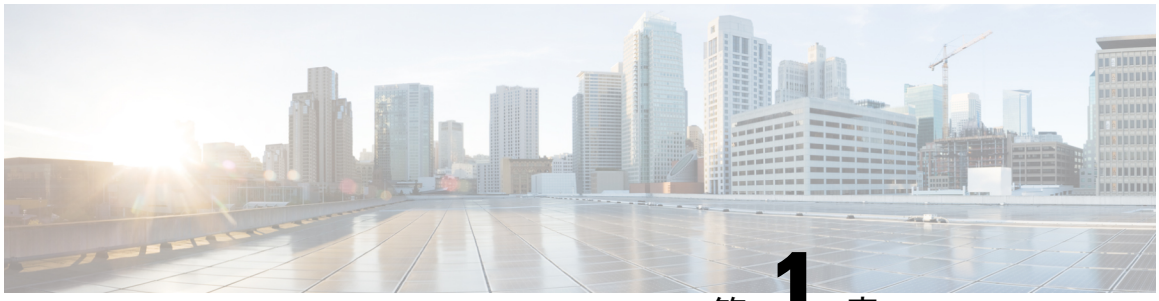
IP SLA コンフィギュレーション ガイド（Cisco IOS XE Gibraltar 16.10.x 向け）

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

目 次



第 1 章

最初にお読みください

Cisco IOS XE 16 に関する重要な情報

現行の Cisco IOS XE Release 3.7.0E（Catalyst スイッチング用）および Cisco IOS XE Release 3.17S（アクセスおよびエッジルーティング用）の 2 つのリリースは、単一バージョンのコンバージドリリース Cisco IOS XE 16 に進化（マージ）しました。これにより、スイッチングおよびルーティング ポートフォリオにおける広範なアクセス製品およびエッジ製品を 1 つのリリースでカバーします。

機能情報

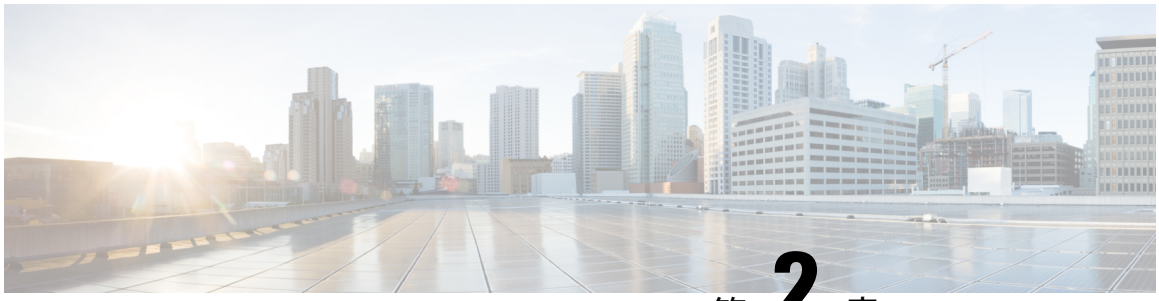
機能のサポート、プラットフォームのサポート、およびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco.com のアカウントは必要ありません。

参考資料

- 『Cisco IOS コマンド リファレンス』、全リリース

マニュアルの入手方法およびテクニカル サポート

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、シスコ サービスにアクセスしてください。
- サービス リクエストを送信するには、シスコ サポートにアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco Marketplace にアクセスしてください。
- 一般的なネットワーキング、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。



第 2 章

IP SLA の概要

ここでは、IP サービス レベル契約（SLA）について説明します。IP SLA により、シスコのお客様は IP アプリケーションとサービスの IP サービス レベルを分析するとともに、生産性の向上、運用コストの削減、ネットワーク停止頻度の低減を実現できます。IP SLA は、アクティブ トラフィック モニタリングを使用します。これにより、継続的で信頼性のある予測可能な方法でトラフィックが生成され、ネットワーク パフォーマンスを測定できます。IP SLA を使用すると、サービス プロバイダーのお客様は測定したうえでサービス レベル契約を提供することができ、企業のお客様はサービス レベルや外部委託しているサービス レベル契約を検証したり、ネットワーク パフォーマンスを把握したりできます。IP SLA は、ネットワーク アセスメントを実行し、Quality of Service（QoS）を検証したり新規サービスの展開を簡易化するとともに、管理者によるネットワークのトラブルシューティングをサポートしますIP SLAによって取得されたデータは、コマンドラインまたは Simple Network Management Protocol（SNMP）による Cisco Round-Trip Time Monitor（RTTMON）や syslog Management Information Base（MIB）のポーリングを通じてアクセスできます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

IP SLA に関する情報

IP SLA 技術の概要

Cisco IP SLA は、アクティブ トラフィック モニタリングを使用します。これにより、継続的で信頼性のある予測可能な方法でトラフィックが生成され、ネットワーク パフォーマンスを測定できます。IP SLA はネットワークにデータを送信し、複数のネットワーク間あるいは複数のネットワーク パス内のパフォーマンスを測定します。ネットワーク データおよび IP サービスをシミュレーションし、ネットワーク パフォーマンス情報をリアル タイムで収集します。収集される情報には、応答時間、一方向遅延、ジッター（パケット間の遅延のばらつき）、パケット損失、音声品質スコアリング、ネットワーク リソースの可用性、アプリケーションのパフォーマンス、およびサーバの応答時間に関するデータが含まれます。IP SLA はトラフィックを生成および分析して、シスコ デバイス間またはシスコ デバイスからネットワーク アプリケーション サーバのようなリモート IP デバイスへのパフォーマンスを測定することにより、アクティブ モニタリングを実行します。さまざまな IP SLA 動作による測定統計情報を、トラブルシューティング、問題分析、ネットワーク トポロジの設計に使用できます。

IP SLA を使用すると、サービス プロバイダーのお客様は測定したうえでサービス レベル契約を提供することができ、企業のお客様はサービス レベルや外部委託しているサービス レベル契約を検証したり、新規または既存の IP サービスおよびアプリケーションのネットワーク パフォーマンスを把握したりできます。IP SLA は、非常に正確で、精度の高いサービス レベル保証の測定を提供するために、独自のサービス レベル保証のメトリックと手法を使用します。

特定の IP SLA 動作に応じて、遅延、パケット損失、ジッター、パケット シーケンス、接続、パス、サーバの応答時間、およびダウンロード時間の統計情報がシスコデバイス内でモニタでき、CLI および SNMP MIB の両方に保存できます。パケットには設定可能な IP レイヤ オプションとアプリケーション層オプションがあります。たとえば、送信元および宛先の IP アドレス、ユーザ データグラム プロトコル（UDP）/TCP ポート番号、サービス タイプ（ToS）バイト（Diffserv コード ポイント（DSCP）および IP プレフィックス ビットを含む）、バーチャル プライベート ネットワーク（VPN）ルーティング/転送インスタンス（VRF）、URL Web アドレスなどが設定できます。

レイヤ 2 トランスポートに依存せず、IP SLA は、異なるネットワーク間にエンドツーエンドを設定してエンドユーザが経験しそうなメトリックを最大限に反映させることができます。IP SLA 動作が収集するパフォーマンス メトリックには次のものがあります。

- 遅延（往復および一方向）
- ジッター（方向性あり）
- パケット損失（方向性あり）
- パケット シーケンス（パケット順序）
- パス（ホップ単位）
- 接続（方向性あり）

- サーバまたは Web サイトのダウンロード時間
- 音声品質スコア

IP SLA には、SNMP を使用してアクセスできるため、CiscoWorks Internet Performance Monitor（IPM）のようなパフォーマンス モニタリング アプリケーションや他のサードパーティ製のシスコ パートナー パフォーマンス管理製品からも使用できます。IP SLA を使用するネットワーク管理製品に関する詳細については、http://www.cisco.com/go/ipsla を参照してください。

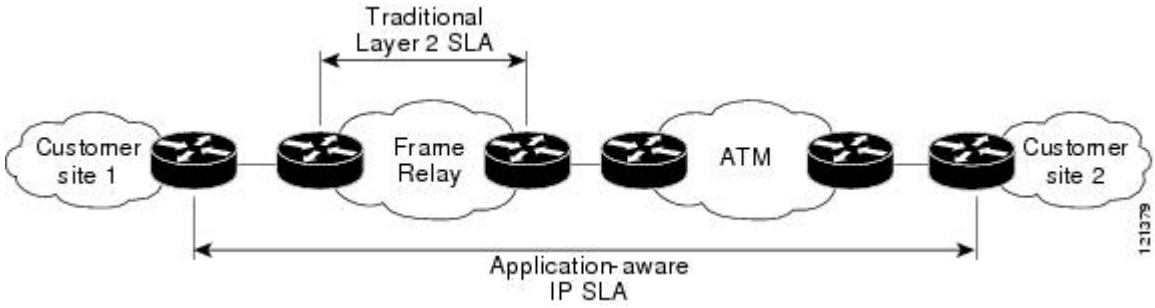
IP SLA 動作によって収集されたデータに基づく SNMP 通知により、パフォーマンスが指定したレベルを下回った場合や問題が修正された場合に、ルータはアラートを受信できます。IP SLA は、外部ネットワーク管理システム（NMS）アプリケーションとシスコ デバイス上で実行されている IP SLA 動作との間のインタラクションに Cisco RTTMON MIB を使用します。IP SLA 機能から参照されるオブジェクト変数の詳細については、Cisco MIB Web サイトから入手できる CISCO-RTTMON-MIB.my ファイルのテキストを参照してください。

サービス レベル契約

インターネット ショッピングはこの数年で急激に成長し、テクノロジーの進化により高速で信頼性の高いインターネット アクセスが提供されるようになりました。多くの企業では現在、オンライン アクセスが必要で、ビジネスのオンラインのほとんどをオンラインで行い、サービスの損失は企業の収益性に影響を及ぼすことがあります。今では、インターネット サービス プロバイダー（ISP）や内部 IT 部門でさえも、定義済みのサービス レベル（サービス レベル契約）を提供して、お客様に一定の予測可能性を提供しています。

ビジネス クリティカルなアプリケーション、Voice over IP（VoIP）ネットワーク、音声および表示による会議、および VPN の最新のパフォーマンス要件により、企業内では、パフォーマンス レベルに合わせた統合 IP ネットワークの最適化が求められています。ネットワーク管理者にとっては、アプリケーション ソリューションを支えるサービス レベル契約をサポートする必要性がますます高まっています。次の図に、アプリケーションのサポートも含め、エンドツーエンドのパフォーマンス測定をサポートするために、IP SLA がどのように従来のレイヤ 2 サービス レベル契約の概念を取り込み、より広い範囲に適用されているかを示します。

図 *1* : 従来のサービス レベル契約と *IP SLA* の範囲



IP SLA では、従来のサービス レベル契約と比べて次のような改善を実現できます。

- エンドツーエンド測定：ネットワークの端からもう一方の端までパフォーマンスを測定できることにより、エンドユーザによるネットワーク利用状況をより広い到達範囲でより正確に表現できます。
- 詳細化：遅延、ジッター、パケットシーケンス、レイヤ3接続、パスとダウンロード時間などの双方向のラウンドトリップの数値に詳細化される統計情報により、レイヤ2リンクの帯域幅だけよりも詳細なデータが得られます。
- 展開の簡易化：IP SLA は、大きいネットワーク内で既存のシスコ デバイスを活用することにより、従来のサービス レベル契約で必要になることの多い物理的なプローブよりも、簡単かつ低コストで実装されます。
- アプリケーション認識型モニタリング：IP SLA は、レイヤ 3 からレイヤ 7 で実行されているアプリケーションによって生成されたパフォーマンス統計情報をシミュレートし、測定できます。従来のサービス レベル契約では、レイヤ2パフォーマンスしか測定できません。
- 普及：IP SLA は、ローエンドからハイエンドまでのデバイスとスイッチに及ぶ、シスコ ネットワーキング デバイスでサポートされています。この幅広い展開により、IP SLA は、従来のサービス レベル契約よりも高い柔軟性を備えています。

ネットワークのコアからエッジまでのさまざまなレベルのトラフィックに対するパフォーマンスの予想がわかっている場合、自信を持ってエンドツーエンドのアプリケーション対応サービス レベル契約を構築できます。

IP SLA の利点

- IP SLA モニタリング
  - サービス レベル契約モニタリング、評価、および検証の提供
- ネットワーク パフォーマンス モニタリング。
  - ネットワーク内のジッタ、遅延、パケット損失が測定できる。
  - 連続的で信頼性のある確実な評価ができる。
- IP サービス ネットワーク稼働状態評価
  - 既存の QoS が新しい IP サービスに対して十分であることの検証
- エッジツーエッジ ネットワーク可用性のモニタリング
  - ネットワーク リソースをあらかじめ検証し接続をテストします（たとえば、リモートサイトからビジネス上の重要なデータを保存するために使用されるネットワーク ファイル システム（NFS）サーバのネットワーク アベイラビリティを示します）。
- ネットワーク動作のトラブルシューティング
  - 問題をただちに特定し、トラブルシューティング時間を節約する、一貫し、信頼性が高い測定を提供します。
- Voice over IP（VoIP）パフォーマンス モニタリング

- マルチプロトコル ラベル スイッチング（MPLS）バーチャル プライベート ネットワーク（VPN）パフォーマンスのモニタリングおよびネットワークの検証

IP SLA の制約事項

start-time now キーワードを使用して設定された IP SLA は、リロード後に再起動する必要があります。

IP SLA v1、v2、v3 は、ASR 903, RSP2、ASR 903、RSP3、および ASR 920 プラットフォーム上の HMAC SHA 1、HMCA SHA 256、HMCA SHA 384、HMCA SHA 512 認証をサポートしていません。

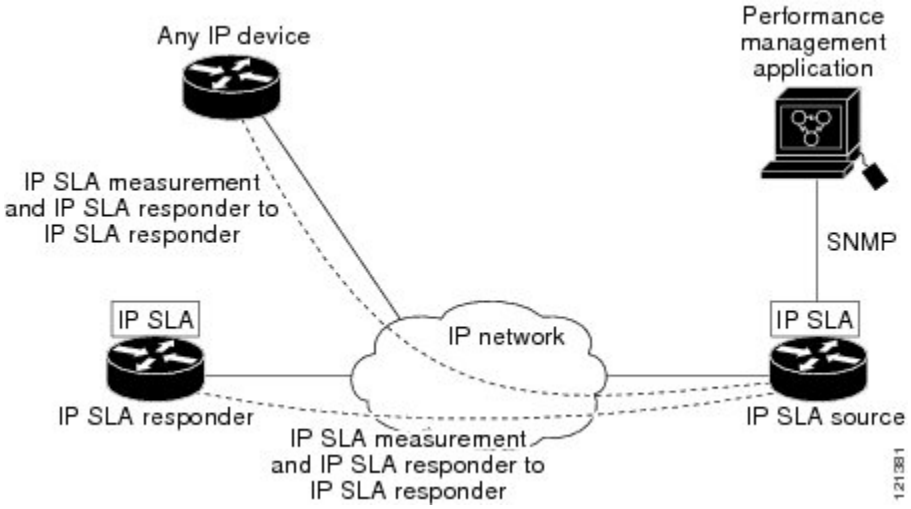
IP SLA を使用したネットワーク パフォーマンスの測定

IP SLA を使用して、ネットワーク エンジニアは、コア、分散、エッジといったネットワークの任意のエリア間のパフォーマンスをモニタできます。モニタリングは、物理的なプローブを展開しなくても、時間と場所を問わず実行できます。

IP SLA プローブの拡張機能は、応答時間、ネットワーク リソースの可用性、アプリケーション パフォーマンス、ジッター（パケット間の遅延変動）、接続時間、スループット、およびパケット損失を測定することによって、ネットワークのパフォーマンスをモニタするアプリケーション認識型の統合的な動作エージェントです。この機能をサポートしているシスコデバイスと、リモート IP ホスト（サーバ）、シスコ ルート デバイス、またはメインフレーム ホストの間のパフォーマンスを測定できます。この機能によって提供されるパフォーマンス測定統計情報は、トラブルシューティング、問題分析、ネットワーク トポロジの設計に使用できます。

IP SLA は、生成されたトラフィックを使用して、2 つのネットワーク デバイス間のネットワーク パフォーマンスを測定します。次の図に、IP SLA が宛先デバイスに生成パケットを送信するときに IP SLA が開始される手順を示します。IP SLA 動作のタイプにもよりますが、宛先デバイスはそのパケットを受信した後、送信元でパフォーマンス メトリックを計算できるようにタイムスタンプ情報を返信します。IP SLA 動作は、特定のプロトコル（UDP など）を使用してネットワークの送信元から宛先へのネットワーク測定を行います。

図 *2 : IP SLA* 動作



IP SLA ネットワーク パフォーマンス測定を実施する手順は次のとおりです。

1. 必要に応じて IP SLA Responder をイネーブルにします。
2. 必要な IP SLA 動作タイプを設定します。
3. 指定された IP SLA 動作タイプに使用可能なオプションを設定します。
4. 必要であれば、しきい値条件を設定します。
5. 動作の実行スケジュールを指定し、しばらく動作を実行して統計情報を収集します。
6. Cisco ソフトウェア コマンドまたは NMS システムで SNMP を使用し、動作の結果を表示および解釈します。

IP SLA Responder と IP SLA コントロール プロトコル

IP SLA Responder は宛先シスコ ルーティング デバイスに組み込まれたコンポーネントで、システムが IP SLA 要求パケットを予想して応答します。IP SLA Responder には、専用プローブがなくても正確な測定ができるという大きな利点があり、標準的な ICMP ベースの測定では得られない追加の統計情報も得られます。特許取得済み IP SLA 制御プロトコルは、IP SLA Responder がどのポートで待ち受けと応答を行うかを通知するために使用するメカニズムを提供します。シスコ デバイスだけが宛先 IP SLA Responder の送信元になります。

「IP SLA を使用したネットワーク パフォーマンスの測定」の項にある図「IP SLA 動作」には、IP ネットワークに関して IP SLA Responder が適合する場所が示されています。IP SLA Responder は、IP SLA 動作から送信されたコントロール プロトコル メッセージを指定されたポートでリッスンします。コントロール メッセージを受信すると、応答側は、指定された UDP ポートまたは TCP ポートを指定された期間イネーブルにします。この間に、レスポンダは要求を受け付け、応答します。Responder は、IP SLA パケットに応答した後、あるいは指定され

た期間が経過すると、ポートをディセーブルにします。セキュリティを強化するために、コントロール メッセージの MD5 認証も使用できます。

すべての IP SLA 動作について、IP SLA Responder を宛先デバイスでイネーブルにしなければならないわけではありません。たとえば、宛先デバイスですでに提供されているサービス（Telnet や HTTP など）が選択される場合、IP SLA Responder をイネーブルにする必要はありません。シスコ以外のデバイスには、IP SLA Responder を設定できません。この場合、IP SLA はこれらのデバイス固有のサービスに対してだけ動作パケットを送信できます。

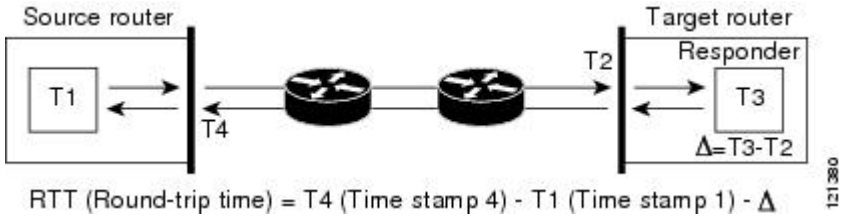
IP SLA の応答時間の計算

デバイスは、他のハイ プライオリティ プロセスがあるために、着信パケットの処理に数十ミリ秒かかることがあります。テストパケットに対する応答は、処理されるのを待ちながらキューに入っていることがあるため、この遅延によって応答時間は変化します。この場合、応答時間は正しいネットワーク遅延を反映しません。IP SLA は送信元デバイスとターゲット デバイス（IP SLA Responder が使用されている場合）の処理遅延を最小化し、正しいラウンドトリップ時間を識別します。IP SLA テスト パケットは、タイム スタンプによって処理遅延を最小化します。

IP SLA Responder がイネーブルの場合、パケットが割り込みレベルでインターフェイスに着信したときおよびパケットが出て行くときにターゲット デバイスでタイム スタンプを 2 回取得でき、処理時間を削減できます。ネットワーク アクティビティが活発なとき、ICMP ping テストによる応答時間は長く、不正確になることがよくあります。それに対して、IP SLA テストは、応答側でのタイム スタンプによって正確な時間が示されます。

次の図に、レスポンダの動作を示します。RTT を算出するためのタイム スタンプが 4 つ付けられます。ターゲット デバイスでレスポンダ機能がイネーブルの場合、タイム スタンプ 3（TS3）からタイム スタンプ 2（TS2）を引いてテストパケットの処理にかかった時間を求め、デルタ（Δ）で表します。次に全体の RTT からこのデルタの値を引きます。IP SLA により、この方法は送信元デバイスにも適用されます。その場合、着信タイム スタンプ 4（TS4）が割り込みレベルで付けられ、より正確な結果を得ることができます。

図 *3 : IP SLA Responder* タイム スタンプ



この他にも、ターゲット デバイスに 2 つのタイム スタンプがあれば一方向遅延、ジッター、方向性を持つパケット損失がトラッキングできるという利点があります。大半のネットワーク動作は非同期なので、このような統計情報があるのは問題です。ただし、一方向遅延の測定を行うには、送信元デバイスとターゲット デバイスの両方をネットワーク タイム プロトコル（NTP）で設定しておく必要があります。ソースとターゲットの両方が同じクロック ソースに同期される必要があります。一方向ジッタ測定にはクロック同期は不要です。

IP SLA 動作のスケジューリング

IP SLA 動作の設定が完了したら、その動作をスケジューリングして、統計情報の取得とエラー情報の収集を開始する必要があります。動作をスケジュールする場合は、すぐに動作を開始するよう指定するか、特定の月、日、時刻に開始するように指定できます。後で動作を開始するように設定する pending オプションもあります。pending オプションは、動作の内部状態の 1 つでもあり、SNMP によって確認できます。トリガーを待機する反応（しきい値）動作の場合も pending オプションを使用します。1 度に 1 つの IP SLA 動作をスケジューリングしたり、グループの動作をスケジューリングすることもできます。

複数動作のスケジューリングでは、単一の Cisco ソフトウェア コマンドまたは CISCO RTTMON-MIB を使用して、複数の IP SLA 動作をスケジュールできます。この機能では、これらの動作を均等な時間間隔で実行するようにスケジューリングすることで、IP SLA モニタリング トラフィックの量を制御できます。このように IP SLA 動作を分散することで、CPU の使用を最小限に抑えることが可能になり、それによりネットワークのスケーラビリティが向上します。

