



ネットワーク プロトコルの設定

この章では、ML シリーズ カードでサポートされている IP ルーティング プロトコルを設定する方法について説明します。ここでは、ネットワーク管理者がプロトコルを起動して実行するために必要な情報を提供します。ただし、各プロトコルの詳細な設定情報については説明しません。詳細については、『Cisco IOS IP and IP Routing Configuration Guide』および『Cisco IOS IP and IP Routing Command Reference』を参照してください。

この章の内容は次のとおりです。

- [IP ルーティング プロトコルの基本設定 \(p.11-2\)](#)
- [IP ルーティングの設定 \(p.11-5\)](#)
- [スタティック ルートのモニタリング \(p.11-34\)](#)
- [IP ネットワークのモニタリングとメンテナンス \(p.11-35\)](#)
- [IP マルチキャストルーティングの概要 \(p.11-36\)](#)
- [IP マルチキャストルーティングの設定 \(p.11-37\)](#)
- [IP マルチキャスト動作のモニタリングと確認 \(p.11-37\)](#)

IP ルーティング プロトコルの基本設定

ML シリーズ カードでは、IP ルーティングがデフォルトでイネーブルになっています。

IP ルーティングの場合は、インターフェイスの設定に次の情報が必要です。

- IP アドレス
- IP サブネット マスク

また、次の操作が必要です。

- ルーティング プロトコルの選択
- アドバタイズする IP ネットワーク 番号の割り当て

ML シリーズでは、以降で紹介するルーティング プロトコルがサポートされます。

IP ルーティング プロトコルをファスト イーサネット インターフェイス、ギガビット イーサネット インターフェイス、または Packet-over-SONET/SDH (POS) インターフェイスで実行できるように設定するには、設定中のプロトコルに応じて、次のいずれかの手順を実行します。

RIP

Routing Information Protocol (RIP; ルーティング情報プロトコル) を設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router(config)# router rip	ルータ コンフィギュレーション モードを開始し、RIP をルーティング プロトコルとして定義して、RIP ルーティング プロセスを開始します。
ステップ 2	Router(config-router)# network net-number	サブネット番号や個別のアドレスではなく、Internet Network Information Center (InterNIC; インターネット ネットワーク 情報センター) のネットワーク番号に基づいて、直接接続するネットワークを指定します。ルーティング プロセスによってインターフェイスと適切なアドレスが関連付けられ、指定したネットワークでパケットの処理が開始されます。
ステップ 3	Router(config-router)# exit	グローバル コンフィギュレーション モードに戻ります。

EIGRPEIGRP

Enhanced Interior Gateway Routing Protocol (EIGRP) を設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router(config)# router eigrp autonomous-system-number	EIGRP を IP ルーティング プロトコルとして定義します。 この Autonomous System (AS; 自律システム) 番号は、ML シリーズ カードが属する AS を表します。
ステップ 2	Router(config-router)# network net-number	EIGRP を実行する直接接続されたネットワークを定義します。 このネットワーク番号は、ML シリーズ カードでアドバタイズされるネットワークの番号です。
ステップ 3	Router(config-router)# exit	グローバル コンフィギュレーション モードに戻ります。

OSPF

Open Shortest Path First (OSPF) プロトコルを設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router(config)# router ospf <i>process-ID</i>	OSPF を IP ルーティング プロトコルとして定義します。 プロセス ID は、一意の OSPF ルータ プロセスを識別します。この番号は、ML シリーズ カードの内部のみで使用されます。このプロセス ID と他のルータのプロセス ID を一致させる必要はありません。
ステップ 2	Router(config-router)# network <i>net-address wildcard-mask area</i> <i>area-ID</i>	特定のエリアにインターフェイスを割り当てます。 <ul style="list-style-type: none"> • net-address : 直接接続されたネットワークまたはサブネットのアドレス • wildcard-mask : 指定されたアドレスとインターフェイスのアドレッシングを比較して、OSPF でこのインターフェイスを使用するかどうかを判断するための逆マスク • area : インターフェイスが属するエリアを特定するパラメータ • area-ID : ネットワーク アドレスに関連付けられたエリアを指定
ステップ 3	Router(config-router)# end	イネーブル EXEC モードに戻ります。

BGP

Border Gateway Protocol (BGP; ボーダー ゲートウェイ プロトコル) を設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router(config)# router bgp <i>autonomous-system-number</i>	BGP を IP ルーティング プロトコルとして定義します。 この AS 番号は、ML シリーズ カードが属する AS を表します。
ステップ 2	Router(config-router)# network <i>net-number</i>	BGP を実行する直接接続されたネットワークを定義します。 このネットワーク番号は、ML シリーズ カードでアドバタイズされるネットワークの番号です。
ステップ 3	Router(config-router)# exit	グローバル コンフィギュレーション モードに戻ります。

IP ルーティングのイネーブル化

IP ルーティングをイネーブルにするには、イネーブル EXEC モードで次の手順を実行します。



(注) デフォルトでは、IP ルーティングがすでにイネーブルに設定されています。

	コマンドの説明	目的
ステップ 1	Router# 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	Router(config)# ip routing	IP ルーティングをイネーブルにします (デフォルト)。
ステップ 3	Router(config)# router ip-routing-protocol	IP ルーティング プロトコルを指定します。このステップでは、他のコマンドも実行する場合があります (network [RIP] ルータ設定コマンドを使用して、ルーティングするネットワークを指定する場合など)。特定のプロトコルの詳細については、この章で後述する情報と『Cisco IOS IP and IP Routing Configuration Guide』を参照してください。
ステップ 4	Router(config-router)# end	イネーブル EXEC モードに戻ります。
ステップ 5	Router(config)# show running-config	エントリを確認します。
ステップ 6	Router(config)# copy running-config startup-config	(任意) コンフィギュレーション ファイルにエントリを保存します。

ルーティングをディセーブルにするには、**no ip routing** グローバル コンフィギュレーション コマンド (例 11-1) を使用します。

例 11-1 ルーティング プロトコルとして RIP を使用した IP ルーティングのイネーブル化

```
Router# configure terminal
Router(config)# ip routing
Router(config)# router rip
Router(config-router)# network 10.0.0.0
Router(config-router)# end
```

IP ルーティングの設定

この説明に従って、選択したルーティング プロトコルのパラメータを設定できます。

- [RIP の設定 \(p.11-5\)](#)
- [OSPF の設定 \(p.11-10\)](#)
- [EIGRP の設定 \(p.11-21\)](#)
- [BGP の設定 \(p.11-28\)](#)
- [IS-IS の設定 \(p.11-31\)](#)
- [スタティック ルートの設定 \(p.11-33\)](#)

RIP の設定

RIP は、小規模な同種ネットワーク向けに作成された Interior Gateway Protocol (IGP; 内部ゲートウェイ プロトコル) です。また、RIP は、ブロードキャスト UDP データ パケットを使用し、ルーティング情報を交換するディスタンス ベクタ ルーティング プロトコルです。このプロトコルは RFC 1058 で規定されています。RIP の詳細については、Cisco Press 発行の『*IP Routing Fundamentals*』を参照してください。

スイッチは、RIP を使用して、ルーティングの更新情報を 30 秒ごとに送信 (アドバタイズ) します。ルータが他のルータから 180 秒以上更新情報を受信しないと、その発信側ルータから配信されるルートを使用不可とマーキングします。さらに 240 秒経過しても、ルータが他のルータから更新情報を受信できない場合は、受信側ルータがその発信側ルータに関連するルーティング テーブルのエントリすべてを削除します。

RIP では、ホップ カウントを使用して、各ルートの値を評価します。ホップ カウントは、1 つのルートで経由するルータの数を表します。直接接続したネットワークのホップ カウントは、0 (ゼロ) です。ホップ カウントが 16 のネットワークは、到達不能であることを表します。RIP のホップ カウントの範囲は 0 ~ 15 と狭いので、RIP は大規模ネットワークに適していません。

ルータにデフォルトのネットワーク パスが設定されている場合は、ルータを擬似ネットワーク 0.0.0.0 にリンクするルートが RIP でアドバタイズされます。0.0.0.0 ネットワークは存在しませんが、RIP では、デフォルトのルーティング機能を実装するためにネットワークとして処理されます。RIP がデフォルト ネットワークを学習している場合、またはルータが最終手段としてゲートウェイを用意しており、RIP がデフォルトのメトリックで設定されている場合は、スイッチは、デフォルトのネットワークをアドバタイズします。RIP は、指定されたネットワークのインターフェイスに更新情報を送信します。インターフェイスのネットワークを指定していない場合は、RIP の更新情報でアドバタイズされません。

表 11-1 に、RIP のデフォルト設定を示します。

表 11-1 RIP のデフォルト設定

機能	デフォルト設定
自動サマリー	イネーブル
デフォルト情報発信	ディセーブル
デフォルトのメトリック	組み込み：自動メトリック変換
IP RIP 認証キー チェーン	認証なし 認証モード：平文
IP RIP 受信バージョン	version ルータ コンフィギュレーション コマンドで指定
IP RIP 送信バージョン	version ルータ コンフィギュレーション コマンドで指定

表 11-1 RIP のデフォルト設定 (続き)

機能	デフォルト設定
IP RIP トリガー	version ルータ コンフィギュレーション コマンドで指定
IP スプリット ホライズン	メディアによって異なる
ネイバ	未定義
ネットワーク	未指定
オフセット リスト	ディセーブル
出力遅延	0 ミリ秒
タイマーの基本値	更新 : 30 秒 無効 : 180 秒 ホールドダウン : 180 秒 フラッシュ : 240 秒
更新情報発信元の確認	イネーブル
バージョン	RIP バージョン 1 とバージョン 2 のパケットを受信 バージョン 1 のパケットを送信

RIP を設定するには、ネットワークで RIP ルーティングをイネーブルにし、他のパラメータを任意に設定します。

RIP をイネーブルにして設定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router# 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	Router(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にのみ必須)
ステップ 3	Router(config)# router rip	RIP ルーティング プロセスをイネーブルにし、ルータ コンフィギュレーション モードを開始します。
ステップ 4	Router(config-router)# network network-number	ネットワークを RIP ルーティング プロセスに関連付けます。複数の network コマンドを指定できます。RIP ルーティング更新は、指定したネットワークだけでインターフェイス経由で送受信されます。
ステップ 5	Router(config-router)# neighbor ip-address	(任意) ルーティング情報を交換する近接ルータを定義します。このステップでは、ブロードキャスト対象外のネットワークに RIP (通常はブロードキャストプロトコル) からのルーティング更新を送信できます。
ステップ 6	Router(config-router)# offset list { [access-list-number name] } { in out } offset [type-number]	(任意) オフセット リストをルーティング メトリックに適用し、RIP 経由で学習したルートに着信と発信のメトリックを増やします。オフセット リストをアクセス リストやインターフェイスで制限することができます。

