



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 インターフェイスの概要」 (P.30-1)
- 「設定時の注意事項」 (P.30-4)
- 「論理レイヤ 3 VLAN インターフェイスの設定」 (P.30-5)
- 「レイヤ 3 インターフェイスとしての VLAN の設定」 (P.30-6)
- 「物理レイヤ 3 インターフェイスの設定」 (P.30-11)
- 「Enhanced Interior Gateway Routing Protocol (EIGRP) スタブルーティングの設定」 (P.30-12)



(注)

この章のスイッチ コマンドの構文および使用方法の詳細については、『*Catalyst 4500 Series Switch Cisco IOS Command Reference*』および次の URL の関連マニュアルを参照してください。

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

レイヤ 3 インターフェイスの概要

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.30-2)
- 「物理レイヤ 3 インターフェイス」 (P.30-2)
- 「Switched Virtual Interface (SVI; スイッチ仮想インターフェイス) 自動ステート除外の概要」 (P.30-3)
- 「レイヤ 3 インターフェイス カウンタの概要」 (P.30-3)

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。

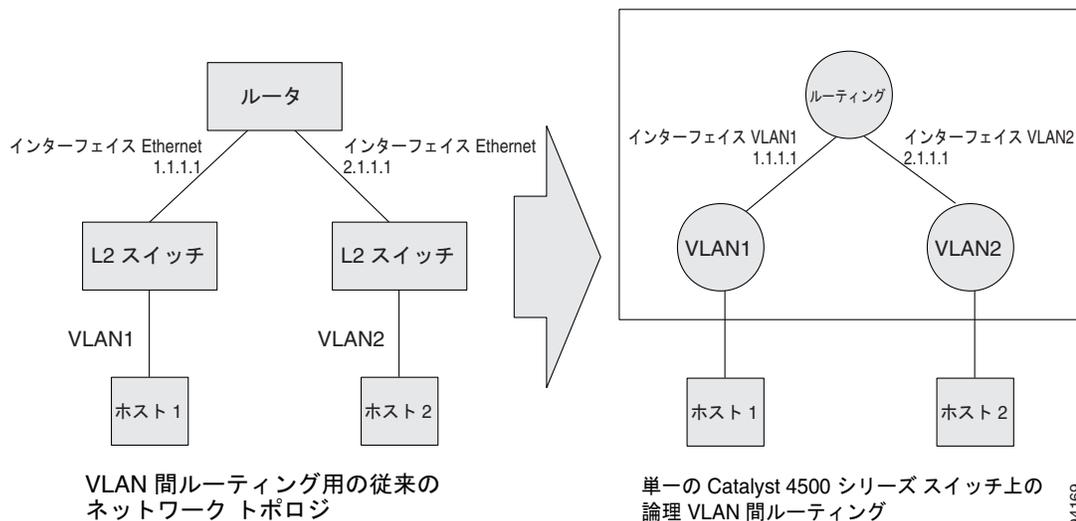
Catalyst 4500 シリーズ スイッチは、2 種類のレイヤ 3 インターフェイスをサポートしています。論理レイヤ 3 Virtual LAN (VLAN; 仮想 LAN) インターフェイスは、ルーティングとブリッジングの機能を統合します。Catalyst 4500 シリーズ スイッチは、物理レイヤ 3 インターフェイスを使用して従来のルータのように設定できます。

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 30-1 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 30-1 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

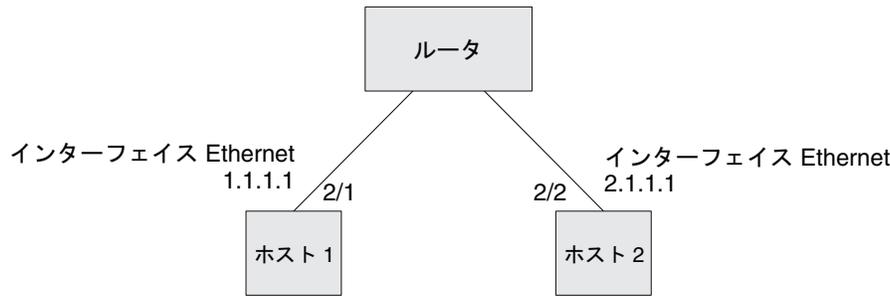


物理レイヤ 3 インターフェイス

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 30-2 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 30-2 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

