IS-IS ルーティングの設定

IS-IS ルーティングに関する情報

Integrated Intermediate System-to-Intermediate System（IS-IS）は、ISO ダイナミック ルーティング プロトコルの一つです（ISO 105890 を参照）。IS-IS をイネーブルするには、IS-IS ルーティングプロセスを作成し、それをネットワークではなく特定のインターフェイスに割り当てる必要があります。マルチエリア IS-IS コンフィギュレーション シンタックスを使用することで、レイヤ 3 デバイスごとに複数の IS-IS ルーティングプロトコルを指定できます。その後、IS-IS ルーティングプロセスのインスタンスごとにパラメータを設定する必要があります。

小規模の IS-IS ネットワークは、ネットワーク内にすべてのデバイスが含まれる単一のエリアとして構築されます。このネットワークは、その規模が大きくなるにしたがって、ローカルエリアに接続されたままの、接続済みのレベル 2 デバイスのセットで構成されるバックボーンエリア内に再編成されます。ローカル エリアの内部では、デバイスがすべてのシステム ID に到達する方法を認識しています。エリア間では、デバイスはバックボーンへの到達方法を認識しており、バックボーン デバイスは他のエリアに到達する方法を認識しています。

デバイスは、ローカルエリア内でルーティングを実行するために、レベル 1 の隣接関係を確立します（ステーションルーティング）。デバイスは、レベル 2 隣接関係を確立して、レベル 1 エリア間でルーティングを実行します（エリアルーティング）。

1 つの Cisco デバイスは、最大 29 エリアのルーティングに参加でき、バックボーンでレベル 2 ルーティングを実行できます。一般に、ルーティング プロセスごとに 1 つのエリアに対応します。デフォルトでは、設定されているルーティングプロセスの最初のインスタンスが、レベル 1 ルーティングと レベル 2 ルーティングの両方を実行します。追加のデバイスインスタンスを設定できます。このインスタンスは、自動的にレベル 1 エリアとして扱われます。IS-IS ルーティング プロセスの各インスタンスごとに個別にパラメータを設定する必要があります。

IS-IS マルチエリア ルーティングでは、シスコの各装置に対して最大 29 個の レベル 1 エリアを定義できますが、レベル 2 ルーティングを実行するプロセスは 1 つだけ設定できます。レベル2ルーティングが任意のプロセス上に設定されている場合、追加のプロセスは、すべて自動的にレベル 1 に設定されます。同時に、このプロセスがレベル 1 ルーティングを実行するように設定することもできます。デバイスインスタンスにレベル2ルーティングが必要でない場合は、 グローバル コンフィギュレーション モードで **is-type** コマンドを使用してレベル 2 の機能を削除します。別のデバイスインスタンスをレベル2デバイスとして設定する場合にも **is-type** コマンドを使用します。

IS-IS 認証

無許可のデバイスがリンクステートデータベースに誤ったルーティング情報を挿入することを防ぐために、インターフェイスごとにプレーンテキストのパスワードを設定するとともにIS-IS エリアごとにエリアパスワードを設定するか、IS-IS 認証を設定することができます。

プレーンテキストのパスワードは、無許可のユーザーに対するセキュリティを提供しません。プレーンテキストのパスワードを設定すると、無許可のネットワーキングデバイスがルータと隣接関係を形成することを防ぐことができます。このパスワードはプレーンテキストで交換されるため、アクセスして IS-IS パケットを表示できるエージェントによって参照されます。

新しい IS-IS 認証方式には、プレーンテキストパスワード設定コマンドに比べて次のような利点があります。

- ソフトウェア設定が表示されるときにパスワードが暗号化されます。
- パスワードの管理や変更がより容易になります。
- ネットワークの運用を中断させることなく、新しいパスワードに変更できます。
- 中断なしで認証を移行できます。

認証モード（IS-IS 認証またはプレーンテキストパスワード）は、特定の範囲（IS-IS インスタンスもしくはインターフェイス）またはレベルのいずれかで設定できますが、両方を設定することはできません。ただし、異なる範囲およびレベルに対して、異なるモードを設定することができます。混合モードが設定されている場合は、異なるモードには異なるキーを使用して、プロトコルデータユニット（PDU）で暗号化されたパスワードが危険にさらされないようにする必要があります。

クリアテキスト認証

IS-IS クリアテキスト認証は **area-password** コマンドまたは **domain-password** コマンドによって提供される機能と同じ機能を提供します。

