳細については、次の URL で『Cisco Catalyst 4500 Series Switch Command Reference』と関連資料を参照してください。

<http://www.cisco.com/en/US/products/hw/switches/ps4324/index.html>

『Catalyst 4500 Series Switch Command Reference』に掲載されていないコマンドについては、より詳細な Cisco IOS ライブラリを参照してください。次の URL で『Catalyst 4500 Series Switch Cisco IOS Command Reference』と関連資料を参照してください。

<http://www.cisco.com/en/US/products/ps6350/index.html>

## レイヤ 3 インターフェイスについて

Catalyst 4500 シリーズ スイッチは、Cisco IOS Internet Protocol (IP) および IP ルーティング プロトコルでレイヤ 3 インターフェイスをサポートしています。ネットワークレイヤであるレイヤ 3 は、主にパケット内データの論理インターネットネットワーク パスへのルーティングを行います。

データ リンク レイヤであるレイヤ 2 は、物理レイヤ (レイヤ 1) を制御するプロトコルと、メディアに伝送される前のデータのフレーミング方法が含まれています。LAN 上の 2 つのセグメント間でフレーム内のデータをフィルタリングおよび転送するレイヤ 2 の機能を、ブリッジングといいます。

Catalyst 4500 シリーズ スイッチは、2 種類のレイヤ 3 インターフェイスをサポートしています。論理レイヤ 3 VLAN インターフェイスは、ルーティングとブリッジングの機能を統合します。

Catalyst 4500 シリーズ スイッチは、物理レイヤ 3 インターフェイスを使用して従来のルータのように設定できます。

ここでは、次の内容について説明します。

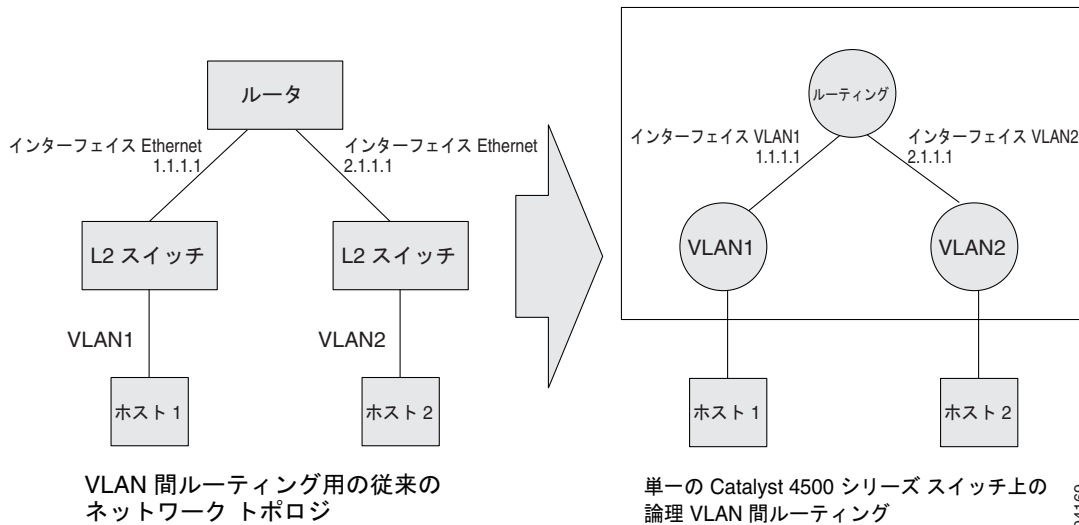
- ・「論理レイヤ 3 VLAN インターフェイス」(P.33-2)
- ・「物理レイヤ 3 インターフェイス」(P.33-2)
- ・「SVI 自動ステート除外の概要」(P.33-3)
- ・「レイヤ 3 インターフェイス カウンタの概要」(P.33-3)

## 論理レイヤ 3 VLAN インターフェイス

論理レイヤ 3 VLAN インターフェイスは、レイヤ 2 スイッチ上の VLAN への論理ルーティング インターフェイスとして機能します。従来のネットワークでは、ルータとスイッチ間の物理インターフェイスが VLAN 間ルーティングを実行する必要がありました。Catalyst 4500 シリーズ スイッチは単一の Catalyst 4500 シリーズ スイッチでのルーティングとブリッジング機能を統合することで、VLAN 間ルーティングをサポートします。

図 33-1 では、従来のネットワークで 3 台の物理デバイスによって実行されていたルーティングとブリッジング機能が、どのようにして 1 台の Catalyst 4500 シリーズ スイッチ上で論理的に実行されているかを示します。

図 33-1 Catalyst 4500 シリーズ スイッチの論理レイヤ 3 VLAN インターフェイス



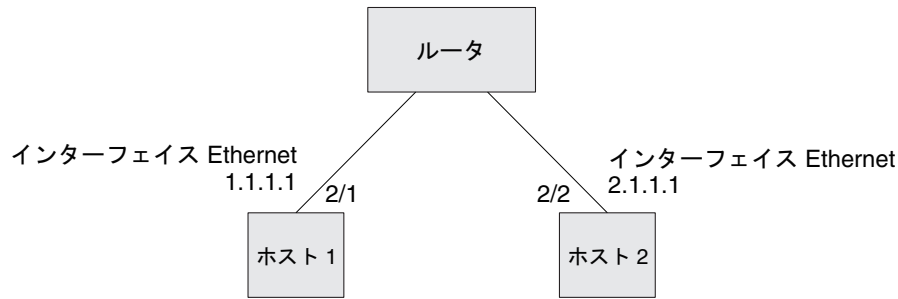
94169

## 物理レイヤ 3 インターフェイス

物理レイヤ 3 インターフェイスは、従来のルータに等しい機能をサポートします。これらのレイヤ 3 インターフェイスは、Catalyst 4500 シリーズ スイッチへの物理ルーティング インターフェイスをホストに提供します。

図 33-2 に、Catalyst 4500 シリーズ スイッチが従来のルータとして機能する例を示します。

図 33-2 Catalyst 4500 シリーズ スイッチの物理レイヤ 3 インターフェイス



Catalyst 4500 シリーズ スイッチ上の物理 VLAN 間ルーティング

94168

## SVI 自動ステート除外の概要

ルータ VLAN インターフェイスはアップ/アップ状態となるために、次の一般的な条件を満たす必要があります。

- VLAN がスイッチの VLAN データベースに存在し、アクティブであること。
- VLAN インターフェイスがルータに存在し、管理上のダウン状態であること。
- 少なくとも 1 つのレイヤ 2 (アクセス ポートまたはトランク) ポートが存在し、この VLAN 上でリンクがアップ状態であり、VLAN でスパニングツリー フォワーディング ステートであること。



(注)

対応する VLAN リンクに属している最初のスイッチ ポートがアップし、スパニングツリー フォワーディング ステートになると、VLAN インターフェイスのプロトコル ライン ステートがアップします。

一般に、VLAN インターフェイスに複数のポートが存在する場合は、VLAN 内のすべてのポートがダウンしたときに SVI がダウンします。VI 自動ステートは、SVI のアップまたはダウン判断時に考慮しないポートにマーキングするつまみとして機能し、そのポートでイネーブルになっているすべての VLAN に適用されます。