	コマンドの説明	目的
ステップ 7	Router(config-router)# timers basic update invalid holddown flush	(任意) ルーティング プロトコル タイマーを調整します。すべてのタイマーの有効値の範囲は、0 ~ 4294967295 秒です。 <ul style="list-style-type: none"> • update — ルーティング更新を送信する間隔 (秒単位)。デフォルトは 30 秒です。 • invalid — ルートが無効だと宣言されるまでの時間 (秒単位)。デフォルトは 180 秒です。 • holddown — ルーティングテーブルからルートを削除するまでに経過する時間 (秒単位)。デフォルトは 180 秒です。 • flush — ルーティングの更新が延期される時間 (秒単位)。デフォルトは 240 秒です。
ステップ 8	Router(config-router)# version {1 2}	(任意) スイッチを設定し、RIP バージョン 1 または RIP バージョン 2 のパケットだけを送受信するようにします。デフォルトでは、スイッチは、バージョン 1 とバージョン 2 を受信しますが、送信するのはバージョン 1 のみです。インターフェイス コマンド ip rip {send receive} version {1 2 1 2} を使用して、インターフェイスでの送受信に使用するバージョンを制御することもできます。
ステップ 9	Router(config-router)# no auto summary	(任意) 自動サマリーをディセーブルにします。デフォルトでは、スイッチは、全クラスのネットワーク境界を通過するときにサブプレフィックスをサマリーします。このサマリーをディセーブルにして (RIP バージョン 2 のみ)、サブネットとホストのルーティング情報を全クラスのネットワーク境界にアダプタイズします。
ステップ 10	Router(config-router)# no validate-update-source	(任意) 着信する RIP ルーティング更新の送信元 IP アドレスの検証をディセーブルにします。デフォルトでは、スイッチは、着信 RIP ルーティング更新の送信元 IP アドレスを検証し、送信元アドレスが無効な場合にその更新情報を廃棄します。通常は、この機能をイネーブルにすることをお勧めします。ただし、ネットワーク外のルータがあり、その更新情報を受信する場合は、このコマンドを使用できます。
ステップ 11	Router(config-router)# output-delay delay	(任意) 送信する RIP 更新パケット間に遅延を追加します。デフォルトでは、複数のパケットを使用する RIP 更新内のパケット間には遅延が追加されていません。パケットをより低速な装置に送信する場合、8 ~ 50 ミリ秒の範囲でパケット間に遅延を追加できます。
ステップ 12	Router(config-router)# end	イネーブル EXEC モードに戻ります。
ステップ 13	Router# show ip protocols	エントリを確認します。
ステップ 14	Router# copy running-config startup-config	(任意) コンフィギュレーション ファイルにエントリを保存します。

RIP ルーティングプロセスを無効にするには、**no router rip** グローバル コンフィギュレーション コマンドを使用します。

アクティブなルーティング プロトコル プロセスのパラメータと最新状態を表示するには、**show ip protocols** イネーブル EXEC コマンド (例 11-2) を使用します。

例 11-2 show ip protocols コマンドの出力 (RIP プロセスの表示)

```

Router# show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 15 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: rip
  Default version control: send version 1, receive any version
  Interface          Send Recv Triggered RIP Key-chain
  FastEthernet0      1     1  2
  POS0                1     1  2
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    192.168.2.0
    192.168.3.0
  Routing Information Sources:
    Gateway           Distance      Last Update
    192.168.2.1       120           00:00:23
  Distance: (default is 120)

```

RIP データベース内のサマリー アドレス エントリを表示するには、**show ip rip database** イネーブル EXEC コマンドを使用します (例 11-3)。

例 11-3 show ip rip database コマンドの出力

```

Router# show ip rip database
192.168.1.0/24   auto-summary
192.168.1.0/24
    [1] via 192.168.2.1, 00:00:24, POS0
192.168.2.0/24   auto-summary
192.168.2.0/24   directly connected, POS0
192.168.3.0/24   auto-summary
192.168.3.0/24   directly connected, FastEthernet0

```

RIP 認証

RIP バージョン 1 では、認証がサポートされません。RIP バージョン 2 のパケットを送受信するには、インターフェイスで RIP 認証をイネーブルにできます。キーチェーンは、インターフェイスで使用できるキーセットを表します。キーチェーンを設定していない場合は、認証が実行されません。デフォルトでも同様です。

このスイッチでは、RIP 認証がイネーブルのインターフェイスで 2 つの認証モード (平文とメッセージダイジェストキー [MD5]) がサポートされています。デフォルトは、平文です。

インターフェイスに RIP 認証を設定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router# 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	Router(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、設定するインターフェイスを指定します。
ステップ 3	Router(config-if)# ip rip authentication key-chain name-of-chain	RIP 認証をイネーブルにします。
ステップ 4	Router(config-if)# ip rip authentication mode {text md5}	平文による認証 (デフォルト) または MD5 ダイジェスト認証を使用するようにインターフェイスを設定します。

	コマンドの説明	目的
ステップ 5	Router(config-if)# end	イネーブル EXEC モードに戻ります。
ステップ 6	Router# show running-config interface [interface-id]	エントリを確認します。
ステップ 7	Router# copy running-config startup-config	(任意) コンフィギュレーション ファイルにエントリを保存します。

平文認証に戻すには、**no ip rip authentication mode** 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。認証を実行しない場合は、**no ip rip authentication key-chain** 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。

サマリー アドレスとスプリット ホライズン

ブロードキャスト型 IP ネットワークに接続され、ディスタンス ベクタ ルーティング プロトコルを使用するルータは、通常、スプリット ホライズン メカニズムを使用してルーティング ループの発生を抑えます。スプリット ホライズンでは、ルータがルート情報をアドバタイズするのを、情報発信側のインターフェイスで防ぎます。この機能によって、通常 (特にリンクに障害がある場合)、複数のルータ間で通信が最適化されます。



(注)

スプリット ホライズンをディセーブルにしないとアプリケーションが正しくルートをアドバタイズできない場合を除き、通常は、スプリット ホライズンをイネーブルにすることをお勧めします。

RIP を実行するインターフェイスを設定し、ダイヤルアップ クライアント用ネットワーク アクセス サーバ上のサマリー ローカル IP アドレス プールをアドバタイズするには、**ip summary-address rip** 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。

インターフェイスを設定し、サマリー ローカル IP アドレス プールをアドバタイズして、このインターフェイスでスプリット ホライズンをディセーブルにするには、イネーブル EXEC モードで次のステップを実行します。

	コマンドの説明	目的
ステップ 1	Router# 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	Router(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、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	Router(config-if)# ip address ip-address subnet-mask	IP アドレスと IP サブネットを設定します。
ステップ 4	Router(config-if)# ip summary-address rip ip-address ip-network-mask	IP アドレスのサマリーと IP ネットワーク マスクを設定します。
ステップ 5	Router(config-if)# no ip split horizon	インターフェイスでのスプリット ホライズンをディセーブルにします。
ステップ 6	Router(config-if)# end	イネーブル EXEC モードに戻ります。
ステップ 7	Router# show ip interface interface-id	エントリを確認します。
ステップ 8	Router# copy running-config startup-config	(任意) コンフィギュレーション ファイルにエントリを保存します。

IP サマリーをディセーブルにするには、**no ip summary-address rip** ルータ設定コマンドを使用します。



(注)

スプリット ホライズンをイネーブルにすると、自動サマリーもインターフェイスでのサマリー アドレス (**ip summary-address rip** ルータ コンフィギュレーション コマンドで設定したサマリー アドレス) もアドバタイズされません。

OSPF の設定

ここでは、OSPF プロトコルの設定方法を簡単に説明します。OSPF のコマンドの詳細については、『Cisco IOS IP and IP Routing Command Reference』の「OSPF Commands」の章を参照してください。

OSPF は、IP ネットワーク用に特別に設計された IGP であり、外部で派生したルーティング情報の IP サブネット化とタギングをサポートします。OSPF では、パケット認証が可能で、パケットの送受信時に IP マルチキャストを使用します。シスコ製品では、RFC 1253 の OSPF MIB がサポートされています。

シスコ製品は、次の機能を持つ OSPF バージョン 2 の規格に準拠しています。

- スタブ エリア — スタブ エリアの定義がサポートされます。
- ルート再配布 — IP ルーティング プロトコルが学習したルートを他の IP ルーティング プロトコルに再配布できます。これは、ドメイン内では、EIGRP や RIP などのプロトコルで学習したルートを OSPF がインポートしたり、エクスポートしたりできることを表します。
- 認証 — エリア内の近接ルータで平文と MD5 による認証がサポートされます。
- ルーティング インターフェイス パラメータ — サポートされている設定可能なパラメータには、インターフェイス出力コスト、再送間隔、インターフェイス送信遅延、ルータのプライオリティ、ルータのデッドおよび Hello インターバル、認証キーなどがあります。
- 仮想リンク — 仮想リンクがサポートされます。
- Not-So-Stubby-Area (NSSA; 準スタブ エリア) — RFC 1587

OSPF では、通常、多数の内部ルータ、複数のエリアに接続された Area Border Router (ABR; エリア境界ルータ)、および Autonomous System Boundary Router (ASBR; 自律システム境界ルータ) の間で調整を行う必要があります。最小設定では、すべてのデフォルトパラメータ値、認証設定 (認証なし)、およびエリアに割り当てられたインターフェイスを使用します。使用中の環境をカスタマイズする場合は、すべてのルータで設定を調整する必要があります。