HMAC-MD5 認証

IS-IS は、クリアテキスト認証より安全性の高いメッセージダイジェストアルゴリズム 5（MD5）認証をサポートしています。

ハッシュメッセージ認証コード（HMAC）は暗号学的ハッシュ関数を使用するメッセージ認証符号（MAC）のためのメカニズムです。HMAC-MD5 認証では、各 IS-IS PDU に HMAC-MD5 ダイジェストを追加します。ダイジェストによって、不正なルーティング メッセージがネットワーク ルーティング ドメインに入り込むのを防御できるため、IS-IS ルーティング プロトコル レベルでの認証が可能になります。

HMAC-MD5 認証の利点は次のとおりです。

- パスワードは、ルーティングメッセージを中断させずに新しいパスワードに変更できます。
- 中断なしで認証を移行できます。デバイスは、認証情報のない PDU や古い認証情報を持つ PDU を受け入れ、現在の認証情報を持つ PDU を送信します。このような移行は、認証なしの状態からあるタイプの認証に移行するとき、認証タイプを変更するとき、また認証キーを変更するときに便利です。

HMAC-SHA 認証

IS-IS では、MD5 認証またはクリアテキスト認証よりも安全性の高いセキュア ハッシュ アルゴリズム（SHA）認証（SHA-1、SHA-256、SHA-384、および SHA-512）がサポートされています。

HMAC-SHA 認証方式を有効にすると、共通ネットワークに接続されているすべてのデバイスで共有秘密キーが設定されます。各パケットでは、このキーを使用して、パケットに追加されるメッセージダイジェストを生成および検証します。メッセージダイジェストはパケットおよび秘密キーの単方向機能です。

ヒットレス アップグレード

使用するセキュリティ認証をあるタイプから別のタイプに移行する前に、次の手順を実行する必要があります。

1. すべてのデバイスに、その新しい認証タイプをサポートする新しいイメージをロードする必要があります。デバイスは、すべてのデバイスが新しい認証方式をサポートする新しいイメージでロードされ、さらにすべてのデバイスがその新しい認証方式を使用するように設定されるまで、元の認証方式を使用し続けます。
2. 現在のキーと新しいキーの両方を含むキーチェーンを追加します。たとえば、HMAC-MD5 から HMAC-SHA1-20 に移行する場合、現在のキーは HMAC-MD5 であり、新しいキーは HMAC-SHA1-20 です。IS-IS が現在のキーを送信しつづけるように、現在のキーが新しいキーよりも send-lifetime フィールドの終了日が遅いことを確認してください。IS-IS が両方のキーを受け入れるように、両方のキーの accept-lifetime 値を infinite に設定してください。
3. 手順 2 が完了したら、リンクまたはエリア内のすべてのデバイスについて、現在のキーをキーチェーンから削除できます。

NSF 認識

統合型 IS-IS ノンストップ フォワーディング（NSF）認識機能は IPv4G でサポートされています。この機能により、NSF を認識する顧客宅内機器（CPE）デバイスが、NFS 対応デバイスによるパケットのノンストップ フォワーディングを実現します。ローカルデバイスでは、必ずしも NSF を実行している必要はありませんが、その NSF を認識機能により、スイッチオーバープロセス時にルーティングデータベースの完全性と精度、および隣接 NSF 対応デバイス上のリンクステートデータベースが保持できます。

統合型 IS-IS ノンストップ フォワーディング（NSF）認識機能は自動的に有効になり、設定は不要です。

IS-IS グローバル パラメータ

次に、設定可能なオプションの IS-IS グローバルパラメータを示します。

- ルートマップによって制御されるデフォルトルートを設定することで、デフォルトルートを IS-IS ルーティングドメイン内に強制的に設定できます。ルートマップで設定可能な、その他のフィルタリングオプションも指定できます。
- 内部チェックサムエラーとともに受信された IS-IS リンクステートパケット（LSP）を無視したり、破損した LSP を消去するようにデバイスを設定できます。これにより、LSP の発信側は、LSP を再生成します。
- エリアおよびドメインにパスワードを割り当てられます。
- ルーティングテーブルでサマリーアドレスによって表される（経路集約に基づいた）集約アドレスを作成できます。他のルーティングプロトコルから学習したルートも集約できます。サマリーをアドバタイズするのに使用されるメトリックは、すべての個別ルートにおける最小のメトリックです。
- 過負荷ビットを設定できます。
- LSP リフレッシュインターバルおよび LSP がリフレッシュなしでデバイスデータベース内にとどまることができる最大時間を設定できます。
- LSP 生成に対するスロットリング タイマー、最短パス優先計算、および部分ルート計算を設定できます。
- IS-IS 隣接関係（アジャセンシー）がステートを変更（アップまたはダウン）する際に、デバイスがログメッセージを生成するように設定できます。
- ネットワーク内のリンクが、1500 バイト未満の最大伝送ユニット（MTU）サイズの場合、それでもルーティングが行われるように LSP MTU の値を低くできます。
- **partition avoidance** コマンドを使用して、レベル 1-2 境界デバイス、隣接レベル 1 デバイス、およびエンドホスト間で完全な接続が失われた場合に、エリアがパーティション化されるのを防ぐことができます。