VLAN インターフェイスは、レイヤ 2 ポートでコンバージェンス (つまり、リスニングおよびラーニングからフォワーディングへの移行) のための時間が経過後にアップします。これにより、ルーティング プロトコルやその他の機能で VLAN インターフェイスがフル稼働可能であるかのように使用されることがなくなります。また、ブラック ホール ルーティングなどの別の問題が発生しないようにします。

## レイヤ 3 インターフェイス カウンタの概要



(注)

Catalyst 4900M、Catalyst 4948E、Supervisor Engine 6-E、Supervisor Engine 6L-E、Supervisor Engine 7-E、および Supervisor Engine 7L-E は、レイヤ 2 インターフェイス カウンタをサポートしません。ただし、レイヤ 3 (SVI) インターフェイス カウンタをサポートします。

Catalyst 4900M、Catalyst 4948E、Supervisor Engine 6-E、Supervisor Engine 6L-E、Supervisor Engine 7-E、および Supervisor Engine 7L-E で IPv4 および IPv6 を実行すると、パケットはフォワーディング エンジンによってハードウェアでルーティングされます。これらは、最大 4092 のインターフェイスでルーティング パケットをカウントするために次の統計情報をサポートします。

- 入力ユニキャスト
- 入力マルチキャスト
- 出力ユニキャスト
- 出力マルチキャスト

各カウンタ タイプについて、パケット数および送受信される合計バイト数の両方がカウントされます。IPv4 および IPv6 トラフィック用に、これらの統計情報を一意に収集できます。

サポートされているレイヤ 3 インターフェイスの総数がハードウェアでサポートされるカウンタ数を超過するため、一部のレイヤ 3 インターフェイスにカウンタがないことがあります。レイヤ 3 インターフェイスにカウンタを割り当てます。レイヤ 3 インターフェイスのデフォルト設定にはカウンタがありません。

統計情報の収集は 4 つのいずれかの方法のインターフェイス レベルで設定できます (表 33-1 を参照)。収集モードに応じてインターフェイスの最大数が設定に適用されます。

表 33-1 統計情報収集ノードの設定

カウンタ モード	コンフィギュレーション CLI	機能	最大
IPv4 のみ	counter ipv4	IPv4 統計情報だけが収集されます。	4092
IPv6 のみ	counter ipv6	IPv6 統計情報だけが収集されます。	4092
IPv4 と IPv6 の結合	counter	IPv4 と IPv6 の両方の統計情報が収集されますが、合計としてのみ表示されます。	4092
IPv4 および IPv6 を個別	counter ipv4 ipv6 separate	IPv4 と IPv6 の両方の統計情報が収集され、個別に表示できます。	2046

これらの設定済みモードを混合した場合のルールは次のとおりです。

$(v4/v6/v4v6combined \text{ インターフェイスの数}) + 2 * (v4v6separate \text{ インターフェイスの数}) \leq 4092$



(注)

レイヤ 3 インターフェイス カウンタをイネーブルにするには、インターフェイス モードで **counter** コマンドを入力する必要があります。手順については、「レイヤ 3 インターフェイス カウンタの設定」(P.33-10) を参照してください。

ハードウェア カウンタは、次の例のように **show interface** コマンドの出力に表示されます。カウンタの設定があるときに更新されるカウンタ フィールドが強調表示されています。

```
Switch# show interface gi3/1
GigabitEthernet3/1 is up, line protocol is up (connected)
  Hardware is Gigabit Ethernet Port, address is 001f.9e9e.f43f (bia 001f.9e9e.f43f)
  Internet address is 10.10.10.2/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s, link type is auto, media type is 10/100/1000-TX
  input flow-control is on, output flow-control is on
  Auto-MDIX on (operational: on)
```

```

ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 53000 bits/sec, 122 packets/sec
5 minute output rate 53000 bits/sec, 122 packets/sec
L3 in Switched: ucast: 37522 pkt, 752892 bytes - mcast: 0 pkt, 0 bytes <===== (A)
L3 out Switched: ucast: 37522 pkt, 752892 bytes - mcast: 0 pkt, 0 bytes <===== (B)
IPv6 L3 in Switched: ucast: 24328 pkt, 145968 bytes - mcast: 0 pkt, 0 bytes <==(C)
IPv6 L3 out Switched: ucast: 24328 pkt, 145968 bytes - mcast: 0 pkt, 0 bytes <==(D)
103639 packets input, 6632896 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 input packets with dribble condition detected
103674 packets output, 6641715 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out

```

以前の設定の出力は、カウンタの設定によって決まります（表 33-2 を参照）。

表 33-2 以前の設定で更新されるフィールドとカウンタの設定

カウンタの設定	更新されるフィールド
IPv4 のみ	(A) および (B) のみ
IPv6 のみ	(C) および (D) のみ
IPv4 と IPv6 の結合	(A) および (B) のみ
IPv4 および IPv6 を個別	IPv4 の場合 (A) および (B) IPv6 の場合 (C) および (D)

## 設定時の注意事項

Catalyst 4500 シリーズ スイッチは、AppleTalk ルーティングおよび IPX ルーティングをサポートします。AppleTalk ルーティングおよび IPX ルーティングについては、次の URL の『Cisco IOS AppleTalk and Novell IPX Configuration Guide』の「Configuring AppleTalk」および「Configuring Novell IPX」を参照してください。

[http://www.cisco.com/en/US/docs/ios/at/configuration/guide/12\\_4/atk\\_12\\_4\\_book.html](http://www.cisco.com/en/US/docs/ios/at/configuration/guide/12_4/atk_12_4_book.html)

[http://www.cisco.com/en/US/docs/ios/novipx/configuration/guide/config\\_novellipx\\_ps6350\\_TSD\\_Products\\_Configuration\\_Guide\\_Chapter.html](http://www.cisco.com/en/US/docs/ios/novipx/configuration/guide/config_novellipx_ps6350_TSD_Products_Configuration_Guide_Chapter.html)



(注)

Catalyst 4900M、Catalyst 4948E、Supervisor Engine 6-E、Supervisor Engine 6L-E、Supervisor Engine 7-E、および Supervisor Engine 7L-E は、AppleTalk および IPX ルーティングをサポートしません。

Catalyst 4500 シリーズ スイッチでは、サブインターフェイスも **encapsulation** キーワードもレイヤ 3 ファストイーサネット、ギガビットイーサネット、10 ギガビットイーサネットのインターフェイスではサポートされていません。



(注)

Cisco IOS ソフトウェアが稼働するすべてのレイヤ 3 インターフェイスと同様に、SVI に割り当てられる IP アドレスおよびネットワークは、スイッチ上の他のレイヤ 3 インターフェイスに割り当てられるものと重複できません。

## 論理レイヤ 3 VLAN インターフェイスの設定



(注)

論理レイヤ 3 VLAN インターフェイスを設定する前に、スイッチ上に VLAN を作成および設定し、レイヤ 2 インターフェイスに VLAN メンバーシップを割り当てる必要があります。また、IP ルーティングがディセーブルの場合は IP ルーティングをイネーブルにし、IP ルーティング プロトコルを指定する必要があります。