表 11-2 にデフォルトの OSPF 設定を示します。

表 11-2 OSPF のデフォルト設定

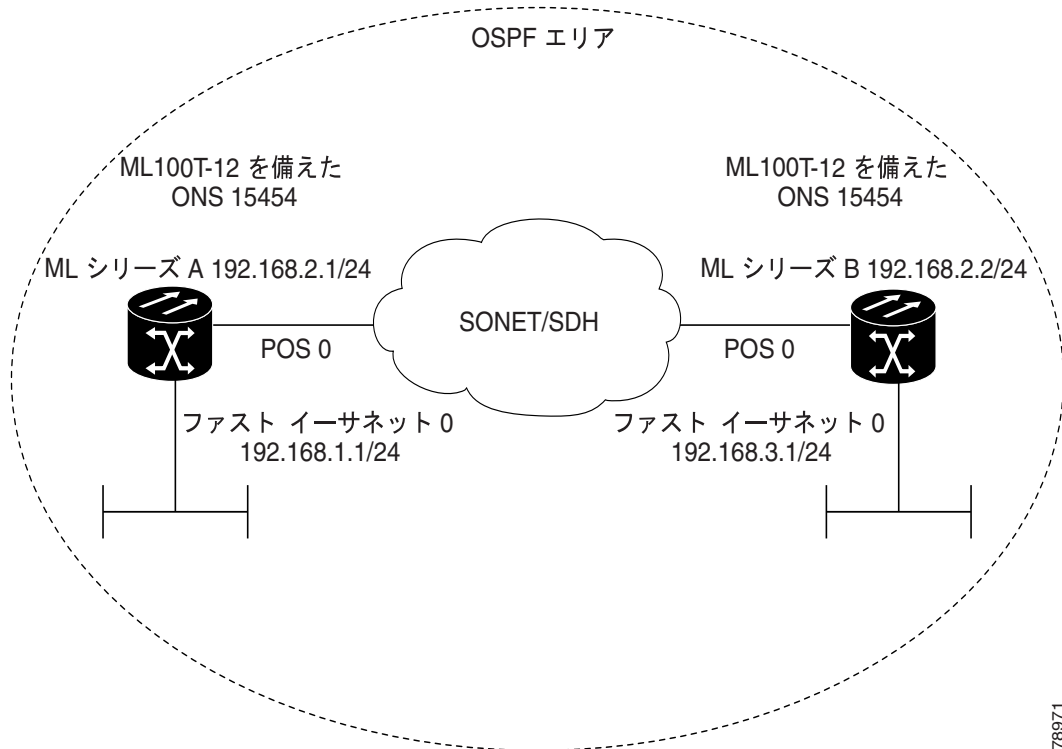
機能	デフォルト設定
インターフェイスのパラメータ	コスト: デフォルト値は未設定 再送間隔: 5 秒 送信遅延: 1 秒 プライオリティ: 1 Hello インターバル: 10 秒 デッド インターバル: Hello インターバルの 4 倍 認証なし パスワード未指定 MD5 認証ディセーブル

表 11-2 OSPF のデフォルト設定 (続き)

機能	デフォルト設定
エリア	認証タイプ : 0 (認証なし) デフォルトのコスト : 1 範囲 : ディセーブル スタブ : スタブ エリア未定義 NSSA : NSSA エリア未定義
自動コスト	100 Mbps
デフォルト情報発信元	ディセーブル。イネーブルにした場合、デフォルトのメトリック設定は 10 で、外部ルート タイプのデフォルト値は Type 2 です。
デフォルトのメトリック	組み込み、自動メトリック変換、各ルーティング プロトコルに適切なメトリック
長距離 OSPF	dist1 (すべてのルートが 1 エリア内に存在) : 110 dist2 (2 つのエリア間のすべてのルート) : 110 dist3 (他のルーティング ドメインからのルート) : 110
OSPF データベース フィルタ	ディセーブル。すべての発信 Link-State Advertisements (LSA; リンクステート アドバタイズメント) がインターフェイスにフラッディングされます。
IP OSPF 名前検索	ディセーブル
隣接関係変更ログ	イネーブル
ネイバ	未指定
ネイバデータベース フィルタ	ディセーブル。すべての発信 LSA がネイバにフラッディングされます。
ネットワーク エリア	ディセーブル
ルータ ID	OSPF ルーティング プロセス未定義
サマリー アドレス	ディセーブル
タイマー LSA グループ ページング	240 秒
タイマー Shortest Path First (SPF; 最短パス優先)	SPF 遅延 : 5 秒 SPF 待機時間 : 10 秒
仮想リンク	エリア ID またはルータ ID は未定義 Hello インターバル : 10 秒 再送間隔 : 5 秒 送信遅延 : 1 秒 デッド インターバル : 40 秒 認証キー : キー未定義 MD5 : キー未定義

図 11-1 に OSPF を使用した IP ルーティング プロトコルの例を示します。

図 11-1 OSPF を使用した IP ルーティング プロトコルの例



78971

OSPF をイネーブルにするには、OSPF ルーティング プロセスを作成し、このルーティング プロセスに関連付ける IP アドレスの範囲を指定して、その範囲に関連付けるエリア ID を割り当てる必要があります。

OSPF をイネーブルにするには、イネーブル EXEC モードを開始し、次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router# <code>configure terminal</code>	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	Router(config)# <code>router ospf process-id</code>	OSPF ルーティングをイネーブルにし、ルータ コンフィギュレーション モードを開始します。プロセス ID は、ローカルに割り当てられ、内部的に使用される識別パラメータです。この ID には、どの正の整数でも指定できます。各 OSPF ルーティング プロセスには、一意の値を指定します。
ステップ 3	Router(config)# <code>network address wildcard-mask area area-id</code>	OSPF を実行するインターフェイスと、そのインターフェイスのエリア ID を定義します。1 つのコマンドで 1 つ以上のインターフェイスを特定の OSPF エリアに関連付けるには、ワイルドカードマスクを使用します。エリア ID は、10 進値または IP アドレスです。
ステップ 4	Router(config)# <code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	Router# <code>show ip protocols</code>	エントリを確認します。
ステップ 6	Router# <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルにエントリを保存します。

OSPF ルーティング プロセスを終了するには、**no router ospf process-id** グローバル コンフィギュレーション コマンドを使用します。

例 11-4 に OSPF ルーティング プロセスの設定例を示します。この例では、プロセス番号 1 を割り当てます。例 11-5 に、OSPF プロセス ID の確認に使用する、コマンド出力を示します。

例 11-4 OSPF ルーティング プロセスの設定

```
Router(config)# router ospf 1
Router(config-router)# network 192.168.1.0 0.0.0.255 area 0
```

例 11-5 show ip protocols イネーブル EXEC コマンドの出力

```
Router# show ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.3.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.2.0 0.0.0.255 area 0
    192.168.3.0 0.0.0.255 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.3.1      110          00:03:34
    192.168.2.1      110          00:03:34
  Distance: (default is 110)
```

OSPF インターフェイス パラメータ

インターフェイスに固有の OSPF パラメータを変更するには、**ip ospf** 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。これらのパラメータを変更する必要はありませんが、一部のインターフェイス パラメータ (Hello インターバル、デッド インターバル、および認証キー) は、接続されたネットワーク内のすべてのルータで一致する必要があります。これらのパラメータを変更する場合は、ネットワーク内のすべてのルータの値に互換性があることを確認してください。



(注) **ip ospf** インターフェイス コンフィギュレーション コマンドは、すべて任意です。

OSPF インターフェイス パラメータを変更するには、イネーブル EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router# 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	Router(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、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	Router(config-if)# ip ospf cost	(任意) インターフェイスでのパケット送信コストを明示的に指定します。

	コマンドの説明	目的
ステップ 4	Router(config-if)# ip ospf retransmit-interval seconds	(任意) リンクステート アドバタイズメントの送信間隔を秒単位で指定します。範囲は、1 ~ 65535 秒です。デフォルト値は、5 秒です。
ステップ 5	Router(config-if)# ip ospf transmit-delay seconds	(任意) リンク ステート更新パケットを送信するまでの待機時間を設定します。範囲は、1 ~ 65535 秒です。デフォルトは 1 秒です。
ステップ 6	Router(config-if)# ip ospf priority number	(任意) ネットワークの OSPF 指定ルータを決定するためのプライオリティを設定します。範囲は 0 ~ 255 です。デフォルトは 1 です。
ステップ 7	Router(config-if)# ip ospf hello-interval seconds	(任意) OSPF インターフェイスで Hello パケットを送信する間隔を秒単位で設定します。この値は、1 つのネットワーク上にあるすべてのノードで統一する必要があります。範囲は、1 ~ 65535 秒です。デフォルトは 10 秒です。
ステップ 8	Router(config-if)# ip ospf dead-interval seconds	(任意) 装置の最後の Hello パケットが検出されてから OSPF ルータが停止していることをネイバが宣言するまでの時間を秒単位で設定します。この値は、1 つのネットワーク上にあるすべてのノードで統一する必要があります。範囲は、1 ~ 65535 秒です。デフォルトは、Hello インターバルの 4 倍です。
ステップ 9	Router(config-if)# ip ospf authentication-key key	(任意) 近接 OSPF ルータが使用するパスワードを割り当てます。このパスワードには、キーボードで入力できる文字列を 8 バイトの長さまで指定できます。OSPF 情報を交換するために、同一ネットワーク上のすべての近接ルータに同じパスワードを指定する必要があります。
ステップ 10	Router(config-if)# ip ospf message digest-key keyid md5 key	(任意) 認証をイネーブルにします。 <ul style="list-style-type: none"> • keyid — 1 ~ 255 の識別子。 • key — 16 バイトまでの英数字パスワード
ステップ 11	Router(config-if)# ip ospf database-filter all out	(任意) OSPF LSA パケットがインターフェイスにフラッドされるのを防ぎます。デフォルトでは、OSPF が同じエリア内のすべてのインターフェイス (LSA が到達済みのインターフェイスを除く) に新しい LSA をフラッドリングします。
ステップ 12	Router(config-if)# end	イネーブル EXEC モードに戻ります。
ステップ 13	Router# show ip ospf interface [interface-name]	OSPF 関連のインターフェイス情報を表示します。
ステップ 14	Router# copy running-config startup-config	(任意) コンフィギュレーション ファイルにエントリを保存します。

設定したパラメータ値を削除する場合、またはデフォルト値に戻す場合は、これらのコマンドの **no** 形式を使用します。例 11-6 に **show ip ospf interface** イネーブル EXEC コマンドの出力を示します。