Switched Virtual Interface (SVI; スイッチ仮想インターフェイス) 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 リンクに属する最初のスイッチポートがアップになり、スパニングツリー フォワーディング ステートとなると、VLAN インターフェイスのプロトコル ライン ステートがアップになります。

通常、VLAN 内に VLAN インターフェイスのポートが複数ある場合は、VLAN 内のすべてのポートが「ダウン」するときに SVI が「ダウン」します。SVI 自動ステート除外機能は、SVI の「アップおよびダウン」カウント時にカウントしないポートをマーキングするノブになり、ポートでイネーブルであるすべての VLAN に適用されます。

VLAN インターフェイスは、レイヤ 2 ポートがコンバージェンス (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に移行) する時間を経過した後、起ち上がります。これにより、ルーティング プロトコルおよびその他の機能が VLAN インターフェイスをフル稼働させるまで使用しないようにします。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)

Supervisor Engine 6-E は、レイヤ 2 インターフェイス カウンタをサポートしていません。Supervisor Engine 6-E は、レイヤ 3 (SVI) インターフェイス カウンタをサポートしています。

Supervisor Engine 6-E では、IP Version 4 (IPv4; IP バージョン 4) パケットおよび IP Version 6 (IPv6; IP バージョン 6) パケットはハードウェア転送エンジンによりルーティングされます。このエンジンは、最大 4095 個のインターフェイスについてルーティングされたパケットのカウンターの統計情報をサポートします。この統計は、次のカウンタが含まれます。

- 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

各種のカウンタについて、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。

サポートされるカウンタの合計数が、サポートされるレイヤ 3 インターフェイスの合計数より少ないため、レイヤ 3 インターフェイスのカウンタがなくなる場合もあります。そのため、ユーザがレイヤ 3 インターフェイスにカウンタを割り当てると、あるレイヤ 3 インターフェイスのデフォルト設定にはカウンタがなくなります。



(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** コマンドを発行する必要があります。レイヤ 3 インターフェイス カウンタを設定する手順については、「レイヤ 3 インターフェイス カウンタの設定」(P.30-10) を参照してください。

これらのハードウェア カウンタは、**show interface** コマンドの出力に表示されます。次に例を示します。

```
Switch# show interface vlan 1
Vlan1 is up, line protocol is up
  Hardware is Ethernet SVI, address is 0005.9a38.6cff (bia 0005.9a38.6cff)
  Internet address is 10.0.0.1/8
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  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
  L3 in Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes    <====
  L3 out Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes  <====
    0 packets input, 0 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
    1 packets output, 46 bytes, 0 underruns
    0 output errors, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
```

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 Internetwork Packet Exchange (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/12_2/atipx/configuration/guide/fatipx_c.html



(注) Supervisor Engine 6-E は、AppleTalk および IPX ルーティングをサポートしていません。

Catalyst 4500 シリーズ スイッチは、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インターフェイスでサブインターフェイスまたは **encapsulation** キーワードをサポートしていません。



(注) Cisco IOS ソフトウェアが稼動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)# vlan <i>vlan_ID</i>	VLAN を作成します。
ステップ 2	Switch(config)# interface vlan <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)# ip address <i>ip_address 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)# no shutdown	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)# end	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# copy running-config startup-config	設定変更内容を Nonvolatile RAM (NVRAM; 不揮発性 RAM) に保存します。
ステップ 7	Switch# show interfaces [<i>type slot/interface</i>] Switch# show ip interfaces [<i>type slot/interface</i>] Switch# show running-config interfaces [<i>type slot/interface</i>] Switch# show running-config interfaces vlan <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.30-7)
- ・「IP 最大伝送ユニット (MTU) サイズの設定」(P.30-8)
- ・「レイヤ 3 インターフェイス カウンタの設定」(P.30-10)

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、Spanning Tree Protocol (STP; スパニングツリープロトコル) 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し、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する場合 (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。

SVI 自動ステート除外は、SVI のステータス定義 (アップまたはダウン) に含まれるアクセスポートまたはトランクを、それが同じ VLAN に属する場合でも除外します。さらに、除外されたアクセスポートまたは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場合でも、SVI ステートはダウンに変更されます。

SVI ステートを「アップ」にするには、少なくとも VLAN 内の 1 つのポートがアップ状態であり、除外されていない必要があります。これは、SVI ステータスの決定時にモニタリングポートのステータスを除外するために役立ちます。