論理レイヤ 3 VLAN インターフェイスを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# <b>vlan</b> <i>vlan_ID</i>	VLAN を作成します。
ステップ 2	Switch(config)# <b>interface</b> <i>vlan</i> <i>vlan_ID</i>	設定するインターフェイスを選択します。
ステップ 3	Switch(config-if)# <b>ip address</b> <i>ip_address</i> <i>subnet_mask</i>	IP アドレスおよび IP サブネットを設定します。
ステップ 4	Switch(config-if)# <b>no shutdown</b>	インターフェイスをイネーブルにします。
ステップ 5	Switch(config-if)# <b>end</b>	コンフィギュレーション モードを終了します。
ステップ 6	Switch# <b>copy running-config startup-config</b>	設定の変更内容を不揮発性 RAM (NVRAM) に保存します。
ステップ 7	Switch# <b>show interfaces</b> [ <i>type slot/interface</i> ] Switch# <b>show ip interfaces</b> [ <i>type slot/interface</i> ] Switch# <b>show running-config interfaces</b> [ <i>type slot/interface</i> ] Switch# <b>show running-config interfaces</b> <i>vlan</i> <i>vlan_ID</i>	設定を確認します。

次に、論理レイヤ 3 VLAN インターフェイス VLAN 2 を設定し、IP アドレスを割り当てる例を示します。

```
Switch> enable
Switch# config term
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# vlan 2
Switch(config)# interface vlan 2
Switch(config-if)# ip address 10.1.1.1 255.255.255.248
Switch(config-if)# no shutdown
Switch(config-if)# end
```

次に、**show interfaces** コマンドを使用して、レイヤ 3 VLAN インターフェイス VLAN 2 のインターフェイス IP アドレスの設定およびステータスを表示する例を示します。

```
Switch# show interfaces vlan 2
Vlan2 is up, line protocol is down
  Hardware is Ethernet SVI, address is 00D.588F.B604 (bia 00D.588F.B604)
  Internet address is 172.20.52.106/29
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
```

```

ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  0 packets input, 0 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
  0 packets output, 0 bytes, 0 underruns
  0 output errors, 0 interface resets
  0 output buffer failures, 0 output buffers swapped out
Switch#

```

次に、**show running-config** コマンドを使用して、レイヤ 3 VLAN インターフェイス VLAN 2 のインターフェイス IP アドレスの設定を表示する例を示します。

```

Switch# show running-config
Building configuration...

Current configuration : !
interface Vlan2
 ip address 10.1.1.1 255.255.255.248
 !
 ip classless
 no ip http server
 !
 !line con 0
 line aux 0
 line vty 0 4
 !
end

```

## レイヤ 3 インターフェイスとしての VLAN の設定

ここでは、次の内容について説明します。

- 「SVI 自動ステート除外の設定」(P.33-7)
- 「IP 最大伝送単位 (MTU) サイズの設定」(P.33-9)
- 「レイヤ 3 インターフェイス カウンタの設定」(P.33-10)

### SVI 自動ステート除外の設定



(注) SVI 自動ステート除外機能は、デフォルトでイネーブルであり、STP ステートと同期しています。

SVI 自動ステート除外機能は、次のポート設定変更が発生した場合に、スイッチのレイヤ 3 インターフェイスのシャットダウン（または起動）を行います。

- VLAN 上の最後のポートがダウンすると、その VLAN 上のレイヤ 3 インターフェイスがシャットダウンします (SVI 自動ステート)。
- VLAN 上の最初のポートが立ち上がった状態に戻り、それまでシャットダウンしていた VLAN 上のレイヤ 3 インターフェイスが立ち上がる場合。

## ■ レイヤ 3 インターフェイスとしての VLAN の設定

SVI 自動ステート除外では、SVI のステータス（アップまたはダウン）を定義する際にアクセスポートおよびトランクを、それが同じ VLAN に属する場合でも除外できます。除外されたアクセスポートおよびトランクがアップ状態であり、VLAN 内の別のポートがダウン状態であるなら、SVI ステータスはダウンに変更されます。

SVI ステータスをアップ状態にするには、VLAN のうち少なくとも 1 つのポートがアップ状態で除外されていない必要があります。このアクションは、SVI ステータスの判定時にモニタリングポートステータスを除外するのに役立ちます。

SVI 自動ステート除外を適用するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# <b>interface interface-id</b>	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	Switch(config-if)# <b>switchport autostate exclude</b>	SVI のステータス（アップまたはダウン）を定義する際にアクセスポートとトランクを除外します。
ステップ 4	Switch(config)# <b>end</b>	コンフィギュレーション モードを終了します。
ステップ 5	Switch# <b>show run interface</b>	実行コンフィギュレーションを表示します。
ステップ 6	Switch# <b>show interface switchport</b>	設定を確認します。

次に、インターフェイス g3/1 に SVI 自動ステート除外を適用する例を示します。

```
Switch# conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface g3/1
Switch(config-if)# switchport autostate exclude
Switch(config-if)# end
Switch# show run int g3/4
Building configuration...

Current configuration : 162 bytes
!
interface GigabitEthernet3/4
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,3
 switchport autostate exclude
 switchport mode trunk
end

Switch# show int g3/4 switchport
Name: Gi3/4
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On Access Mode VLAN: 1 (default) Trunking Native Mode VLAN: 1
(default) Administrative Native VLAN tagging: enabled Voice VLAN: none Administrative
private-vlan host-association: none Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none Administrative private-vlan trunk
Native VLAN tagging: enabled Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none Administrative private-vlan trunk
associations: none Administrative private-vlan trunk mappings: none Operational
private-vlan: none Trunking VLANs Enabled: 2,3 Pruning VLANs Enabled: 2-1001 Capture Mode
Disabled Capture VLANs Allowed: ALL
Autostate mode exclude
```



```
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
Switch#
```

## IP 最大伝送単位 (MTU) サイズの設定

インターフェイスから送信された IPv4 パケットまたは IPv6 パケットの最大伝送単位 (MTU) サイズをプロトコルごとに設定できます。

MTU の制限事項については、「最大伝送単位」(P.27) を参照してください。



(注) インターフェイスにプロトコルに限定されない MTU 値を設定するには、**mtu** インターフェイス コンフィギュレーション コマンドを使用します。MTU 値の (**mtu** インターフェイス コンフィギュレーション コマンドを使用した) 変更は、IP MTU 値に影響を与えます。IP MTU 値と MTU 値が一致しているときに MTU 値を変更すると、IP MTU 値が新しい MTU と一致するよう自動的に変更されます。ただし、逆の場合は同様ではありません。IP MTU 値を変更しても **mtu** コマンドの値には影響がありません。

MTU サイズの設定については、「MTU サイズの設定」(P.28) を参照してください。

インターフェイスから送信された IPv4 パケットまたは IPv6 パケットの最大伝送単位 (MTU) サイズをプロトコルごとに設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# <b>interface interface-id</b>	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	Switch(config-if)# [no] <b>ip mtu mtu_size</b> or Switch(config-if)# [no] <b>ipv6 mtu mtu_size</b>	IPv4 MTU サイズを設定します。  IPv6 MTU サイズを設定します。  このコマンドの <b>no</b> 形式を使用すると、デフォルトの MTU サイズ (1500 バイト) に戻ります。
ステップ 4	Switch(config-if)# <b>exit</b>	インターフェイス コンフィギュレーション モードを終了します。
ステップ 5	Switch(config)# <b>end</b>	コンフィギュレーション モードを終了します。
ステップ 6	Switch# <b>show run interface interface-id</b>	実行コンフィギュレーションを表示します。