例 11-6 show ip ospf interface イネーブル EXEC コマンドの出力

```

Router# show ip ospf interface
FastEthernet0 is up, line protocol is up
  Internet Address 192.168.3.1/24, Area 0
  Process ID 1, Router ID 192.168.3.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.3.1, Interface address 192.168.3.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
POS0 is up, line protocol is up
  Internet Address 192.168.2.2/24, Area 0
  Process ID 1, Router ID 192.168.3.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.3.1, Interface address 192.168.2.2
  Backup Designated router (ID) 192.168.2.1, Interface address 192.168.2.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 2, maximum is 2
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.2.1 (Backup Designated Router)
  Suppress hello for 0 neighbor(s)

```

OSPF エリア パラメータ

任意で複数の OSPF エリア パラメータを設定できます。これらのパラメータには、エリア、スタブエリア、および NSSA への不正アクセスを防ぐためにパスワードベースで保護する認証があります。スタブエリアは、外部ルート情報が送信されないエリアです。代わりに、ABR によって AS 外の宛先について、スタブエリアへのデフォルトの外部ルートが作成されます。NSSA では、すべての LSA がコアからエリアにフラッドされるわけではありませんが、再配布により AS の外部ルートをエリア内にインポートできます。

経路集約は、アドバタイズされたアドレスを 1 つのサマリールートに統合し、他のエリアでアドバタイズする機能です。ネットワーク番号が連続している場合は、**area range** ルータ コンフィギュレーション コマンドを使用して、ABR を設定し、その範囲内のすべてのネットワークをカバーするサマリールートをアドバタイズできます。



(注) OSPF の **area** ルータ設定コマンドは、すべてオプションです。

エリア パラメータを設定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router# 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	Router(config)# router ospf process-id	OSPF ルーティングをイネーブルにし、ルータ コンフィギュレーション モードを開始します。

	コマンドの説明	目的
ステップ 3	Router(config)# area area-id authentication	(任意) 指定したエリアへの不正アクセスに対してパスワードベースの保護を可能にします。この ID は、10 進値または IP アドレスです。
ステップ 4	Router(config)# area area-id authentication message-digest	(任意) このエリアで MD5 認証をイネーブルにします。
ステップ 5	Router(config)# area area-id stub [no-summary]	(任意) エリアをスタブ エリアとして定義します。 no-summary キーワードを指定すると、ABR がスタブ エリア内にサマリー リンク アドバタイズメントを送信するのを防ぐことができます。
ステップ 6	Router(config)# area area-id nssa {no-redistribution default-information-originate no-summary}	(任意) エリアを NSSA として定義します。同一エリア内のすべてのルータは、このエリアが NSSA であることを認識している必要があります。次のいずれかのキーワードを指定します。 <ul style="list-style-type: none"> • no-redistribution — ルータが NSSA ABR であり、redistribute コマンドを使用して NSSA 以外の通常のエリア内にルートをインポートする場合に選択します。 • default-information-originate — ABR で NSSA 内にタイプ 7 の LSA をインポートする場合に選択します。 • no-summary — NSSA 内にサマリー LSA を送信しない場合に選択します。
ステップ 7	Router(config)# area area-id range address-mask	(任意) アドレスの範囲を指定し、その範囲に 1 つのルートをアドバタイズします。このコマンドは、ABR だけで使用します。
ステップ 8	Router(config)# end	イネーブル EXEC モードに戻ります。
ステップ 9	Router# show ip ospf [process-id]	OSPF ルーティング プロセスの全般情報を表示するか、または、指定したプロセス ID について情報を表示して確認します。
ステップ 10	Router# copy running-config startup-config	(任意) コンフィギュレーション ファイルにエントリを保存します。

設定したパラメータ値を削除する場合、またはデフォルト値に戻す場合は、これらのコマンドの **no** 形式を使用します。例 11-7 に、**show ip ospf database** および **show ip ospf** イネーブル EXEC コマンドの出力を示します。

例 11-7 show ip ospf database および show ip ospf イネーブル EXEC コマンドの出力

```

Router# show ip ospf database

      OSPF Router with ID (192.168.3.1) (Process ID 1)

          Router Link States (Area 0)

Link ID        ADV Router    Age           Seq#           Checksum Link count
192.168.2.1    192.168.2.1   428           0x80000003    0x004AB8 2
192.168.3.1    192.168.3.1   428           0x80000003    0x006499 2

          Net Link States (Area 0)

Link ID        ADV Router    Age           Seq#           Checksum
192.168.2.2    192.168.3.1   428           0x80000001    0x00A4E0

Router# show ip ospf
Routing Process "ospf 1" with ID 192.168.3.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
  Area BACKBONE(0)
    Number of interfaces in this area is 2
    Area has no authentication
    SPF algorithm executed 4 times
    Area ranges are
    Number of LSA 3. Checksum Sum 0x015431
    Number of opaque link LSA 0. Checksum Sum 0x000000
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0

```

OSPF のその他の動作パラメータ

ルータ コンフィギュレーション モードでは、他の OSPF パラメータも任意で設定できます。

- 経路集約 — 他のプロトコルからのルートを再配布する場合は、各ルートが外部 LSA 内で個別にアドバタイズされます。OSPF リンク状態データベースのサイズを減らすには、**summary-address** ルータ コンフィギュレーション コマンドを使用して、指定したネットワークアドレスとマスクに含まれるすべての再配布ルートについて 1 つのルータをアドバタイズします。
- 仮想リンク — OSPF では、すべてのエリアをバックボーン エリアに接続する必要があります。1 つの仮想リンクのエンドポイントとして 2 つの ABR を設定することにより、バックボーンの導通性が損なわれた場合に仮想リンクを確立できます。設定情報には、他の仮想エンドポイント (他の ABR) の ID、2 つのルータが共通して把握するバックボーン以外のリンク (中継エリア) などが含まれます。スタブ エリア経由で仮想リンクを設定することはできません。
- デフォルトルート — OSPF ルーティング ドメイン内にルートの再配布を個別に設定すると、そのルートが自動的に ASBR になります。ASBR によって OSPF ルーティング ドメイン内にデフォルトルートを強制的に作成できます。
- OSPF のすべての **show** イネーブル EXEC コマンド表示で Domain Name Server (DNS; ドメインネーム サーバ) 名を使用すると、ルータ ID またはネイバ ID でルータを表示する場合よりも、ルータを識別しやすくなります。

- デフォルトのメトリック — OSPF は、インターフェイスの帯域幅に基づいてそのインターフェイスの OSPF メトリックを計算します。このメトリックは、帯域幅で除算された *ref-bw* として計算されます。*ref* のデフォルト値は 10 で、帯域幅 (*bw*) は、**bandwidth** インターフェイス コンフィギュレーション コマンドで判別する値です。高帯域幅を持つ複数のリンクについては、より大きい数値を指定して、これらのリンクのコストを区別できます。
- 管理距離 — ルーティング情報の送信元の信頼性について 0 ~ 255 の整数で評価します。値が大きいほど、信頼性が低いことを表します。管理距離が 255 の場合は、ルーティング情報の送信元がまったく信頼できず、無視する必要があります。OSPF では、3 種類の管理距離 (エリア内のルート [*intra-area*]、他のエリアへのルート [*interarea*]、および再配布によって学習された他のルーティング ドメインからのルート [*external*]) を使用します。管理距離の値は、どれにでも変更できます。
- 受動インターフェイス — イーサネット上の 2 つの装置の間にあるインターフェイスは、1 つのネットワーク セグメントだけを表すので、OSPF が送信側インターフェイスに対して Hello パケットを送信するのを防ぐには、送信側の装置を受動インターフェイスとして設定する必要があります。両方の装置は、受信インターフェイス用の Hello パケットで互いを識別できます。
- ルート計算タイマー — OSPF がトポロジー変更を受信してから SPF 計算を開始するまでの遅延時間を設定できます。2 つの SPF 計算の間の待機時間も設定できます。
- ネイバ変更のログ — OSPF ネイバの状態が変化した場合に Syslog メッセージを送信するようにルータを設定できます。この場合、ルータの変化を高度なビューで表示できます。

これらの OSPF パラメータを設定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router# 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	Router(config)# router ospf process-id	OSPF ルーティングをイネーブルにし、ルータ 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	Router(config)# summary-address address-mask	(任意) 1 つのサマリー ルートだけをアドバタイズするように、再配布ルートアドレスと IP サブネットマスクを指定します。
ステップ 4	Router(config)# area area-id virtual-link router-id [hello-interval seconds] [retransmit-interval seconds] [trans] { [authentication-key key] [message-digest-key key-id md5 key] }	(任意) 仮想リンクを確立し、そのパラメータを設定します。パラメータの定義については、「 OSPF インターフェイス パラメータ 」(p.11-13) を参照してください。仮想リンクのデフォルトについては、 表 11-2 (p.11-10) を参照してください。
ステップ 5	Router(config)# default-information originate [always] [metric metric-value] [metric-type type-value] [route-map map-name]	(任意) ASBR が強制的に OSPF ルーティング ドメイン内にデフォルト ルートを作成します。パラメータは、すべて任意です。
ステップ 6	Router(config)# ip ospf name-lookup	(任意) DNS 名検索を設定します。デフォルトではディセーブルに設定されています。
ステップ 7	Router(config)# ip auto-cost reference-bandwidth ref-bw	(任意) アドレスの範囲を指定し、その範囲に 1 つのルートをアドバタイズします。このコマンドは、ABR だけで使用します。
ステップ 8	Router(config)# distance ospf { [inter-area dist1] [inter-area dist2] [external dist3] }	(任意) OSPF の距離の値を変更します。各ルート タイプのデフォルトの距離は 110 です。指定できる範囲は 1 ~ 255 です。
ステップ 9	Router(config)# passive-interface type number	(任意) 指定したインターフェイス経由での Hello パケットの送信を停止します。

	コマンドの説明	目的
ステップ 10	Router(config)# timers spf spf-delay spf-holdtime	(任意) ルート計算タイマーを設定します。 <ul style="list-style-type: none"> spf-holdtime — 0 ~ 65535 の整数を入力します。デフォルトは 5 秒です。値 0 は、遅延させないことを表します。 spf-holdtime — 0 ~ 65535 の整数を入力します。デフォルトは 10 秒です。値 0 は、遅延させないことを表します。
ステップ 11	Router(config)# ospf log-adj-changes	(任意) ネイバの状態が変化した場合に、Syslog メッセージを送信します。
ステップ 12	Router(config)# end	イネーブル EXEC モードに戻ります。
ステップ 13	Router# show ip ospf [process-id [area-id]] database	指定したルータの OSPF データベースに関連する情報のリストを表示します。一部のキーワードオプションについては、「 OSPF のモニタリング 」(p.11-20) を参照してください。
ステップ 14	Router# copy running-config startup-config	(任意) コンフィギュレーション ファイルにエントリを保存します。