IP SLA 複数動作のスケジューリング機能の詳細については、『*IP SLA* コンフィギュレーション ガイド』の「IP SLA 動作の IP SLA 複数動作のスケジューリング」モジュールを参照してください。

IP SLA 動作のしきい値のモニタリング

サービス レベル契約モニタリングを適切にサポートするには、あるいはネットワーク パフォーマンスを予防的に測定するには、しきい値機能が最も重要になります。信頼性のある一貫した測定を行えば、問題はただちに特定され、トラブルシューティングにかかる時間を短縮できます。自信を持ってサービス レベル契約を展開するには、異常の可能性がただちに通知されるメカニズムを用意する必要があります。IP SLA は次のような場合にイベントによってトリガーされる SNMP トラップを送信できます。

- 接続の損失
- タイムアウト
- RTT しきい値
- 平均ジッターしきい値
- 一方向パケット損失
- 一方向ジッター
- 一方向平均オピニオン評点（MOS）
- 一方向遅延

または、IP SLA しきい値違反が発生した場合、あとで分析するために別の IP SLA 動作がトリガーされる場合があります。たとえば、回数を増やしたり、ICMP パス エコーや ICMP パス ジッター動作を開始してトラブルシューティングを行うことができます。

しきい値タイプとレベル設定の決定は複雑で、ネットワークで使用する IP サービス タイプによって異なります。IP SLA 動作でのしきい値の使用に関する詳細については、『*IP SLA* コンフィギュレーション ガイド』の「IP SLA 動作の IP SLA 予防的しきい値モニタリング」モジュールを参照してください。

MPLS VPN 認識

IP SLA MPLS VPN 認識機能を使用すると、マルチプロトコル ラベル スイッチング（MPLS）バーチャル プライベート ネットワーク（VPN）内で IP サービス レベルをモニタできます。MPLS VPN 内で IP SLA を使用することにより、サービス プロバイダーは、お客様のサービス レベル契約に従って IP VPN サービスを計画、プロビジョニング、および管理できます。IP SLA 動作は、VPN ルーティングおよび転送（VRF）の名前を指定して、特定の VPN に対して設定できます。

履歴統計情報

IP SLA には、次に示す 3 つのタイプの履歴統計情報が保持されます。

- 集約統計情報：デフォルトでは、IP SLA によって動作ごとに 2 時間の集計統計情報が保持されます。各動作サイクルからの値は、所定の 1 時間以内のすでに利用可能なデータとともに集約されます。IP SLA の拡張履歴機能を使用すると、集約間隔を 1 時間未満にできます。
- 動作スナップショット履歴：IP SLA は、設定可能なフィルタ（すべて、しきい値超過、障害など）と一致する動作インスタンスごとに、データのスナップショットを保持します。データ セット全体が使用可能であり、集約は行われません。
- 分散統計情報：IP SLA は、設定可能な時間間隔にわたり、頻度分布を維持します。IP SLA によって動作が開始されるたびに、履歴バケット数が指定したサイズに一致するまで、または動作のライフタイムが期限切れになるまで、新しい履歴バケットが作成されます。デフォルトでは、IP SLA 動作の履歴は収集されません。履歴を収集する場合は、動作の 1 つまたは複数の履歴エントリが各バケットに格納されます。履歴バケットのラップは行われません。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IP SLA コマンド	『*IP SLAs Command Reference*』

標準

標準	タイトル
ITU-T G.711 u-law および G.711 a-law	『Pulse code modulation (PCM) of voice frequencies』
ITU-T G.729A	『Reduced complexity 8 kbit/s CS-ACELP speech codec』

MIB

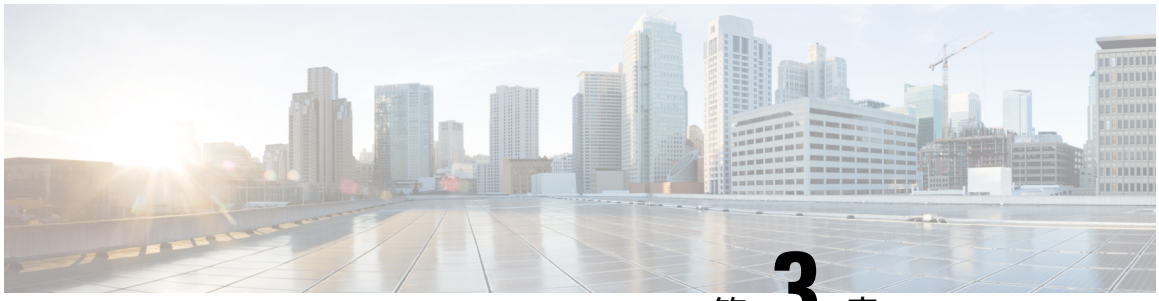
MIB	MIB のリンク
CISCO-RTTMON-MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャセットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

テクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html



第 3 章

IP SLA UDP ジッター動作の設定

このマニュアルでは、IP サービス レベル契約（SLA）UDP ジッター動作を設定して、IPv4 または IPv6 ネットワークで UDP トラフィックを伝送するネットワークのラウンド トリップ遅延、一方向遅延、一方向ジッター、一方向パケット損失、および接続を分析する方法について説明します。このモジュールでは、UDP ジッター動作を使用して収集されたデータを Cisco ソフトウェア コマンドを使用して表示および分析する方法についても説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

IP SLA UDP ジッター動作の前提条件

- 一方向遅延を正確に測定するには、送信元デバイスとターゲット デバイスの間でネットワーク タイム プロトコル（NTP）が提供するクロック同期が必要です。送信元デバイスおよびターゲットデバイスでNTPを設定するには、『*Basic System Management Configuration Guide*』の「Performing Basic System Management」の章の作業を実行します。一方向ジッターおよびパケット損失を測定する場合は、クロック同期は不要です。送信元デバイスとターゲットデバイスの間でクロックが同期していない場合、一方向ジッターとパケット損失のデータは返されますが、UDP ジッター動作による一方向遅延測定値として「0」が返されます。
- IP サービス レベル契約（SLA）アプリケーションを設定する前に、**show ip sla application** コマンドを使用して、動作タイプがソフトウェアイメージでサポートされていることを確認します。

IP SLA UDP ジッター動作に関する制約事項

- 同じ送信元アドレス、宛先IPアドレスおよびポート番号を使用して設定された複数のSLAプローブは、同時に実行することはできません。

IP SLA UDP ジッター動作に関する情報

IP SLA UDP ジッター動作

IP サービス レベル契約（SLA）UDP ジッター動作は、VoIP、Video over IP、またはリアルタイム会議などのリアルタイム トラフィック アプリケーションのネットワーク適合性を診断します。

ジッターとは、パケット間の遅延のばらつきを意味します。複数のパケットが発信元から宛先に連続的に送信される場合（たとえば 10 ミリ秒間隔で）、ネットワークが理想的に動作していれば、宛先は10ミリ秒間隔でパケットを受信します。しかし、ネットワーク内に遅延（キューイング、代替ルートを介した受信など）が存在する場合、パケット間の到着遅延は、10 ミリ秒より大きい場合も、10 ミリ秒より小さい場合もあります。この例を使用すると、正のジッター値は、パケットの到着間隔が 10 ミリ秒を超えていることを示します。パケットが 12 ミリ秒間隔で到着する場合、正のジッターは 2 ミリ秒です。パケットが 8 ミリ秒間隔で到着する場合、負のジッターは 2 ミリ秒です。Voice over IP（VoIP）など遅延に影響されやすいネットワークでは、正のジッター値は望ましくありません。0 のジッター値が理想的です。

しかし、IP SLA UDP ジッター動作の機能は、ジッタのモニタリングだけではありません。UDP ジッター動作には IP SLA UDP 動作によって返されたデータが含まれているため、UDP ジッター動作は多目的データ収集動作に使用できます。IP SLA が生成するパケットは、シーケン

ス情報を送受信するパケット、および送信元および動作ターゲットからのタイムスタンプを送受信するパケットを搬送します。UDP ジッター動作は、この情報に基づいて次のデータを測定できます。

- 方向別ジッター（送信元から宛先へ、宛先から送信元へ）
- 方向別パケット損失
- 方向別遅延（一方向遅延）
- ラウンドトリップ遅延（平均 RTT）

データの送信と受信でパスが異なる場合もあるので（非対称）、方向別データを使用すれば、ネットワークで発生している輻輳や他の問題が発生している場所を簡単に突き止めることができます。

UDP ジッター動作は、合成（シミュレーション）UDP トラフィックを生成して機能します。非対称プローブは、方向ごとのカスタム定義パケットサイズをサポートしており、それを使用して、異なるパケットサイズを要求パケット（送信元デバイスから宛先デバイスへ）および応答パケット（宛先デバイスから送信元デバイスへ）で送信できます。

UDP ジッター動作は、指定された頻度 F で、送信元デバイスから宛先デバイスに、サイズ S の N 個の UDP パケットを T ミリ秒間隔で送信します。それに応じて、サイズ P の UDP パケットが宛先デバイスから送信元デバイスに送信されます。デフォルトでは、ペイロードサイズが 10 バイト（S）のパケットフレーム 10 個（N）を 10 ミリ秒（T）ごとに生成し、60 秒（F）ごとに動作を繰り返します。次の表に示すように、これらのパラメータは、指定した IP サービスを最適にシミュレートできるようにユーザ設定可能です。

表 *1 : UDP* ジッター動作パラメータ

UDP ジッター動作パラメータ	**デフォルト**	**コンフィギュレーション コマンド**
パケット数（n）	10 パケット	**udp-jitter num-packets**
要求パケット単位のペイロードサイズ（S）	10 バイト	**request-data-size**
応答パケット単位のペイロードサイズ（P）	デフォルトの応答データ サイズは、設定している IP SLA 動作のタイプによって異なります。 （注） **response-data-size** コマンドが設定されていない場合、応答データ サイズ値は要求データ サイズ値と同じです。	**response-data-size**
パケット間隔（ミリ秒単位）（T）	10 ミリ秒	**udp-jitter interval**

UDP ジッター動作パラメータ	デフォルト	コンフィギュレーション コマンド
動作を繰り返すまでの経過時間（秒単位）（F）	60 秒	**frequency (IP SLA)**

IP SLA 動作は、合成（シミュレーション）ネットワーク トラフィックを生成して機能します。1 つの IP SLA 動作（たとえば IP SLA 動作 10）は、動作の存続期間の間、指定された頻度で繰り返されます。

IP SLA UDP ジッター動作の設定方法

宛先デバイスでの IP SLA Responder の設定

（注） Responder では、送信元に対して固定ポートを設定しないでください。Responder が送信元に対して固定ポートを設定すると、パケットが正常に（タイムアウトまたはパケット損失の問題が発生せずに）送信されたとしても、ジッター値はゼロになります。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します。
   - **ip sla responder**
   - **ip sla responder udp-echo ipaddress** *ip-address* **port** *port***vrf** *vrf*
4. **end**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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。

	コマンドまたはアクション	目的

ステップ 3	次のいずれかのコマンドを入力します。
	• **ip sla responder**
	• **ip sla responder udp-echo ipaddress** *ip-address* **port** *port***vrf** *vrf*
	例：
	`Device(config)# ip sla responder`
	`Device(config)# ip sla responder udp-echo ipaddress 192.0.2.132 port 5000 vrf vrf1`
		（任意）送信元からの制御メッセージに応じて、シスコ デバイスにおける IP SLA Responder 機能を一時的にイネーブルにします。
		（任意：送信元でプロトコル制御がディセーブルである場合にのみ必須です。）指定の IP アドレス、ポート、および VRF で、IP SLA Responder の機能をイネーブルにします。
		• プロトコル制御は、デフォルトでイネーブルになっています。

ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

送信元デバイスの UDP ジッター動作の設定とスケジューリング

次のいずれかの作業のみを実行します。

- 送信元デバイスでの基本 UDP ジッター動作の設定
- 追加特性を指定した UDP ジッター動作の設定

送信元デバイスでの基本 UDP ジッター動作の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **udp-jitter** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*}] [**source-port** *port-number*] [**control** {**enable** | **disable**}] [**num-packets** *number-of-packets*] [**interval** *interpacket-interval*]
5. **frequency** *seconds*
6. **end**
7. **show ip sla configuration** [*operation-number*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	`Device> enable`	
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	**ip sla** *operation-number* 例： `Device(config)# ip sla 10`	IP SLA 動作の設定を開始し、IP SLA 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	**udp-jitter** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*}] [**source-port** *port-number*] [**control** {**enable** | **disable**}] [**num-packets** *number-of-packets*] [**interval** *interpacket-interval*] 例： `Device(config-ip-sla)# udp-jitter 192.0.2.135 5000`	IP SLA 動作を UDP ジッター動作として設定し、UDP ジッター コンフィギュレーション モードを開始します。 • 送信元デバイスと宛先デバイスの両方で IP SLA 制御プロトコルをディセーブルにする場合のみ **control disable** キーワードの組み合わせを使用します。
ステップ 5	**frequency** *seconds* 例： `Device(config-ip-sla-jitter)# frequency 30`	（任意）指定した IP SLA 動作を繰り返す間隔を設定します。
ステップ 6	**end** 例： `Device(config-ip-sla-jitter)# end`	UDP ジッター コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 7	**show ip sla configuration** [*operation-number*] 例： `Device# show ip sla configuration 10`	（任意）すべての IP SLA 動作または指定した IP SLA 動作に関する設定値を、すべてのデフォルト値を含めて表示します。

次のタスク

動作のパーセンタイル オプションを設定するには、「IP SLA の設定：異常値のフィルタリングのパーセンタイル サポート」モジュールを参照してください。

追加特性を指定した UDP ジッター動作の設定

（注）
- UDP ジッター動作には大量のデータが含まれるため、IP サービス レベル契約（SLA）UDP ジッター動作では IP SLA 履歴機能はサポートされていません。つまり、次のコマンドは UDP ジッター動作ではサポートされていません：**history buckets-kept**、**history filter**、**history lives-kept**、**samples-of-history-kept**、および **show ip sla history**
- UDP ジッター動作の統計情報保存時間は、IP SLA で使用される MIB（CISCO-RTTMON-MIB）によって 2 時間に制限されます。**history hours-of-statistics** *hours* グローバル コンフィギュレーションを使用して、これより大きな値に設定しても、保持される期間が 2 時間を超えることはありません。ただし、Data Collection MIB を使用して動作の履歴データを収集することはできます。詳細については、「CISCO-DATA-COLLECTION-MIB」を参照してください。

始める前に

送信元デバイスでの UDP ジッター動作を設定する前に、ターゲット デバイス（動作ターゲット）で IP SLA Responder をイネーブルにしておく必要があります。IP SLA Responder を使用できるのは、Cisco IOS ソフトウェアベースのデバイスだけです。Responder をイネーブルにするために、「宛先デバイスでの IP SLA Responder の設定」の項の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **udp-jitter** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*}] [**source-port** *port-number*] [**control** {**enable** | **disable**}] [**num-packets** *number-of-packets*] [**interval** *interpacket-interval*]
5. **history distributions-of-statistics-kept** *size*
6. **history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*]
7. **frequency** *seconds*
8. **history hours-of-statistics-kept** *hours*
9. **owner** *owner-id*
10. **request-data-size** *bytes*
11. **response-data-size** *bytes*
12. **history statistics-distribution-interval** *milliseconds*
13. **tag** *text*
14. **threshold** *milliseconds*
15. **timeout** *milliseconds*
16. 次のいずれかのコマンドを入力します。
    - **tos** *number*
    - **traffic-class** *number*
17. **flow-label** *number*

18. **verify-data**
19. **vrf** *vrf-name*
20. **end**
21. **show ip sla configuration** [*operation-number*]

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	**ip sla** *operation-number* 例： `Device(config)# ip sla 10`	IP SLA 動作の設定を開始し、IP SLA コンフィギュレーション モードに移行します。
ステップ 4	**udp-jitter** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*}] [**source-port** *port-number*] [**control** {**enable** | **disable**}] [**num-packets** *number-of-packets*] [**interval** *interpacket-interval*] 例： `Device(config-ip-sla)# udp-jitter 192.0.2.134 5000`	IP SLA 動作を UDP ジッター動作として設定し、UDP ジッター コンフィギュレーション モードを開始します。 • 送信元デバイスとターゲット デバイスの両方で IP SLA 制御プロトコルをディセーブルにする場合のみ **control disable** キーワードの組み合わせを使用します。
ステップ 5	**history distributions-of-statistics-kept** *size* 例： `Device(config-ip-sla-jitter)# history distributions-of-statistics-kept 5`	（任意）IP SLA 動作にホップ単位で保持する統計情報の配信数を設定します。
ステップ 6	**history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*] 例： `Device(config-ip-sla-jitter)# history enhanced interval 900 buckets 100`	（任意）IP SLA 動作に対する拡張履歴収集をイネーブルにします。
ステップ 7	**frequency** *seconds* 例：	（任意）指定した IP SLA 動作を繰り返す間隔を設定します。

	コマンドまたはアクション	目的
	`Device(config-ip-sla-jitter)# frequency 30`	
ステップ 8	**history hours-of-statistics-kept** *hours* 例： `Device(config-ip-sla-jitter)# history hours-of-statistics-kept 4`	（任意）IP SLA 動作の統計情報を保持する時間数を設定します。
ステップ 9	**owner** *owner-id* 例： `Device(config-ip-sla-jitter)# owner admin`	（任意）IP SLA 動作の簡易ネットワーク管理プロトコル（SNMP）所有者を設定します。
ステップ 10	**request-data-size** *bytes* 例： `Device(config-ip-sla-jitter)# request-data-size 64`	（任意）IP SLA 動作の要求パケットのペイロード内でのプロトコル データ サイズを設定します。
ステップ 11	**response-data-size** *bytes* 例： `Device(config-ip-sla-jitter)# response-data-size 25`	（任意）IP SLA 動作の応答パケットのペイロード内でのプロトコル データ サイズを設定します。
ステップ 12	**history statistics-distribution-interval** *milliseconds* 例： `Device(config-ip-sla-jitter)# history statistics-distribution-interval 10`	（任意）IP SLA 動作で維持する各統計情報の配信間隔を設定します。
ステップ 13	**tag** *text* 例： `Device(config-ip-sla-jitter)# tag TelnetPollServer1`	（任意）IP SLA 動作のユーザ指定 ID を作成します。
ステップ 14	**threshold** *milliseconds* 例： `Device(config-ip-sla-jitter)# threshold 10000`	（任意）IP SLA 動作によって作成されるネットワーク モニタリング統計情報を計算するための上限しきい値を設定します。
ステップ 15	**timeout** *milliseconds* 例： `Device(config-ip-sla-jitter)# timeout 10000`	（任意）IP SLA 動作がその要求パケットからの応答を待機する時間を設定します。

	コマンドまたはアクション	目的

ステップ 16	次のいずれかのコマンドを入力します。
	• **tos** *number*
	• **traffic-class** *number*
	例：
	`Device(config-ip-sla-jitter)# tos 160`
	`Device(config-ip-sla-jitter)# traffic-class 160`
		（任意）IP SLA 動作の IPv4 ヘッダーに ToS バイトを定義します。
		または
		（任意）サポートされている IP SLA 動作に対する IPv6 ヘッダーにトラフィック クラス バイトを定義します。

ステップ 17	**flow-label** *number* 例： `Device(config-ip-sla-jitter)# flow-label 112233`	（任意）サポートされている IP SLA 動作に対する IPv6 ヘッダーにフロー ラベル フィールドを定義します。
ステップ 18	**verify-data** 例： `Device(config-ip-sla-jitter)# verify-data`	（任意）IP SLA 動作が各応答パケットに対してデータ破壊の有無をチェックするようにします。
ステップ 19	**vrf** *vrf-name* 例： `Device(config-ip-sla-jitter)# vrf vpn-A`	（任意）IP SLA 動作を使用したマルチプロトコル ラベル スイッチング（MPLS）VPN 内をモニタリングを許可します。
ステップ 20	**end** 例： `Device(config-ip-sla-jitter)# end`	UDP ジッター コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 21	**show ip sla configuration** [*operation-number*] 例： `Device# show ip sla configuration 10`	（任意）すべての IP SLA 動作または指定した IP SLA 動作に関する設定値を、すべてのデフォルト値を含めて表示します。

次のタスク

動作のパーセンタイル オプションを設定するには、「IP SLA の設定：異常値のフィルタリングのパーセンタイル サポート」モジュールを参照してください。

IP SLA 動作のスケジューリング

始める前に

- スケジュールされるすべての IP サービス レベル契約（SLA）動作がすでに設定されている必要があります。
- 複数動作グループでスケジュールされたすべての動作の頻度が同じでなければなりません。
- 複数動作グループに追加する 1 つ以上の動作 ID 番号のリストは、カンマ（,）を含めて最大 125 文字に制限する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します。
   - **ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {[*hh*:*mm*:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**]
   - **ip sla group schedule** *group-operation-number operation-id-numbers* { **schedule-period** *schedule-period-range* | **schedule-together**} [**ageout** *seconds*] **frequency** *group-operation-frequency* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm* [:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm* [:*ss*]}]
4. **end**
5. **show ip sla group schedule**
6. **show ip sla configuration**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	次のいずれかのコマンドを入力します。 • **ip sla schedule** *operation-number* [**life** {**forever**	*seconds*}] [**start-time** {[*hh*:*mm*:*ss*] [*month day*	*day month*]	**pending**	**now**	**after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**]	• 個々の IP SLA 動作のスケジューリング パラメータを設定します。 • 複数動作スケジューラ用に IP SLA 動作グループ番号と動作番号の範囲を指定します。

	コマンドまたはアクション	目的

	• **ip sla group schedule** *group-operation-number operation-id-numbers* { **schedule-period** *schedule-period-range* | **schedule-together**} [**ageout** *seconds*] **frequency** *group-operation-frequency* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm* [:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm* [:*ss*]}]
	例：
	`Device(config)# ip sla schedule 10 life forever start-time now`
	`Device(config)# ip sla group schedule 10 schedule-period frequency`
	`Device(config)# ip sla group schedule 1 3,4,6-9 life forever start-time now`
	`Device(config)# ip sla schedule 1 3,4,6-9 schedule-period 50 frequency range 80-100`	

ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	**show ip sla group schedule** 例： `Device# show ip sla group schedule`	（任意）IP SLA グループ スケジュールの詳細を表示します。
ステップ 6	**show ip sla configuration** 例： `Device# show ip sla configuration`	（任意）IP SLA 設定の詳細を表示します。

トラブルシューティングのヒント

- IP サービス レベル契約（SLA）動作が実行中でなく、統計情報が生成されていない場合は、設定に **verify-data** コマンドを追加して（IP SLA コンフィギュレーション モードで設定）、データ検証をイネーブルにします。データ検証をイネーブルにすると、各動作の応答で破損の有無がチェックされます。通常の動作時に **verify-data** コマンドを使用すると、不要なオーバーヘッドがかかるので注意してください。
- IP SLA 動作に関する問題をトラブルシューティングするには、**debug ip sla trace** コマンドと **debug ip sla error** コマンドを使用します。

次の作業

トラップを生成する目的（または別の動作を開始する目的）で、IPサービス レベル契約（SLA）動作に予防的しきい値条件と反応トリガーを追加するには、「予防的しきい値モニタリングの設定」の項を参照してください。

IP SLA UDP ジッター動作の確認

手順の概要

1. **enable**
2. **show ip sla configuration**
3. **show ip sla group schedule**
4. **show ip sla statistics**
5. **show ip sla statistics 2 details**

手順の詳細

ステップ 1 **enable**

特権 EXEC モードをイネーブルにします。

- パスワードを入力します（要求された場合）。

例：

```
Device> enable
```

ステップ 2 **show ip sla configuration**

IP SLA 設定の詳細を表示します。

例：

```
Device# show ip sla configuration

IP SLAs Infrastructure Engine-III
Entry number: 5
Owner: ownername
Tag: text
Operation timeout (milliseconds): 9999
Type of operation to perform: udp-jitter
Target address/Source address: 192.0.2.115/0.0.0.0
Target port/Source port: 5/0
Type Of Service parameter: 0x5
Request size (ARR data portion): 100
Response size (ARR data portion): 200
Packet Interval (milliseconds)/Number of packets: 20/10
Verify data: No
Operation Stats Precision : microseconds
Timestamp Location Optimization: enabled
Operation Packet Priority : high
```

```
NTP Sync Tolerance : 0 percent
Vrf Name:
Control Packets: enabled
```

ステップ 3 show ip sla group schedule

IP SLA グループ スケジュールの詳細を表示します。

例：

```
Device# show ip sla group schedule

Group Entry Number: 1
Probes to be scheduled: 6-9,3-4
Total number of probes: 6
Schedule period: 10
Mode: even
Group operation frequency: Equals schedule period
Status of entry (SNMP RowStatus): Active
Next Scheduled Start Time: Pending trigger
Life (seconds): 3600
Entry Ageout (seconds): never
```

ステップ 4 show ip sla statistics

IP SLA 統計情報を表示します。

例：

```
Device# show ip sla statistics

Type of operation: udp-jitter
Packet Loss Values:
Loss Source to Destination: 19
Source to Destination Loss Periods Number: 19
Source to Destination Loss Period Length Min/Max: 1/1
Source to Destination Inter Loss Period Length Min/Max: 1/546
Loss Destination to Source: 0
Destination to Source Loss Periods Number: 0
Destination to Source Loss Period Length Min/Max: 0/0
Destination to Source Inter Loss Period Length Min/Max: 0/0
Out Of Sequence: 0 Tail Drop: 0
Packet Late Arrival: 0 Packet Skipped: 0
```

- udp-jitter には、パケットが失われた方向を検出する機能があります。また、パケット損失の期間に関する統計情報を計算します。
- Loss Source to Destination: 19：19 個のパケットが送信者から送信されたが、レスポンダには届かなかったことを示します。
- Source to Destination Loss Periods Number: 19：19 個のパケット損失のインシデントがあったことを示します（パケット損失のインシデントとは、実際の損失パケット数に関係なく、パケットが失われた期間のことです）。
- Source to Destination Loss Period Length Min/Max: 1/1：この方向で失われたすべてのパケットが隔離されていることを示します。複数の損失パケットのバックツーバックのインスタンスはありません。

- Source to Destination Inter Loss Period Length Min/Max: 1/546：損失パケット間の最小間隔が 1 であり、連続するパケット損失の最大間隔が 546 個の正常に送信されたパケットであることを示します。

ステップ 5 show ip sla statistics 2 details

IPSLA の最新の動作統計情報を表示します。

例：

```
Device# show ip sla statistics 2 details

IPSLA operation id: 2
Type of operation: udp-jitter
Latest RTT: 1 milliseconds
Latest operation start time: 07:45:28 GMT Thu Aug 28 2014
Latest operation return code: OK
Over thresholds occurred: FALSE
RTT Values:
Number Of RTT: 10 RTT Min/Avg/Max: 1/1/1 milliseconds
Latency one-way time:
Number of Latency one-way Samples: 6
Source to Destination Latency one way Min/Avg/Max: 1/1/1 milliseconds
Destination to Source Latency one way Min/Avg/Max: 0/0/0 milliseconds
Source to Destination Latency one way Sum/Sum2: 6/6
Destination to Source Latency one way Sum/Sum2: 0/0
Jitter Time:
Number of SD Jitter Samples: 9
Number of DS Jitter Samples: 9
Source to Destination Jitter Min/Avg/Max: 0/1/1 milliseconds
Destination to Source Jitter Min/Avg/Max: 0/0/0 milliseconds
Source to destination positive jitter Min/Avg/Max: 1/1/1 milliseconds
Source to destination positive jitter Number/Sum/Sum2: 3/3/3
Source to destination negative jitter Min/Avg/Max: 1/1/1 milliseconds
Source to destination negative jitter Number/Sum/Sum2: 3/3/3
Destination to Source positive jitter Min/Avg/Max: 0/0/0 milliseconds
Destination to Source positive jitter Number/Sum/Sum2: 0/0/0
Destination to Source negative jitter Min/Avg/Max: 0/0/0 milliseconds
Destination to Source negative jitter Number/Sum/Sum2: 0/0/0
Interarrival jitterout: 0 Interarrival jitterin: 0
Jitter AVG: 1
Over Threshold:
Number Of RTT Over Threshold: 0 (0%)
Packet Loss Values:
Loss Source to Destination: 0
Source to Destination Loss Periods Number: 0
Source to Destination Loss Period Length Min/Max: 0/0
Source to Destination Inter Loss Period Length Min/Max: 0/0
Loss Destination to Source: 0
Destination to Source Loss Periods Number: 0
Destination to Source Loss Period Length Min/Max: 0/0
Destination to Source Inter Loss Period Length Min/Max: 0/0
Out Of Sequence: 0 Tail Drop: 0 Packet Late Arrival: 0
Packet Skipped: 0
Voice Score Values:
Calculated Planning Impairment Factor (ICPIF): 0
Mean Opinion Score (MOS): 0
Number of successes: 2
Number of failures: 0
Operation time to live: Forever
```

```
Operational state of entry: Active
Last time this entry was reset: Never
```

IP SLA UDP ジッター動作の設定例

例：UDP ジッター動作の設定

次の例では、2 つの動作が、動作 2 が最初の動作の 5 秒後に開始される UDP ジッター動作として設定されています。どちらの動作も無期限に実行されます。

```
configure terminal
 ip sla 1
  udp-jitter 192.0.2.115 65051 num-packets 20
  request-data-size 160
  tos 128
  frequency 30
 ip sla schedule 1 start-time after 00:05:00
 ip sla 2
  udp-jitter 192.0.2.115 65052 num-packets 20 interval 10
  request-data-size 20
  tos 64
  frequency 30
 ip sla schedule 2 start-time after 00:05:05
```

送信元デバイスからの制御メッセージに応じて、シスコ デバイスで IP SLA Responder 機能を一時的に有効にするには、ターゲット（宛先）デバイスで次のコマンドを入力します。

```
ip sla responder
```

IP SLA UDP ジッター動作に関するその他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Cisco IOS IP SLA コマンド	『Cisco IOS IP SLAs Command Reference』

MIB

MIB	MIB のリンク
• CISCO-DATA-COLLECTION-MIB • CISCO-RTTMON-MIB • IPV6-FLOW-LABEL-MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

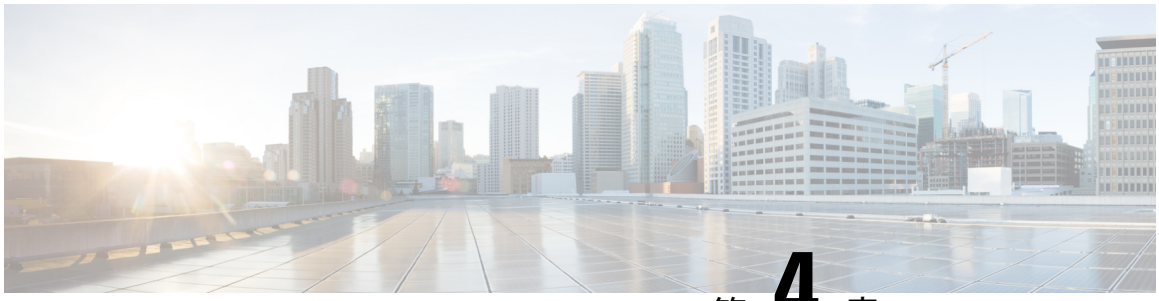
説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IP SLA UDP ジッター動作の機能情報

表 *2 : IP SLA UDP* ジッター動作に関する機能情報

機能名	リリース	機能情報
IP SLA：UDP ジッター動作	Cisco IOS XE Release 2.1 Cisco IOS XE 3.1.0SG Cisco IOS XE Release 3.2SE	IP SLA UDP ジッター動作を使用すると、UDP トラフィックを伝送するネットワーク内におけるラウンドトリップ遅延、一方向遅延、一方向ジッター、一方向パケット損失、および接続を測定できます。
IPv6 用 IP SLA（UDP ジッター、UDP エコー、ICMP エコー、TCP 接続）	Cisco IOS XE Release 2.1 Cisco IOS XE 3.1.0SG Cisco IOS XE Release 3.2SE	IPv6 用 IP SLA（UDP ジッター、UDP エコー、ICMP エコー、TCP 接続）機能によって、IPv6 ネットワークにおける動作性に対するサポートが追加されています。

機能名	リリース	機能情報
IP SLA：UDP ジッターの非対称プローブサポート	Cisco IOS XE Release 3.10S	IP SLA：UDP ジッターの非対称プローブ サポート機能では、応答パケット内のカスタム定義パケット サイズの設定をサポートしています。 次のコマンドが導入されました。 **response-data-size** Cisco IOS XE リリース 3.10S では、Cisco ASR 1000 シリーズ ルータのサポートが追加されました。



第 4 章

IP SLA マルチキャスト サポート

このモジュールでは、ユーザが指定するマルチキャスト グループ内の各マルチキャスト受信者の一方向遅延、ジッター、およびパケット損失などの統計情報を測定および報告するために、IP サービス レベル契約（SLA）マルチキャスト UDP ジッター動作を設定してスケジューリングする方法について説明します。.

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

IP SLA マルチキャスト サポートの前提条件

- 一方向遅延を正確に測定するには、送信元デバイスとターゲット デバイスの間でネットワーク タイム プロトコル（NTP）が提供するクロック同期が必要です。送信元デバイスおよびターゲット デバイスで NTP を設定するには、『*Network Management Configuration*

Guide』の「Performing Basic System Management」の章の作業を実行します。一方向ジッタおよびパケット損失を測定する場合は、クロック同期は不要です。だたし、送信元デバイスとターゲット デバイスとの間でクロックが同期していない場合、一方向ジッターとパケット損失データは返されますが、UDP ジッター動作による一方向遅延測定は「0」の値が返されます。

- IP SLA マルチキャストが成功するには、すべてのデバイスが同一 VRF の一部でなければなりません。
- レスポンダとプローブが設定されているデバイスはともに、IP SLA マルチキャスト サポート機能をサポートしている Cisco ソフトウェア イメージを実行している必要があります。IP SLA アプリケーションを設定する前に、**show ip sla application** コマンドを使用して、ご使用のソフトウェア イメージでサポートされている動作タイプを確認してください。

IP SLA マルチキャスト サポートの制限事項

マルチキャスト UDP ジッター動作は、一方向（OW）データのみ提供できます。

IP SLA マルチキャスト サポートに関する情報

マルチキャスト UDP ジッター動作

マルチキャスト UDP ジッター動作は、ユーザが指定するマルチキャスト グループ内の各マルチキャスト受信者の一方向遅延、ジッター、およびパケット損失などの統計情報を測定および報告します。マルチキャスト UDP ジッター動作によって、次のタスクを実行できます。

- ネットワークに新しいマルチキャスト ネットワーク アプリケーションを導入後または新しいマルチキャスト ベースのプロトコルを実装後の、マルチキャスト ネットワークのパフォーマンスの分析と評価。
- 重要なイベントに対してマルチキャスト ネットワークを実際に利用する前の、マルチキャストのネットワーク動作の確認。
- ネットワークを監視して、考えられる問題領域を分離するための予防的アプローチの実行。

マルチキャスト UDP ジッター動作の送信者は、送信元デバイスからマルチキャスト IP アドレスに指定された間隔で UDP パケットを送信します。初期設定時に、指定されたエンドポイント リストに、特定のマルチキャスト動作についての連絡先となるすべてのレスポンダのリストが提供されます。マルチキャスト サブシステムは、ユニキャスト パスを利用して、ユニキャスト制御パケットをエンドポイント リストに記載された各マルチキャスト受信者に送信します。受信者がマルチキャスト グループに参加できるように、制御メッセージが各受信者に送信されます。

マルチキャスト受信者の IP SLA マルチキャスト レスポンダは、UDP パケットを受信し、タイムスタンプ データを記録します。

IGMP への参加が正常に完了した有効なレスポンダのリストは、送信者側で保持されます。レスポンダ リストを受信すると、マルチキャスト パケットの生成を開始できます。

すべてのマルチキャスト トラフィックは、送信元の送信者から受信者のレスポンダへの一方向であるため、動作の一部である各レスポンダは、ローカル計算の実行と統計情報の保存を担います。統計情報は、動作の各サイクルの最後に表示される送信者に送り返されます（すべてのパケットがレスポンダに送信された後）。レスポンダは統計情報の履歴を保持せず、情報を送信者に送信後にすべての関連するメモリを解放するので、スケジューリングされている各動作（頻度に基づく）は、マルチキャスト レスポンダによって新しい動作とみなされ、以前の動作とは関連がないものとみなされます。

マルチキャスト UDP ジッター動作は、IPv4 ネットワークでサポートされます。

IP SLA マルチキャスト サポートの設定方法

宛先デバイスでの IP SLA Responder の設定

（注） Responder では、送信元に対して固定ポートを設定しないでください。Responder が送信元に対して固定ポートを設定すると、パケットが正常に（タイムアウトまたはパケット損失の問題が発生せずに）送信されたとしても、ジッター値はゼロになります。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します。
   - **ip sla responder**
   - **ip sla responder udp-echo ipaddress** *ip-address* **port** *port***vrf** *vrf*
4. **end**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
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	次のいずれかのコマンドを入力します。
	• **ip sla responder**
	• **ip sla responder udp-echo ipaddress** *ip-address* **port** *port***vrf** *vrf*
	例：
	`Device(config)# ip sla responder`
	`Device(config)# ip sla responder udp-echo ipaddress 192.0.2.132 port 5000 vrf vrf1`
		（任意）送信元からの制御メッセージに応じて、シスコ デバイスにおける IP SLA Responder 機能を一時的にイネーブルにします。
		（任意：送信元でプロトコル制御がディセーブルである場合にのみ必須です。）指定の IP アドレス、ポート、および VRF で、IP SLA Responder の機能をイネーブルにします。
		• プロトコル制御は、デフォルトでイネーブルになっています。

ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

送信元デバイスのマルチキャスト レスポンダのリストの作成

始める前に

（レスポンダの）エンドポイント リストに追加するすべてのレスポンダは、宛先デバイスで最初に設定する必要があります。設定情報については、「宛先デバイスでの IP SLA Responder の設定」の項を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla endpoint-list type ip** *template-name*
4. **description** *description*
5. **ip-address** *address* [**-***address* | **,** *... ,* *address*] **port** *port*
6. **end**
7. **show ip sla endpoint-list** [**type ip** [*template-name*]]

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	**ip sla endpoint-list type ip** *template-name* 例： `Device(config)# ip sla endpoint-list type ip mcast-rcvrs`	エンドポイント リストの設定を開始し、エンドポイント リスト 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	**description** *description* 例： `Device(config-epl)# description list of receivers`	（任意）設定されているテンプレートに説明テキストを追加します。
ステップ 5	**ip-address** *address* [**-***address* | **,** *... ,* *address*] **port** *port* 例： `Device(config-epl)# ip-address 10.1.1.1-13 port 6500`	設定されているエンドポイント リストにマルチキャスト レスポンダの IPv4 または IPv6 アドレスを追加します。 • 必要なすべてのアドレスが設定されるまで、このコマンドを繰り返します。 • 1 つ以上のアドレスを削除することでエンドポイント リストを変更するには、このコマンドの **no** 形式を使用します。
ステップ 6	**end** 例： `Device(config-epl)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show ip sla endpoint-list** [**type ip** [*template-name*]] 例： `Device# show ip sla endpoint-list type ip mcast-rcvrs`	（任意）エンドポイント リストの設定を表示します。

マルチキャスト UDP ジッター動作の設定

（注）
- UDP ジッター動作には大量のデータが含まれるため、IP SLA UDP ジッター動作では IP SLA 履歴機能（統計情報の履歴バケット）はサポートされていません。つまり、次のコマンドは UDP ジッター動作ではサポートされていません：**history buckets-kept**、**history filter**, **history lives-kept**、**samples-of-history-kept**、および **show ip sla history**
- UDP ジッター動作の統計情報保存時間は、IP SLA で使用される MIB（CISCO-RTTMON-MIB）によって 2 時間に制限されます。**history hours-of-statistics** *hours* グローバル コンフィギュレーションを使用して、これより大きな値に設定しても、保持される期間が 2 時間を超えることはありません。ただし、Data Collection MIB を使用して動作の履歴データを収集することはできます。詳細については、「CISCO-DATA-COLLECTION-MIB」（http://www.cisco.com/go/mibs）を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **udp-jitter** {*destination-ip-address* | *destination-hostname*} *destination-port* **endpoint-list** *endpoint-list* [**ssm**] [**source-ip** *ip-address*] [**source-port** *port-number*] [**num-packets** *number-of-packets*] [**interval** *interpacket-interval*]
5. **control retry** *retries*
6. **control timeout** *seconds*
7. **dscp** *dscp-value*
8. **tree-init** *number*
9. **history distributions-of-statistics-kept** *size*
10. **history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*]
11. **frequency** *seconds*
12. **history hours-of-statistics-kept** *hours*
13. **owner** *owner-id*
14. **request-data-size** *bytes*
15. **history statistics-distribution-interval** *milliseconds*
16. **tag** *text*
17. **threshold** *milliseconds*
18. **timeout** *milliseconds*
19. **tos** *number*
20. **verify-data**
21. **vrf** *vrf-name*
22. **end**
23. **show ip sla configuration** [*operation-number*]

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	**ip sla** *operation-number* 例： `Device(config)# ip sla 10`	IP SLA 動作の設定を開始し、IP SLA コンフィギュレーション モードに移行します。
ステップ 4	**udp-jitter** {*destination-ip-address* | *destination-hostname*} *destination-port* **endpoint-list** *endpoint-list* [**ssm**] [**source-ip** *ip-address*] [**source-port** *port-number*] [**num-packets** *number-of-packets*] [**interval** *interpacket-interval*] 例： `Device(config-ip-sla)# udp-jitter 239.1.1.1 5000 endpoint-list mcast-rcvrs source-ip 10.10.10.106 source-port 7012 num-packets 50 interval 25`	IP SLA 動作をマルチキャスト UDP ジッター動作として設定し、マルチキャスト UDP ジッター コンフィギュレーション モードを開始します。
ステップ 5	**control retry** *retries* 例： `Device(config-ip-sla-multicast-jitter-oper)# control retry 2`	（任意）送信側デバイスが制御プロトコル メッセージを再送信する回数を設定します。
ステップ 6	**control timeout** *seconds* 例： `Device(config-ip-sla-multicast-jitter)# control timeout 4`	（任意）宛先デバイスが制御プロトコル メッセージを待機する秒数を設定します。
ステップ 7	**dscp** *dscp-value* 例： `Device(config-ip-sla-multicast-jitter-oper)# dscp 10`	（任意）動作の DSCP 値を設定します。
ステップ 8	**tree-init** *number* 例： `Device(config-ip-sla-multicast-jitter-oper)# tree-init 1`	（任意）マルチキャスト ツリーを設定します。

	コマンドまたはアクション	目的
ステップ 9	**history distributions-of-statistics-kept** *size* 例： `Device(config-ip-sla-multicast-jitter-oper)# history distributions-of-statistics-kept 5`	（任意）IP SLA 動作中にホップ単位で保持する統計情報の配信数を設定します。
ステップ 10	**history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*] 例： `Device(config-ip-sla-multicast-jitter-oper)# history enhanced interval 900 buckets 100`	（任意）IP SLA 動作に対する拡張履歴収集をイネーブルにします。
ステップ 11	**frequency** *seconds* 例： `Device(config-ip-sla-multicast-jitter-oper)# frequency 30`	（任意）指定した IP SLA 動作を繰り返す間隔を設定します。
ステップ 12	**history hours-of-statistics-kept** *hours* 例： `Device(config-ip-sla-multicast-jitter-oper)# history hours-of-statistics-kept 4`	（任意）IP SLA 動作の統計情報を保持する時間数を設定します。
ステップ 13	**owner** *owner-id* 例： `Device(config-ip-sla-multicast-jitter-oper)# owner admin`	（任意）IP SLA 動作の簡易ネットワーク管理プロトコル（SNMP）所有者を設定します。
ステップ 14	**request-data-size** *bytes* 例： `Device(config-ip-sla-multicast-jitter-oper)# request-data-size 64`	（任意）IP SLA 動作の要求パケットのペイロードにおけるプロトコル データ サイズを設定します。
ステップ 15	**history statistics-distribution-interval** *milliseconds* 例： `Device(config-ip-sla-multicast-jitter-oper)# history statistics-distribution-interval 10`	（任意）IP SLA 動作で維持する各統計情報の配信間隔を設定します。
ステップ 16	**tag** *text* 例： `Device(config-ip-sla-multicast-jitter-oper)# tag TelnetPollServer1`	（任意）IP SLA 動作のユーザ指定 ID を作成します。