次の例では、インターフェイスに IPv4 MTU を設定する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.End with CNTL/Z.
Switch(config)# interface vlan 1
Switch(config-if)# ip mtu 68
Switch(config-if)# exit
Switch(config)# end
Switch# show ip interface vlan 1
Vlan1 is up, line protocol is up
  Internet address is 10.10.10.1/24
  Broadcast address is 255.255.255.255
```

## ■ レイヤ 3 インターフェイスとしての VLAN の設定

```

Address determined by setup command
MTU is 68 bytes
Helper address is not set
.....(continued)

```

次に、インターフェイスで IPv6 MTU を設定する例を示します。

```

Switch# configure terminal
Enter configuration commands, one per line.End with CNTL/Z.
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 mtu 1280
Switch(config)# end

```

次に、設定を確認する例を示します。

```

Switch# show ipv6 interface vlan 1
Vlan1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::214:6AFF:FEBC:DEEA
Global unicast address(es):
  1001::1, subnet is 1001::/64
Joined group address(es):
  FF02::1
  FF02::1:FF00:1
  FF02::1:FFBC:DEEA
MTU is 1280 bytes
.....(continued)

```



(注)

いずれかの CLI コマンドを使用して IPv6 がインターフェイス上でイネーブルにされている場合、次のメッセージが表示されることがあります。

```
% Hardware MTU table exhausted
```

この場合、ハードウェアでプログラムされている IPv6 MTU 値は、IPv6 インターフェイス MTU 値とは異なります。この状況は、追加の値を保存する余裕がハードウェア MTU テーブルにない場合に発生します。使用していない MTU 値の設定を解除することでテーブル内のスペースを空けてから、インターフェイスで IPv6 をディセーブルにして再度イネーブルにするか、MTU 設定を再度適用します。

## レイヤ 3 インターフェイス カウンタの設定



(注)

Catalyst 4900M、Catalyst 4948E、Supervisor Engine 6-E、Supervisor Engine 6L-E、Supervisor Engine 7-E、および Supervisor Engine 7L-E は、レイヤ 2 インターフェイス カウンタをサポートしません。

レイヤ 3 インターフェイス カウンタを設定する（カウンタをレイヤ 3 インターフェイスに割り当てる）には、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# <b>interface interface-id</b>	インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	Switch(config-if)# <b>counter</b> { <b>ipv4</b>   <b>ipv6</b>   <b>ipv4 ipv6 separate</b> }>	<p>カウンタをイネーブルにします。</p> <p><b>counter</b> : IPv4 および IPv6 統計情報の収集をイネーブルにして合計として表示します</p> <p><b>counter ipv4</b> : IPv4 統計情報のみの収集をイネーブルにします</p> <p><b>counter ipv6</b> : IPv6 統計情報のみの収集をイネーブルにします</p> <p><b>counter ipv4 ipv6 separate</b> : IPv4 および IPv6 統計情報の収集をイネーブルにして個別に表示します</p>
ステップ 4	Switch(config)# <b>end</b>	コンフィギュレーション モードを終了します。
ステップ 5	Switch# <b>show run interface</b> <i>interface-id</i>	実行コンフィギュレーションを表示します。

次に、インターフェイス VLAN 1 のカウンタをイネーブルにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.End with CNTL/Z.
Switch(config)# interface vlan 1
Switch(config-if)# counter ipv4
Switch(config-if)# end
Switch#
00:17:15: %SYS-5-CONFIG_I: Configured from console by console
Switch# show run interface vlan 1
Building configuration...

Current configuration : 63 bytes
!
interface Vlan1
 ip address 10.0.0.1 255.0.0.0
 counter ipv4
end
```



(注) カウンタを削除するには、**no counter** コマンドを使用します。

すでにカウンタの最大数を割り当てている場合は、**counter** コマンドは失敗し、エラーメッセージが表示されます。

```
Switch# config terminal
Enter configuration commands, one per line.End with CNTL/Z.
Switch(config)# interface fa3/2
Switch(config-if)# no switchport
Switch(config-if)# counter ipv6
Counter resource exhausted for interface fa3/2
Switch(config-if)# end
Switch#
00:24:18: %SYS-5-CONFIG_I: Configured from console by console
```

この場合、別のインターフェイスのカウンタを解放して新しいインターフェイスが使用できるようにする必要があります。

# 物理レイヤ 3 インターフェイスの設定



(注)

物理レイヤ 3 インターフェイスを設定する前に、IP ルーティングがディセーブルの場合は IP ルーティングをイネーブルにし、IP ルーティングプロトコルを指定する必要があります。

物理層 3 インターフェイスを設定するには、次の作業を行います。

コマンド	目的
ステップ 1 Switch(config)# <b>ip routing</b>	IP ルーティングをイネーブルにします (ディセーブルになっている場合のみ必要)。
ステップ 2 Switch(config)# <b>interface</b> {fastethernet   gigabitethernet   tengigabitethernet} slot/port}   {port-channel port_channel_number}	設定するインターフェイスを選択します。
ステップ 3 Switch(config-if)# <b>no switchport</b>	このポートを物理レイヤ 2 ポートから物理レイヤ 3 ポートに変換します。
ステップ 4 Switch(config-if)# <b>ip address</b> ip_address subnet_mask	IP アドレスおよび IP サブネットを設定します。
ステップ 5 Switch(config-if)# <b>no shutdown</b>	インターフェイスをイネーブルにします。
ステップ 6 Switch(config-if)# <b>end</b>	コンフィギュレーション モードを終了します。
ステップ 7 Switch# <b>copy running-config startup-config</b>	設定の変更内容を不揮発性 RAM (NVRAM) に保存します。
ステップ 8 Switch# <b>show interfaces</b> [type slot/interface] Switch# <b>show ip interfaces</b> [type slot/interface] Switch# <b>show running-config interfaces</b> [type slot/interface]	設定を確認します。

次に、ファストイーサネット インターフェイス 2/1 に IP アドレスを設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# interface fastethernet 2/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.1.1.1 255.255.255.248
Switch(config-if)# no shutdown
Switch(config-if)# end
Switch#
```

次に、**show running-config** コマンドを使用して、ファストイーサネット インターフェイス 2/1 のインターフェイス IP アドレスの設定を表示する例を示します。

```
Switch# show running-config
Building configuration...
!
interface FastEthernet2/1
  no switchport
  ip address 10.1.1.1 255.255.255.248
!
...
ip classless
no ip http server
!
!
```