LSA グループ ペーシングの変更

OSPF の LSA グループ ペーシング機能では、ルータをより効率的に使用できるように、ルータによって OSPF LSA がグループ化され、更新機能、チェックサム機能、およびエージング機能の発生頻度が設定されます。この機能は、デフォルトでイネーブルになっています。デフォルトのペーシング間隔は 4 分ですが、通常は、このパラメータを変更する必要はありません。最適なグループペーシング間隔は、ルータが更新、チェックサム、およびエージングを行う LSA の数に反比例します。たとえば、データベースに約 10,000 個の LSA があるような場合は、ペーシング間隔の値を減らすと、より効率化できます。データベースのサイズが非常に小さい場合 (LSA 数が 40 ~ 100 の場合) は、ペーシング間隔の値を 10 ~ 20 分に増やすと、やや効率化されます。

OSPF LSA ペーシングを設定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router# 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	Router(config)# router ospf process-id	OSPF ルーティングをイネーブルにし、ルータ 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	Router(config)# timers lsa-group-pacing seconds	LSA のグループ ペーシングを変更します。
ステップ 4	Router(config)# end	イネーブル EXEC モードに戻ります。
ステップ 5	Router# show running-config	エントリを確認します。
ステップ 6	Router# copy running-config startup-config	(任意) コンフィギュレーション ファイルにエントリを保存します。

デフォルト値に戻すには、**no timers lsa-group-pacing** ルータ コンフィギュレーション コマンドを使用します。

ループバック インターフェイス

OSPF では、インターフェイスに設定されている最も数値の高い IP アドレスをルータ ID として使用します。このインターフェイスが故障したり、取り外されたりした場合は、OSPF のプロセスで新しいルータ ID を再計算し、インターフェイスからすべてのルーティング情報を再送する必要があります。IP アドレスを使用してループバック インターフェイスを設定した場合、OSPF はこの IP アドレスをルータ ID として使用します。他のインターフェイスがより数値の高い IP アドレスを持っている場合でも同様です。ループバック インターフェイスで障害が発生することはないので、この方法により安定性が向上します。OSPF では、他のインターフェイスよりループバック インターフェイスが自動的に優先され、すべてのループバック インターフェイスの中で最も数値の高い IP アドレスを持つループバック インターフェイスが選択されます。

ループバック インターフェイスを設定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router# 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	Router(config)# interface loopback 0	ループバック インターフェイスを作成し、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	Router(config)# ip address address mask	このインターフェイスに IP アドレスを割り当てます。
ステップ 4	Router(config)# end	イネーブル EXEC モードに戻ります。
ステップ 5	Router# show ip interface	エントリを確認します。
ステップ 6	Router# copy running-config startup-config	(任意) コンフィギュレーション ファイルにエントリを保存します。

ループバック インターフェイスをディセーブルにするには、**no interface loopback 0** グローバル コンフィギュレーション コマンドを使用します。

OSPF のモニタリング

IP ルーティング テーブル、キャッシュ、およびデータベースの内容など、特定の統計を表示できます。

表 11-3 に統計を表示するためのイネーブル EXEC コマンドの一部をリストします。**show ip ospf database** イネーブル EXEC コマンド オプションとコマンド出力内のフィールドの詳細については、『Cisco IOS IP and IP Routing Command Reference』を参照してください。

表 11-3 Show IP OSPF 統計コマンド

コマンドの説明	目的
Router(config)# show ip ospf [process-id]	OSPF ルーティング プロセスの全般情報を表示します。
Router(config)# show ip ospf [process-id] database [router] [link-state-id]	OSPF データベース関連情報のリストを表示します。
Router(config)# show ip ospf border-routes	内部 OSPF ルーティング ABR テーブルおよび ASBR テーブルのエントリを表示します。
Router(config)# show ip ospf interface [interface-name]	OSPF 関連のインターフェイス情報を表示します。
Router(config)# show ip ospf neighbor [interface-name] [neighbor-id] detail	OSPF インターフェイスのネイバ情報を表示します。
Router(config)# show ip ospf virtual-links	OSPF 関連の仮想リンク情報を表示します。

EIGRP の設定

EIGRP は、Interior Gateway Routing Protocol (IGRP) をシスコが独自に拡張したバージョンです。EIGRP では、IGRP と同じディスタンス ベクタ アルゴリズムと距離情報を使用していますが、EIGRP のコンバージェンスのプロパティと運用効率は、大きく向上しました。

コンバージェンス テクノロジーでは、Diffusing Update Algorithm (DUAL; 拡散更新アルゴリズム) というアルゴリズムを採用しています。このアルゴリズムでは、ルート計算中は常にループしないことが保証されており、トポロジー変更に関係するすべての装置を同時に同期させることができます。トポロジー変更の影響を受けないルータは、再計算に関係しません。

IP EIGRP によりネットワークの規模が拡大します。RIP では、ネットワークの最大幅は、15 ホップでした。IGRP をイネーブルにすると、最大 224 ホップが可能で、EIGRP メトリックでは数千ホップがサポートされるので、ネットワークを拡大する場合の唯一の障害は、トランスポート層のホップ カウントになります。EIGRP では、IP パケットが 15 個のルータを経由したあと、EIGRP が宛先までのネクスト ホップを学習している場合だけに、転送制御フィールドの値が増加します。宛先までのネクスト ホップとして RIP ルートが使用された場合は、転送制御フィールドの値が通常どおりに増加します。

EIGRP には、次の機能があります。

- 高速コンバージェンス
- 宛先の状態が変化した場合の差分更新。ルーティング テーブルの内容全体を送信する代わりに、EIGRP パケットに必要な帯域幅を最小限に抑えます。
- IGRP より低い CPU 使用率 (完全に更新されたパケットは、受信するたびに処理する必要がないため)
- プロトコルに関係なく、近接ルータ情報を学習するネイバ検出メカニズム
- Variable-Length Subnet Mask (VLSM; 可変長サブネット マスク)
- 任意の経路集約
- EIGRP による大規模ネットワークへの拡大

EIGRP には、次の 4 つの基本的なコンポーネントがあります。

- ネイバ検出および回復は、ルータが、直接接続されたネットワーク上の他のルータについて動的に学習するために使用するプロセスです。ルータは、ネイバが到達不能または動作不能になった場合も検出できる必要があります。ネイバ検出および回復機能では、定期的に少量の Hello パケットを送信するだけなので、オーバーヘッドが少なくすみずみます。Cisco IOS ソフトウェアでは、Hello パケットを受信している限り、ネイバが機能しているものと判断されます。この状態にあると判断された場合、近接ルータはルーティング情報を交換できます。
- 高信頼性転送プロトコルにより、すべてのネイバに EIGRP パケットを確実に順序どおりに転送できます。マルチキャスト パケットとユニキャスト パケットが混在している場合でも転送が可能です。EIGRP パケットには、確実に送信する必要があるパケットとその必要がないパケットがあります。効率化するために、必要な場合に限って信頼性を確保します。たとえば、マルチアクセス ネットワークにはマルチキャスト機能 (イーサネットなど) がありますが、すべてのネイバそれぞれに Hello パケットを確実に送信する必要はありません。そのため、EIGRP では、マルチキャスト Hello パケットを 1 つ送信し、そのパケット内でそのパケットの確認応答が不要であることを受信側に通知します。その他のタイプのパケット (更新など) では、確認応答が必要なため、パケット内でそのことを通知します。転送の信頼性を確保するには、確認応答を受信していないパケットがある場合に、すぐにマルチキャストパケットを送信するように設定します。この方法により、速度が異なるリンクがある場合にも、コンバージェンス時間を短く抑えることができます。

- DUAL 有限状態マシンは、すべてのルート計算を決定するプロセスです。このプロセスは、すべてのネイバからアドバタイズされたすべてのルートをトラッキングします。DUAL は、距離情報（メトリック）を使用して、効率がよい、ループフリー パスを選択します。また、DUAL は、サクセサ候補に基づいて、ルーティング テーブルに挿入するルートを選択します。サクセサとは、パケット転送に使用する近接ルータを指します。サクセサとなる近接ルータは、宛先までの最短コスト パスが設定されていて、ルーティング ループに関与しないことが保証されています。サクセサ候補がないにもかかわらず、ネイバが宛先をアドバタイズしている場合は、再計算が必要です。新しいサクセサは、このような方法で決定されます。ルートの再計算時間は、コンバージェンス時間に影響します。再計算には、大量のプロセッサ リソースが集中的に必要なので、できるだけ再計算しない方が便利です。トポロジー変更が発生すると、DUAL によってサクセサ候補がテストされます。サクセサ候補が検出されると、不必要な再計算を避けるために、その候補が使用されます。
- プロトコル依存型モジュールは、ネットワーク層プロトコル固有のタスクを実行します。このタイプのモジュールの例として、IP にカプセル化された EIGRP パケットを送受信する IP EIGRP モジュールがあげられます。このモジュールは、EIGRP パケットの解析、および新着情報の DUAL への通知も処理します。EIGRP は、DUAL にルーティングを決定するように要求しますが結果は IP ルーティング テーブルに保存されます。EIGRP は、他の IP ルーティング プロトコルが学習したルートも再配布します。