	コマンドまたはアクション	目的
ステップ 17	**threshold** *milliseconds* 例： `Device(config-ip-sla-multicast-jitter-oper)# threshold 10000`	（任意）IP SLA 動作によって作成されるネットワーク モニタリング統計情報を計算するための上限しきい値を設定します。
ステップ 18	**timeout** *milliseconds* 例： `Device(config-ip-sla-multicast-jitter-oper)# timeout 10000`	（任意）IP SLA 動作がその要求パケットからの応答を待機する時間を設定します。
ステップ 19	**tos** *number* 例： `Device(config-ip-sla-multicast-jitter-oper)# tos 160`	（任意）IPv4 ネットワークに限り、IP SLA 動作の IPv4 ヘッダーの ToS バイトを定義します。
ステップ 20	**verify-data** 例： `Device(config-ip-sla-multicast-jitter-oper)# verify-data`	（任意）IP SLA 動作が各応答パケットに対してデータ破壊の有無をチェックするようにします。
ステップ 21	**vrf** *vrf-name* 例： `Device(config-ip-sla-multicast-jitter-oper)# vrf vpn-A`	（任意）IP SLA 動作を使用したマルチプロトコル ラベル スイッチング（MPLS）VPN 内をモニタリングを許可します。
ステップ 22	**end** 例： `Device(config-ip-sla-multicast-jitter-oper)# end`	特権 EXEC モードに戻ります。
ステップ 23	**show ip sla configuration** [*operation-number*] 例： `Device# show ip sla configuration 10`	（任意）すべての IP SLA 動作または指定した IP SLA 動作に関する設定値を、すべてのデフォルト値を含めて表示します。

IP SLA 動作のスケジューリング

始める前に

- スケジュールされるすべての IP サービス レベル契約（SLA）動作がすでに設定されている必要があります。

- 複数動作グループでスケジュールされたすべての動作の頻度が同じでなければなりません。
- 複数動作グループに追加する 1 つ以上の動作 ID 番号のリストは、カンマ（,）を含めて最大 125 文字に制限する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します。
   - **ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {[*hh*:*mm*:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**]
   - **ip sla group schedule** *group-operation-number operation-id-numbers* { **schedule-period** *schedule-period-range* | **schedule-together**} [**ageout** *seconds*] **frequency** *group-operation-frequency* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm* [:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm* [:*ss*]}]
4. **end**
5. **show ip sla group schedule**
6. **show ip sla configuration**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	次のいずれかのコマンドを入力します。 • **ip sla schedule** *operation-number* [**life** {**forever**	*seconds*}] [**start-time** {[*hh*:*mm*:*ss*] [*month day*	*day month*]	**pending**	**now**	**after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**] • **ip sla group schedule** *group-operation-number operation-id-numbers* { **schedule-period** *schedule-period-range*	**schedule-together**} [**ageout** *seconds*] **frequency** *group-operation-frequency* [**life** {**forever**	*seconds*}] [**start-time** {*hh*:*mm* [:*ss*] [*month day*	*day month*]	**pending**	**now**	**after** *hh*:*mm* [:*ss*]}] 例：	• 個々の IP SLA 動作のスケジューリング パラメータを設定します。 • 複数動作スケジューラ用に IP SLA 動作グループ番号と動作番号の範囲を指定します。

	コマンドまたはアクション	目的

	`Device(config)# ip sla schedule 10 life forever start-time now`
	
	`Device(config)# ip sla group schedule 10 schedule-period frequency`
	
	`Device(config)# ip sla group schedule 1 3,4,6-9 life forever start-time now`
	
	`Device(config)# ip sla schedule 1 3,4,6-9 schedule-period 50 frequency range 80-100`	

ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	**show ip sla group schedule** 例： `Device# show ip sla group schedule`	（任意）IP SLA グループ スケジュールの詳細を表示します。
ステップ 6	**show ip sla configuration** 例： `Device# show ip sla configuration`	（任意）IP SLA 設定の詳細を表示します。

トラブルシューティングのヒント

- IP サービス レベル契約（SLA）動作が実行中でなく、統計情報が生成されていない場合は、設定に **verify-data** コマンドを追加して（IP SLA コンフィギュレーション モードで設定）、データ検証をイネーブルにします。データ検証をイネーブルにすると、各動作の応答で破損の有無がチェックされます。通常の動作時に **verify-data** コマンドを使用すると、不要なオーバーヘッドがかかるので注意してください。
- IP SLA 動作に関する問題をトラブルシューティングするには、**debug ip sla trace** コマンドと **debug ip sla error** コマンドを使用します。

次の作業

トラップを生成する目的（または別の動作を開始する目的）で、IPサービス レベル契約（SLA）動作に予防的しきい値条件と反応トリガーを追加するには、「予防的しきい値モニタリングの設定」の項を参照してください。

IP SLA マルチキャスト サポートの設定例

例：マルチキャスト UDP ジッター動作

```
Device# show ip sla endpoint-list

Endpoint-list Name: multicast
    Description:
    ip-address 192.0.2.1 port 1111
    ip-address 192.0.2.2 port 2222
    ip-address 192.0.2.3 port 3333

Device# show ip sla configuration 22

IP SLAs Infrastructure Engine-III
Entry number: 22
Owner:
Tag:
Operation timeout (milliseconds): 5000
Type of operation to perform: udp-jitter
Target address/Source address: 224.1.1.1/0.0.0.0
Target port/Source port: 2460/0
Type Of Service parameter: 0x0
Request size (ARR data portion): 32
Packet Interval (milliseconds)/Number of packets: 20/10
Verify data: No
Vrf Name:
Control Packets: enabled
Schedule:
   Operation frequency (seconds): 60  (not considered if randomly scheduled)
   Next Scheduled Start Time: Pending trigger
   Group Scheduled : FALSE
   Randomly Scheduled : FALSE
   Life (seconds): 3600
   Entry Ageout (seconds): never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
   Number of statistic hours kept: 2
   Number of statistic distribution buckets kept: 1
   Statistic distribution interval (milliseconds): 20
Enhanced History:

  sno    oper-id             dest-ip-addr  !<---Responders in endpoint list: multicast
    1   976271337              192.0.2.1
    2  1632881300              192.0.2.2
    3  2138021658              192.0.2.3
```

IP SLA マルチキャスト サポートに関するその他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IP SLA コマンド	『Cisco IOS IP SLAs Command Reference』
Cisco IP SLA に関する情報	『*IP SLA* コンフィギュレーション ガイド』の「Cisco IOS IP SLA の概要」モジュール

MIB

MIB	MIB のリンク
CISCO-IPSLA-TC-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

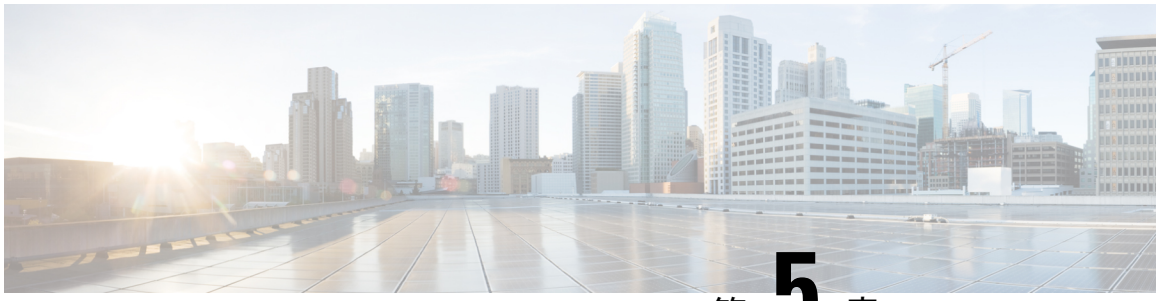
IPSLA マルチキャスト サポートに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *3 : IPSLA* マルチキャスト サポートに関する機能情報

機能名	リリース	機能情報
IPSLA マルチキャストのサポート	15.2(4)M 15.3(1)S Cisco IOS XE Release 3.8S 15.1(2)SG Cisco IOS XE Release 3.4SG	この機能では、ユーザが指定するマルチキャスト グループ内の各マルチキャスト受信者の一方向遅延、ジッター、およびパケット損失などの統計情報を測定および報告するためのマルチキャストUDP ジッター動作が導入されました。 次のコマンドが導入または変更されました。 **clock-tolerance ntp oneway**、**control (IP SLA)**、**dscp (IP SLA)**、**history distributions-of-statistics-kept**、**history enhanced**、**history hours-of-statistics-kept**、**ip-address (endpoint list)**、**operation-packet priority**、**owner**、**precision**、**show ip sla application**、**show ip sla configuration**、**show ip sla endpoint-list**、**show ip sla statistics**、**show ip sla statistics aggregated**、 **tag (IP SLA)**、**timeout (IP SLA)**、**tos**、**tree-init**、**udp-jitter**、**verify-data (IP SLA)**、**vrf**



第 5 章

VoIP 用の IP SLA UDP ジッター動作の設定

このマニュアルでは、IP サービス レベル契約（SLA）ユーザ データグラム プロトコル（UDP）ジッター動作を設定してネットワーク内の Voice over IP（VoIP）品質レベルを予防的にモニタし、IPv4 または IPv6 ネットワーク内のユーザに VoIP 品質レベルを保証できるようにする方法について説明します。IP SLA VoIP UDP ジッター動作は、共通のコーデックを使用して VoIP トラフィックを正確にシミュレーションし、ネットワーク内のシスコデバイス間で一貫性のある音声品質スコア（MOS および ICPIF）を算出します。

（注） このマニュアルで使用される「音声」という用語は、あらゆるインターネット テレフォニー アプリケーションを意味します。「Voice over IP」という用語には、IP ネットワーク経由のマルチメディア（音声とビデオの両方）の伝送が含まれることもあります。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

VoIP 用の IP SLA UDP ジッター動作の制約事項

- この機能は、UDP トラフィックを使用して適切な Voice over IP スコアを生成します。Real-Time Transport Protocol（RTP）はサポートされていません。
- この機能で算出される ICPIF 値および MOS 値には IP SLA 内での一貫性はありますが、相対的に比較するために生成された予想値に過ぎません。これらの値は、他の方法で測定された値とは異なる可能性があります。
- 任意の方法で測定されたカスタマー オピニオンの予測値（E-Model 伝送評価係数 R や算出された平均オピニオン評点に対して示された値など）は、伝送計画および分析のみを目的として生成された値です。実際のカスタマー オピニオンを反映する値ではありません。

VoIP 用の IP SLA UDP ジッター動作に関する情報

Calculated Planning Impairment Factor（ICPIF）

ICPIF は、式 *Icpif = Itot - A* の一部として、1996 年版の ITU-T 勧告 G.113『Transmission impairments』で最初に開発されました。ICPIF は、実際には「（Impairment）Calculated Planning Impairment Factor」の頭字語で、単純に「計画劣化係数の算出値」を意味すると理解してください。ICPIF は、比較および計画用に、ネットワークに生じた音声品質に対する主な劣化の定量化を試みます。

ICPIF は、測定された劣化係数の合計（総劣化、つまり *Itot*）からユーザ定義のアクセス アドバンテージ係数（*A*）を引いたものです。アクセスアドバンテージ係数（A）は、通話方法（携帯電話からの通話対固定電話からの通話など）に基づいた、ユーザの期待を表す値です。この式を拡張すると、完全な式は次のようになります。

Icpif = Io + Iq + Idte + Idd + Ie - A

値は次のとおりです。

- *Io* は、最適ではないラウドネス定格が原因の劣化を表します。
- *Iq* は、PCM の量子化歪みが原因の劣化を表します。
- *Idte* は、送話者エコーによる劣化を表します。
- *Idd* は、一方向の伝送の時間（一方向遅延）により発生した劣化を表します。
- *Ie* は、通話に使用されたコーデック タイプ、パケット損失など装置の影響が原因の劣化を表します。

- *A* は、アクセスの容易性の代償としてユーザがある程度の劣化を許容するという事実を補う、アクセス アドバンテージ係数（ユーザ期待係数とも呼ばれます）を表します。

ICPIF の値は、通常、5（非常に軽い障害）から 55（非常に重い障害）の範囲で表されます。20 未満の ICPIF 値は、通常、「適切」と見なされます。ICPIF 値の目的は音声品質の客観的測定ですが、この値は、劣化の組み合わせの主観的影響を予測するためにも使用されます。G.113（1996 年 2 月）に記載された、主観的品質判定に対応することが期待されるサンプル ICPIF 値を、次の図に示します。

表 *4*：総劣化係数 *ICPIF* に応じた品質レベル

ICPIF の上限	音声通信の品質
5	きわめて良好
10	良好
20	適切
30	限定された状況で許容可
45	きわめて限定された状況で許容可
55	ユーザが強い不満を示す可能性が高い（苦情、ネットワーク オペレータの変更）

ICPIF の詳細については、1996 年版の G.113 の仕様を参照してください。

（注） 最新版の ITU-T G.113 勧告（2001 年）には、ICPIF モデルについての記載はありません。代わりに、事業者に対して次のように G.107 を紹介しています。「ITU-T G.107 の E-model で使用される『劣化係数法』が推奨されます。量子化歪み単位を使用していた初期の方法は、現在では推奨されません」と記述されています。完全な E-Model（ITU-T 伝送評価モデルとも呼ばれます）は、*R = Ro - Is - Id - Ie + A* として表現され、劣化係数の定義の改善により、コール品質のより正確な測定の可能性を提供します（詳細については、G.107、2003 年版を参照してください）。ICPIF と E-Model は劣化に関する用語を共有していますが、これら 2 つのモデルを混同しないでください。IP SLA VoIP UDP 動作機能では、ICPIF、伝送評価係数 R、および MOS 値の間で観測された対応関係が活用されますが、E-Model はサポートされていません。

IP SLA は単純化された ICPIF 式を使用します（この式の詳細については、以降のこのマニュアルで定義します）。

平均オピニオン評点（MOS）

伝送される音声の品質は、聞き手の主観的な反応です。Voice over IP の伝送に使用する各コーデックは特定のレベルの品質を提供します。特定のコーデックによってもたらされる音質の測定に使用される共通のベンチマークは、MOS です。MOS では、幅広い聞き手が、特定のコー

デックを使用して送信された音声サンプルの品質を1（貧弱）～5（優良）で判定します。オピニオン評点は平均化されて、各サンプルの平均が算出されます。次の表に、各値に対するMOS評点および対応する品質の説明を示します。

表 *5: MOS* 評価

スコア	品質	品質劣化の説明
5	優良	ほとんど感じられない
4	良	わずかに感じられるが、気にならない
3	可	感じられ、やや気になる
2	貧弱	気になるが、不快ではない
1	不可	非常に気になり、不快である

コーデックおよび他の伝送劣化に関するMOS評点がよく知られているため、測定された劣化に基づいてMOSの予測値を算出し、表示できます。ITUでは、この予測値を客観的MOSまたは主観的MOS値と区別するために、Mean Opinion Score; Conversational Quality, Estimated（MOS-CQE）と表しています（詳細は、*P.800.1 Mean Opinion Score (MOS) terminology - ITU* を参照）。

IP SLA を使用した音声パフォーマンスのモニタリング

IPネットワーク上で音声品質およびビデオ品質を測定する際に重要なメトリックの1つはジッタです。ジッタとは、着信パケット間の遅延のばらつき（パケット間の遅延の分散）を示すのに使用される名前です。ジッタは、通話者の音声パターンに不均等なずれを生じさせて、音声品質に影響を与えます。IPネットワーク上での音声伝送およびビデオ伝送に関するその他の重要なパフォーマンス パラメータには、遅延やパケット損失が挙げられます。IP SLAは、Ciscoソフトウェアの埋め込み型アクティブモニタリング機能であり、ユーザとのサービスレベル契約以上のサービス レベルをネットワークが確保するためにシミュレーションし、これらのパラメータを測定するための手段を提供します。

IP SLAは、送信元デバイスから特定の宛先（動作ターゲットと呼ばれます）にネットワーク経由で送信されたUDPプローブ パケットで構成されるUDPジッター動作を提供します。この合成トラフィックは、接続のジッタ量、ラウンドトリップ時間、方向別パケット損失、および一方向遅延を記録するために使用されます「合成トラフィック」という用語は、ネットワークトラフィックがシミュレートされていることを示します。つまり、トラフィックは、IP SLAによって生成されます。収集された統計情報の形式でのデータは、ユーザ定義した期間内の複数のテストに対して表示でき、たとえば、1日の異なる時間、または週の経過におけるネット

ワークのパフォーマンスを確認できます。ジッタープローブには、受信側で最小の遅延を提供するために IP SLA Responder を使用できます。

IP SLA VoIP UDP ジッター動作は、UDP ジッター動作によって既に収集されているメトリックに加えて、動作によって収集されたデータに MOS スコアおよび ICPIF スコアを返す機能を追加することによって標準的な UDP ジッター動作を変更します。この VoIP 固有の実装では、VoIP ネットワークのパフォーマンスを測定する際にさらに役立つ情報が提供されるため、ネットワークの評価、トラブルシューティング、およびヘルスモニタリングを実行する機能を向上できます。

IP SLA でのコーデックのシミュレーション

IP SLA VoIP UDP ジッター動作は、指定された頻度 f で、指定された送信元デバイスから指定されたターゲット デバイスに、サイズ s の n 個の UDP パケットを t ミリ秒間隔で送信して統計情報を計算します。ターゲット デバイスは、プローブ動作を処理するために、Cisco IP SLA Responder を実行している必要があります。

MOS スコアと ICPIF スコアを生成するには、VoIP UDP ジッター動作を設定するときに、接続に使用するコーデック タイプを指定する必要があります。動作に設定したコーデック タイプに基づいて、パケット数（n）、各ペイロードのサイズ（s）、パケット間間隔（t）、および動作の頻度（f）がデフォルト値に自動設定されますただし、必要な場合は、**udp-jitter** コマンドの構文でこれらのパラメータを手動で設定することもできます。

次の表に、コーデックによる動作に設定されるデフォルト パラメータを示します。

表 *6 :* デフォルトの *VoIP UDP* ジッター動作パラメータ（コーデック タイプ別）

コーデック	デフォルトの要求サイズ（パケットペイロード）（**s**）	デフォルトのパケット間間隔（**t**）	デフォルトのパケット数（**n**）	プローブ動作の頻度（**f**）
G.711 mu-Law（g711ulaw）	160 + 12 RTP バイト	20 ms	1000	1 分に 1 回
G.711 A-Law（g711alaw）	160 + 12 RTP バイト	20 ms	1000	1 分に 1 回
G.729A（g729a）	20 + 12 RTP バイト	20 ms	1000	1 分に 1 回

たとえば、g711ulaw コーデックの特性を使用する VoIP UDP ジッター動作を設定した場合、プローブ動作はデフォルトで 1 分に 1 回（**f**）送信されます。各プローブ動作は 1000 パケット（**n**）で構成され、各パケットは 180 バイトの合成データ（**s**）を含み、20 ミリ秒間隔（**t**）で送信されます。

IP SLA ICPIF 値

Cisco ソフトウェアを使用する ICPIF 値の計算は、主として音声品質を損なう 2 つの主要因（遅延パケットと損失パケット）に基づいています。パケット遅延およびパケット損失は IP SLA

で測定できます。したがって、完全な ICPIF 式（*Icpif = Io + Iq + Idte + Idd + Ie - A*）は、*Io*、*Iq*、および *Idte*の各値が 0 であると仮定して、次のように単純化できます。

総劣化係数（*Icpif*） = 遅延劣化係数*r*（*Idd*） + 機器劣化係数（*Ie*） - 期待/アドバンテージ係数（*A*）

つまり ICPIF 値は、遅延パケットの測定値に基づいた遅延劣化係数と、損失パケットの測定値に基づいた機器劣化係数を加算して算出されます。ネットワーク内で測定されたこの総劣化の合計値から劣化変数（期待係数）を引くと、ICPIF になります。

これは、Cisco Gateways が受信した VoIP データ ストリームの ICPIF を計算する際に使用する式と同じです。

遅延劣化係数

遅延劣化係数（*Idd*）は、2 つの値に基づいた数値です。1 つの値は、固定値です。（ITU 規格で規定された）コーデック遅延、先読み遅延、およびデジタル信号処理（DSP）遅延の固定値を使用して算出されます。2 番めの値は、変数です。測定された一方向遅延（ラウンドトリップ時間測定値を 2 で割った値）に基づいています。一方向遅延値は、G.107（2002 年版）の分析式に基づいたマッピング テーブルを使用して数値にマップされます。次の表に、IP SLA によって測定された一方向遅延と遅延劣化係数値の対応関係の例を示します。

表 *7*: 一方向遅延と *ICPIF* 遅延劣化係数の対応関係の例

一方向遅延（ミリ秒）	遅延劣化係数
50	1
100	2
150	4
200	7

機器劣化係数

機器劣化係数（*Ie*）は、測定されたパケット損失量に基づいた数値です。測定されたパケット損失量は総送信パケット数の割合として表され、コーデックによって定義される機器劣化係数に対応します。次の表に、IP SLA によって測定されたパケット損失と機器劣化係数値の対応関係の例を示します。

表 *8*: 測定されたパケット損失と *ICPIF* 機器劣化の対応関係の例

パケット損失（送信済みパケットの総数のパーセント）	PCM（G.711）コーデックの機器劣化値	CS-ACELP（G.729A）コーデックの機器劣化値
2 %	12	20
4 %	22	30

パケット損失（送信済みパケットの総数のパーセント）	PCM（G.711）コーデックの機器劣化値	CS-ACELP（G.729A）コーデックの機器劣化値
6 %	28	38
8 %	32	42

期待計数

アドバンテージ係数（*A*）とも呼ばれる期待計数は、アクセスの容易性の代償としてユーザがある程度の品質の劣化を許容するという事実を表すことを目的としています。たとえば、到達困難な場所にいる携帯電話ユーザは、接続品質が従来の固定電話接続ほど良好ではないことを予測している可能性があります。この変数は、向上したアクセスの利便性と音声品質の低下の釣り合いを保つことを目的としているので、アドバンテージ係数（アクセスアドバンテージ係数の略）とも呼ばれます。

次の表は ITU-T 勧告G.113 を改良したもので、*A* の暫定最大値のセットを、提供されるサービスごとに定義しています。

表 *9:* アドバンテージ係数の推奨最大値

通信サービス	アドバンテージ/期待係数 A の最大値
従来の有線（固定電話）	0
建物内のモビリティ（セルラー接続）	5
地域内または車内のモビリティ	10
到達困難な場所へのアクセス（たとえば、マルチホップ衛星接続を介したアクセスなど）	20