```
line con 0
line aux 0
line vty 0 4
!
end
```

## EIGRP スタブ ルーティングの設定

ここでは、次の内容について説明します。

- 「EIGRP スタブ ルーティングについて」(P.33-13)
- 「EIGRP スタブ ルーティングの設定」(P.33-14)
- 「EIGRP のモニタリングおよびメンテナンス」(P.33-20)
- 「EIGRP の設定例」(P.33-20)

## EIGRP スタブ ルーティングについて

EIGRP スタブ ルーティング機能は、すべてのイメージで使用でき、エンド ユーザの近くにルーテッドトラフィックを移動することでリソースの利用率を低減させます。

IP ベース イメージには EIGRP スタブ ルーティングだけが含まれています。IP サービス イメージには、完全な EIGRP ルーティングが含まれています。

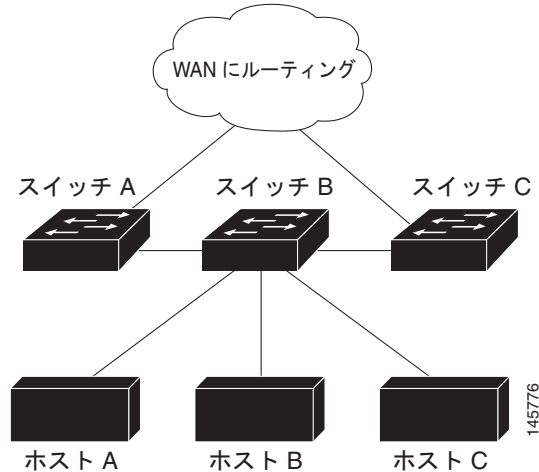
EIGRP スタブ ルーティングを使用するネットワークでは、IP トラフィックがユーザに到達するには、ルート EIGRP スタブ ルーティングを設定しているスイッチを通過する必要があります。スイッチは、ユーザ インターフェイスとして設定されているインターフェイスまたは他のデバイスに接続されているインターフェイスにルーテッドトラフィックを送信します。

EIGRP スタブ ルーティングを使用する場合、EIGRP を使用するよう、ディストリビューション スイッチおよびリモート スイッチを設定し、さらにスイッチだけをスタブとして設定する必要があります。指定したルートだけがスイッチから伝播されます。スイッチは、サマリー、接続ルート、およびルーティング アップデートに対するすべてのクエリーに応答します。

スタブであることを通知するパケットを受信するネイバーは、スタブ スイッチに対してルートのクエリーを実行せず、スタブ ピアを持つスイッチはそのピアに対するクエリーを実行しません。スタブ スイッチは、ディストリビューション スイッチによってすべてのピアに適切なアップデートを送信します。

図 33-3 では、スイッチ B が EIGRP スタブ スイッチとして設定されています。スイッチ A および C は残りの WAN に接続されています。スイッチ B は、接続ルート、スタティック ルート、再配布ルート、集約ルートをスイッチ A および C からホスト A、B、および C にアドバタイズします。スイッチ B は、スイッチ A から学習したルートをアドバタイズしません（逆の場合も同様です）。

図 33-3 EIGRP スタブ スイッチの構成



EIGRP スタブ ルーティングの詳細については、『Cisco IOS IP Configuration Guide, Volume 2 of 3: Routing Protocols, Release 12.2』の「Configuring EIGRP Stub Routing」を参照してください。

## EIGRP スタブ ルーティングの設定

EIGRP スタブ ルーティング機能は、ネットワークの安定性を高め、リソース利用率を抑え、スタブ スイッチ構成を簡素化します。

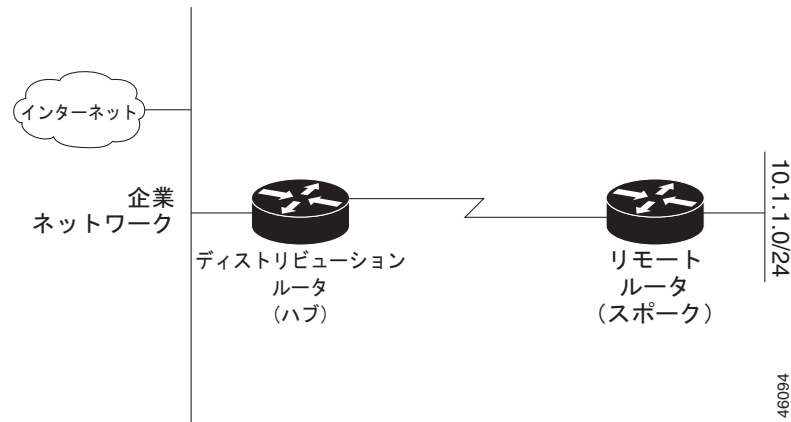
スタブ ルーティングは、一般的に、ハブ アンド スポーク型のネットワーク トポロジで使用されます。ハブ アンド スポーク ネットワークでは、1 つ以上のエンド (スタブ) ネットワークが 1 台のリモート スイッチ (スポーク) に接続され、そのリモート ルータは 1 つ以上のディストリビューション スイッチ (ハブ) に接続されています。リモート スイッチは 1 つまたは複数のディストリビューション スイッチにのみ隣接します。IP トラフィックがリモート スイッチに到達する唯一のルートは、ディストリビューション スイッチを経由するものです。このタイプの構成は、一般的に、ディストリビューション スイッチが直接 WAN に接続している WAN トポロジで使用されています。ディストリビューション スイッチは多くのリモート スイッチに接続できます。ディストリビューションが 100 台以上のリモート ルータに接続されていることがよくあります。ハブ アンド スポーク型トポロジでは、リモート ルータがすべての非ローカルトラフィックをディストリビューション ルータに転送する必要があります。これにより、リモート ルータが完全なルーティング テーブルを保持する必要はなくなります。一般に、ディストリビューション ルータはデフォルト ルート以外の情報をリモート ルータに送信する必要はありません。

EIGRP スタブ ルーティング機能を使用する場合、EIGRP を使用するように、ディストリビューション ルータおよびリモート ルータを設定し、さらにリモート ルータだけをスタブとして設定する必要があります。指定されたルートのみが、リモート (スタブ) ルータから伝播されます。スタブ ルータは、サマリー、接続ルート、再配布されたスタティック ルート、外部ルート、内部ルートに対するクエリーのすべてに、「アクセスできない」メッセージで対応します。スタブとして設定されたルータは、すべての隣接ルータに特別なピア情報パケットを送信して、自身のスタブ ルータとしての状態を報告します。

スタブ ルータの状態を通知するパケットを受信した隣接ルータは、ルートについてはスタブ ルータに照会しません。また、スタブ ピアを持つルータは、そのピアについては照会しません。スタブ ルータは、ディストリビューション ルータに依存して適切なアップデートをすべてのピアに送信します。

図 33-4 は、単純なハブ アンド スポーク型設定を示します。

図 33-4 単純なハブ アンド スポーク ネットワーク



スタブ ルーティング機能は、ルートがリモート ルータにアドバタイズされるのを防ぐことはありません。図 33-4 の例では、リモート ルータはディストリビューション ルータだけを使用して企業ネットワークおよびインターネットにアクセスできます。この例では、企業ネットワークとインターネットへのパスが常にディストリビューション ルータを使用するため、リモート ルータ上に完全なルート テーブルを持つことに何の意味もありません。より大きいルート テーブルでは、リモート ルータに必要なメモリ量が減るだけです。帯域幅とメモリは、ディストリビューション ルータのルートを集約およびフィルタリングすることによって節約できます。リモート ルータは、宛先に関わりなく、ディストリビューション ルータにすべての非ローカル トラフィックを送信する必要があるため、他のネットワークから学習されたルートを受け取る必要がありません。真のスタブ ネットワークが望ましい場合、ディストリビューション ルータはリモート ルータにデフォルト ルートだけを送信するように設定する必要があります。EIGRP スタブ ルーティング機能では、ディストリビューション ルータでのサマライズは自動的にイネーブルにされません。ほとんどの場合、ネットワーク管理者が、ディストリビューション ルータにサマライズを設定する必要があります。



(注)

ディストリビューション ルータがリモート ルータにデフォルト ルートだけを送信するように設定する場合、リモート ルータで **ip classless** コマンドを使用する必要があります。デフォルトでは、**ip classless** コマンドは、EIGRP スタブ ルーティング機能をサポートするすべての Cisco IOS イメージでイネーブルになっています。

スタブ機能がない場合、ディストリビューション ルータからリモート ルータに送信されたルートがフィルタリングまたはサマライズされた後でも、問題が発生することがあります。企業ネットワーク内でルートが失われると、EIGRP はクエリーをディストリビューション ルータに送信することがあります。ルートがサマライズされている場合でも、ディストリビューション ルータが代わりにリモート ルータにクエリーを送信します。WAN リンクを使用したディストリビューション ルータとリモート ルータ間の通信に問題がある場合、EIGRP Stuck In Active (SIA) 状態が発生し、ネットワークのどこかで不安定になる可能性があります。EIGRP スタブ ルーティング機能を使用すると、ネットワーク管理者は、クエリーがリモート ルータに送信されないようにできます。

## デュアルホーム接続リモート トポロジ

リモート ルータを単一のディストリビューション ルータに接続する簡単なハブ アンド スポーク型ネットワーク以外に、リモート ルータを複数のディストリビューション ルータにデュアルホーム接続できます。この構成では冗長性が増し、一意性の問題が生じますが、スタブ機能がこれらの問題の対処に役立ちます。