表 11-4 にデフォルトの EIGRP 設定を示します。

表 11-4 EIGRP のデフォルト設定

機能	デフォルト設定
自動サマリー	イネーブル。サブプレフィックスは、全クラスを使用したネットワーク境界を通過するときに、そのネットワーク境界に集約されます。
デフォルト情報	外部ルートが許可され、再配布時に IGRP プロセスまたは EIGRP プロセスの間でデフォルトの情報が渡されます。
デフォルトのメトリック	デフォルトのメトリックを使用せずに、接続されたルートとインターフェイスのスタティックルートだけを再配布できます。このメトリックには、次の情報が含まれています。 <ul style="list-style-type: none"> • 帯域幅：0 Kbps 以上 • 遅延（10 マイクロ秒単位）：0、または 39.1 ナノ秒の倍数である正数。 • 信頼性：0 ~ 255 の任意の数値（255 は信頼性 100 %） • ロード：有効帯域幅。0 ~ 255 の任意の数値（255 はロード 100 %） • MTU：ルートの最大伝送ユニット サイズ（秒単位）。0 または正の整数。
距離	内部距離：90 外部距離：170
EIGRP 近隣ルータの変更ログ	ディセーブル。隣接関係の変更はログに記録されません。
IP 認証キーチェーン	認証なし
IP 認証モード	認証なし
IP 帯域幅 (%)	50 %
IP Hello 間隔	低速 Nonbroadcast Multiaccess (NBMA) ネットワークの場合は 60 秒、他のすべてのネットワークの場合は 5 秒。
IP 待機時間	低速 NBMA ネットワークの場合は 180 秒、他のすべてのネットワークの場合は 15 秒。

表 11-4 EIGRP のデフォルト設定 (続き)


機能	デフォルト設定
IP スプリット ホライズン	イネーブル。
IP サマリー アドレス	サマリー集約アドレスは未定義
メトリックの重み	tos : 0 k1 と k3 : 1 k2、k4、および k5 : 0
ネットワーク	未指定
オフセットリスト	ディセーブル
ルータ EIGRP	ディセーブル
メトリック設定	ルートマップでのメトリックは未設定
トラフィック共有	メトリックの割合に比例して分散
分散	1 (等コストロードバランシング)

EIGRP ルーティング プロセスを作成するには、EIGRP をイネーブルにして、ネットワークを関連付けます。EIGRP は、指定されたネットワークのインターフェイスに更新情報を送信します。インターフェイスのネットワークを指定しない場合は、EIGRP の更新情報でアドバタイズされません。

EIGRP ルータ モード コマンド

EIGRP を設定するには、イネーブル EXEC モードで次の手順を実行します。ルーティング プロセスの設定は必須ですが、それ以外は任意です。

	コマンドの説明	目的
ステップ 1	Router# <code>configure terminal</code>	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	Router(config)# <code>router eigrp autonomous-system-number</code>	EIGRP ルーティング プロセスをイネーブルにし、ルータ コンフィギュレーション モードを開始します。AS 番号により他の EIGRP ルータへのルートが指定されます。この番号は、ルーティング情報のタグ付けに使用されます。
ステップ 3	Router(config)# <code>network network-number</code>	ネットワークを EIGRP ルーティング プロセスに関連付けます。EIGRP は、指定されたネットワークのインターフェイスに更新情報を送信します。インターフェイスのネットワークを指定していない場合は、EIGRP または EIGRP の更新情報でアドバタイズされません。
ステップ 4	Router(config)# <code>eigrp log-neighbor-changes</code>	(任意) EIGRP ネイバ変更のログをイネーブルにし、ルーティング システムの安定性をモニタリングします。

	コマンドの説明	目的
ステップ 5	Router(config)# metric weights tos k1 k2 k3 k4 k5	(任意) EIGRP メトリックを調整します。デフォルト値は、ほとんどのネットワークで効率的に運用できるように慎重に決定されていますが、カスタマイズすることもできます。  注意 メトリックの決定は複雑なので、カスタマイズする場合は、必ず経験豊富なネットワーク設計者の指示を受けてください。
ステップ 6	Router(config)# offset list [<i>{access-list-number name}</i>] { <i>in out</i> } <i>offset</i> [<i>type-number</i>]	(任意) オフセット リストをルーティング メトリックに適用し、EIGRP 経由で学習したルートに着信と発信のメトリックを増やします。オフセット リストをアクセス リストやインターフェイスで制限することができます。
ステップ 7	Router(config)# no auto-summary	(任意) ネットワークレベルのルートへのサブネット ルートの自動サマリーをディセーブルにします。
ステップ 8	Router(config)# ip summary-address eigrp <i>autonomous-system-number</i> <i>address-mask</i>	(任意) サマリー集約を設定します。
ステップ 9	Router(config)# end	イネーブル EXEC モードに戻ります。
ステップ 10	Router# show ip protocols	エントリを確認します。
ステップ 11	Router# copy running-config startup-config	(任意) コンフィギュレーション ファイルにエントリを保存します。

この機能をディセーブルにする場合、またはデフォルト値に戻す場合は、これらのコマンドの **no** 形式を使用します。例 11-8 に **show ip protocols** イネーブル EXEC コマンドの出力を示します。

例 11-8 show ip protocols イネーブル EXEC コマンドの出力 (EIGRP の場合)

```
Router# show ip protocols
Routing Protocol is "eigrp 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 1
  Automatic network summarization is in effect
  Automatic address summarization:
    192.168.3.0/24 for POS0
    192.168.2.0/24 for FastEthernet0
  Maximum path: 4
  Routing for Networks:
    192.168.2.0
    192.168.3.0
  Routing Information Sources:
    Gateway         Distance      Last Update
  192.168.2.1             90          00:03:16
  Distance: internal 90 external 170
```


EIGRP インターフェイス モード コマンド

他の任意の EIGRP パラメータは、インターフェイス ベースで設定できます。

イネーブル EXEC モードを開始し、次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router# <code>configure terminal</code>	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	Router(config)# <code>interface interface-id</code>	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、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	Router(config)# <code>ip bandwidth-percent eigrp autonomous-system-number percent</code>	(任意) インターフェイスで EIGRP に使用できる帯域幅の最大パーセンテージを設定します。デフォルトは 50% です。
ステップ 4	Router(config)# <code>ip summary-address eigrp autonomous-system-number address mask</code>	(任意) 指定したインターフェイスについて、サマリー集約アドレスを設定します (自動サマリーをイネーブルにしている場合は、通常不要)。
ステップ 5	Router(config)# <code>ip hello-interval eigrp autonomous-system-number seconds</code>	(任意) EIGRP ルーティング プロセスの Hello 時間間隔を変更します。範囲は、1 ~ 65535 秒です。低速 NBMA ネットワークのデフォルトは 60 秒、他のすべてのネットワークのデフォルトは 5 秒です。
ステップ 6	Router(config)# <code>ip hold-time eigrp autonomous-system-number seconds</code>	(任意) EIGRP ルーティング プロセスの待機時間間隔を変更します。範囲は、1 ~ 65535 秒です。低速 NBMA ネットワークのデフォルトは 180 秒、他のすべてのネットワークのデフォルトは 15 秒です。  注意 待機時間を調整する場合は、シスコのテクニカル サポートに相談してください。
ステップ 7	Router(config)# <code>no ip split-horizon eigrp autonomous-system-number</code>	(任意) スプリット ホライズンをディセーブルにし、ルート情報を発信したインターフェイス上にあるルータがそのルート情報をアドバタイズできるようにします。
ステップ 8	Router# <code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 9	Router# <code>show ip eigrp interface</code>	EIGRP がアクティブなインターフェイスとこれらのインターフェイスに関する EIGRP 情報を表示します。
ステップ 10	Router# <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルにエントリを保存します。

この機能をディセーブルにする場合、またはデフォルト値に戻す場合は、これらのコマンドの `no` 形式を使用します。例 11-9 に `show ip eigrp interface` イネーブル EXEC コマンドの出力を示します。

例 11-9 show ip eigrp interface イネーブル EXEC コマンドの出力

```
Router# show ip eigrp interface
IP-EIGRP interfaces for process 1

      Xmit Queue  Mean   Pacing Time  Multicast    Pending
Interface  Peers  Un/Reliable  SRTT  Un/Reliable  Flow Timer  Routes
PO0                1     0/0        20    0/10        50          0
Fa0                0     0/0         0     0/10         0          0
```

EIGRP ルート認証の設定

EIGRP のルート認証では、EIGRP ルーティング プロトコルからのルーティング更新を MD5 認証し、承認されていない送信元から権限がないルーティング メッセージや不正ルーティング メッセージを受信するのを防ぐことができます。

認証をイネーブルにするには、イネーブル EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router# 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	Router(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、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	Router(config-if)# ip authentication mode eigrp autonomous-system-number md5	IP EIGRP パケットで MD5 認証をイネーブルにします。
ステップ 4	Router(config-if)# ip authentication key-chain eigrp autonomous-system-number key-chain	IP EIGRP パケットの認証をイネーブルにします。
ステップ 5	Router(config-if)# exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	Router(config)# key chain name-of-chain	キーチェーンを指定し、キーチェーン コンフィギュレーション モードを開始します。ステップ 4 で設定した名前を指定します。
ステップ 7	Router(config-keychain)# key number	キーチェーン コンフィギュレーション モードで、キー番号を指定します。
ステップ 8	Router(config-keychain)# key-string text	キーチェーンのキー コンフィギュレーション モードで、キー文字列を指定します。
ステップ 9	Router(config-keychain-key)# accept-lifetime start-time {infinite end-time duration seconds}	(任意) キーを受信できる期間を指定します。 <i>start-time</i> と <i>end-time</i> の構文には、 <i>hh:mm:ss Month date year</i> または <i>hh:mm:ss date Month year</i> のいずれかを使用します。デフォルトの <i>start-time</i> (および指定可能な最も古い日付) は、1993 年 1 月 1 日です。デフォルトの <i>end-time</i> と duration に制限はありません。
ステップ 10	Router(config-keychain-key)# send-lifetime start-time {infinite end-time duration seconds}	(任意) キーを送信できる期間を指定します。 <i>start-time</i> と <i>end-time</i> の構文には、 <i>hh:mm:ss Month day year</i> または <i>hh:mm:ss day Month year</i> のいずれかを指定します。デフォルトの <i>start-time</i> (および指定可能な最も古い日付) は、1993 年 1 月 1 日です。デフォルトの <i>end-time</i> と duration に制限はありません。

	コマンドの説明	目的
ステップ 11	Router(config)# end	イネーブル EXEC モードに戻ります。
ステップ 12	Router# show key chain	認証キー情報を表示します。
ステップ 13	Router# copy running-config startup-config	(任意) コンフィギュレーション ファイルにエントリを保存します。

機能をディisableにするか、または設定値をデフォルトに戻す場合は、これらのコマンドの **no** 形式を指定します。

EIGRP のモニタリングとメンテナンス

ネイバテーブルからネイバを削除できます。各種の EIGRP ルーティング統計情報も表示できます。表 11-5 に、ネイバを削除して統計情報を表示するイネーブル EXEC コマンドを示します。コマンド出力のフィールドの詳細については、『Cisco IOS IP and IP Routing Command Reference』を参照してください。