これらの値は推奨値に過ぎません。意味のある値にするには、係数（*A*）と特定のアプリケーションで選択した係数値を、採用する任意のプランニングモデルで一貫して使用する必要があります。ただし、上の表の値は、*A* の絶対的な上限と見なす必要があります。

IP SLA VoIP UDP ジッター動作のデフォルトのアドバンテージ係数は常に 0 です。

IP SLA MOS 値

IP SLA は、ICPIF 値と MOS 値との測定された対応関係を使用して MOS 値を予測します。この機能の文脈で MOS という略語を使用する場合、Mean Opinion Score; Conversational Quality, Estimated（MOS-CQE）を表すと理解してください。

G.107（2003 年 3 月）で定義された E-Model は、伝送パラメータが原因の劣化（損失、遅延など）を組み合わせて 1 つの評価、つまり伝送評価係数 R（R 係数）を算出することによって、平均的な聞き手が感じる主観的な品質を予測します。0（最低）～100（最高）で表されるこの

評価は、MOS などユーザの主観的な反応を予測するために使用されます。具体的には、MOS はR係数から変換式を使用して算出できます。逆に言うと、この式を逆変換式に修正して使用すれば、MOS 値から R 係数を算出できます。

ICPIF 値と R 係数との間にも関係があります。IP SLA は、ICPIF スコアから算出された R 係数の予測値から適切なMOSスコアの概算値を算出して、この対応関係を利用します。次の表に、対応する ICPIF 値に対して生成される MOS 値を示します。

表 *10 : MOS* 値に対する *ICPIF* 値の対応関係

ICPIF の範囲	MOS	品質のカテゴリ
0 ～ 3	5	最良
4 ～ 13	4	大きい
14 ～ 23	3	普通
24 ～ 33	2	小さい
34 ～ 43	1	きわめて小さい

IP SLA は、MOS 予測値を常に 1 ～ 5 で表します（5 が最高品質です）。MOS 値が 0（ゼロ）の場合は、その動作に対して MOS データを生成できなかったことを示します。

VoIP 用の IP SLA UDP ジッター動作の設定方法

宛先デバイスでの IP SLA Responder の設定

（注） Responder では、送信元に対して固定ポートを設定しないでください。Responder が送信元に対して固定ポートを設定すると、パケットが正常に（タイムアウトまたはパケット損失の問題が発生せずに）送信されたとしても、ジッター値はゼロになります。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します。
   - **ip sla responder**
   - **ip sla responder udp-echo ipaddress** *ip-address* **port** *port***vrf** *vrf*
4. **end**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	次のいずれかのコマンドを入力します。
	• **ip sla responder**
	• **ip sla responder udp-echo ipaddress** *ip-address* **port** *port***vrf** *vrf*
	例：
	`Device(config)# ip sla responder`
	`Device(config)# ip sla responder udp-echo ipaddress 192.0.2.132 port 5000 vrf vrf1`
		（任意）送信元からの制御メッセージに応じて、シスコ デバイスにおける IP SLA Responder 機能を一時的にイネーブルにします。
		（任意：送信元でプロトコル制御がディセーブルである場合にのみ必須です。）指定の IP アドレス、ポート、および VRF で、IP SLA Responder の機能をイネーブルにします。
		• プロトコル制御は、デフォルトでイネーブルになっています。

ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IP SLA VoIP UDP ジッター動作の設定およびスケジューリング

（注）
- 現時点では、IP SLA は次の音声コーデック（圧縮法）のみをサポートします。
  - G.711 A Law（g711alaw: 64 kbps PCM 圧縮法）
  - G.711 mu Law（g711ulaw: 64 kbps PCM 圧縮法）
  - G.729A（g729a: 8 kbps CS-ACELP 圧縮法）
- 次のコマンドは UDP ジッタ コンフィギュレーション モードでは使用できますが、UDP ジッタ（コーデック）動作では使用できません。
  - **history distributions-of-statistics-kept**
  - **history statistics-distribution-interval**
  - **request-data-size**
- コーデック タイプを指定すると、**codec-interval**、**codec-size**、および **codec-numpacket** の各オプションに適切なデフォルト値が設定されます。デフォルト値よりも優先させる特別な理由（異なるコーデックの概算など）がある場合を除き、間隔、サイズ、およびパケット数の各オプションの値を指定しないでください。
- **show ip sla configuration** コマンドを設定すると、「Number of statistic distribution buckets kept」および「Statistic distribution interval (milliseconds)」の値が表示されますが、これらの値はジッター（コーデック）動作には適用されません。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **udp-jitter** {*destination-ip-address* | *destination-hostname*} *destination-port* **codec** *codec-type* [**codec-numpackets** *number-of-packets*] [**codec-size** *number-of-bytes*] [**codec-interval** *milliseconds*] [**advantage-factor** *value*] [**source-ip** {*ip-address* | *hostname*}] [**source-port** *port-number*] [**control** {**enable** | **disable**}]
5. **history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*]
6. **frequency** *seconds*
7. **history hours-of-statistics-kept** *hours*
8. **owner** *owner-id*
9. **tag** *text*
10. **threshold** *milliseconds*
11. **timeout** *milliseconds*
12. 次のいずれかを実行します。
    - **tos** *number*
    - **traffic-class** *number*
13. **flow-label** *number*
14. **verify-data**

15. **vrf** *vrf-name*
16. **end**
17. **show ip sla configuration** [*operation-number*]

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	**ip sla** *operation-number* 例： `Device(config)# ip sla 10`	IP SLA 動作の設定を開始し、IP SLA コンフィギュレーション モードに移行します。
ステップ 4	**udp-jitter** {*destination-ip-address* | *destination-hostname*} *destination-port* **codec** *codec-type* [**codec-numpackets** *number-of-packets*] [**codec-size** *number-of-bytes*] [**codec-interval** *milliseconds*] [**advantage-factor** *value*] [**source-ip** {*ip-address* | *hostname*}] [**source-port** *port-number*] [**control** {**enable** | **disable**}] 例： `Device(config-ip-sla)# udp-jitter 209.165.200.225 16384 codec g711alaw advantage-factor 10`	遅延、ジッタ、およびパケット損失の統計情報に加えて、VoIP スコアを生成するジッタ（コーデック）動作としてこの動作を設定します。
ステップ 5	**history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*] 例： `Device(config-ip-sla-jitter)# history enhanced interval 900 buckets 100`	（任意）IP SLA 動作に対する拡張履歴収集をイネーブルにします。
ステップ 6	**frequency** *seconds* 例： `Device(config-ip-sla-jitter)# frequency 30`	（任意）指定した IP SLA 動作を繰り返す間隔を設定します。
ステップ 7	**history hours-of-statistics-kept** *hours* 例：	（任意）IP SLA 動作の統計情報を保持する時間数を設定します。

	コマンドまたはアクション	目的
	`Device(config-ip-sla-jitter)# history hours-of-statistics-kept 4`	
ステップ 8	**owner** *owner-id* 例： `Device(config-ip-sla-jitter)# owner admin`	（任意）IP SLA 動作の簡易ネットワーク管理プロトコル（SNMP）所有者を設定します。
ステップ 9	**tag** *text* 例： `Device(config-ip-sla-jitter)# tag TelnetPollServer1`	（任意）IP SLA 動作のユーザ指定 ID を作成します。
ステップ 10	**threshold** *milliseconds* 例： `Device(config-ip-sla-jitter)# threshold 10000`	（任意）IP SLA 動作によって作成されるネットワーク モニタリング統計情報を計算するための上限しきい値を設定します。
ステップ 11	**timeout** *milliseconds* 例： `Device(config-ip-sla-jitter)# timeout 10000`	（任意）IP SLA 動作がその要求パケットからの応答を待機する時間を設定します。

ステップ 12	次のいずれかを実行します。
	• **tos** *number*
	• **traffic-class** *number*
	例：
	`Device(config-ip-sla-jitter)# tos 160`
	例：
	`Device(config-ip-sla-jitter)# traffic-class 160`
		（任意）IPv4 ネットワークに限り、IP SLA 動作の IPv4 ヘッダーの ToS バイトを定義します。
		または
		（任意）IPv6 ネットワークに限り、サポートされている IP 動作に対する IPv6 ヘッダーのトラフィック クラス バイトを定義します。

ステップ 13	**flow-label** *number* 例： `Device(config-ip-sla-jitter)# flow-label 112233`	（任意）IPv6 ネットワークに限り、サポートされている IP SLA 動作に対する IPv6 ヘッダーのフローラベル フィールドを定義します。
ステップ 14	**verify-data** 例： `Device(config-ip-sla-jitter)# verify-data`	（任意）IP SLA 動作が各応答パケットに対してデータ破壊の有無をチェックするようにします。

	コマンドまたはアクション	目的
ステップ 15	**vrf** *vrf-name* 例： `Device(config-ip-sla-jitter)# vrf vpn-A`	（任意）IP SLA 動作を使用して、マルチプロトコル ラベル スイッチング（MPLS）バーチャル プライベート ネットワーク（VPN）内をモニタリングできるようにします。
ステップ 16	**end** 例： `Device(config-ip-sla-jitter)# end`	特権 EXEC モードに戻ります。
ステップ 17	**show ip sla configuration** [*operation-number*] 例： `Device# show ip sla configuration 10`	（任意）すべての IP SLA 動作または指定した IP SLA 動作に関する設定値を、すべてのデフォルト値を含めて表示します。

IP SLA 動作のスケジューリング

始める前に

- スケジュールされるすべての IP サービス レベル契約（SLA）動作がすでに設定されている必要があります。
- 複数動作グループでスケジュールされたすべての動作の頻度が同じでなければなりません。
- 複数動作グループに追加する 1 つ以上の動作 ID 番号のリストは、カンマ（,）を含めて最大 125 文字に制限する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します。
   - **ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {[*hh*:*mm*:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**]
   - **ip sla group schedule** *group-operation-number operation-id-numbers* { **schedule-period** *schedule-period-range* | **schedule-together**} [**ageout** *seconds*] **frequency** *group-operation-frequency* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm* [:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm* [:*ss*]}]
4. **end**
5. **show ip sla group schedule**
6. **show ip sla configuration**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	次のいずれかのコマンドを入力します。
	• **ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {[*hh*:*mm*:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**]
	• **ip sla group schedule** *group-operation-number operation-id-numbers* { **schedule-period** *schedule-period-range* | **schedule-together**} [**ageout** *seconds*] **frequency** *group-operation-frequency* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm* [:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm* [:*ss*]}]
	例：
	`Device(config)# ip sla schedule 10 life forever start-time now`
	`Device(config)# ip sla group schedule 10 schedule-period frequency`
	`Device(config)# ip sla group schedule 1 3,4,6-9 life forever start-time now`
	`Device(config)# ip sla schedule 1 3,4,6-9 schedule-period 50 frequency range 80-100`
		• 個々の IP SLA 動作のスケジューリング パラメータを設定します。
		• 複数動作スケジューラ用に IP SLA 動作グループ番号と動作番号の範囲を指定します。

ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	**show ip sla group schedule** 例： `Device# show ip sla group schedule`	（任意）IP SLA グループ スケジュールの詳細を表示します。

	コマンドまたはアクション	目的
ステップ 6	**show ip sla configuration** 例： `Device# show ip sla configuration`	（任意）IP SLA 設定の詳細を表示します。

トラブルシューティングのヒント

- IP サービス レベル契約（SLA）動作が実行中でなく、統計情報が生成されていない場合は、設定に **verify-data** コマンドを追加して（IP SLA コンフィギュレーション モードで設定）、データ検証をイネーブルにします。データ検証をイネーブルにすると、各動作の応答で破損の有無がチェックされます。通常の動作時に **verify-data** コマンドを使用すると、不要なオーバーヘッドがかかるので注意してください。
- IP SLA 動作に関する問題をトラブルシューティングするには、**debug ip sla trace** コマンドと **debug ip sla error** コマンドを使用します。

次の作業

トラップを生成する目的（または別の動作を開始する目的）で、IPサービス レベル契約（SLA）動作に予防的しきい値条件と反応トリガーを追加するには、「予防的しきい値モニタリングの設定」の項を参照してください。

VoIP 用の IP SLA UDP ジッター動作の設定例

IP SLA VoIP UDP 動作の設定例

次の例では、209.165.200.225 のデバイスで Cisco IP SLA Responder がイネーブルであると仮定します。

```
Device> enable

Password:
Device# configure terminal

Enter configuration commands, one per line.  End with the end command.
Device(config)# ip sla 10
Device(config-sla)# udp-jitter 209.165.200.225 16384 codec g711alaw advantage-factor 2

Device(config-sla-jitter)# owner admin_bofh
Device(config-sla-jitter)# exit

Device(config)# ip sla schedule 10 start-time now

Device(config)# exit

Device#
```

```
Device# show running-config | begin ip sla 10

ip sla 10
 udp-jitter 209.165.200.225 16384 codec g711alaw advantage-factor 2
 owner admin_bofh
ip sla schedule 10 start-time now
 .
 .
 .
Device# show ip sla configuration 10

Entry number: 10
Owner: admin_bofh
Tag:
Type of operation to perform: jitter
Target address: 209.165.200.225
Source address: 0.0.0.0
Target port: 16384
Source port: 0
Operation timeout (milliseconds): 5000
Codec Type: g711alaw
Codec Number Of Packets: 1000
Codec Packet Size: 172
Codec Interval (milliseconds): 20
Advantage Factor: 2
Type Of Service parameters: 0x0
Verify data: No
Vrf Name:
Control Packets: enabled
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Life (seconds): 3600
Entry Ageout (seconds): never
Status of entry (SNMP RowStatus): Active
Connection loss reaction enabled: No
Timeout reaction enabled: No
Verify error enabled: No
Threshold reaction type: Never
Threshold (milliseconds): 5000
Threshold Falling (milliseconds): 3000
Threshold Count: 5
Threshold Count2: 5
Reaction Type: None
Number of statistic hours kept: 2
Number of statistic distribution buckets kept: 1
Statistic distribution interval (milliseconds): 20
Enhanced History:
```

コーデック タイプがジッター動作用に設定されている場合、標準ジッターの「Request size (ARR data portion)」、「Number of packets」、および「Interval (milliseconds)」のパラメータは **show ip sla configuration** コマンドの出力に表示されません。代わりに、「Codec Packet Size」、「Codec Number of Packets」、および「Codec Interval (milliseconds)」の値が表示されます。