IS-IS インターフェイス パラメータ

任意で、特定のインターフェイス固有の IS-IS パラメータを、付加されている他のデバイスとは別に設定できます。ただし、デフォルト値（乗数およびタイムインターバルなど）を変更する場合、複数のデバイスおよびインターフェイス上でもこれを変更する必要があります。ほとんどのインターフェイスパラメータは、レベル1、レベル2、またはその両方で設定できます。

設定可能なインターフェイスレベルのパラメータは次のとおりです。

- インターフェイスのデフォルトメトリック：Quality of Service（QoS）ルーティングが実行されない場合に、IS-IS メトリックの値として使用され、割り当てられます。
- helloインターバル（インターフェイスから送信されるhelloパケットの間隔）またはデフォルトのhelloパケット乗数：インターフェイス上で使用されて、IS-IS helloパケットで送信されるホールド タイムを決定します。ホールド タイムは、ネイバーがダウンしていると宣言するまでに、別の hello パケットを待機する時間を決定します。これにより、障害リンクまたはネイバーが検出される速さも決定し、ルートを再計算できるようになります。hello パケットが頻繁に失われ、IS-IS 隣接に無用な障害が発生する場合は、hello 乗数を変更してください。hello 乗数を大きくし、それに対応して hello インターバルを小さくすると、リンク障害を検出するのに必要な時間を増やすことなく、helloプロトコルの信頼性を高めることができます。
- その他のタイム インターバル：
  - Complete Sequence Number PDU（CSNP）インターバル：CSNP は、データベースの同期を維持するために指定デバイスによって送信されます。
  - 再送信インターバル：これは、ポイントツーポイントリンクの IS-IS LSP の再送信間隔です。
  - IS-IS LSP 再送信スロットルインターバル：これは、IS-IS LSP がポイントツーポイントリンク上で再送信される最大レート（パケット間のミリ秒数）です。この間隔は、同じ LSP の連続した再送信の間隔である再送信インターバルとは異なります。
- 指定デバイスの選択の優先順位：マルチアクセスネットワークで必要な隣接数を削減し、その代わりに、ルーティング プロトコル トラフィックの量およびトポロジデータベースのサイズを削減できます。
- インターフェイス回線タイプ：指定されたインターフェイス上のネイバーに必要な隣接タイプです。
- インターフェイスのパスワード認証。

IS-IS の設定方法

ここでは、インターフェイスで IS-IS を有効にする方法、IS-IS グローバルパラメータを設定する方法、および IS-IS インターフェイスパラメータを設定する方法について説明します。

IS-IS のデフォルト設定

表 *1: IS-IS* のデフォルト設定

機能	デフォルト設定
リンクステート PDU（LSP）エラーを無視	イネーブル。
IS-IS タイプ	従来型の IS-IS：ルータは、レベル 1（ステーション）とレベア）両方のルータとして機能します。 マルチエリア IS-IS：IS-IS ルーティングプロセスの最初のインレベル 1-2 ルータです。残りのインスタンスは、レベル 1 ル
デフォルト情報送信元	ディセーブル。
IS-IS 隣接関係のステート変更を記録	ディセーブル。
LSP 生成スロットリング タイマー	連続した 2 つのオカレンス間の最大インターバル：5000 ミリ 初期 LSP 生成遅延：50 ミリ秒 最初と 2 番目の LSP 生成の間のホールド時間：200 ミリ秒
LSP 最大ライフ タイム（リフレッシュなし）	LSP パケットが削除されるまで 1200 秒（20 分）
LSP リフレッシュ インターバル	900 秒（15 分）ごと
最大 LSP パケット サイズ	1497 バイト
NSF 認識	イネーブル。レイヤ3デバイスでは、ハードウェアやソフト中に、隣接するノンストップ フォワーディング対応ルータがトを転送し続けることができます。
部分ルート計算（PRC）スロットリング タイマー	最大 PRC 待機インターバル：5000 ミリ秒 トポロジの変更後の初期 PRC 計算遅延：50 ミリ秒 最初と 2 番目の PRC 計算の間のホールド時間：200 ミリ秒
パーティション回避	ディセーブル。
パスワード	エリアまたはドメインのパスワードが定義されておらず、認証ブルになっています。
過負荷ビットの設定	ディセーブル。有効の際に引数が入力されない場合、過負荷ビちに設定され、**no set-overload-bit** コマンドが入力されるまでままになります。