表 11-5 IP EIGRP の Clear コマンドと Show コマンド

コマンドの説明	目的
Router# clear ip eigrp neighbors {ip-address interface}	ネイバ テーブルからネイバを削除します。
Router# show ip eigrp interface [interface] [as-number]	EIGRP に設定したインターフェイスの情報を表示します。
Router# show ip eigrp neighbors [type-number]	EIGRP で検出されたネイバを表示します。
Router# show ip eigrp topology {autonomous-system-number [ip-address] mask}	特定のプロセスについて EIGRP トポロジー テーブルを表示します。
Router# show ip eigrp traffic [autonomous-system-number]	すべての EIGRP プロセス、または指定した EIGRP プロセスについて送受信されたパケットの数を表示します。

例 11-10 に show ip eigrp interface イネーブル EXEC コマンドの出力を示します。例 11-11 に show ip eigrp neighbors イネーブル EXEC コマンドの出力を示します。例 11-12 に show ip eigrp topology イネーブル EXEC コマンドの出力を示します。例 11-13 に show ip eigrp traffic イネーブル EXEC コマンドの出力を示します。

例 11-10 show ip eigrp interface イネーブル EXEC コマンドの出力

```
Router# show ip eigrp interface
IP-EIGRP interfaces for process 1

Interface      Peers  Xmit Queue  Mean  Pacing Time  Multicast  Pending
                Un/Reliable SRTT  Un/Reliable  Flow Timer  Routes
PO0             1      0/0         20    0/10         50         0
Fa0             0      0/0         0     0/10         0          0
```

例 11-11 show ip eigrp neighbors イネーブル EXEC コマンドの出力

```
Router# show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address                Interface  Hold Uptime  SRTT  RTO  Q  Seq Type
                   (sec)      (ms)      Cnt  Num
0   192.168.2.1              PO0       13 00:08:15  20   200  0  2
```

例 11-12 show ip eigrp topology イネーブル EXEC コマンドの出力

```
Router# show ip eigrp topology
IP-EIGRP Topology Table for AS(1)/ID(192.168.3.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 192.168.1.0/24, 1 successors, FD is 30720
   via 192.168.2.1 (30720/28160), POS0
P 192.168.2.0/24, 1 successors, FD is 10752
   via Connected, POS0
P 192.168.3.0/24, 1 successors, FD is 28160
   via Connected, FastEthernet0
```

例 11-13 show ip eigrp traffic イネーブル EXEC コマンドの出力

```
Router# show ip eigrp traffic
IP-EIGRP Traffic Statistics for process 1
  Hellos sent/received: 273/136
  Updates sent/received: 5/2
  Queries sent/received: 0/0
  Replies sent/received: 0/0
  Acks sent/received: 1/2
  Input queue high water mark 1, 0 drops
  SIA-Queries sent/received: 0/0
  SIA-Replies sent/received: 0/0
```

BGP と CIDR

Border Gateway Protocol (BGP) は、AS 間でループフリーなルーティング情報交換を自動的に保証するようにドメイン間のルーティング システムをセットアップするための Exterior Gateway Protocol (EGP; 外部ゲートウェイ プロトコル) です。BGP では、各ルートが、ネットワーク番号、情報が通過した AS (AS パス) のリスト、および他のパス属性のリストで構成されます。

レイヤ 3 のスイッチングでは、Classless Interdomain Routing (CIDR) を含む BGP バージョン 4 がサポートされます。CIDR では、集約ルートを作成してスーパーネットにすることで、ルーティング テーブルのサイズを減らすことができます。CIDR により、BGP 内のネットワーク クラスの概念が取り除かれ、IP プレフィックスのアドバタイズがサポートされます。CIDR のルートは、OSPF、EIGRP、および RIP で伝送されます。

BGP の設定

BGP ルーティングを設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router(config)# ip routing	IP ルーティングをイネーブルにします (デフォルト)。
ステップ 2	Router(config)# router bgp <i>autonomous-system</i>	BGP をルーティング プロトコルとして定義して、BGP ルーティング プロセスを開始します。
ステップ 3	Router(config-router)# network <i>network-number [mask network-mask]</i> <i>[route-map route-map-name]</i>	ネットワークがこの AS に対してローカルであることを表すフラグを設定し、BGP テーブルにそのフラグを追加します。
ステップ 4	Router(config-router)# end	イネーブル EXEC モードに戻ります。

例 11-14 に BGP ルーティングの設定例を示します。

例 11-14 BGP ルーティングの設定

```
Router(config)# ip routing
Router(config)# router bgp 30
Router(config-router)# network 192.168.1.1
Router(config-router)# neighbor 192.168.2.1
Router(config-router)# end
```

BGP ルーティング設定の詳細については、『Cisco IOS IP and IP Routing Configuration Guide』の「Configuring BGP」の章を参照してください。

BGP 設定の確認

表 11-6 に BGP 設定を表示するための共通 EXEC コマンドの一部を示します。また、例 11-15 に表 11-6 でリストされたコマンドの出力を示します。

表 11-6 BGP の Show コマンド

コマンドの説明	目的
Router# <code>show ip protocols [summary]</code>	プロトコル設定を表示します。
Router# <code>show ip bgp neighbor</code>	各ネイバへの BGP 接続と TCP 接続の詳細情報を表示します。
Router# <code>show ip bgp summary</code>	すべての BGP 接続のステータスを表示します。
Router# <code>show ip bgp</code>	BGP ルーティング テーブルの内容を表示します。

例 11-15 BGP 設定情報

```
Router# show ip protocols
Routing Protocol is "bgp 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  IGP synchronization is enabled
  Automatic route summarization is enabled
  Redistributing: connected
  Neighbor(s):
    Address          FiltIn FiltOut DistIn DistOut Weight RouteMap
    192.168.2.1
  Maximum path: 1
  Routing for Networks:
  Routing Information Sources:
    Gateway          Distance      Last Update
  Distance: external 20 internal 200 local 200

Router# show ip bgp neighbor
BGP neighbor is 192.168.2.1, remote AS 1, internal link
  BGP version 4, remote router ID 192.168.2.1
  BGP state = Established, up for 00:08:46
  Last read 00:00:45, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family IPv4 Unicast: advertised and received
  Received 13 messages, 0 notifications, 0 in queue
  Sent 13 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Default minimum time between advertisement runs is 5 seconds
```

```

For address family: IPv4 Unicast
  BGP table version 3, neighbor version 3
  Index 1, Offset 0, Mask 0x2
  2 accepted prefixes consume 72 bytes
  Prefix advertised 2, suppressed 0, withdrawn 0
  Number of NLRI in the update sent: max 2, min 0

Connections established 1; dropped 0
Last reset never
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Local host: 192.168.2.2, Local port: 179
Foreign host: 192.168.2.1, Foreign port: 11001

Enqueued packets for retransmit: 0, input: 0 mis-ordered: 0 (0 bytes)

Event Timers (current time is 0x45B7B4):
Timer           Starts      Wakeups      Next
Retrans          13          0            0x0
TimeWait         0           0            0x0
AckHold          13          9            0x0
SendWnd          0           0            0x0
KeepAlive        0           0            0x0
GiveUp           0           0            0x0
PmtuAger         0           0            0x0
DeadWait         0           0            0x0

iss: 3654396253  snduna: 3654396567  sndnxt: 3654396567  sndwnd: 16071
irs: 3037331955  rcvnxt: 3037332269  rcvwnd: 16071  delrcvwnd: 313

SRTT: 247 ms, RTTO: 663 ms, RTV: 416 ms, KRTT: 0 ms
minRTT: 4 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: passive open, nagle, gen tcbs

Datagrams (max data segment is 1460 bytes):
Rcvd: 15 (out of order: 0), with data: 13, total data bytes: 313
Sent: 22 (retransmit: 0), with data: 12, total data bytes: 313

Router# show ip bgp summary
BGP router identifier 192.168.3.1, local AS number 1
BGP table version is 3, main routing table version 3
3 network entries and 4 paths using 435 bytes of memory
2 BGP path attribute entries using 120 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP activity 3/6 prefixes, 4/0 paths, scan interval 60 secs

Neighbor      V    AS MsgRcvd MsgSent  TblVer  InQ  OutQ Up/Down  State/PfxRcd
192.168.2.1   4    1    14     14      3     0    0 00:09:45      2

Router# show ip bgp
BGP table version is 3, local router ID is 192.168.3.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop           Metric LocPrf Weight Path
* i192.168.1.0      192.168.2.1         0     100      0 ?
* i192.168.2.0      192.168.2.1         0     100      0 ?
*>                 0.0.0.0             0           32768 ?
*> 192.168.3.0      0.0.0.0             0           32768 ?

```

IS-IS の設定

Intermediate System-to-Intermediate System (IS-IS) ルーティングを設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router(config)# router isis [tag]	IS-IS を IP ルーティングプロトコルとして定義します。
ステップ 2	Router(config-router)# net network-entity-title	ルーティング プロセスについて Network Entity Title (NET) を設定します。NET には、名前とアドレスを指定できます。
ステップ 3	Router(config-router)# interface interface-type 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 4	Router(config-if)# ip address ip-address mask	このインターフェイスに IP アドレスを割り当てます。
ステップ 5	Router(config-if)# ip router isis [tag]	このインターフェイスで IS-IS を実行することを指定します。
ステップ 6	Router(config-if)# end	イネーブル EXEC モードに戻ります。

例 11-16 に IS-IS ルーティングの設定例を示します。

例 11-16 IS-IS ルーティングの設定

```
Router(config)# router isis
Router(config-router)# net 49.0001.0000.0000.000a.00
Router(config-router)# interface gigabitethernet 0
Router(config-if)# ip router isis
Router(config-if)# end
```

IS-IS ルーティング設定の詳細については、『Cisco IOS IP and IP Routing Configuration Guide』の「Configuring Integrated IS-IS」の章を参照してください。

IS-IS 設定の確認

IS-IS 設定を確認するには、表 11-7 に示した EXEC コマンドを使用します。例 11-17 に表 11-7 のコマンドとその出力の例を示します。

表 11-7 IS-IS の Show コマンド

コマンドの説明	目的
Router# show ip protocols [summary]	プロトコル設定を表示します。
Router# show isis database	IS-IS リンク状態データベースを表示します。
Router# show clns neighbor	ES と IS のネイバを表示します。