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# configure terminal	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)# interface interface-id	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)# switchport autostate exclude	SVI のステータス定義 (アップまたはダウン) に含まれるアクセスポートまたはトランクを除外します。
ステップ 4	Switch(config)# end	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# show run int g3/4	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# show int g3/4 switchport	設定を確認します。

次に、SVI 自動ステート除外をインターフェイス g3/1 に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
```

<=====

■ レイヤ 3 インターフェイスとしての VLAN の設定

```

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 最大伝送ユニット (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 Maximum Transmission Unit (MTU; 最大伝送ユニット) 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、「最大伝送ユニット (MTU)」(P.6-24) 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。現在の IP MTU 値が MTU 値と一致する場合に MTU 値を変更すると、IP MTU 値は新しい 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.6-26) 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ユニット (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# configure terminal	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)# interface interface-id	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] ip mtu mtu_size or Switch(config-if)# [no] ipv6 mtu mtu_size	MPv4 MTU サイズを設定します。 MPv6 MTU サイズを設定します。 このコマンドの no 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。

	コマンド	目的
ステップ 4	Switch(config-if)# exit	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)# end	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# show run interface interface-id	実行コンフィギュレーションを表示します。

次に、インターフェイスで IPv4 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)# 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
  Address determined by setup command
  MTU is 68 bytes
  Helper address is not set
.....(continued)
```

The following example shows how to configure ipv6 mtu on an interface

```
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
Switch# show ipv6 nterface vlan 1
```

次に、設定を確認する例を示します。

```
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)

Command Line Interface (CLI; コマンドライン インターフェイス) を使用して IPv6 をインターフェイスでイネーブルにする場合、次のメッセージが表示される場合があります。

「% Hardware MTU table exhausted」このようなシナリオでは、ハードウェアでプログラムされている IPv6 MTU 値が IPv6 インターフェイス MTU 値と異なっています。この状況は、ハードウェア MTU テーブルにさらに値を保存する容量が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) Supervisor Engine 6-E は、インターフェイス カウンタをサポートしていません。



(注) ラインカードを削除すると、このラインカードのポート上でイネーブルにされているレイヤ 3 カウンタは未設定となります。そのため、ラインカードを再度挿入するときにレイヤ 3 カウンタを再度イネーブルにするには、そのラインカードのレイヤ 3 ポートに対してカウンタ CLI を再設定する必要があります。

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# configure terminal	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)# interface interface-id	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)# counter	カウンタをイネーブルにします。
ステップ 4	Switch(config)# end	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# show run interface interface-id	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 上で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
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
end
```



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

最大数のカウンタがすでに割り当てられている場合は、**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
Counter resource exhausted
```

```
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。

物理レイヤ 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)# ip routing	IP ルーティングをイネーブルにします (IP ルーティングがディセーブルになっている場合だけ)。
ステップ 2	Switch(config)# interface {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)# no switchport	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)# ip address 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)# no shutdown	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)# end	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# copy running-config startup-config	設定変更内容を NVRAM に保存します。
ステップ 8	Switch# show interfaces [type slot/interface] Switch# show ip interfaces [type slot/interface] Switch# show running-config interfaces [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

```

Enhanced Interior Gateway Routing Protocol (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。

- 「概要」 (P.30-12)
- 「EIGRP スタブ ルーティングの設定方法」 (P.30-13)
- 「EIGRP のモニタリングおよびメンテナンス」 (P.30-18)
- 「EIGRP の設定例」 (P.30-19)

概要

EIGRP スタブ ルーティング機能は、すべてのイメージで使用することができ、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。

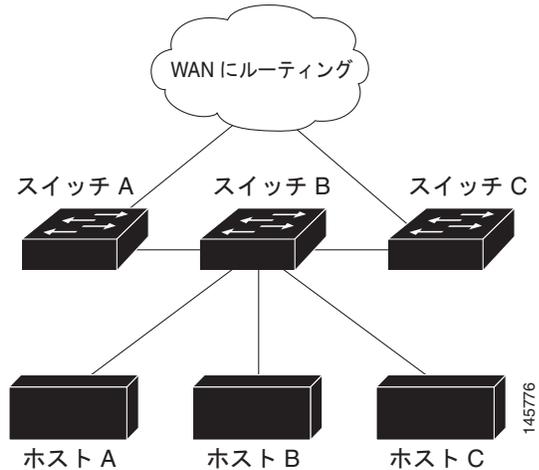
EIGRP スタブ ルーティングを使用するネットワークでは、IP トラフィックがユーザに到達するには、ルート EIGRP スタブ ルーティングを設定しているスイッチを通過する必要があります。スイッチは、ユーザ インターフェイスとして設定されているインターフェイスまたは他のデバイスに接続されているインターフェイスにルーテッド トラフィックを送信します。