機能	デフォルト設定
Shortest Path First（SPF）スロットリング タイマー	連続した SFP 間の最大インターバル：5000 ミリ秒 トポロジの変更後の初期 SFP 計算：200 ミリ秒 最初と 2 番目の SFP 計算の間のホールド時間：50 ミリ秒
サマリー アドレス	ディセーブル

IS-IS ルーティングのイネーブル化

IS-IS をイネーブルにするには、各ルーティングプロセスに名前とネットワーク エンティティ タイトル（NET）を指定します。インターフェイス上でIS-ISルーティングをイネーブルにし、ルーティングプロセスの各インスタンスに対してエリアを指定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device>enable`	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device#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 3	**clns routing** 例： `Device(config)#clns routing`	デバイス上で ISO コネクションレス型ルーティングをイネーブルに設定します。
ステップ 4	**router isis** [*area tag*] 例： `Device(config)#router isis tag1`	指定したルーティングプロセスに対して IS-IS ルーティングをイネーブルにし、IS-IS ルーティング コンフィギュレーション モードを開始します。 （任意）*area tag* 引数を使用して、IS-IS ルータが割り当てられているエリアを特定します。複数の IS-IS エリアを設定する場合は、値を入力します。 最初に設定された IS-IS インスタンスは、デフォルトでレベル 1-2 です。後のインスタンスは、自動的にレベル 1

	コマンドまたはアクション	目的
		に設定されます。グローバル コンフィギュレーション モードで **is-type** コマンドを使用してルーティングのレベルを変更できます。
ステップ 5	**net** *network-entity-title* 例： `Device(config-router)#net 47.0004.004d.0001.0001.0c11.1111.00`	ルーティング プロセスに NET を設定します。マルチエリア IS-IS を設定する場合は、各ルーティングプロセスに NET を指定します。NET およびアドレスの名前を指定します。
ステップ 6	**is-type** {**level-1** | **level-1-2** | **level-2-only**} 例： `Device(config-router)#is-type level-2-only`	（任意）レベル 1（ステーション）ルータ、マルチエリアルーティング用のレベル 2（エリア）ルータ、または両方（デフォルト）として機能するようにルータを設定します。 • **level 1**：ステーションルータとしてだけ機能します。 • **level 1-2**：ステーションルータおよびエリアルータの両方として機能します。 • **level 2**：エリアルータとしてだけ機能します。
ステップ 7	**exit** 例： `Device(config-router)#end`	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 8	**interface** *interface-id* 例： `Device(config)#interface gigabitethernet 1/0/1`	IS-IS をルーティングするインターフェイスを指定し、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。インターフェイスがまだレイヤ 3 インターフェイスとして設定されていない場合は、**no switchport** コマンドを入力してインターフェイスをレイヤ 3 モードに設定します。
ステップ 9	**ip router isis** [*area tag*] 例： `Device(config-if)#ip router isis tag1`	インターフェイスに IS-IS ルーティング プロセスを設定し、エリア指示子をルーティング プロセスに割り当てます。

	コマンドまたはアクション	目的
ステップ 10	**ip address** *ip-address-mask* 例： `Device(config-if)#ip address 10.0.0.5 255.255.255.0`	インターフェイスのIPアドレスを定義します。インターフェイスのいずれかで IS-IS ルーティングが設定されている場合は、IS-ISがイネーブルになっているエリアに含まれるすべてのインターフェイスに IP アドレスが必要です。
ステップ 11	**end** 例： `Device(config)#end`	特権 EXEC モードに戻ります。
ステップ 12	**show isis** [*area tag*] **database detail** 例： `Device#show isis database detail`	入力を確認します。

IS-IS グローバル パラメータの設定

グローバル IS-IS パラメータを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device>enable`	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device#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 3	**router isis** 例： `Device(config)#router isis`	IS-IS ルーティング プロトコルを指定し、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	**default-information originate** [**route-map** *map-name*] 例：	（任意）デフォルトルートをIS-ISルーティングドメインに強制的に設定します。**route-map** *map-name* コマンドを入力すると、にルーティングロセスに