IP SLA VoIP UDP 動作統計情報の出力例

ジッター（コーデック）動作の音声スコア（ICPIF 値と MOS 値）を表示するには、**show ip sla statistics** コマンドを使用します。

```
Device# show ip sla statistics 10
```

```
Entry number: 10
Modification time: 12:57:45.690 UTC Sun Oct 26 2003
Number of operations attempted: 1
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 19
Latest operation start time: 12:57:45.723 Sun Oct 26 2003
Latest operation return code: OK
!
Voice Scores:
ICPIF:  20          MOS Score:  3.20
!
RTT Values:
NumOfRTT: 10     RTTAvg: 19      RTTMin: 19     RTTMax: 20
RTTSum:  191    RTTSum2: 3649
Packet Loss Values:
PacketLossSD: 0 PacketLossDS: 0
PacketOutOfSequence: 0  PacketMIA: 0    PacketLateArrival: 0
InternalError: 0        Busies: 0
Jitter Values:
NumOfJitterSamples: 9
MinOfPositivesSD: 0     MaxOfPositivesSD: 0
NumOfPositivesSD: 0     SumOfPositivesSD: 0     Sum2PositivesSD: 0
MinOfNegativesSD: 0     MaxOfNegativesSD: 0
NumOfNegativesSD: 0     SumOfNegativesSD: 0     Sum2NegativesSD: 0
MinOfPositivesDS: 1     MaxOfPositivesDS: 1
NumOfPositivesDS: 1     SumOfPositivesDS: 1     Sum2PositivesDS: 1
MinOfNegativesDS: 1     MaxOfNegativesDS: 1
NumOfNegativesDS: 1     SumOfNegativesDS: 1     Sum2NegativesDS: 1
Interarrival jitterout: 0       Interarrival jitterin: 0
One Way Values:
NumOfOW: 0
OWMinSD: 0      OWMaxSD: 0      OWSumSD: 0      OWSum2SD: 0
OWMinDS: 0      OWMaxDS: 0      OWSumDS: 0      OWSum2DS: 0
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
Cisco IOS IP SLA コマンド	『Cisco IOS IP SLAs Command Reference』
Voice over IP（VoIP）コーデック	『Understanding Codecs: Complexity, Hardware Support, MOS, and Negotiation』
パケット音声ネットワークのジッタ	『Understanding Jitter in Packet Voice Networks (Cisco IOS Platforms) shtml』

標準および RFC

標準[1]/RFC[2]	タイトル
ITU-T 勧告 G.107（2003 年）	『The E-model, a computation model for use in transmission planning』
ITU-T 勧告 G.113（1996 年）	*Transmission impairments*
ITU-T 勧告 G.113（2001 年）	『Transmission impairments due to speech processing』
ITU-T 勧告 G.711（1998 年）	『*Pulse code modulation (PCM) of voice frequencies*』（G.711 音声コーデックともいう）
ITU-T 勧告 G.729 Annex A（1996 年）	『*Reduced complexity 8 kbit/s CS-ACELP speech codec*』（G.729/A/B 音声コーデックともいう）
ITU-T 勧告 P.800.1（2003 年）	『Mean Opinion Score (MOS) terminology』
RFC 768	*User Datagram Protocol*
RFC 1889	『*RTP: A Transport Protocol for Real-Time Applications*』

1 この機能による、表示されている RFC の完全なサポートを主張するものではありません。ITU 電気通信規格（「現在有効な ITU-T 勧告」）は、http://www.itu.ch で入手できます。規定の概要は、各種インターネット サイトで入手できます。

2 この機能による、表示されている RFC の完全なサポートを主張するものではありません。

MIB

MIB	MIB のリンク
CISCO-RTTMON-MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IP SLA VoIP UDP ジッター動作の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *11 : IP SLA VoIP UDP* ジッター動作の機能情報

機能名	リリース	機能情報
IP SLA - UDP ベース VoIP 動作		IP SLA ユーザ データグラム プロトコル（UDP）ジッター動作を使用すると、UDP トラフィックを伝送するネットワーク内におけるラウンドトリップ遅延、一方向遅延、一方向ジッター、一方向パケット損失、および接続を測定できます。
IPv6 用 IP SLA（UDP ジッター、UDP エコー、ICMP エコー、TCP 接続）		IPv6 ネットワークでの動作を可能にするためにサポートが追加されました。

用語集

codec ：IP テレフォニー分野におけるコーデックは、音声データとビデオ データの伝送効率を向上させるために使用される圧縮/圧縮解除アルゴリズムです。音声コーデック タイプは、通常、アルゴリズムを規定する ITU 勧告番号（「PCM」ではなく「G.711」など）を使用して表されます。

CS-ACELP ：参考文書 G.729 および G.729A『*Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear-prediction (CS-ACELP)*』で規定されたコーデック タイプ。

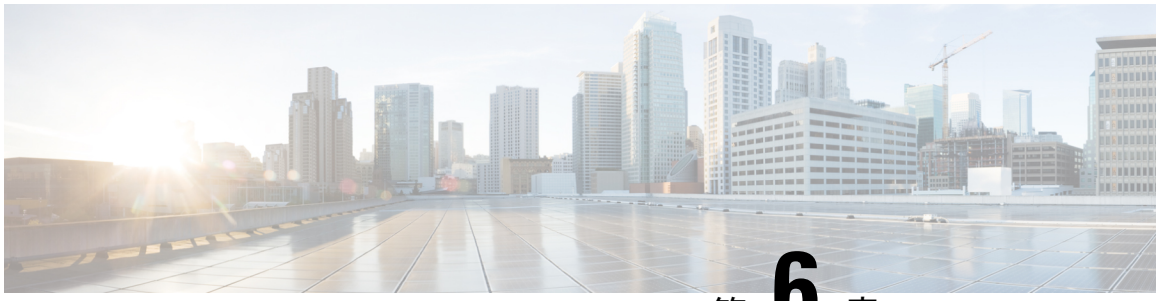
ITU ：国際電気通信連合。ITU は、政府機関および民間セクターが世界規模の電気通信ネットワークおよびサービスに関する調整を行う、国際連合内の国際組織です。国際電気通信連合電気通信標準化部門（ITU-T）は、電気通信のあらゆる分野を対象とする規格（勧告）を規定する部門であり、ITU の 3 つの作業部門の 1 つです。ITU の Web サイトは、http://www.itu.int です。

ITU-T ：ITU 電気通信標準化部門。ITU-T は ITU の 3 つの作業部門の 1 つです。電気通信のあらゆる分野を対象とする規格（ITU-T 勧告と呼ばれます）を規定する部門です。

MOS-CQE （Mean Opinion Score; Conversational Quality, Estimated）：会話型アプリケーションの状況下での品質予測を目的とするネットワーク計画モデルによって算出されるスコア。ITU-T 勧告に従って実行された会話品質の予測。G.107 が Mean Opinion Score（MOS）に変換されると、MOS-CQE の観点での結果が得られます。[3]

PCM ：参考文書 G.711『*Pulse code modulation (PCM) of voice frequencies*』で規定されたコーデック タイプ。

[3] ITU-T 勧告 P.800.1 で規定されています。ITU の著作権および免責事項に従って使用されます。



第 6 章

IP SLA QFP タイム スタンプ

このモジュールでは、IP サービス レベル契約（SLA）UDP ジッター動作の IP SLA QFP タイム スタンプ機能を設定する方法について説明します。この新しいプローブおよびレスポンダ構造により、より正確なネットワーク パフォーマンス測定が可能になります。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

IP SLA QFP タイム スタンプの前提条件

- IP SLA QFP タイム スタンプ機能が動作するためには、レスポンダとプローブが設定されているデバイスがともに、QFP タイム スタンプをサポートしている Cisco ソフトウェア イメージを実行している必要があります。

- 一方向遅延を正確に測定するには、NTP などによる送信元デバイスとターゲット デバイスとの間のクロック同期が必要です。送信元デバイスおよびターゲット デバイスで NTP を設定するには、『*Network Management Configuration Guide*』の「Performing Basic System Management」の章の作業を実行します。
- IP SLA アプリケーションを設定する前に、**show ip sla application** コマンドを使用して、ご使用のソフトウェア イメージでサポートされている動作タイプを確認してください。

IP SLA QFP タイム スタンプの制限事項

- 送信者またはレスポンダのデバイスをリブートした後、SNTP が FP クロックを RP クロックに同期するまで、転送プロセッサ（FP）およびルート プロセッサ（RP）の時刻が正確でない場合があります。デバイス FP と RP の時刻が安定する前に動作が実行されるのを回避するには、UDP ジッター動作を開始する前にリブート後に数分待機します。
- IP SLA UDP ジッター動作によって報告される一方向遅延の値は、NTP 同期レベルによって決まります。デバイスが同期されていても、デバイスの NTP オフセット値が大きいと、一方向値が正しくない場合があります。オフセット値が大きくなりすぎた場合は、一方向値が報告されない場合があります。また、デバイスの NTP オフセット値は変動する場合があるので、これらの変更は報告される一方向値に反映されます。
- 送信元デバイスに最適化されたタイム スタンプの場所を設定し、ターゲット IP SLA Responder が設定されているデバイスが最適化されたタイム スタンプの場所をサポートしていない場合、IP SLA 動作は失敗します。
- IP SLA QFP タイム スタンプは、Cisco CSR 1000v または Cisco ISRv ではサポートされていません。

IP SLA QFP タイム スタンプに関する情報

IP SLA UDP ジッター動作

IP サービス レベル契約（SLA）UDP ジッター動作は、VoIP、Video over IP、またはリアルタイム会議などのリアルタイム トラフィック アプリケーションのネットワーク適合性を診断します。

ジッターとは、パケット間の遅延のばらつきを意味します。複数のパケットが発信元から宛先に連続的に送信される場合（たとえば 10 ミリ秒間隔で）、ネットワークが理想的に動作していれば、宛先は10ミリ秒間隔でパケットを受信します。しかし、ネットワーク内に遅延（キューイング、代替ルートを介した受信など）が存在する場合、パケット間の到着遅延は、10ミリ秒より大きい場合も、10ミリ秒より小さい場合もあります。この例を使用すると、正のジッター値は、パケットの到着間隔が 10 ミリ秒を超えていることを示します。パケットが 12 ミリ秒間隔で到着する場合、正のジッターは 2 ミリ秒です。パケットが 8 ミリ秒間隔で到着する場合、

負のジッターは 2 ミリ秒です。Voice over IP（VoIP）など遅延に影響されやすいネットワークでは、正のジッター値は望ましくありません。0 のジッター値が理想的です。

しかし、IP SLA UDP ジッター動作の機能は、ジッタのモニタリングだけではありません。UDP ジッター動作には IP SLA UDP 動作によって返されたデータが含まれているため、UDP ジッター動作は多目的データ収集動作に使用できます。IP SLA が生成するパケットは、シーケンス情報を送受信するパケット、および送信元および動作ターゲットからのタイムスタンプを送受信するパケットを搬送します。UDP ジッター動作は、この情報に基づいて次のデータを測定できます。

- 方向別ジッター（送信元から宛先へ、宛先から送信元へ）
- 方向別パケット損失
- 方向別遅延（一方向遅延）
- ラウンドトリップ遅延（平均 RTT）

データの送信と受信でパスが異なる場合もあるので（非対称）、方向別データを使用すれば、ネットワークで発生している輻輳や他の問題が発生している場所を簡単に突き止めることができます。

UDP ジッター動作は、合成（シミュレーション）UDP トラフィックを生成して機能します。非対称プローブは、方向ごとのカスタム定義パケットサイズをサポートしており、それを使用して、異なるパケットサイズを要求パケット（送信元デバイスから宛先デバイスへ）および応答パケット（宛先デバイスから送信元デバイスへ）で送信できます。

UDP ジッター動作は、指定された頻度 F で、送信元デバイスから宛先デバイスに、サイズ S の N 個の UDP パケットを T ミリ秒間隔で送信します。それに応じて、サイズ P の UDP パケットが宛先デバイスから送信元デバイスに送信されます。デフォルトでは、ペイロードサイズが 10 バイト（S）のパケットフレーム 10 個（N）を 10 ミリ秒（T）ごとに生成し、60 秒（F）ごとに動作を繰り返します。次の表に示すように、これらのパラメータは、指定した IP サービスを最適にシミュレートできるようにユーザ設定可能です。

表 *12 : UDP* ジッター動作パラメータ

UDP ジッター動作パラメータ	デフォルト	コンフィギュレーション コマンド
パケット数（n）	10 パケット	**udp-jitter num-packets**
要求パケット単位のペイロードサイズ（S）	10 バイト	**request-data-size**

UDP ジッター動作パラメータ	デフォルト	コンフィギュレーション コマンド
応答パケット単位のペイロード サイズ（P）	デフォルトの応答データ サイズは、設定している IP SLA 動作のタイプによって異なります。 （注） **response-data-size** コマンドが設定されていない場合、応答データ サイズ値は要求データ サイズ値と同じです。	**response-data-size**
パケット間隔（ミリ秒単位）（T）	10 ミリ秒	**udp-jitter interval**
動作を繰り返すまでの経過時間（秒単位）（F）	60 秒	**frequency (IP SLA)**

IP SLA 動作は、合成（シミュレーション）ネットワーク トラフィックを生成して機能します。1 つの IP SLA 動作（たとえば IP SLA 動作 10）は、動作の存続期間の間、指定された頻度で繰り返されます。

QFP タイム スタンプ

IP SLA UDP ジッターは、ラウンドトリップ時間、一方向遅延、ジッター、およびパケット損失などのメトリックを測定するための、最も広く利用されている IP SLA 動作です。測定の精度は、パケットが送信者とレスポンダの間で移動し戻る間に、タイム スタンプが取得される場所によって異なります。

通常、IP SLA 動作のタイム スタンプは、ルート プロセッサ（RP）の IP SLA プロセスで取得されます。タイム スタンプは、RP で発生したスケジューリング遅延の影響を受けるので、このタイムスタンプの場所が不正確で一貫性のない測定につながります。QFP タイム スタンプは、RP から Cisco Packet Processor（CPP）にタイム スタンプの場所を移動します。

ただし、一方向遅延を測定するには、送信元デバイスとターゲットデバイスのクロックを同期する必要があります。デバイスの CPP クロックは外部のクロック ソースと直接同期することができないため、RP クロックが外部のクロック ソースと同期され、SNTP を使用して RP とフォワーディング プロセッサ（FP）のクロックが同期されます。RP-FP 同期の精度は十分ではありません。この問題に対処するために、QFP タイム スタンプ機能の拡張 UDP ジッター プローブで RP と CPP 両方のタイム スタンプが保存されます。RTT とジッターの計算には CPP タイム スタンプが使用され、一方向計算は引き続き RP タイム スタンプに基づきます。そのため、一方向遅延を正確に測定するには、NTP などによる送信元デバイスとターゲット デバイスとの間のクロック同期が必要です。一方向遅延値は RP タイム スタンプを使用して計算され、CPP タイム スタンプに基づく予測補正アルゴリズムを適用して修正されます。

QFP タイム スタンプには、拡張 UDP プローブと拡張レスポンダが含まれています。UDP プローブと IP SLA Responder が設定されているデバイスは共に、QFP タイム スタンプと最適化

されたタイム スタンプの場所をサポートする Cisco ソフトウェア イメージを実行している必要があります（より正確な RTT 測定のため）。UDP ジッター動作が、最適化されたタイム スタンプの場所をサポートしていないデバイス上のレスポンダを対象としている場合、IP SLA プローブは失敗します。

IP SLA QFP タイム スタンプの設定方法

宛先デバイスでの IP SLA Responder の設定

（注） Responder では、同じ送信元に対して固定ポートを設定しないでください。Responder が同じ送信元に対して固定ポートを設定すると、パケットが正常に（タイムアウトまたはパケット損失の問題が発生せずに）送信されたとしても、ジッター値はゼロになります。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかを実行します。
   - **ip sla responder**
   - **ip sla responder udp-echo ipaddress** *ip-address* **port** *port*
4. **exit**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	次のいずれかを実行します。 • **ip sla responder** • **ip sla responder udp-echo ipaddress** *ip-address* **port** *port* 例：	（任意）送信元からの制御メッセージに応じて、シスコ デバイスにおける IP SLA Responder 機能を一時的にイネーブルにします。 （任意）送信元でプロトコル制御がディセーブルである場合にのみ必須です。指定の IP アドレスおよび

	コマンドまたはアクション	目的

	`Device(config)# ip sla responder`
	例：
	`Device(config)# ip sla responder udp-echo ipaddress 172.29.139.132 port 5000`
		ポートで、IP SLA Responder の機能をイネーブルにします。
		• プロトコル制御は、デフォルトでイネーブルになっています。

ステップ 4	**exit** 例： `Device(config)# exit`	（任意）グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

送信元デバイスの UDP ジッター動作の設定とスケジューリング

次のいずれかの作業のみを実行します。

- 送信元デバイスでの基本 UDP ジッター動作の設定
- 追加特性を指定した UDP ジッター動作の設定

QFP タイム スタンプを指定した基本 UDP ジッター動作の設定

送信元デバイスで QFP タイム スタンプを指定した UDP ジッター プローブを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **udp-jitter** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*}] [**source-port** *port-number*] [**control** {**enable** | **disable**}] [**num-packets** *number-of-packets*] [**interval** *interpacket-interval*]
5. **frequency** *seconds*
6. **precision microseconds**
7. **optimize timestamp**
8. **end**
9. **show ip sla configuration** [*operation-number*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	`Device> enable`	
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	**ip sla** *operation-number* 例： `Device(config)# ip sla 10`	IP SLA 動作の設定を開始し、IP SLA コンフィギュレーション モードに移行します。
ステップ 4	**udp-jitter** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*}] [**source-port** *port-number*] [**control** {**enable** | **disable**}] [**num-packets** *number-of-packets*] [**interval** *interpacket-interval*] 例： `Device(config-ip-sla)# udp-jitter 172.29.139.134 5000`	IP SLA 動作を UDP ジッター動作として設定し、UDP ジッタ コンフィギュレーション サブモードを開始します。 • 送信元デバイスと宛先デバイスの両方で IP SLA 制御プロトコルをディセーブルにする場合のみ **control disable** キーワードの組み合わせを使用します。
ステップ 5	**frequency** *seconds* 例： `Device(config-ip-sla-jitter)# frequency 30`	（任意）指定した IP SLA 動作を繰り返す間隔を設定します。
ステップ 6	**precision microseconds** 例： `Device(config-ip-sla-jitter)# precision microseconds`	QFP タイム スタンプを有効にします。
ステップ 7	**optimize timestamp** 例： `Device(config-ip-sla-jitter)# optimize timestamp`	（任意）Cisco ASR 1000 シリーズ ルータの場合のみ。cpp UNIX 時間よりも正確な CPP ティックを有効にします。 （注） Responder が cpp ティックをサポートしていない場合、IP SLA 動作は失敗します。
ステップ 8	**end** 例： `Device(config-ip-sla-jitter)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 9	**show ip sla configuration** [*operation-number*] 例： `Device# show ip sla configuration 10`	（任意）すべての IP SLA 動作または指定した IP SLA 動作に関する設定値を、すべてのデフォルト値を含めて表示します。

QFP タイム スタンプと追加特性を指定した UPD ジッター動作の設定

（注）
- UDP ジッター動作には大量のデータが含まれるため、IP SLA UDP ジッター動作では IP SLA 履歴機能（統計情報の履歴バケット）はサポートされていません。つまり、次のコマンドは UDP ジッター動作ではサポートされていません：**history buckets-kept**、**history filter**、**history lives-kept**、**samples-of-history-kept**、および **show ip sla history**
- UDP ジッター動作の統計情報保存時間は、IP SLA で使用される MIB（CISCO-RTTMON-MIB）によって 2 時間に制限されます。**history hours-of-statistics** *hours* グローバル コンフィギュレーションを使用して、これより大きな値に設定しても、保持される期間が 2 時間を超えることはありません。ただし、Data Collection MIB を使用して動作の履歴データを収集することはできます。詳細については、「CISCO-DATA-COLLECTION-MIB」（http://www.cisco.com/go/mibs）を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **udp-jitter** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*}] [**source-port** *port-number*] [**control** {**enable** | **disable**}] [**num-packets** *number-of-packets*] [**interval** *interpacket-interval*]
5. **precision microseconds**
6. **optimize timestamp**
7. **history distributions-of-statistics-kept** *size*
8. **history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*]
9. **frequency** *seconds*
10. **history hours-of-statistics-kept** *hours*
11. **owner** *owner-id*
12. **request-data-size** *bytes*
13. **history statistics-distribution-interval** *milliseconds*
14. **tag** *text*
15. **threshold** *milliseconds*
16. **timeout** *milliseconds*
17. 次のいずれかを実行します。
    - **tos** *number*

- **traffic-class** *number*

18. **flow-label** *number*
19. **verify-data**
20. **vrf** *vrf-name*
21. **end**
22. **show ip sla configuration** [*operation-number*]

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	**ip sla** *operation-number* 例： `Device(config)# ip sla 10`	IP SLA 動作の設定を開始し、IP SLA コンフィギュレーション モードに移行します。
ステップ 4	**udp-jitter** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*}] [**source-port** *port-number*] [**control** {**enable** | **disable**}] [**num-packets** *number-of-packets*] [**interval** *interpacket-interval*] 例： `Device(config-ip-sla)# udp-jitter 172.29.139.134 5000`	IP SLA 動作を UDP ジッター動作として設定し、UDP ジッタ コンフィギュレーション サブモードを開始します。 • 送信元デバイスとターゲット デバイスの両方で IP SLA 制御プロトコルをディセーブルにする場合のみ **control disable** キーワードの組み合わせを使用します。
ステップ 5	**precision microseconds** 例： `Device(config-ip-sla-jitter)# precision microseconds`	QFP タイム スタンプを有効にします。
ステップ 6	**optimize timestamp** 例： `Device(config-ip-sla-jitter)# optimize timestamp`	（任意）Cisco ASR 1000 シリーズ ルータのみに対し、IP SLA のタイム スタンプの場所を最適化します。

	コマンドまたはアクション	目的
		（注） ターゲット IP SLA Responder が設定されているデバイスが最適化されたタイム スタンプの場所もサポートしていない場合、IP SLA 動作は失敗します。
ステップ 7	**history distributions-of-statistics-kept** *size* 例： `Device(config-ip-sla-jitter)# history distributions-of-statistics-kept 5`	（任意）IP SLA 動作中にホップ単位で保持する統計情報の配信数を設定します。
ステップ 8	**history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*] 例： `Device(config-ip-sla-jitter)# history enhanced interval 900 buckets 100`	（任意）IP SLA 動作に対する拡張履歴収集をイネーブルにします。
ステップ 9	**frequency** *seconds* 例： `Device(config-ip-sla-jitter)# frequency 30`	（任意）指定した IP SLA 動作を繰り返す間隔を設定します。
ステップ 10	**history hours-of-statistics-kept** *hours* 例： `Device(config-ip-sla-jitter)# history hours-of-statistics-kept 4`	（任意）IP SLA 動作の統計情報を保持する時間数を設定します。
ステップ 11	**owner** *owner-id* 例： `Device(config-ip-sla-jitter)# owner admin`	（任意）IP SLA 動作の簡易ネットワーク管理プロトコル（SNMP）所有者を設定します。
ステップ 12	**request-data-size** *bytes* 例： `Device(config-ip-sla-jitter)# request-data-size 64`	（任意）IP SLA 動作の要求パケットのペイロードにおけるプロトコル データ サイズを設定します。
ステップ 13	**history statistics-distribution-interval** *milliseconds* 例： `Device(config-ip-sla-jitter)# history statistics-distribution-interval 10`	（任意）IP SLA 動作で維持する各統計情報の配信間隔を設定します。

	コマンドまたはアクション	目的
ステップ 14	**tag** *text* 例： `Device(config-ip-sla-jitter)# tag TelnetPollServer1`	（任意）IP SLA 動作のユーザ指定 ID を作成します。
ステップ 15	**threshold** *milliseconds* 例： `Device(config-ip-sla-jitter)# threshold 10000`	（任意）IP SLA 動作によって作成されるネットワーク モニタリング統計情報を計算するための上限しきい値を設定します。
ステップ 16	**timeout** *milliseconds* 例： `Device(config-ip-sla-jitter)# timeout 10000`	（任意）IP SLA 動作がその要求パケットからの応答を待機する時間を設定します。

ステップ 17	次のいずれかを実行します。
	• **tos** *number*
	• **traffic-class** *number*
	例：
	`Device(config-ip-sla-jitter)# tos 160`
	例：
	`Device(config-ip-sla-jitter)# traffic-class 160`
		（任意）IPv4 ネットワークに限り、IP SLA 動作の IPv4 ヘッダーの ToS バイトを定義します。
		または
		（任意）IPv6 ネットワークに限り、サポートされている IP 動作に対する IPv6 ヘッダーのトラフィック クラス バイトを定義します。

ステップ 18	**flow-label** *number* 例： `Device(config-ip-sla-jitter)# flow-label 112233`	（任意）IPv6 ネットワークに限り、サポートされている IP SLA 動作に対する IPv6 ヘッダーのフローラベル フィールドを定義します。
ステップ 19	**verify-data** 例： `Device(config-ip-sla-jitter)# verify-data`	（任意）IP SLA 動作が各応答パケットに対してデータ破壊の有無をチェックするようにします。
ステップ 20	**vrf** *vrf-name* 例： `Device(config-ip-sla-jitter)# vrf vpn-A`	（任意）IP SLA 動作を使用して、マルチプロトコル ラベル スイッチング（MPLS）バーチャル プライベート ネットワーク（VPN）内をモニタリングできるようにします。
ステップ 21	**end** 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config-ip-sla-jitter)# end`	
ステップ 22	**show ip sla configuration** [*operation-number*] 例： `Device# show ip sla configuration 10`	（任意）すべての IP SLA 動作または指定した IP SLA 動作に関する設定値を、すべてのデフォルト値を含めて表示します。

IP SLA 動作のスケジューリング

始める前に

- スケジュールされるすべての IP サービス レベル契約（SLA）動作がすでに設定されている必要があります。
- 複数動作グループでスケジュールされたすべての動作の頻度が同じでなければなりません。
- 複数動作グループに追加する 1 つ以上の動作 ID 番号のリストは、カンマ（,）を含めて最大 125 文字に制限する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します。
   - **ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {[*hh*:*mm*:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**]
   - **ip sla group schedule** *group-operation-number operation-id-numbers* { **schedule-period** *schedule-period-range* | **schedule-together**} [**ageout** *seconds*] **frequency** *group-operation-frequency* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm* [:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm* [:*ss*]}]
4. **end**
5. **show ip sla group schedule**
6. **show ip sla configuration**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
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	次のいずれかのコマンドを入力します。
	• **ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {[*hh*:*mm*:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**]
	• **ip sla group schedule** *group-operation-number operation-id-numbers* { **schedule-period** *schedule-period-range* |**schedule-together**} [**ageout** *seconds*] **frequency** *group-operation-frequency* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm* [:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm* [:*ss*]}]
	例：
	`Device(config)# ip sla schedule 10 life forever start-time now`
	`Device(config)# ip sla group schedule 10 schedule-period frequency`
	`Device(config)# ip sla group schedule 1 3,4,6-9 life forever start-time now`
	`Device(config)# ip sla schedule 1 3,4,6-9 schedule-period 50 frequency range 80-100`
		• 個々のIP SLA動作のスケジューリング パラメータを設定します。
		• 複数動作スケジューラ用に IP SLA 動作グループ番号と動作番号の範囲を指定します。

ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	**show ip sla group schedule** 例： `Device# show ip sla group schedule`	（任意）IP SLA グループ スケジュールの詳細を表示します。
ステップ 6	**show ip sla configuration** 例： `Device# show ip sla configuration`	（任意）IP SLA 設定の詳細を表示します。

トラブルシューティングのヒント

- IP SLA 動作が実行中でなく、統計情報が生成されていない場合は、動作の設定に **verify-data** コマンドを追加して（IP SLA コンフィギュレーション モードで設定）、データ検証をイネーブルにします。データ検証をイネーブルにすると、各動作の応答で破損の有無がチェックされます。通常の動作時に **verify-data** コマンドを使用すると、不要なオーバーヘッドがかかるので注意してください。
- IP SLA 動作に関する問題をトラブルシューティングするには、**debug ip sla trace** コマンドと **debug ip sla error** コマンドを使用します。

次の作業

トラップを生成する目的（または別の動作を開始する目的）で、IP SLA 動作に予防的しきい値条件と反応トリガーを追加するには、「予防的しきい値モニタリングの設定」の項を参照してください。

operation)

IP SLA 動作の結果を表示し、内容を確認するには、**show ip sla statistics** コマンドを使用します。サービス レベル契約の基準に対応するフィールドの出力を確認し、サービス メトリックが許容範囲内であるかどうかを判断します。

IP SLA QFP タイム スタンプの設定例

例：QFP タイム スタンプを指定した UDP 動作の設定

次の例では、2 つの動作が QFP タイム スタンプと最適化されたタイム スタンプの場所を指定した拡張 UDP ジッター動作として設定されています。動作 2 は、最初の動作の 5 秒後に開始します。

（注） レスポンダが設定されているデバイスは、最適化されたタイム スタンプの場所をサポートしている必要が（も）あり、そうでないとプローブが失敗します。

送信元（送信者）デバイス側：

```
ip sla 1
 udp-jitter 192.0.2.134 5000 num-packets 20
 request-data-size 160
 tos 128
 frequency 30
 precision microseconds     !enables QFP time stamping
 optimize timestamp         !configures optimized time stamp location
ip sla schedule 1 start-time after 00:05:00
ip sla 2
 udp-jitter 192.0.2.134 65052 num-packets 20 interval 10
 request-data-size 20
```

```
 tos 64
 frequency 30
 precision microseconds
 optimize timestamp
ip sla schedule 2 start-time after 00:05:05
```

宛先（レスポンダ）デバイス側：

```
ip sla responder
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Cisco IOS IP SLA コマンド	『Cisco IOS IP SLAs Command Reference』

MIB

MIB	MIB のリンク
• CISCO-RTTMON-MIB • IPV6-FLOW-LABEL-MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