EIGRP スタブ ルーティングを使用する場合、EIGRP を使用するように、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 スイッチに依存してすべてのピアに適切なアップデートを送信します。

図 30-3 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 30-3 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方法

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。

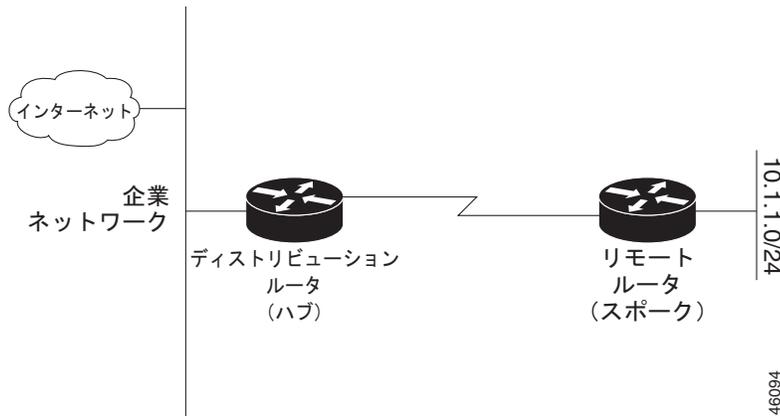
スタブ ルーティングは、一般的に、ハブ アンド スポーク型のネットワーク トポロジで使用されます。ハブ アンド スポーク型ネットワークでは、1 つまたは複数のエンド ネットワーク (スタブ) が、1 つまたは複数のディストリビューション スイッチ (ハブ) に接続したリモート スイッチ (スポーク) に接続しています。リモート スイッチは 1 つまたは複数のディストリビューション スイッチにだけ隣接します。IP トラフィックがリモート スイッチに到達する唯一のルートは、ディストリビューション スイッチを経由するものです。このタイプの構成は、一般的に、ディストリビューション スイッチが直接 WAN 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。多くの場合、ディストリビューション スイッチは 100 以上のリモート ルータに接続されます。ハブ アンド スポーク型のトポロジでは、リモート ルータは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るため、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、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。指定したルートだけがリモート (スタブ) ルータから伝播されます。スタブ ルータはサマリ、接続ルート、再配布スタティック ルート、外部ルート、および内部ルートのすべてのクエリを「アクセス不可」のメッセージで応答します。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、自身がスタブ ルータであることを報告します。

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 ルータに対してルートのクエリを実行せず、スタブ ピアを持つルータはそのピアに対するクエリを実行しません。スタブ ルータは、ディストリビューション ルータに依存してすべてのピアに適切なアップデートを送信します。

図 30-4 に、単純なハブ アンド スポーク構成を示します。

図 30-4 単純なハブ アンド スポーク型ネットワーク



スタブ ルーティング機能自体は、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 30-4 の例では、リモート ルータはディストリビューション ルータだけを通じ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、リモート ルータが完全なルート テーブルを保有しても機能面での意味はありません。企業ネットワークとインターネットへのパスは常にディストリビューション ルータを経由するためです。ルート テーブルが大きくなると、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、自動的にディストリビューション ルータでのサマリーをイネーブルにしません。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 ルータでの集約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、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 **ip classless** コマンドがイネーブルになっています。

スタブ機能を使用しない場合、ディストリビューション ルータからリモート ルータに送信されるルートがフィルタリングまたは集約されたあとでも、問題が生じることがあります。ルートが企業ネットワーク内のどこかで失われた場合、EIGRP はディストリビューション ルータにクエリーを送信できます。そのあと、ディストリビューション ルータはルートが集約されている場合でもリモート 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ことにより、ネットワーク管理者はリモート ルータへクエリーが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 ルータは、複数のディストリビューション ルータ (ハブ) を使用します。ただし、スタブ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 30-5 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 ルータは最適なルートを使用して宛先に到達します。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 30-5 単純なデュアルホーム接続リモート トポロジ