	コマンドまたはアクション	目的
	`Device(config-router)#default-information originate route-map map1`	よって有効なルートマップのデフォルトルートが生成されます。
ステップ 5	**ignore-lsp-errors** 例： `Device(config-router)#ignore-lsp-errors`	（任意）LSP を消去する代わりに、内部チェックサムにエラーがある LSP を無視するようにデバイスを設定します。このコマンドは、デフォルトでイネーブルになっています（破損した LSP はドロップされます）。破損した LSP を消去するには、ルータ コンフィギュレーション モードで **no ignore-lsp-errors** コマンドを入力します。
ステップ 6	**area-password** *password* 例： `Device(config-router)#area-password 1password`	（任意）レベル 1（ステーションルータレベル）LSP に挿入されるエリア認証パスワードを設定します。
ステップ 7	**domain-password** *password* 例： `Device(config-router)#domain-password 2password`	（任意）レベル 2（エリアルータレベル）LSP に挿入されるルーティングドメイン認証パスワードを設定します。
ステップ 8	**summary-address** *address mask* [**level-1** | **level-1-2** | **level-2**] 例： `Device(config-router)#summary-address 10.1.0.0 255.255.0.0 level-2`	（任意）所定のレベルのアドレスのサマリーを作成します。
ステップ 9	**set-overload-bit** [**on-startup** {*seconds* | **wait-for-bgp**}] 例： `Device(config-router)#set-overload-bit on-startup wait-for-bgp`	（任意）デバイスに問題がある場合に、他のデバイスが最短パス優先（SPF）計算でこのデバイスを無視するように過負荷ビットを設定します。 • （任意）**on-startup**：スタートアップ時だけ過負荷ビットを設定します。**on-startup** が指定されない場合、過負荷ビットが即座に設定され、**no set-overload-bit** コマンドを入力するまで設定されたままになります。**on-startup** が指定されている場合は、秒数または

	コマンドまたはアクション	目的
		wait-for-bgp のどちらかを入力する必要があります。 • *seconds*：**on-startup** キーワードが設定されている場合、システム起動時に過負荷ビットが設定されて、指定した秒数の間設定されたままになります。指定できる範囲は 5 ～ 86400 秒です。 • **wait-for-bgp**：**on-startup** キーワードが設定されている場合、過負荷ビットがシステム起動時に設定され、BGP が収束するまで設定されたままになります。BGP が収束されたことが IS-IS に通知されない場合、IS-IS は 10 分後に過負荷ビットをオフにします。
ステップ 10	**lsp-refresh-interval** *seconds* 例： `Device(config-router)#lsp-refresh-interval 1080`	（任意）LSP リフレッシュインターバル（秒）を設定します。範囲は 1 ～ 65535 秒です。デフォルトでは、LSP リフレッシュを 900 秒（15 分）ごとに送信します。
ステップ 11	**max-lsp-lifetime** *seconds* 例： `Device(config-router)#max-lsp-lifetime 1000`	（任意）LSP パケットがリフレッシュされずにルータ データベース内に存続する最大時間を設定します。範囲は 1 ～ 65535 秒です。デフォルト値は 1200 秒（20 分）です。指定された時間間隔のあと、LSP パケットは削除されます。
ステップ 12	**lsp-gen-interval** [**level-1** | **level-2**] *lsp-max-wait* [*lsp-initial-wait lsp-second-wait*] 例： `Device(config-router)#lsp-gen-interval level-2 2 50 100`	（任意）IS-IS 生成スロットリング タイマーを設定します。 • *lsp-max-wait*：生成される LAP の連続した 2 つのオカレンス間の最大インターバル（ミリ秒）。指定できる範囲は 1 ～ 120 ミリ秒です。デフォルト値は 5000 ミリ秒です。 • *lsp-initial-wait*：最初の LSP 生成遅延（ミリ秒）。指定できる範囲は 1 ～ 10000 ミリ秒です。デフォルト値は 50 ミリ秒です。

	コマンドまたはアクション	目的
		• *lsp-second-wait*：最初と 2 番目の LSP 生成間（ミリ秒）のホールド時間。指定できる範囲は1～10000 ミリ秒です。デフォルト値は 200 ミリ秒です。
ステップ 13	**spf-interval** [**level-1** | **level-2**] *spf-max-wait* [*spf-initial-wait spf-second-wait*] 例： `Device(config-router)#spf-interval level-2 5 10 20`	（任意）IS-IS SPF スロットリングタイマーを設定します。 • *spf-max-wait*：連続する SFP 間（ミリ秒）の最大インターバル。指定できる範囲は 1 ～ 120 ミリ秒です。デフォルト値は5000 ミリ秒です。 • *spf-initial-wait*：トポロジ変更後の最初の SFP 計算（ミリ秒）。指定できる範囲は 1 ～ 10000 ミリ秒です。デフォルト値は 50 ミリ秒です。 • *spf-second-wait*：最初と 2 番目の SFP 計算間（ミリ秒）のホールド時間。指定できる範囲は1～10000 ミリ秒です。デフォルト値は 200 ミリ秒です。
ステップ 14	**prc-interval** *prc-max-wait* [*prc-initial-wait prc-second-wait*] 例： `Device(config-router)#prc-interval 5 10 20`	（任意）IS-IS PRC スロットリングタイマーを設定します。 • *prc-max-wait*：2 つの連続する PRC 計算間の最大インターバル（ミリ秒）。指定できる範囲は 1 ～ 120 ミリ秒です。デフォルト値は5000 ミリ秒です。 • *prc-initial-wait*：トポロジ変更後の最初の PRC 計算遅延（ミリ秒）。指定できる範囲は 1 ～ 10,000 ミリ秒です。デフォルト値は 50 ミリ秒です。 • *prc-second-wait*：最初と 2 番目の PRC 計算間（ミリ秒）のホールドタイム。指定できる範囲は 1 ～