デュアルホーム接続リモート ルータには、複数のディストリビューション ルータ（ハブ）が組み込まれています。ただし、スタブルルーティングの原理はハブアンドスポーク型トポロジの場合と同じです。図 33-5 にリモート ルータを 1 つ使用した一般的なデュアルホーム接続リモート トポロジを示していますが、ディストリビューション ルータ 1 とディストリビューション ルータ 2 の同じインターフェイスに 100 以上のルータを接続できます。リモート ルータは、その宛先に到達するために最適なルートを使用します。ディストリビューション ルータ 1 に障害が発生した場合、リモート ルータはディストリビューション ルータ 2 を使用して企業ネットワークに到達できます。

図 33-5 単純なデュアルホーム接続リモート トポロジ

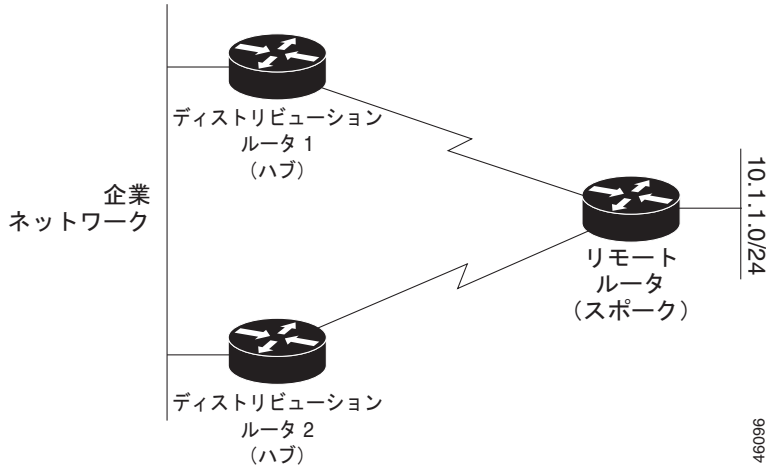


図 33-5 に、リモート ルータ 1 つとディストリビューション ルータ 2 つから構成される簡単なデュアルホーム接続リモートを示します。いずれのディストリビューション ルータも企業ネットワークとスタブ ネットワーク 10.1.1.0/24 へのルートを維持します。

デュアルホーム接続ルーティングによって、EIGRP ネットワークが不安定になる場合があります。

図 33-6 では、ディストリビューション ルータ 1 はネットワーク 10.3.1.0/24 に直接接続しています。ディストリビューション ルータ 1 上で集約またはフィルタリングが適用された場合は、そのルータが、直接接続されているすべての EIGRP ネイバー（ディストリビューション ルータ 2 とリモート ルータ）にネットワーク 10.3.1.0/24 をアドバタイズします。



図 33-6 ディストリビューションルータ 1 を 2 つのネットワークに接続したデュアルホーム接続リモートトポロジ

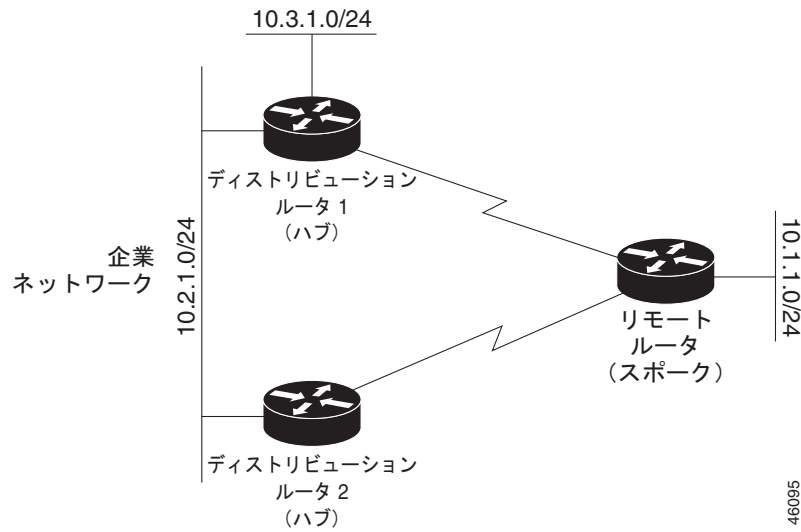
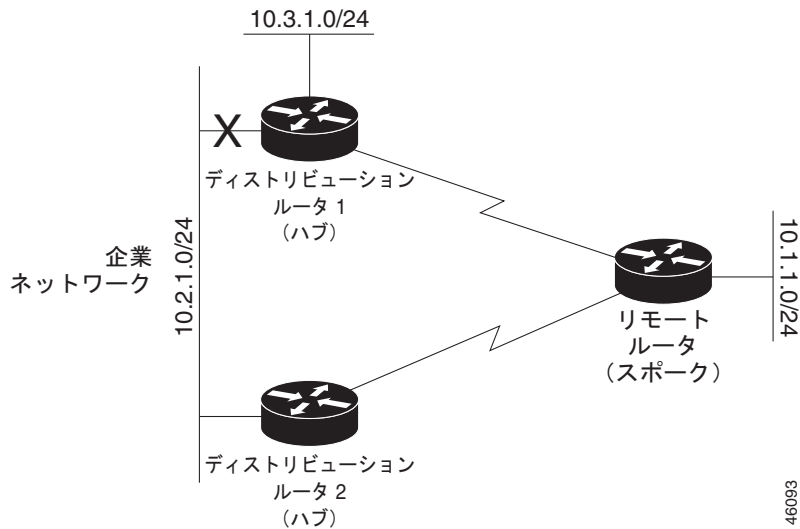


図 33-6 に、ディストリビューションルータ 1 をネットワーク 10.3.1.0/24 とネットワーク 10.2.1.0/24 の両方に接続した単純なデュアルホーム接続リモートルータを示します。

ディストリビューションルータ 1 とディストリビューションルータ 2 間の 10.2.1.0/24 リンクに障害が発生した場合、ディストリビューションルータ 2 からネットワーク 10.3.1.0/24 までの最低コストパスはリモートルータの使用です (図 33-7 を参照)。それまで企業ネットワーク 10.2.1.0/24 を通過していたトラフィックが、今度は帯域幅の非常に低い接続に送信されるため、このルートは望ましくありません。低帯域幅 WAN 接続の利用率が高くなりすぎると、企業ネットワーク全体に影響するような多くの問題の原因になります。リモートルータを使用して通過する低帯域幅ルートの利用によって、WAN EIGRP ディストリビューションルータがドロップする場合があります。ディストリビューションおよびリモートルータのシリアル回線もドロップし、ディストリビューションおよびコアルータで EIGRP SIA エラーが発生する可能性があります。

図 33-7 ディストリビューション ルータへのルートに障害が発生したデュアルホーム接続リモート トポロジ



ディストリビューション ルータ 2 からのトラフィックがネットワーク 10.3.1.0/24 に到達するために、リモート ルータを通過するのは望ましくありません。リンクが負荷を処理できるサイズであれば、バックアップ ルートの 1 つを使用することもできます。ただし、このタイプのほとんどのネットワークは、リモート ルータをリンク速度が比較的遅いリモート オフィスに配置しています。この問題は、ディストリビューション ルータとリモート ルータで適切な集約が設定されていれば防ぐことができます。

通常、ディストリビューション ルータからのトラフィックが中継パスとしてリモート ルータを使用するのは不適切です。ディストリビューション ルータからリモート ルータへの一般的な接続は、ネットワーク コアにおける接続よりも帯域幅が相当低くなります。中継パスとして接続帯域幅に限りがあるリモート ルータを使用した場合、一般にリモート ルータに過度の輻輳が生じます。EIGRP スタブルルーティング機能は、リモート ルータがディストリビューション ルータにコア ルートをアドバタイズしないようにしてこの問題を防ぎます。ディストリビューション ルータ 1 を通じてリモート ルータが学習したルートは、ディストリビューション ルータ 2 にアドバタイズされません。リモート ルータはディストリビューション ルータ 2 にコア ルートをアドバタイズしないため、ディストリビューション ルータはネットワーク コアに向けられたトラフィック用の中継点としてリモート ルータを使用しません。

EIGRP スタブルルーティング機能は、ネットワークの安定性を高めるのに役立ちます。ネットワークが不安定になったときに、EIGRP クエリーが非中継ルータへの制限された帯域幅リンクを介して送信されるのを防ぎます。代わりに、スタブルルータの接続先のディストリビューション ルータがスタブルルータに代わってクエリーに応答します。この機能により、輻輳している、または問題のある WAN リンクによってネットワークが不安定になる可能性が低減されます。また EIGRP スタブルルーティング機能は、ハブアンドスポーク型ネットワークの設定とメンテナンスを簡易化します。スタブルルーティングをデュアルホーム接続のリモート設定でイネーブルにすると、リモート ルータがハブ ルータへの中継パスとして表示されないようにリモート ルータでフィルタリングを設定する必要がなくなります。



#### 注意

EIGRP スタブルルーティングはスタブルルータだけで使用します。スタブルルータは、コアトラフィックが通過しない、ネットワーク コアまたはディストリビューション レイヤに接続されたルータです。スタブルルータがディストリビューション ルータ以外の EIGRP ネイバーを持つことはできません。この制限を無視すると、望ましくない動作が発生します。



(注) ATM、イーサネット、フレーム リレー、ISDN PRI、X.25 などのマルチアクセス インターフェイスは、そのインターフェイス上のすべてのルータ（ハブ以外）がスタブ ルータとして設定されている場合にだけ、EIGRP スタブ ルーティング機能によってサポートされます。

## EIGRP スタブ ルーティングの設定作業

ここでは、EIGRP スタブ ルーティングを設定するために実行する作業について説明します。最初に説明する作業は必須で、最後の作業は任意です。

- [EIGRP スタブ ルーティングの設定](#)（必須）
- [EIGRP スタブ ルーティングの確認](#)（任意）

### EIGRP スタブ ルーティングの設定

EIGRP スタブ ルーティングのリモート ルータまたはスポーク ルータを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# <b>router eigrp 1</b>	EIGRP プロセスを実行するリモート ルータまたはディストリビューション ルータを設定します。
ステップ 2	Switch(config-router)# <b>network network-number</b>	EIGRP ディストリビューション ルータのネットワーク アドレスを指定します。
ステップ 3	Switch(config-router)# <b>eigrp stub [receive-only   connected   static   summary   redistributed]</b>	<p>リモート ルータを EIGRP スタブ ルータとして設定します。</p> <p><b>receive-only</b> キーワードは、受信専用ネイバーとしてルータを設定します。</p> <p><b>connected</b> キーワードは、接続されたルートをアドバタイズします。</p> <p><b>static</b> キーワードは、スタティック ルートをアドバタイズします。</p> <p><b>summary</b> キーワードは、サマリー ルートをアドバタイズします。</p> <p><b>redistributed</b> キーワードは、他のダイナミック ルーティング プロトコルから再配布されたルートを送信できるようにします。</p> <p>(注) <b>redistribute</b> コマンドで他のルーティング プロセスからルートを再配布する必要があります。</p>

### EIGRP スタブ ルーティングの確認

リモート ルータが、EIGRP でのスタブ ルータとして設定されていることを確認するには、特権 EXEC モードのディストリビューション ルータから **show ip eigrp neighbor detail** コマンドを使用します。出力の最後の行は、リモート ルータまたはスポーク ルータのスタブ ステータスを示します。次の例は、**show ip eigrp neighbor detail** コマンドの出力を示します。