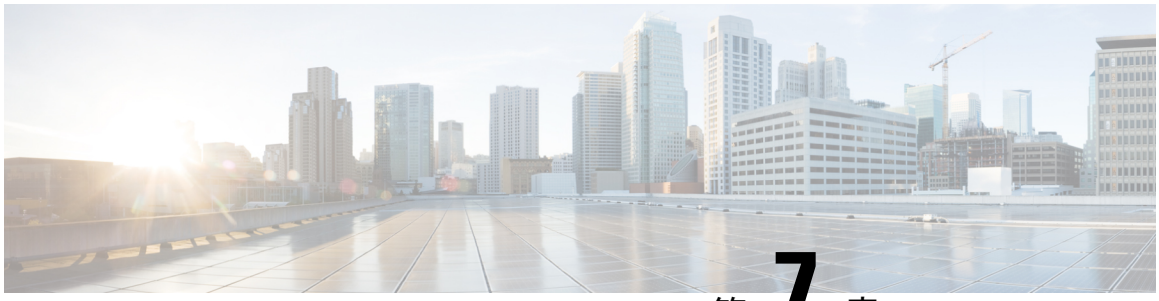
IP SLA QFP タイム スタンプに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *13 : IP SLA QFP* タイム スタンプに関する機能情報

機能名	リリース	機能情報
IP SLA QFP タイム スタンプ	Cisco IOS XE Release 3.7S	この機能では、IP SLA UDP ジッター動作の精度を高めるために、IP SLA Cisco パケット プロセッサ（CPP）のタイム スタンプを有効にできます。 Cisco ASR 1000 シリーズ ルータでのみ、この機能は、より正確な RTT を測定するためのタイム スタンプの場所の最適化もサポートしています。 次のコマンドが導入または変更されました。**optimize timestamp**、**precision microseconds**、**show ip sla configuration**



第 7 章

IP SLA LSP ヘルス モニタ動作の設定

このモジュールでは、IP サービス レベル契約（SLA）ラベル スイッチド パス（LSP）のヘルス モニタを設定する方法について説明します。LSP ヘルス モニタを使用すると、レイヤ 3 マルチプロトコル ラベル スイッチング（MPLS）バーチャル プライベート ネットワーク（VPN）を予防的にモニタできます。この機能により、参加しているプロバイダー エッジ（PE）デバイス間のすべての LSP に対して、コントロール プレーンおよびデータ プレーン内での自動化されたエンドツーエンド検証が提供されます。このエンドツーエンド（PE-to-PE デバイス）アプローチにより、LSP 接続はカスタマー トラフィックの送信パスに沿って確実に検証されます。その結果、MPLS コア内で発生し顧客に影響を与えるネットワーク接続の問題が LSP ヘルス モニタによって検出されます。LSP ヘルス モニタを設定すると、ネットワーク トポロジに基づいて、自動的に IP SLA LSP ping または LSP traceroute 処理が生成または削除されます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

LSP ヘルス モニタ動作の前提条件

- LSP ヘルス モニタ動作の参加 PE デバイスは、MPLS LSP ping 機能をサポートしている必要があります。詳細なエラー レポーティングと診断情報を得るために、プロバイダー（P）デバイスも MPLS LSP ping 機能をサポートしていることが推奨されます。
- 送信元 PE デバイスに、目的の LSP ヘルス モニタ機能をサポートするのに十分なメモリがあるかどうかを確認します。LSP ディスカバリ オプションをイネーブルにすると、デバイスのメモリに著しい影響を与える可能性があります。LSP ディスカバリ プロセス中に使用可能なメモリが不足すると、そのプロセスはグレースフル終了し、エラー メッセージが表示されます。

（注） LSP ヘルス モニタ動作の宛先 PE デバイスで IP SLA Responder を有効にする必要はありません。

LSP ヘルス モニタ動作の制限事項

- LSP ヘルス モニタ動作の開始後は、その動作が終了するまで、コンフィギュレーション パラメータを変更してはいけません。動作がアクティブに実行しているときにコンフィギュレーション パラメータを変更すると、ネットワーク接続統計情報の取得に遅延が発生する可能性があります。

LSP ヘルス モニタ動作に関する情報

LSP ヘルス モニタの利点

- 等コスト マルチパス間のエンドツーエンド LSP 接続測定による MPLS ネットワーク内でのネットワーク アベイラビリティの確認やネットワーク接続のテスト
- SNMP トラップ通知と Syslog メッセージを使用した予防的しきい値モニタリング
- MPLS ネットワークに対するネットワークのトラブルシューティングにかかる時間の短縮
- 高速再試行機能を使用したスケーラブルなネットワーク エラー検出
- ネットワーク トポロジに基づいた IP SLA 動作の作成と削除
- ローカル VPN ルーティングおよび転送（VRF）インスタンスとグローバル ルーティング テーブルに基づいたボーダー ゲートウェイ プロトコル（BGP）ネクスト ホップ ネイバーの検出

- IP SLA 動作の複数動作スケジューリング
- しきい値違反とスケーラブルな動作スケジューリングによる、MPLS ネットワーク エッジ間の擬似回線接続のテスト
- ラウンドトリップ時間（RTT）しきい値違反、接続損失、およびコマンド応答タイムアウトのモニタリングと SNMP トラップ警告

LSP ヘルス モニタの動作方法

LSP ヘルス モニタ機能では、レイヤ 3 MPLS VPN を予防的にモニタできます。LSP ヘルス モニタの動作方法の一般的なプロセスは次のとおりです。

1. ユーザが LSP ヘルス モニタ動作を設定すると、BGP ネクスト ホップ ネイバー探索プロセスが有効になります。

   LSP ヘルス モニタ動作の設定方法は、標準的な IP SLA 動作の設定方法と同様です。たとえば、LSP ヘルス モニタ動作のすべての動作パラメータは、動作の ID 番号を指定した後で設定します。ただし、標準的な IP SLA 動作と異なり、これらの設定されたパラメータは、LSP ヘルス モニタによって作成される個々の IP SLA LSP ping および LSP traceroute 動作の基本設定として使用されます。LSP 検出プロセスは、送信元 PE デバイスのメモリや CPU に大きな影響を与える可能性があります。不要なデバイス パフォーマンス問題の発生を防ぐために、LSP ヘルス モニタ動作の動作パラメータとスケジューリング パラメータを設定するときには、細心の注意が必要です。

   BGP ネクスト ホップ ネイバー探索プロセスがイネーブルな場合、ローカル VRF とグローバル ルーティング テーブルの情報に基づいて、送信元 PE デバイスに関連付けられているすべての VRF によって使用中の BGP ネクスト ホップ ネイバーのデータベースが生成されます。BGP ネクスト ホップ ネイバー探索プロセスの詳細については、「隣接 PE デバイスの検出」の項を参照してください。

（注） デフォルトでは、送信元と宛先の PE デバイス間に 1 つのパスだけが検出されます。LSP ディスカバリ オプションがイネーブルの場合、送信元 PE デバイスと宛先 PE デバイスの間で等コストマルチパスが検出されます。LSP 検出プロセスの動作の詳細については、「LSP 検出プロセス」の項を参照してください。

2. ユーザが、LSP ヘルス モニタ動作の予防的しきい値モニタリング パラメータを設定します。予防的しきい値モニタリングの詳細については、「LSP ヘルス モニタの予防的しきい値モニタリング」の項を参照してください。

   選択した予防的しきい値モニタリング設定オプションに応じて、しきい値違反が発生したときに SNMP トラップ通知または syslog メッセージが生成されます。

3. ユーザが、LSP ヘルス モニタ動作の複数動作スケジューリング パラメータを設定します。複数動作スケジューリングの詳細については、「LSP ヘルス モニタの複数動作スケジューリング」の項を参照してください。

LSP ヘルス モニタ動作が開始されると、単一の IP SLA 動作が適用される各 PE（BGP ネクスト ホップ）ネイバーに対して自動的に作成されます（手順 1 で設定したパラメータに基づく）。IP SLA 動作は、送信元 PE デバイスと検出された宛先 PE デバイス間のネットワーク接続を測定します。各測定の開始時間と頻度は、ユーザによって定義された複数動作スケジューリング パラメータに基づきます。

IP SLA 動作の追加と削除

LSP ヘルス モニタは、特定の VPN に対して追加または削除された BGP ネクスト ホップ ネイバーについて定期的な通知を受けます。この情報は、LSP ヘルス モニタが保持するキューに格納されます。キュー内の情報とユーザ指定の期間に基づき、新たに検出された PE ルデバイス対して新しい IP SLA 動作が自動的に作成され、有効でなくなった PE デバイスに対する既存の IP SLA 動作は自動的に削除されます。動作の自動削除は無効にできます。しかし、この機能をディセーブルにすることは推奨されません。ディセーブルにした場合、それらの動作を手動で削除しなければならないためです。

LSP ディスカバリ オプションを有効にした場合は、「LSP 検出プロセス」の項で説明するプロセスと同じプロセスに従い、新たに検出された BGP ネクスト ホップ ネイバーに対する LSP ディスカバリ グループの作成を実行します。BGP ネクスト ホップ ネイバーが特定の VPN から削除されると、対応するすべての LSP ディスカバリ グループおよび関連する個々の IP SLA 動作と統計情報が LSP ディスカバリ グループ データベースから削除されます。

BGP ネクスト ホップ ネイバーをフィルタリングするためのアクセス リスト

標準 IP アクセス リストを設定して、LSP ヘルス モニタによって自動的に作成される IP SLA 動作の数を制限できます。IP SLA アクセス リスト パラメータを設定すると、LSP ヘルス モニタによって検出された BGP ネクスト ホップ ネイバーのリストが、関連する標準 IP アクセス リストで定義されている条件に基づいてフィルタリングされます。つまり、送信元アドレスが標準 IP アクセス リストで許可された条件を満たしている BGP ネクスト ホップ ネイバーの IP SLA 動作だけが、LSP ヘルス モニタによって自動的に作成されます。

自動的に作成された各 IP SLA 動作の一意の識別子

LSP ヘルス モニタによって自動的に作成された IP SLA 動作は、所有者フィールドで一意に識別されます。動作の所有者フィールドは、その個別の動作に設定可能なすべてのパラメータを使用して生成されます。所有者フィールドの長さが 255 文字を超えると、超えた文字は切り捨てられます。

隣接 PE デバイスの検出

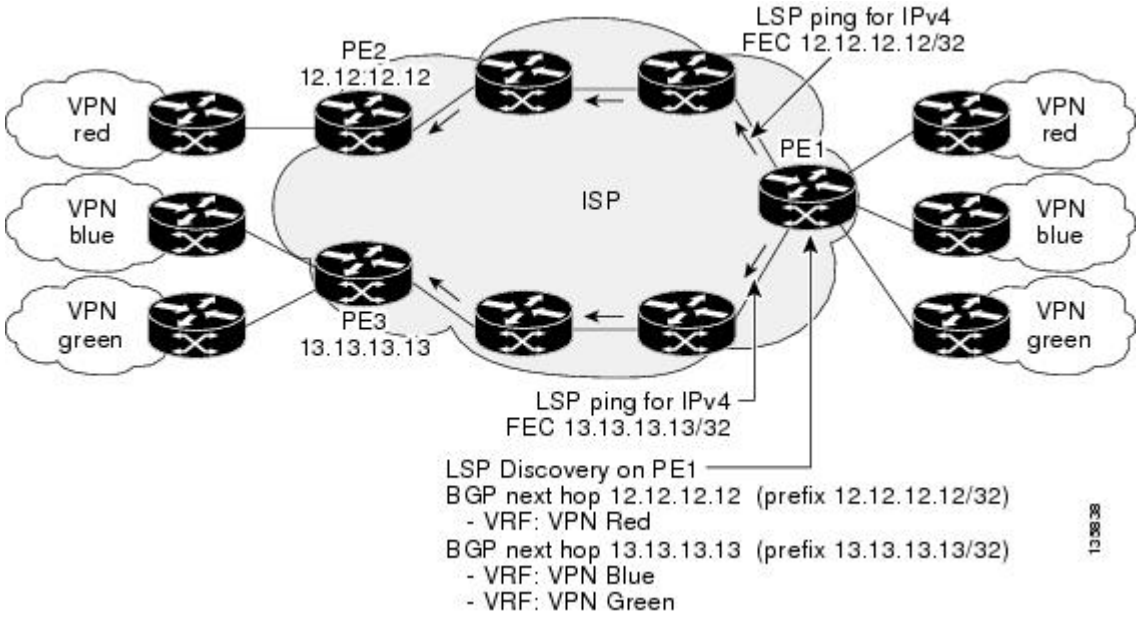
BGP ネクスト ホップ ネイバー探索プロセスは、送信元 PE デバイスに関連付けられているすべての VRF によって使用中の BGP ネクスト ホップ ネイバーを見つけるために使用されます。ほとんどの場合、これらのネイバーは PE デバイスです。

BGP ネクスト ホップ ネイバー探索プロセスがイネーブルな場合、ローカル VRF とグローバル ルーティング テーブルの情報に基づいて、送信元 PE デバイスに関連付けられているすべての VRF によって使用中の BGP ネクスト ホップ ネイバーのデータベースが生成されます。ルー

ティング アップデートが受信されると、新しい BGP ネクスト ホップ ネイバーがただちにデータベースに追加され、データベースから削除されます。

次の図に、インターネット サービス プロバイダー（ISP）の単純な VPN シナリオでの BGP ネクスト ホップ ネイバー探索プロセスの動作を示します。この例で、デバイス PE1 に関連付けられた 3 つの VPN があります（赤、青、緑）。デバイス PE1 から見ると、これらの VPN には、BGP ネクスト ホップ ネイバー PE2（デバイス ID：12.12.12.12）および PE3（デバイス ID：13.13.13.13）を経由してリモートで到達可能です。BGP ネクスト ホップ ネイバー探索プロセスがデバイス PE1 でイネーブルになっている場合、ローカル VRF とグローバル ルーティング テーブルに基づいてデータベースが生成されます。この例のデータベースには、2 つの BGP ネクスト ホップ デバイス エントリとして PE2 12.12.12.12 および PE3 13.13.13.13 が格納されます。ルーティング エントリは、どのネクスト ホップ デバイスがどの特定の VRF 内に属しているか区別するために、ネクスト ホップ デバイス単位で維持されます。各ネクスト ホップ デバイス エントリに対し、グローバル ルーティング テーブル内の BGP ネクスト ホップ デバイスの IPv4 Forward Equivalence Class（FEC）が、MPLS LSP ping 動作で使用するために提供されます。

図 *4 :* 単純な *VPN* の *BGP* ネクスト ホップ ネイバー探索



LSP ディスカバリ

LSP ヘルス モニタ動作の LSP ディスカバリ オプションでは、送信元と宛先の PE デバイス間の MPLS トラフィックを伝送するための等コスト マルチパスを検出する機能が提供されます。その後、検出されたそれぞれのパスに対してネットワーク接続測定を実行できます。

LSP ディスカバリの一般的なプロセスは次のとおりです。

1. BGP ネクスト ホップ ネイバーは、BGP ネクスト ホップ ネイバー探索プロセスを使用して検出されます。BGP ネクスト ホップ ネイバー探索プロセスの詳細については、「隣接 PE ルータの検出」の項を参照してください。

   LSP ヘルス モニタ動作が開始されると、単一の IP SLA 動作が適用される各 PE（BGP ネクスト ホップ）ネイバーに対して自動的に作成されます。LSP ディスカバリ プロセスのこの最初のステップでは、適用可能な PE ネイバーごとに 1 つのパスだけが検出されます。ネクスト ホップ ネイバーごとに、LSP ヘルス モニタは LSP ディスカバリ グループを作成し（最初は検出された 1 つのパスだけで構成される）、そのグループに一意の識別番号を割り当てます。LSP ディスカバリ グループの詳細については、「LSP ディスカバリ グループ」の項を参照してください。

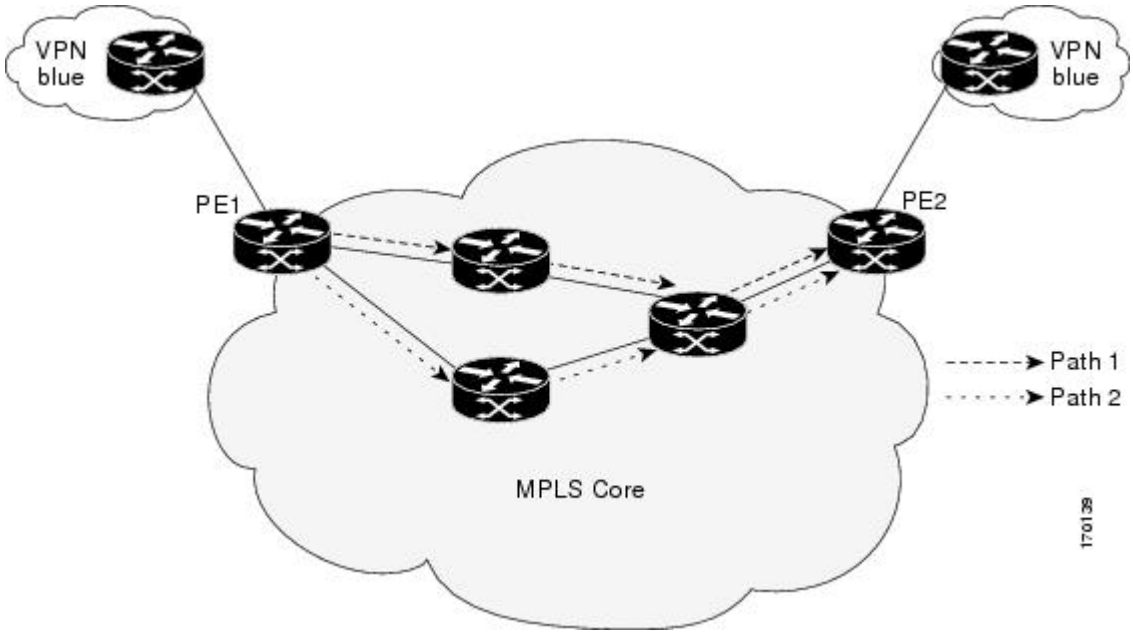
2. LSP ヘルス モニタによって、LSP ディスカバリ要求が、適用可能な各 BGP ネクスト ホップ ネイバーの LSP ディスカバリ サブシステムに送信されます。適切な応答が受信される各ネクストホップ ネイバーの場合は、等コスト マルチパスを検出するための MPLS エコー要求が送信元 PE デバイスから 1 つずつ送信されます。それぞれの等コスト マルチパスを一意に識別するパラメータ（127/8 宛先 IP アドレス（LSP セレクタ）および PE 発信インターフェイス）が、関連付けられた LSP 検出データベースに追加されます。

（注） 個別の LSP ヘルス モニタ動作に対し、ユーザは、同時に LSP ディスカバリを実行できる BGP ネクスト ホップ ネイバーの最大数を定義できます。

3. 個々の IP SLA 動作（適用可能な PE ネイバーごとに作成される）は、IP SLA LSP ping 上位動作を使用して、送信元 PE デバイスと検出された宛先 PE デバイスの間のすべての等コスト マルチパスでネットワーク接続を測定します。IP SLA 上位動作は、LSP ping パケットを宛先 PE デバイスに送信し、検出された等コスト マルチパスごとに LSP ping 127/8 LSP セレクタ IP アドレスを調整することで動作します。たとえば、宛先 PE デバイスに対して 3 つの等コスト マルチパスが存在し、識別された LSP セレクタ IP アドレスが 127.0.0.1、127.0.0.5、および 127.0.0.6 であるとします。IP SLA 上位動作は、3 つのパスすべてに上位動作を誘導するために、識別された LSP セレクタ IP アドレスを使用して 3 つの LSP ping パケットを連続して送信します。この技術により、送信元 PE デバイスと宛先 PE デバイスのペアごとに 1 つの IP SLA LSP ping 動作しか存在しないことが保証され、送信元 PE デバイスによって送信されるアクティブな LSP ping 動作の数が大幅に削減されます。

次の図に、単純な VPN のシナリオを示します。このネットワークは、VPN blue という名前の VRF に属している 2 台の PE デバイス（デバイス PE1 とデバイス PE2）とコア MPLS VPN で構成されます。デバイス PE1 は、LSP ディスカバリ オプションをイネーブルにした LSP ヘルス モニタ動作の送信元 PE デバイスであるとし、デバイス PE2 は BGP ディスカバリ プロセスでデバイス PE1 の BGP ネクスト ホップ ネイバーとして検出されるものとします。パス 1 とパス 2 がデバイス PE1 からデバイス PE2 までの等コスト マルチパスである場合、LSP ディスカバリ プロセスによって、パス 1 とパス 2 で構成される LSP ディスカバリ グループが作成されます。各パスのネットワーク アベイラビリティをモニタするために、IP SLA LSP ping 上位動作も作成されます。

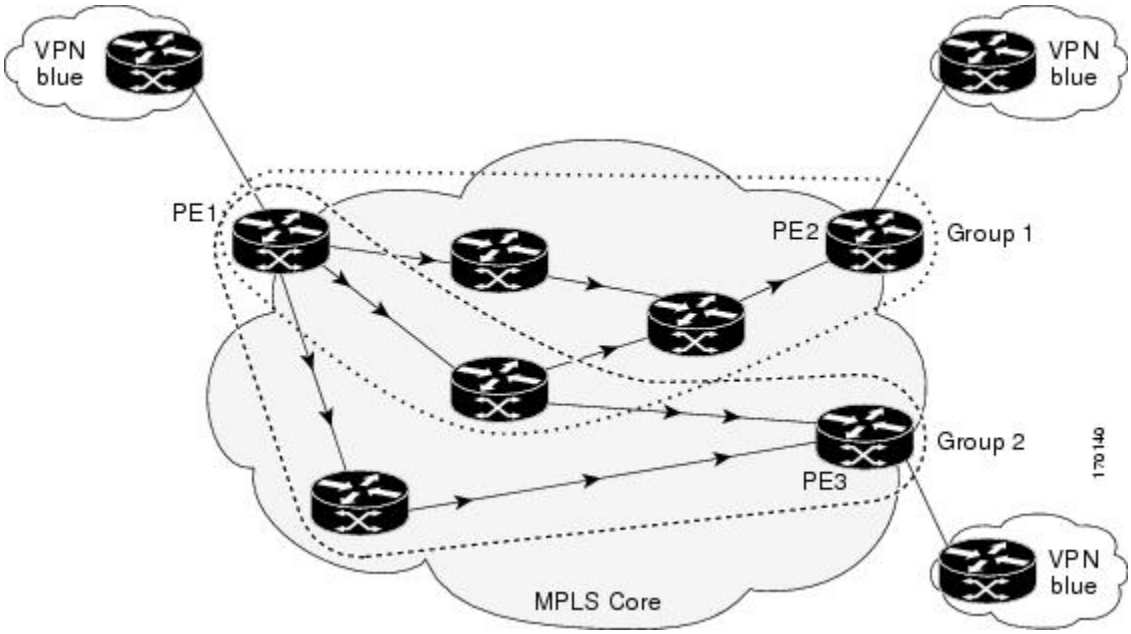
図 *5 :* 単純な *VPN* の *LSP* ディスカバリ



LSP ディスカバリ グループ

1 つの LSP ヘルス モニタ動作は、BGP ネクスト ホップ ネイバー探索プロセスで検出される BGP ネクスト ホップ ネイバーの数に応じて、複数の LSP ディスカバリ グループで構成されます。各 LSP ディスカバリ グループは、1 つの BGP ネクスト ホップ ネイバーに対応し、一意の識別番号（番号 1 から開始）が割り当てられます。次の図に、単純な VPN のシナリオを示します。このネットワークは、VPN blue という名前の VRF に属している 3 台の PE デバイス（デバイス PE1、PE2、および PE3）とコア MPLS VPN で構成されます。デバイス PE1 は、LSP ディスカバリ オプションをイネーブルにした LSP ヘルス モニタ動作の送信元 PE デバイスであるとし、デバイス PE2 および PE3 は BGP ディスカバリ プロセスでデバイス PE1 への BGP ネクスト ホップ ネイバーとして検出されるものとします。LSP ディスカバリ グループ 1 は、デバイス PE1 からデバイス PE2 までの等コスト マルチパスとして作成され、LSP ディスカバリ グループ 2 は、デバイス PE1 からデバイス PE3 までの等コスト マルチパスとして作成されます。