	コマンドまたはアクション	目的
		10,000 ミリ秒です。デフォルト値は 200 ミリ秒です。
ステップ 15	**log-adjacency-changes** [**all**] 例： `Device(config-router)#log-adjacency-changes all`	（任意）IS-IS 隣接ステート変更をログするようルータを設定します。End System-to-Intermediate System PDU および LSP など、IS-IS hello に関連しないイベントにより生成されたすべての変更をログに含めるには、**all** を入力します。
ステップ 16	**lsp-mtu** *size* 例： `Device(config-router)#lsp mtu 1560`	（任意）最大 LSP パケットサイズ（バイト）を指定します。指定できる範囲は 128 ～ 4352 バイトです。デフォルト値は 1497 バイトです。 （注） ネットワーク内のリンクで MTU サイズが縮小された場合、ネットワーク内のすべてのデバイスで LSP MTU サイズを変更する必要があります。
ステップ 17	**partition avoidance** 例： `Device(config-router)#partition avoidance`	（任意）境界ルータ、すべての隣接レベル 1 ルータ、およびエンド ホスト間で、フル接続が切断された場合、IS-IS レベル 1-2 境界ルータがレベル 1 エリア プレフィックスをレベル 2 バックボーンにアドバタイズしないようにします。
ステップ 18	**end** 例： `Device(config)#end`	特権 EXEC モードに戻ります。

IS-IS インターフェイス パラメータの設定

IS-IS インターフェイス固有のパラメータを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device>enable`	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device#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 3	**interface** *interface-id* 例： `Device(config)#interface gigabitethernet 1/0/1`	設定するインターフェイスを指定し、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。インターフェイスがまだレイヤ 3 インターフェイスとして設定されていない場合は、**no switchport** コマンドを入力してインターフェイスをレイヤ 3 モードに設定します。
ステップ 4	**isis metric** *default-metric* [**level-1** | **level-2**] 例： `Device(config-if)#isis metric 15`	（任意）指定したインターフェイスにメトリック（またはコスト）を設定します。指定できる範囲は 0 ～ 63 です。デフォルトは 10 です。レベルが入力されない場合は、レベル 1 ルータとレベル 2 ルータの両方にデフォルト値が適用されます。
ステップ 5	**isis hello-interval** {*seconds* | **minimal**} [**level-1** | **level-2**] 例： `Device(config-if)#isis hello-interval minimal`	（任意）デバイスが hello パケットを送信する間隔を指定します。デフォルトでは、hello インターバル *seconds* の 3 倍の値が、送信される hello パケットの *holdtime* としてアドバタイズされます。hello インターバルが狭まると、トポロジ変更の検出も速くなりますが、ルーティング トラフィック量は増大します。 • **minimal**：結果として得られるホールドタイムが 1 秒になるように、hello 乗数に基づいて hello 間隔が計算されます。

	コマンドまたはアクション	目的
		• *seconds*：指定できる範囲は 1 ー 65535 です。デフォルトは 10 秒です。
ステップ 6	**isis hello-multiplier** *multiplier* [**level-1** | **level-2**] 例： `Device(config-if)#isis hello-multiplier 5`	（任意）ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、デバイスは隣接がダウンしていると宣言します。指定できる範囲は 3 ～ 1000 です。デフォルトは 3 です。 （注） hello 乗数を小さくすると、高速コンバージェンスとなりますが、ルーティングが不安定になる場合があります。
ステップ 7	**isis csnp-interval** *seconds* [**level-1** | **level-2**] 例： `Device(config-if)#isis csnp-interval 15`	（任意）インターフェイスに IS-IS CSNP を設定します。指定できる範囲は 0 ～ 65535 です。デフォルトは 10 秒です。
ステップ 8	**isis retransmit-interval** *seconds* 例： `Device(config-if)#isis retransmit-interval 7`	（任意）ポイントツーポイントリンクの IS-IS LSP の再送信間隔（秒）を設定します。整数で、ネットワーク上の 2 つのルータ間で予測されるラウンドトリップ遅延よりも大きい値を指定してください。指定できる範囲は 0 ～ 65535 です。デフォルトは 5 秒です。
ステップ 9	**isis retransmit-throttle-interval** *milliseconds* 例： `Device(config-if)#isis retransmit-throttle-interval 4000`	（任意）IS-IS LSP 再送信スロットルインターバルを設定します。これは、IS-IS LSP がポイントツーポイントリンク上で再送信される最大レート（パケット間のミリ秒数）です。指定できる範囲は 0 ー 65535 です。デフォルトは **isis lsp-interval** コマンドによって決定されます。
ステップ 10	**isis priority** *value* [**level-1** | **level-2**] 例： `Device(config-if)#isis priority 50`	（任意）指定ルータの優先順位を設定します。指定できる範囲は 0 ～ 127 です。デフォルトは 64 です。