```
Switch# show ip eigrp neighbor detail
```

## ■ EIGRP スタブルルーティングの設定

```

IP-EIGRP neighbors for process 1
H   Address                Interface    Hold Uptime    SRTT   RTO  Q  Seq Type
                               (sec)          (ms)          Cnt  Num
0   10.1.1.2                Se3/1       11 00:00:59   1  4500  0  7
Version 12.1/1.2, Retrans: 2, Retries: 0
Stub Peer Advertising ( CONNECTED SUMMARY ) Routes

```

## EIGRP のモニタリングおよびメンテナンス

ネイバー テーブルからネイバーを削除するには、次のコマンドを使用します。

コマンド	目的
Switch# <b>clear ip eigrp neighbors</b> [ <i>ip-address</i>   <i>interface</i> ]	ネイバー テーブルからネイバーを削除します。

各種のルーティング統計情報を表示するには、次のコマンドを使用します。

コマンド	目的
Switch# <b>show ip eigrp interfaces</b> [ <i>interface</i> ] [ <i>as-number</i> ]	EIGRP に設定されているインターフェイスに関する情報を表示します。
Switch# <b>show ip eigrp neighbors</b> [ <i>type number static</i> ]	EIGRP によって検出されたネイバーを表示します。
Switch# <b>show ip eigrp topology</b> [ <i>autonomous-system-number</i>   [[ <i>ip-address</i> ] <i>mask</i> ]]	指定されたプロセスの EIGRP トポロジ テーブルを表示します。
Switch# <b>show ip eigrp traffic</b> [ <i>autonomous-system-number</i> ]	すべてまたは指定された EIGRP プロセスの送受信パケット数を表示します。

## EIGRP の設定例

ここでは、次の例を示します。

- [ルート集約の例](#)
- [ルート認証の例](#)
- [スタブルルーティングの例](#)

### ルート集約の例

次に、自動サマライズをディセーブルにして、EIGRP がネットワーク 10.0.0.0 をイーサネット インターフェイス 0 のみに集約する例を示します。