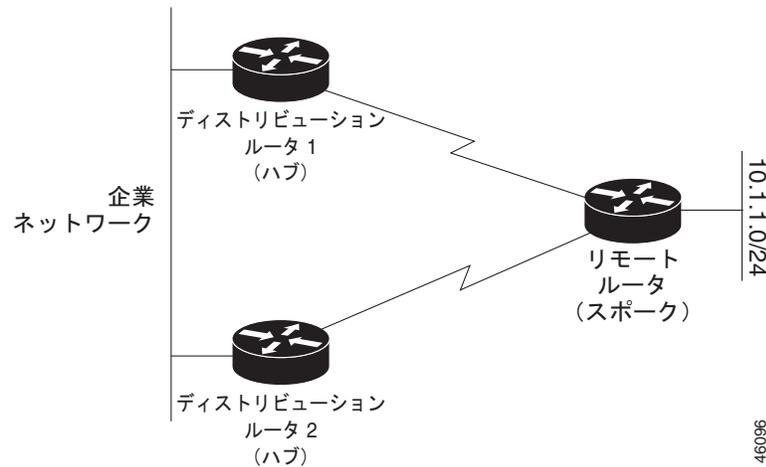


図 30-5 に、リモート ルータ 1 つとディストリビューション ルータ 2 つから構成される簡単なデュアルホーム接続リモートを示します。いずれのディストリビューション ルータも企業ネットワークとスタブ ネットワーク 10.1.1.0/24 へのルートを維持します。

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 30-6 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 に集約またはフィルタリングが適用された場合、このルータは直接接続したすべての EIGRP ネイバー (ディストリビューション ルータ 2 およびリモート 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 30-6 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

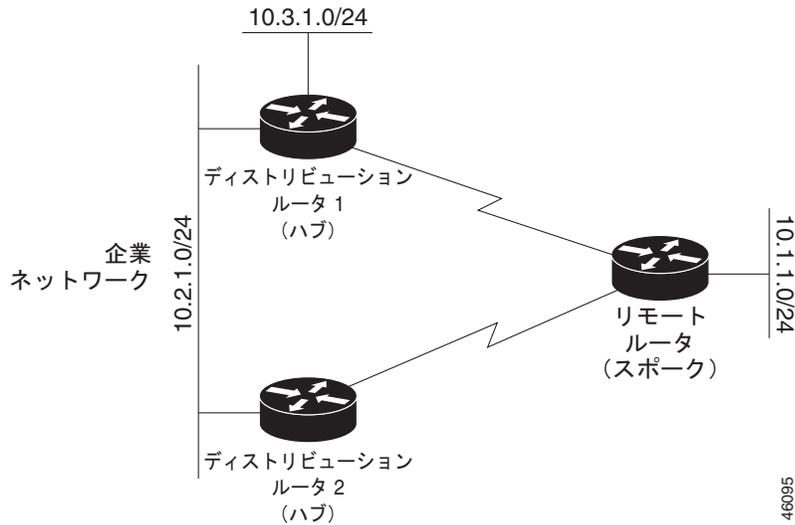
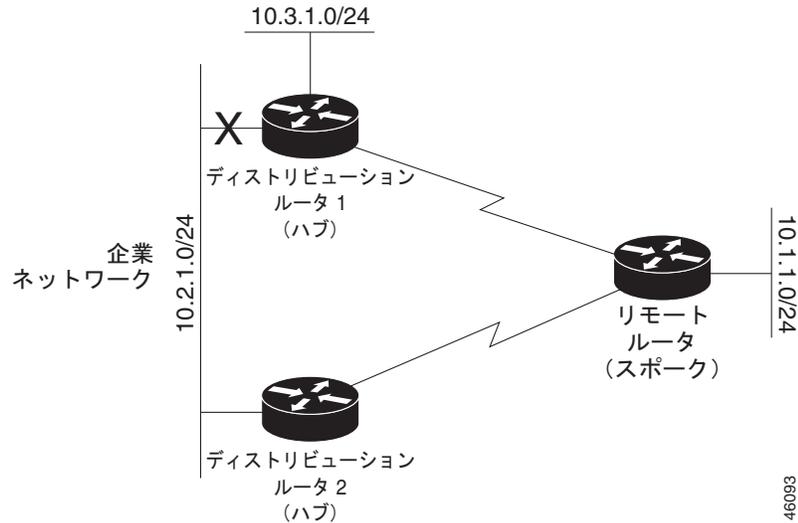