	コマンドまたはアクション	目的
ステップ 11	**isis circuit-type** {**level-1** | **level-1-2** | **level-2-only**} 例： `Device(config-if)#isis circuit-type level-1-2`	（任意）指定されたインターフェイス上のネイバーで必要な隣接タイプを設定します（インターフェイスの回線タイプを指定します）。 • **level-1**：このノードとネイバーの両方に共通のエリアアドレスが少なくとも 1 つある場合、レベル 1 隣接関係が確立されます。 • **level-1-2**：ネイバーもレベル 1 およびレベル 2 の両方として設定されていて、少なくとも 1 つの共通のエリアがある場合、レベル 1 およびレベル 2 隣接関係が確立されます。共通のエリアがない場合は、レベル 2 隣接関係が確立されます。これはデフォルト設定です。これがデフォルトのオプションです。 • **level 2**：レベル 2 隣接関係が確立されます。ネイバールータがレベル 1 ルータである場合、隣接関係は確立されません。
ステップ 12	**isis password** *password* [**level-1** | **level-2**] 例： `Device(config-if)#isis password secret`	（任意）インターフェイスの認証パスワードを設定します。デフォルトでは、認証はディセーブルに設定されています。レベル 1 またはレベル 2 を指定すると、それぞれレベル 1 またはレベル 2 ルーティング用のパスワードだけがイネーブルになります。レベルを指定しない場合、デフォルトはレベル 1 およびレベル 2 です。
ステップ 13	**end** 例： `Device(config)#end`	特権 EXEC モードに戻ります。

IS-IS 認証の設定方法

ここでは、認証キーを生成する方法、インターフェイスの IS-IS 認証を設定する方法、およびインスタンスの IS-IS 認証を設定する方法について説明します。

認証キーの設定

複数のキーにライフタイムを設定できます。認証パケットを送信するために、最新の送信ライフタイム設定を持つキーが選択されます。複数のキーが同じ送信ライフタイム設定を持つ場合、キーはランダムに選択されます。受信した認証パケットを調べて受け入れるには、**accept-lifetime** コマンドを使用します。デバイスは、これらのライフタイムを認識している必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device>enable`	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device#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 3	**key chain** *name-of-chain* 例： `Device(config)#key chain key10`	キーチェーンを識別し、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	**key** *number* 例： `Device(config-keychain)#key 2000`	キー番号を識別します。範囲は 0 ～ 65535 です。
ステップ 5	**key-string** *text* 例： `Device(config-keychain-key)#Room 20, 10th floor`	キー ストリングを確認します。ストリングには 1 ～ 80 文字の大文字および小文字の英数字を指定できますが、最初の文字に数字を指定できません。
ステップ 6	**accept-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*} 例：	（任意）キーを受信できる期間を指定します。

	コマンドまたはアクション	目的
	`Device(config-keychain-key)#accept-lifetime 12:30:00 Jan 25 1009 infinite`	*start-time* および *end-time* 構文には、*hh:mm:ss month date year* または *hh:mm:ss date month year* のいずれかを使用できます。デフォルトは、デフォルトの *start-time* 以降、無制限です。指定できる最初の日付は 1993 年 1 月 1 日です。デフォルトの *end-time* および **duration** は **infinite** です。
ステップ 7	**send-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*} 例： `Device(config-keychain-key)#accept-lifetime 23:30:00 Jan 25 1019 infinite`	（任意）キーを送信できる期間を指定します。 *start-time* および *end-time* 構文には、*hh:mm:ss month date year* または *hh:mm:ss date month year* のいずれかを使用できます。デフォルトの *start-time* は **infinite** で、指定できる最初の日付は 1993 年 1 月 1 日です。デフォルトの *end-time* および **duration** は **infinite** です。
ステップ 8	**cryptographic-algorithm** {**hmac-sha-1** | **hmac-sha-256** | **hmac-sha-384** | **hmac-sha-512** | **md5** } 例： `Device(config-keychain-key)#cryptographic-algorithm hmac-sha1-256`	（任意）暗号化アルゴリズムを指定します。
ステップ 9	**end** 例： `Device(config-keychain-key)#end`	特権 EXEC モードに戻ります。
ステップ 10	**show key chain** 例： `Device#show key chain`	認証キーの情報を表示します。