```

interface Ethernet 0
 ip summary-address eigrp 1 10.0.0.0 255.0.0.0
!
router eigrp 1
 network 172.16.0.0
 no auto-summary

```



(注)

**ip summary-address eigrp** コマンドを使用してインターフェイスからのデフォルト ルート (0.0.0.0) を生成しないでください。アドミニストレーティブ ディスタンス 5 で null 0 インターフェイスに対して、EIGRP サマリー デフォルト ルートが作成されるからです。このデフォルト ルートのアドミニストレーティブ ディスタンスの値が小さいと、ルーティング テーブル内の他のネイバーから学習されたデフォルト ルートにこのルートが置き換えられてしまうことがあります。ネイバーから学習されたデフォルト ルートがサマリー デフォルト ルートによって置き換えられた場合、またはサマリー ルートが唯一のデフォルト ルートの場合、デフォルト ルートを宛先とするトラフィックすべてがルータから出るわけではありません。代わりに、このトラフィックは null 0 インターフェイスに送信されて、そこでドロップされます。

所定のインターフェイスからのデフォルト ルートだけを送信するようにするには、**distribute-list** コマンドを使用することを推奨します。このコマンドを設定して、インターフェイスから送信されるデフォルト (0.0.0.0) 以外のすべての発信ルート アドバタイズメントをフィルタリングできます。

## ルート認証の例

次の例では、自律システム 1 で EIGRP パケットの MD5 認証をイネーブルにします。

### ルータ A

```
interface ethernet 1
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 holly
key chain holly
 key 1
  key-string 0987654321
  accept-lifetime 04:00:00 Dec 4 1996 infinite
  send-lifetime 04:00:00 Dec 4 1996 04:48:00 Dec 4 1996
 exit
 key 2
  key-string 1234567890
  accept-lifetime 04:00:00 Dec 4 1996 infinite
  send-lifetime 04:45:00 Dec 4 1996 infinite
```

### ルータ B

```
interface ethernet 1
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 mikel
key chain mikel
 key 1
  key-string 0987654321
  accept-lifetime 04:00:00 Dec 4 1996 infinite
  send-lifetime 04:00:00 Dec 4 1996 infinite
 exit
 key 2
  key-string 1234567890
  accept-lifetime 04:00:00 Dec 4 1996 infinite
  send-lifetime 04:45:00 Dec 4 1996 infinite
```

ルータ A は、キー 1 のすべての EIGRP パケットを受け取り、MD5 ダイジェストの確認を試みます。また、キー 2 のパケットも受け取ります。その他の MD5 パケットはすべてドロップされます。ルータ A は、キー 2 を含むすべての EIGRP パケットを送信します。

ルータ B は、キー 1 またはキー 2 を受け取って、キー 1 を送信します。このシナリオでは、MD5 が認証します。

## スタブ ルーティングの例

**eigrp stub** コマンドでスタブとして設定されたルータは、デフォルトで接続および集約ルーティング情報をすべての隣接ルータと共有します。この動作を変更する場合、**eigrp stub** コマンドで 4 つのオプション キーワードを使用できます。

- receive-only
- connected
- static
- summary

ここでは、**eigrp stub** コマンドのすべての形式の設定例を示します。**eigrp stub** コマンドはいくつかのオプションを指定して変更できます。これらのオプションは、**receive-only** キーワードを除いて、どのような組み合わせも可能です。**receive-only** キーワードは、ルータがその EIGRP 自律システム内の他のルータとどのルートも共有しないように制限します。また、**receive-only** キーワードは、あらゆる種類のルートの送信を阻止するため、他のオプションと併用できません。他の 3 つのオプション キーワード (**connected**、**static**、および **summary**) は、どのように組み合わせても使用できますが、**receive-only** キーワードと一緒に使用できません。この 3 つのキーワードのいずれかを **eigrp stub** コマンドで使用した場合は、接続ルートと集約ルートが自動的に送信されません。

**connected** キーワードは、EIGRP スタブ ルーティング機能による接続ルートの送信を許可します。接続ルートがネットワーク文で扱われない場合、EIGRP プロセスで **redistribute connected** コマンドを使用して接続ルートを再配布する必要が生じる場合があります。このオプションは、デフォルトでイネーブルです。

**static** キーワードは、EIGRP スタブ ルーティング機能によるスタティック ルートの送信を許可します。**static** キーワードを指定しない場合、EIGRP は、通常は自動的に再配布される内部スタティック ルートを含むスタティック ルートを送信しません。**redistribute static** コマンドを使用してスタティック ルートを再配布する必要もあります。

**summary** キーワードは、EIGRP スタブ ルーティング機能によるサマリー ルートの送信を許可します。集約ルートは、**summary address** コマンドを使用して手動で作成することもでき、**auto-summary** コマンドをイネーブルにしてメジャー ネットワークの境界ルータで自動的に作成することもできます。このオプションは、デフォルトでイネーブルです。

次に、接続および集約ルートをアドバタイズするスタブとしてルータを設定するために **eigrp stub** コマンドが使用する例を示します。

```
router eigrp 1
network 10.0.0.0
eigrp stub
```

次に、接続およびスタティック ルート（集約ルートの送信は禁止）をアドバタイズするスタブとしてルータを設定するために **eigrp stub connected static** コマンドを使用する例を示します。

```
router eigrp 1
network 10.0.0.0
eigrp stub connected static
```

次に、ルータをスタブとして設定するために **eigrp stub receive-only** コマンドを使用する例を示します。この設定では、接続、集約、またはスタティック ルートは送信されません。

```
router eigrp 1
network 10.0.0.0 eigrp
stub receive-only
```

次に、再配布されたルート（接続、スタティック、または集約ルートの送信は禁止）をアドバタイズするスタブとしてルータを設定するために **eigrp stub redistributed** コマンドを使用する例を示します。

```
router eigrp 1
```

```
network 10.0.0.0
eigrp stub redistributed
```

次に、再配布された、スタティック、接続および集約ルートをアドバタイズするスタブとしてルータを設定するために **eigrp stub** コマンドを使用する例を示します。

```
router eigrp 1
network 10.0.0.0
eigrp stub connected static summary redistributed
```