(注) ML シリーズでは、Connectionless Network Service (CLNS; コネクションレス型ネットワーク サービス) プロトコルのルーティングがサポートされません。

例 11-17 IS-IS の設定

```

Router# show ip protocols
Routing Protocol is "isis"
  Invalid after 0 seconds, hold down 0, flushed after 0
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: isis
  Address Summarization:
    None
  Maximum path: 4
  Routing for Networks:
    FastEthernet0
    POS0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.2.1     115          00:06:48
  Distance: (default is 115)

Router# show isis database

IS-IS Level-1 Link State Database:
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
Router_A.00-00  0x00000003   0xA72F        581            0/0/0
Router_A.02-00  0x00000001   0xA293        581            0/0/0
Router.00-00    * 0x00000004  0x79F9        582            0/0/0
IS-IS Level-2 Link State Database:
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
Router_A.00-00  0x00000004   0xF0D6        589            0/0/0
Router_A.02-00  0x00000001   0x328C        581            0/0/0
Router.00-00    * 0x00000004  0x6A09        586            0/0/0

Router# show clns neighbors

System Id      Interface  SNPA              State  Holdtime  Type Protocol
Router_A       PO0       0005.9a39.6790   Up     7          L1L2 IS-IS

```


スタティック ルートの設定

スタティック ルートは、ユーザが定義するルートです。パケットは、ユーザが指定したパスを通じて、送信元と宛先の間で移動します。スタティック ルートは、ルータが特定の宛先までのルートを作成できない場合に重要になります。また、最終手段としてゲートウェイを指定し、ルーティングできないパケットをすべてそのゲートウェイに送信する場合にも便利です。

スタティック ルートを設定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router# 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	Router(config)# ip route prefix mask { address interface } [distance]	スタティック ルートを設定します。例 11-18 に例を示します。
ステップ 3	Router(config)# end	イネーブル EXEC モードに戻ります。
ステップ 4	Router# copy running-config startup-config	(任意) コンフィギュレーション ファイルにエントリを保存します。

例 11-18 スタティック ルート

```
Router(config)# ip route 0.0.0.0 0.0.0.0 192.168.2.1
```

スタティック ルートを削除するには、**no ip route prefix mask {address | interface}** グローバル コンフィギュレーション コマンドを使用します。スタティック IP ルートの情報を表示するには、**show ip routes** イネーブル EXEC コマンドを使用します (例 11-19)。

例 11-19 show ip route イネーブル EXEC コマンドの出力 (スタティック ルートを設定した場合)

```
Router# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is 192.168.2.1 to network 0.0.0.0

C    192.168.2.0/24 is directly connected, POS0
C    192.168.3.0/24 is directly connected, FastEthernet0
S*   0.0.0.0/0 [1/0] via 192.168.2.1
```

show ip route イネーブル EXEC コマンドの出力では、ルーティング プロトコルのコードが表示されます。表 11-8 に、これらのルーティング プロトコルに関するデフォルトの管理距離を示します。

表 11-8 ルーティング プロトコルのデフォルトの管理距離

ルート ソース	デフォルトの距離
接続されたインターフェイス	0
スタティック ルート	1
EIRGP サマリー ルート	5
外部 BGP	20
内部 EIGRP	90
OSPF	110
RIP	120
外部 EIGRP	170
内部 BGP	200
不明	225

スタティック ルートのモニタリング

スタティック ルートの統計情報を表示するには、**show ip route** コマンドを使用します (例 11-20)。**show ip** イネーブル EXEC コマンドのオプションとコマンド出力内のフィールドの詳細については、『Cisco IOS IP and IP Routing Command Reference』を参照してください。

例 11-20 show ip route コマンドの出力 (スタティック ルートを設定した場合)

```
Router# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.2.1 to network 0.0.0.0

C    192.168.2.0/24 is directly connected, POS0
C    192.168.3.0/24 is directly connected, FastEthernet0
S*  0.0.0.0/0 [1/0] via 192.168.2.1
```

IP ネットワークのモニタリングとメンテナンス

特定のキャッシュ、テーブル、またはデータベースの内容をすべて削除することができます。また、特定の統計情報も表示できます。ルートのクリアやステータスの表示には、表 11-9 のイネーブル EXEC コマンドを使用します。

表 11-9 IP ルートのクリアまたはルート ステータスの表示を行うコマンド

コマンドの説明	目的
Router# <code>clear ip route {network [mask *]}</code>	IP ルーティング テーブルから 1 つまたは複数のルートをクリアします。
Router# <code>show ip protocols</code>	パラメータとアクティブなルーティング プロトコル プロセスの状態を表示します。
Router# <code>show ip route [{address [mask] [longer-prefixes] [protocol [process-id]]}]</code>	ルーティング テーブルの現在の状態を表示します。
Router# <code>show ip interface interface</code>	インターフェイスの詳細情報を表示します。
Router# <code>show ip interface brief</code>	すべてのインターフェイスの状態に関する要約情報を表示します。
Router# <code>show ip route summary</code>	ルーティング テーブルの現在の状態を要約して表示します。
Router# <code>show ip route supernets-only</code>	スーパーネットを表示します。
Router# <code>show ip cache</code>	IP トラフィックのスイッチングに使用するルーティング テーブルを表示します。
Router# <code>show route-map [map-name]</code>	設定済みのすべてのルート マップまたは指定したルート マップだけを表示します。

IP マルチキャスト ルーティングの概要

ネットワークの規模が拡大するにつれて、マルチキャスト トラフィックを必要としているセグメントとそれ以外のセグメントを判断する上で、マルチキャスト ルーティングの重要性が非常に高まります。IP マルチキャストでは、IP トラフィックを 1 つまたは多数の送信元から多数の宛先に伝播させることができます。1 つのパケットを各宛先に送信するのではなく、1 つのパケットを 1 つの IP 宛先グループアドレスによって識別されるマルチキャスト グループに送信します。

IP マルチキャストの最も重要なコンポーネントは、Internet Group Management Protocol (IGMP) です。ホストは、IGMP メッセージを ML シリーズカードに送信して、マルチキャスト グループのメンバーシップを識別します。トラフィックは、マルチキャスト グループのすべてのメンバーに送信されます。1 つのホストを同時に複数のグループのメンバーに指定することも可能です。また、ホストがデータ送信先グループのメンバーである必要はありません。インターフェイスで Protocol Independent Multicast (PIM; プロトコル独立型マルチキャスト) を有効にすると、同じインターフェイスで IGMP の操作もイネーブルになります。

ML シリーズカードでは、PIM ルーティング プロトコルと Auto-RP 設定がサポートされます。

PIM には、トラフィック密度環境（密および疎）に関する 3 種類の動作モードがあります。これらのモードは、dense（密）モード、sparse（疎）モード、および疎/密モードと呼ばれます。

PIM の密モードでは、ダウンストリーム ネットワークがそこに転送されるデータグラムの受信を要求していると見なします。ML シリーズカードは、プルーニングや切り捨てが発生するまで、すべての発信インターフェイスですべてのパケットを転送します。PIM の密モードをイネーブルにしているインターフェイスは、タイムアウトするまでマルチキャスト データ ストリームを受信できません。次の条件下では、PIM の密モードが最も便利です。

- 送信側と受信側が近接して存在している。
- ネットワーク間で受信側より送信側が少ない。
- マルチキャスト トラフィックのストリームが一定である。

PIM の疎モードでは、トラフィックで明示的に要求されていない限り、ダウンストリーム ネットワークがグループに対するマルチキャスト パケットの転送を要求していないとみなします。PIM の疎モードでは、パケットを正しくルーティングするための登録ポイントとして使用する Rendezvous Point (RP; ランデブー ポイント) を定義します。

送信側がデータを送信する場合は、そのデータを RP に送信します。ML シリーズカードでデータを受信する準備が整っている場合は、このカードが RP に登録されます。データ ストリームが送信側から RP 経由で受信側に送信され始めると、データ パス内にある ML シリーズカードが不要なホップ（RP を含む）を自動的に削除してパスを最適化します。

PIM の疎モードは、マルチポイント データ ストリームが多く、各マルチキャスト ストリームがネットワーク内の比較的少数の LAN に送信される環境に適しています。次の条件下では、PIM の疎モードが最も便利です。

- グループ内に受信側がほとんどない。
- 送信側と受信側の間が WAN リンク で区切られている。
- マルチキャスト トラフィックのストリームが途切れがちである。



(注) ML シリーズカードでは、Reverse Path Forwarding (RPF; リバース パス転送) マルチキャストがサポートされますが、RPF ユニキャストはサポートされません。

IP マルチキャストルーティングの設定

IP マルチキャストルーティングを設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router(config)# ip multicast-routing	ML シリーズ カードで IP マルチキャストをイネーブルにします。
ステップ 2	Router(config)# interface type number	インターフェイスを設定するために、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	Router(config-if)# ip pim {dense-mode sparse mode sparse-dense-mode}	このコマンドを入力する各インターフェイスで IP マルチキャストルーティングを実行します。dense (密) モード、sparse (疎) モード、または疎 / 密モードを指定する必要があります。
ステップ 4	Router(config)# ip pim rp-address rendezvous-point ip-address	マルチキャスト グループの RP を設定します。
ステップ 5	Router(config-if)# end	イネーブル EXEC モードに戻ります。
ステップ 6	Router# copy running-config startup-config	(任意) 設定の変更を NVRAM に保存します。

IP マルチキャスト動作のモニタリングと確認

IP マルチキャストルーティングの設定後に、イネーブル EXEC モードで表 11-10 のコマンドを実行すると、設定した IP マルチキャストルーティングの動作をモニタリングして確認できます。

表 11-10 IP マルチキャストルーティングの Show コマンド

コマンドの説明	目的
Router# show ip mroute	完全なマルチキャストルーティング テーブルと処理済みパケットの複合統計を表示します。
Router# show ip pim neighbor	このコマンドを EXEC モードで使用すると、Cisco IOS ソフトウェアで検出された PIM ネイバが表示されます。
Router# show ip pim interface	PIM に設定したインターフェイスの情報を表示します。
Router# show ip pim rp	このコマンドを EXEC モードで使用すると、関連するマルチキャストルーティング エントリとともにキャッシュされたアクティブな RP が表示されます。