IS-IS インスタンスの HMAC-MD5 またはクリアテキスト認証の設定

ある認証方法から別の認証方法へ円滑に移行を実現し、IS-IS PDU の継続的な認証を可能にするには、ネットワークで通信する各デバイスでこの手順を実行します。

始める前に

認証文字列キーが生成されている必要があります。ネットワーク内のすべてのデバイスで同じ認証文字列キーを設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device>enable`	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device#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 3	**router isis** [**area** *tag*] 例： `Device(config)#router isis 1`	IP ルーティング プロトコルとして IS-IS を有効化し、必要に応じてプロセスにタグを割り当てます。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	**authentication send-only** [**level-1** | **level-2**] 例： `Device(config-router)#authentication send-only`	指定した IS-IS インスタンスについて送信された（受信ではなく）PDU に対してのみ認証が実行されるように指定します。
ステップ 5	**authentication mode** {**md5** | **text**}[**level-1** | **level-2**] 例： `Device(config-router)#authentication mode md5`	指定された IS-IS インスタンスについて PDU で使用される認証のタイプを指定します。 • **md5**：MD5 認証。 • **text**：クリアテキスト認証。
ステップ 6	**authentication key-chain** *name-of-chain* [**level-1** | **level-2**] 例： `Device(config-router)#authentication key-chain remote3754`	指定された IS-IS インスタンスについて認証が有効になります。
ステップ 7	**no authentication send-only** 例： `Device(config-router)#no authentication send-only`	指定した IS-IS インスタンスについて送信および受信された PDU に対してのみ認証が実行されるように指定します。

IS-IS インターフェイスの HMAC-MD5 またはクリア テキスト認証の設定

ある認証方法から別の認証方法へ円滑に移行を実現し、IS-IS PDU の継続的な認証を可能にするには、ネットワークで通信する各デバイスでこの手順を実行します。

始める前に

認証文字列キーが生成されている必要があります。ネットワーク内のすべてのデバイスで同じ認証文字列キーを設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device>enable`	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device#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 3	**interface** *type number* 例： `Device(config)#interface ethernet 0`	インターフェイスを設定します。
ステップ 4	**isis authentication send-only** [**level-1** | **level-2**] 例： `Device(config-if)#isis authentication send-only`	指定した IS-IS インターフェイスについて送信された（受信ではなく）PDU に対してのみ認証が実行されるように指定します。
ステップ 5	**isis authentication mode** {**md5** | **text**}[**level-1** | **level-2**] 例： `Device(config-if)#isis authentication mode md5`	指定された IS-IS インスタンスについて PDU で使用される認証のタイプを指定します。 • **md5**：MD5 認証。 • **text**：クリアテキスト認証。
ステップ 6	**isis authentication key-chain** *name-of-chain* [**level-1** | **level-2**] 例：	指定された IS-IS インスタンスについて MD5 認証が有効になります。

	コマンドまたはアクション	目的
	`Device(config-if)#isis authentication key-chain multistate87723`	
ステップ 7	**no isis authentication send-only** 例： `Device(config-if)#no isis authentication send-only`	IS-IS インスタンスについて送信および受信された PDU に対してのみ認証が実行されるように指定します。

IS-IS のモニタリングおよびメンテナンス

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 IS-IS の統計情報を表示できます。また、特定のインターフェイス、フィルタ、またはネイバーに関する情報も表示できます。

次の表に、IS-IS ルーティングを消去および表示するために使用する特権 EXEC コマンドを示します。

表 *2 : IS-IS show* コマンド

コマンド
show ip route isis
show isis database
show isis routes
show isis spf-log
show isis topology
show route-map
trace clns *[*接続先（*Destination*）*]*

IS-IS の機能情報

表 *3 : IS-IS* の機能情報

機能名	リリース	機能情報
Intermediate System-to-Intermediate System（IS-IS）	Cisco IOS XE Everest 16.5.1a	この機能が導入されました。
	Cisco IOS XE Gibraltar 16.10.1	IS-IS は、セキュア ハッシュ アルゴリズム（SHA）認証（SHA-1、SHA-256、SHA-384、およびSHA-512）をサポートするようになりました。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。