図 30-6 に、ディストリビューションルータ 1 をネットワーク 10.3.1.0/24 とネットワーク 10.2.1.0/24 の両方に接続した単純なデュアルホーム接続リモートルータを示します。

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を経由します (図 30-7 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相当低い接続を介して送信されるため、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多くの問題の原因になります。リモートルータを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 30-7 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にはリモート ルータを中継点として使用しません。

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場合、この機能は EIGRP クエリーが帯域幅に限りのあるリンクを使用して非中継 ルータに送信されるのを防ぎます。その代わりに、スタブル ルータが接続された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。この機能は輻輳のある、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を大幅に減らします。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。デュアルホーム接続リモート構成でスタブルルーティングがイネーブルになっている場合、リモート ルータにフィルタリングを設定して、リモート ルータがハブ ルータへの中継パスのように見えないようにする必要はありません。



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、コア中継トラフィックが通過すべきでないネットワーク 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として定義されます。スタブル ルータは、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。この制約事項を無視すると、好ましくない動作が生じます。



(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 ルーティング機能がサポートされます。

EIGRP スタブ ルーティングの設定作業リスト

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、最後の作業はオプションです。

- [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 ルーティングをリモート ルータまたはスポーク ルータに設定するには、ルータ コンフィギュレーション モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	Switch(config)# router eigrp 1	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)# network network-number	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)# eigrp stub [receive-only connected static summary]	リモート ルータを EIGRP スタブ ルータとして設定します。

EIGRP スタブ ルーティングの確認

リモート ルータが EIGRP でスタブ 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 モードで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。

```
router# show ip eigrp neighbor detail

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、EXEC モードで次のコマンドを使用します。

コマンド	目的
Switch# <code>clear ip eigrp neighbors [ip-address interface]</code>	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を表示するには、EXEC モードで次のコマンドを使用します。

コマンド	目的
Switch# <code>show ip eigrp interfaces [interface] [as-number]</code>	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# <code>show ip eigrp neighbors [type number static]</code>	EIGRP によって検出されたネイバーを表示します。
Switch# <code>show ip eigrp topology [autonomous-system-number [[ip-address] mask]]</code>	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# <code>show ip eigrp traffic [autonomous-system-number]</code>	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、次の例について説明します。

- ルート集約の例
- ルート認証の例
- スタブルーティングの例

ルート集約の例

次の例では、インターフェイス上にルート集約を設定し、また、自動サマリー機能を設定します。この設定によって、EIGRP は、イーサネット インターフェイス 0 からのネットワーク 10.0.0.0 だけを集約するようになります。さらに、この例では自動集約をディセーブルにします。

```
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)

インターフェイスからのデフォルト ルート (0.0.0.0) を生成するのに、`ip summary-address eigrp` サマライズ コマンドは使用しないでください。このコマンドを使用すると、管理ディスタンスが 5 で、ヌル 0 インターフェイスへの EIGRP 集約デフォルト ルートが作成されます。このデフォルト ルートの管理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。ネイバーによって学習されたデフォルト ルートが集約デフォルト ルートによって置き換えられた場合、または集約ルートが存在する唯一のデフォルト ルートである場合、そのデフォルト ルート宛てのすべてのトラフィックはルータを離れず、その代わりに、このトラフィックがヌル 0 インターフェイスに送信され、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 Message Digest 5 (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 1 のキーを使用した EIGRP パケットの MD5 ダイジェストを受け入れ、確認を試みます。また、2 のキーを使用したパケットも受け入れます。他のすべての MD5 パケットがドロップされます。ルータ A は、キー 2 を使用したすべての 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 を受け入れ、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ルートとを共有することを制限します。また **receive-only** キーワードを使用すると、すべてのタイプのルートの送信が停止するため、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。これらの 3 つのキーワードのいずれかを **eigrp stub** コマンドで個別に使用した場合、接続および集約ルートは自動的に送信されません。

connected キーワードを指定すると、EIGRP スタブルーティング機能によって接続ルートが送信されます。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に設定されています。

static キーワードを指定すると、EIGRP スタブルーティング機能によってスタティック ルートが送信されます。このオプションを指定しない場合、EIGRP は通常は自動的に再配布される内部スタティック ルートを含むすべてのスタティック ルートを送信しません。ただし、**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があります。

summary キーワードを使用すると、EIGRP スタブルーティング機能によって集約ルートが送信されます。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に設定されています。

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のに **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
```