図 *6 :* 単純な *VPN* の *LSP* ディスカバリ グループ



LSP ヘルス モニタ動作が開始されると、単一の IP SLA 動作が適用される各 PE（BGP ネクストホップ）ネイバーに対して自動的に作成されます。各 IP SLA 動作（適用可能な PE ネイバーごとに作成される）は、IP SLA LSP ping 上位動作を使用して、送信元 PE デバイスと検出された宛先 PE デバイスの間のすべての等コスト マルチパスでネットワーク接続を測定します。各 LSP ping 上位動作は、単一の LSP ディスカバリ グループと対応します。

LSP ping 上位動作は、LSP ping パケットを宛先 PE デバイスに送信し、検出された等コスト マルチパスごとに LSP ping 127/8 LSP セレクタ IP アドレスを調整することで動作します。それぞれの等コスト マルチパスによって収集されたネットワーク接続の統計情報は、集約されて、1 時間単位で保存されます（最大 2 時間分のデータを収集できます）。結果は、特定の 1 時間分について、LSP ディスカバリ グループ内のすべての等コスト マルチパスのグループ平均代表値として格納されます。

送信元 PE デバイスと BGP ネクスト ホップ ネイバー間で検出されたそれぞれの等コスト マルチパスは、次のパラメータを使用して一意に識別されます。

- ローカル ホスト IP アドレスの範囲内の 127/8 宛先 IP アドレス（LSP セレクタ）
- PE 発信インターフェイス

LSP ディスカバリ グループのデータベースは、次のいずれかのイベントが発生すると更新されます。

- 対応する LSP ping 上位動作による LSP ping パケットの送信
- LSP ディスカバリ グループへのアクティブな等コスト マルチパスの追加または削除
- 特定の LSP ディスカバリ グループのすべての集約された統計データを削除する Cisco コマンドをユーザが入力

IP SLA LSP ping と LSP traceroute

LSP ヘルス モニタ機能により、IP SLA LSP ping 動作と IP SLA LSP traceroute 動作に対するサポートが追加されます。これらの動作は、ネットワークの接続性の問題をトラブルシューティングし、MPLS VPN のネットワークのアベイラビリティを判定するために役立ちます。LSP ヘルス モニタを使用する場合、送信元 PE デバイスと検出された宛先 PE デバイスの間のネットワーク接続を測定するために、IP SLA LSP ping 動作と LSP traceroute 動作が自動的に作成されます。個々の IP SLA LSP ping 動作と LSP traceroute 動作を手動で設定することもできます。これらの動作の手動の設定は、接続性の問題をトラブルシューティングするために役立ちます。

IP SLA LSP ping 動作と IP SLA LSP traceroute 動作は、それぞれ MPLS LSP ping 機能と MPLS LSP traceroute 機能で使用されるのと同じインフラストラクチャに基づいて、LSP をテストするためのエコー応答パケットとエコー要求パケットを送受信します。

LSP ディスカバリは、IP SLA traceroute 動作をサポートしません。

LSP ヘルス モニタの予防的しきい値モニタリング

LSP ヘルス モニタの予防的しきい値モニタリング サポート機能では、ユーザ定義の応答条件（接続損失やタイムアウトなど）が満たされたときに、SNMP トラップ通知と Syslog メッセージをトリガーできます。LSP ヘルス モニタのしきい値モニタリング動作の設定方法は、標準的な IP SLA 動作の設定方法と同様です。

イネーブルにされた LSP ディスカバリ オプション

LSP ヘルス モニタの LSP ディスカバリ オプション動作がイネーブルにされている場合、次のいずれかのイベントが発生したときに SNMP トラップ通知を生成できます。

- 特定の BGP ネクスト ホップ ネイバーの LSP ディスカバリが失敗
- LSP ディスカバリ グループの動作ステータスが変化

特定の BGP ネクスト ホップ ネイバーに対する LSP ディスカバリが失敗する理由として、次のものが考えられます。

- BGP ネクスト ホップ ネイバーが LSP ディスカバリ要求に応答できる時間の期限切れ
- BGP ネクストホップ ネイバーに通じるすべてのパスに対してリターン コードが「Broken」または「Unexplorable」

次の表では、LSP ディスカバリ グループの動作ステータスが変化する条件を説明しています。LSP ディスカバリ グループの個々の IP SLA LSP ping 動作が実行されるたびに、戻りコードが生成されます。リターン コードの値と LSP ディスカバリ グループの現在のステータスに応じて、グループ ステータスは変化します。

表 *14 : LSP* ディスカバリ グループ ステータスが変化する条件

個々の IP SLA 動作のリターン コード	現在のグループ ステータス = UP	現在のグループ ステータス = PARTIAL	現在のグループ ステータス = DOWN
OK	グループ ステータスは変化しません。	グループ内のすべてのパスに対するリターン コードが OK の場合、グループ ステータスは UP に変化します。	グループ ステータスは PARTIAL に変化します。
Broken または Unexplorable	グループ ステータスは PARTIAL に変化します。	グループ内のすべてのパスに対するリターン コードが Broken または Unexplorable の場合、グループ ステータスは DOWN に変化します。	グループ ステータスは変化しません。

個々の IP SLA LSP ping 動作に対するリターン コードは、次のいずれかです。

- OK：LSP が正常に機能していることを示します。カスタマー VPN トラフィックは、このパスを経由して送信されます。
- Broken：LSP が壊れていることを示します。カスタマー VPN トラフィックは、このパスを経由して送信されず、場合によっては廃棄されます。
- Unexplorable：この PE ネイバーへの一部のパスが検出されていないことを示します。これは、LSP 上に中断がある場合や、LSP 選択に使用される 127/8 IP アドレスの数が足りなくなった場合になることがあります。

LSP ディスカバリ グループのステータスは、次のいずれかです。

- UNKNOWN：グループ ステータスがまだ決定されていないこと、およびグループに属しているパスが最初のテスト中であることを示します。この初期テストが完了すると、グループ ステータスは UP、PARTIAL、または DOWN に変化します。
- UP：グループ内のすべてのパスがアクティブで、動作の失敗は検出されていないことを示します。
- PARTIAL：グループ内のすべてではないが、1 つ以上のパスに対して動作の失敗が検出されていることを示します。
- DOWN：グループ内のすべてのパスに対して動作の失敗が検出されていることを示します。

セカンダリ頻度オプション

LSP ヘルス モニタ機能の導入により、セカンダリ頻度を指定できる新しいしきい値モニタリング パラメータが追加されています。特定のパスでセカンダリ頻度オプションが設定され、障害（接続損失やタイムアウトなど）が検出された場合、パスが再測定される頻度がセカンダリ頻度値（高速でのテスト）に増やされます。設定された応答条件が満たされると（連続する N 回

の接続損失、または連続する N 回のタイムアウトなど）、SNMP トラップおよび syslog メッセージが送信されて、測定頻度が元の頻度値に戻ります。

LSP ヘルス モニタの複数動作スケジューリング

LSP ヘルス モニタの複数動作スケジューリング サポート機能では、（各 LSP ヘルス モニタ動作に対して）自動的に作成された IP SLA 動作を、指定された期間（スケジュール期間）にわたって均等に分散される間隔で開始し、指定された頻度で再開するように簡単にスケジューリングできます。複数動作スケジューリングは、多数の PE ネイバーが存在し、その結果として多数の IP SLA 動作が同時に稼働している送信元 PE デバイス上で LSP ヘルス モニタがイネーブルにされる場合に特に有用です。

（新たに検出された BGP ネクスト ホップ ネイバーに対して）新たに作成された IP SLA 動作は、現在稼働している動作と同じスケジュール期間に追加されます。同時に開始する動作が多くなりすぎないように、複数動作スケジューリング機能は、それらの動作を、スケジュール期間にわたって均一に分散されるランダムな間隔で開始するようにスケジューリングします。

LSP ヘルス モニタの複数動作スケジュールの設定方法は、個々の IP SLA 動作のグループに対する標準的な複数動作スケジュールの設定方法と同様です。

LSP ディスカバリのイネーブル化

LSP ディスカバリありの LSP ヘルス モニタ動作の複数動作スケジュールが開始されると、BGP ネクスト ホップ ネイバーが検出され、適用可能な各ネイバーへのネットワーク接続が単一の LSP だけを使用してモニタされます。最初は、送信元 PE デバイスと検出された宛先 PE デバイスの間のネットワーク接続は単一パス上でだけ測定されます。この初期状態は、LSP ヘルス モニタ動作が LSP ディスカバリなしで実行された場合と同じです。

後に続く LSP ディスカバリ プロセスの繰り返しで等コスト パスが新たに検出されると、IP SLA LSP ping 動作が作成され、その動作に関する具体的な情報が LSP ディスカバリ グループ データベースに保存されます。これらの新たに作成された IP SLA LSP ping 動作は、それらに関連付けられた LSP ディスカバリ グループの次のネットワーク接続測定の繰り返しからデータの収集を開始します。

各 LSP ディスカバリ グループの個々の IP SLA LSP ping 動作の開始時間は、LSP ディスカバリ グループの数と複数動作スケジュールのスケジュール期間に基づきます。たとえば、3 つの LSP ディスカバリ グループ（グループ 1、グループ 2、およびグループ 3）を 60 秒の期間にわたって実行するようにスケジューリングすると、グループ 1 の最初の LSP ping 動作は 0 秒に開始し、グループ 2 の最初の LSP ping 動作は 20 秒に開始し、グループ 3 の最初の LSP ping 動作は 40 秒に開始します。各 LSP ディスカバリ グループの残りの個々の IP SLA LSP ping 動作は、最初の LSP ping 動作の完了後に順次実行されます。LSP ディスカバリ グループごとに、1 つの LSP ping 動作しか同時には実行されません。

LSP ヘルス モニタ動作の設定方法

LSP ヘルス モニタ動作の設定

次のいずれかの作業のみを実行します。

PE デバイスでの LSP ディスカバリなしの LSP ヘルス モニタ動作の設定

（注） LSP ディスカバリがディセーブルの場合、送信元 PE デバイスと各 BGP ネクスト ホップ ネイバーの間のパスは 1 つしか検出されません。

手順の概要

1. **enable**
2. **configure terminal**
3. **mpls discovery vpn next-hop**
4. **mpls discovery vpn interval** *seconds*
5. **auto ip sla mpls-lsp-monitor** *operation-number*
6. 次のいずれかを実行します。
   - **type echo** [**ipsla-vrf-all** | **vrf** *vpn-name*]
   - **type pathEcho** [**ipsla-vrf-all** | **vrf** *vpn-name*]
7. **access-list** *access-list-number*
8. **scan-interval** *minutes*
9. **delete-scan-factor** *factor*
10. **force-explicit-null**
11. **exp** *exp-bits*
12. **lsp-selector** *ip-address*
13. **reply-dscp-bits** *dscp-value*
14. **reply-mode** {**ipv4** | **router-alert**}
15. **request-data-size** *bytes*
16. **secondary-frequency** {**both** | **connection-loss** | **timeout**} *frequency*
17. **tag** *text*
18. **threshold** *milliseconds*
19. **timeout** *milliseconds*
20. **ttl** *time-to-live*
21. **exit**
22. **auto ip sla mpls-lsp-monitor reaction-configuration** *operation-number* **react** {**connectionLoss** | **timeout**} [**action-type** *option*] [**threshold-type** {**consecutive** [*occurrences*] | **immediate** | **never**}]
23. **exit**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	**mpls discovery vpn next-hop** 例： `Device(config)# mpls discovery vpn next-hop`	（任意）MPLS VPN BGP ネクスト ホップ ネイバー探索プロセスをイネーブルにします。 （注） このコマンドは、**auto ip sla mpls-lsp-monitor** コマンドを入力すると自動的にイネーブルになります。
ステップ 4	**mpls discovery vpn interval** *seconds* 例： `Device(config)# mpls discovery vpn interval 120`	（任意）有効ではなくなったルーティング エントリが MPLS VPN の BGP ネクスト ホップ ネイバー探索データベースから削除される間隔を指定します。
ステップ 5	**auto ip sla mpls-lsp-monitor** *operation-number* 例： `Device(config)# auto ip sla mpls-lsp-monitor 1`	LSP ヘルス モニタ動作の設定を開始し、自動 IP SLA MPLS コンフィギュレーション モードを開始します。 （注） このコマンドを入力すると、**mpls discovery vpn next-hop** コマンドが自動的にイネーブルになります。

ステップ 6	次のいずれかを実行します。
	• **type echo** [**ipsla-vrf-all** | **vrf** *vpn-name*]
	• **type pathEcho** [**ipsla-vrf-all** | **vrf** *vpn-name*]
	例：
	`Device(config-auto-ip-sla-mpls)# type echo ipsla-vrf-all`
	例：
	`Device(config-auto-ip-sla-mpls)# type pathEcho ipsla-vrf-all`
		MPLS パラメータ コンフィギュレーション サブモードを開始し、ユーザが LSP ヘルス モニタを使用して IP SLA LSP ping 動作のパラメータを設定できるようにします。
		または
		MPLS パラメータ コンフィギュレーション サブモードを開始し、ユーザが LSP ヘルス モニタを使用して IP SLA LSP traceroute 動作のパラメータを設定できるようにします。

ステップ 7	**access-list** *access-list-number* 例：	（任意）LSP ヘルス モニタ動作に適用するアクセス リストを指定します。

	コマンドまたはアクション	目的
	`Device(config-auto-ip-sla-mpls-params)# access-list 10`	
ステップ 8	**scan-interval** *minutes* 例： `Device(config-auto-ip-sla-mpls-params)# scan-interval 5`	（任意）IP SLA LSP ヘルス モニタ データベースのタイマーを設定します。
ステップ 9	**delete-scan-factor** *factor* 例： `Device(config-auto-ip-sla-mpls-params)# delete-scan-factor 2`	（任意）有効ではなくなった BGP ネクスト ホップ ネイバーに対する IP SLA 動作を自動的に削除するまでに、LSP ヘルス モニタがスキャン キューをチェックする回数を指定します。 • デフォルトのスキャン ファクタは 1 です。LSP ヘルスモニタがスキャンキューで更新をチェックするたびに、有効ではなくなった BGP ネクスト ホップ ネイバーの IP SLA 動作が削除されます。 • スキャン ファクタを 0 に設定すると、LSP ヘルス モニタは IP SLA 動作を自動的に削除しなくなります。この設定は推奨されません。 • このコマンドは、**scan-interval** コマンドと同時に使用する必要があります。
ステップ 10	**force-explicit-null** 例： `Device(config-auto-ip-sla-mpls-params)# force-explicit-null`	（任意）明示的な Null ラベルを IP SLA 動作のすべてのエコー要求パケットに追加します。
ステップ 11	**exp** *exp-bits* 例： `Device(config-auto-ip-sla-mpls-params)# exp 5`	（任意）IP SLA 動作のエコー要求パケットのヘッダーの試験的フィールド値を指定します。
ステップ 12	**lsp-selector** *ip-address* 例： `Device(config-auto-ip-sla-mpls-params)# lsp-selector 127.0.0.10`	（任意）IP SLA 動作の LSP を選択するために使用されるローカル ホスト IP アドレスを指定します。

	コマンドまたはアクション	目的
ステップ 13	**reply-dscp-bits** *dscp-value* 例： `Device(config-auto-ip-sla-mpls-params)# reply-dscp-bits 5`	（任意）IP SLA 動作のエコー応答パケットの Differentiated Services Codepoint（DSCP）値を指定します。
ステップ 14	**reply-mode** {**ipv4** | **router-alert**} 例： `Device(config-auto-ip-sla-mpls-params)# reply-mode router-alert`	（任意）IP SLA 動作のエコー要求パケットの応答モードを指定します。 • デフォルトの応答モードは、IPv4 UDP パケットです。
ステップ 15	**request-data-size** *bytes* 例： `Device(config-auto-ip-sla-mpls-params)# request-data-size 200`	（任意）IP SLA 動作の要求パケットのプロトコル データ サイズを指定します。
ステップ 16	**secondary-frequency** {**both** | **connection-loss** | **timeout**} *frequency* 例： `Device(config-auto-ip-sla-mpls-params)# secondary-frequency connection-loss 10`	（任意）より高い測定頻度（セカンダリ頻度）を設定します。応答条件時に IP SLA 動作の測定頻度がこの値に変化します。
ステップ 17	**tag** *text* 例： `Device(config-auto-ip-sla-mpls-params)# tag testgroup`	（任意）IP SLA 動作のユーザ指定 ID を作成します。
ステップ 18	**threshold** *milliseconds* 例： `Device(config-auto-ip-sla-mpls-params)# threshold 6000`	（任意）IP SLA 動作によって作成されるネットワーク モニタリング統計情報を計算するための上限しきい値を設定します。
ステップ 19	**timeout** *milliseconds* 例： `Device(config-auto-ip-sla-mpls-params)# timeout 7000`	（任意）IP SLA 動作がその要求パケットからの応答を待機する時間を指定します。
ステップ 20	**ttl** *time-to-live* 例： `Device(config-auto-ip-sla-mpls-params)# ttl 200`	（任意）IP SLA 動作のエコー要求パケットの最大ホップ カウントを指定します。

	コマンドまたはアクション	目的
ステップ 21	**exit** 例： `Device(config-auto-ip-sla-mpls-params)# exit`	MPLS パラメータ コンフィギュレーション サブモードを終了し、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 22	**auto ip sla mpls-lsp-monitor reaction-configuration** *operation-number* **react** {**connectionLoss** | **timeout**} [**action-type** *option*] [**threshold-type** {**consecutive** [*occurrences*] | **immediate** | **never**}] 例： `Device(config)# auto ip sla mpls-lsp-monitor reaction-configuration 1 react connectionLoss action-type trapOnly threshold-type consecutive 3`	（任意）LSP ヘルス モニタの制御下のイベントに基づいて発生する特定のアクションを設定します。
ステップ 23	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

PE デバイスで LSP ディスカバリありの LSP ヘルス モニタ動作の設定

（注）
- LSP ディスカバリ付き LSP ヘルス モニタ機能では、レイヤ 3 MPLS VPN だけがサポートされます。
- LSP ディスカバリ オプションは、IP SLA LSP traceroute 動作をサポートしません。
- LSP ディスカバリ オプションは、IP SLA VCCV 動作をサポートしません。
- LSP 検出プロセスは、送信元 PE デバイスのメモリや CPU に大きな影響を与える可能性があります。不要なデバイス パフォーマンス問題の発生を防ぐために、LSP ヘルス モニタ動作の動作パラメータとスケジューリング パラメータを設定するときには、細心の注意が必要です。

手順の概要

1. **enable**
2. **configure terminal**
3. **mpls discovery vpn next-hop**
4. **mpls discovery vpn interval** *seconds*
5. **auto ip sla mpls-lsp-monitor** *operation-number*
6. **type echo** [**ipsla-vrf-all** | **vrf** *vpn-name*]
7. IP SLA LSP エコー動作用の省略可能なパラメータを設定します。
8. **path-discover**
9. **hours-of-statistics-kept** *hours*

10. **force-explicit-null**
11. **interval** *milliseconds*
12. **lsp-selector-base** *ip-address*
13. **maximum-sessions** *number*
14. **scan-period** *minutes*
15. **session-timeout** *seconds*
16. **timeout** *seconds*
17. **exit**
18. **exit**
19. **auto ip sla mpls-lsp-monitor reaction-configuration** *operation-number* **react lpd** {**lpd-group** [**retry** *number*] | **tree-trace**} [**action-type trapOnly**]
20. **ip sla logging traps**
21. **exit**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	**mpls discovery vpn next-hop** 例： `Device(config)# mpls discovery vpn next-hop`	（任意）MPLS VPN BGP ネクスト ホップ ネイバー探索プロセスをイネーブルにします。 （注） このコマンドは、**auto ip sla mpls-lsp-monitor** コマンドを入力すると自動的にイネーブルになります。
ステップ 4	**mpls discovery vpn interval** *seconds* 例： `Device(config)# mpls discovery vpn interval 120`	（任意）有効ではなくなったルーティング エントリが MPLS VPN の BGP ネクスト ホップ ネイバー探索データベースから削除される間隔を指定します。
ステップ 5	**auto ip sla mpls-lsp-monitor** *operation-number* 例： `Device(config)# auto ip sla mpls-lsp-monitor 1`	LSP ヘルス モニタ動作の設定を開始し、自動 IP SLA MPLS コンフィギュレーション モードを開始します。 （注） このコマンドを入力すると、**mpls discovery vpn next-hop** コマンドが自動的にイネーブルになります。

	コマンドまたはアクション	目的
ステップ 6	**type echo** [**ipsla-vrf-all** | **vrf** *vpn-name*] 例： `Device(config-auto-ip-sla-mpls)# type echo ipsla-vrf-all`	MPLS パラメータ コンフィギュレーション モードを開始し、ユーザが LSP ヘルス モニタを使用して IP SLA LSP ping 動作のパラメータを設定できるようにします。
ステップ 7	IP SLA LSP エコー動作用の省略可能なパラメータを設定します。	（任意）「PE デバイスで LSP ディスカバリなしの LSP ヘルス モニタ動作の設定」の項の手順 7 ～ 21 を参照してください。
ステップ 8	**path-discover** 例： `Device(config-auto-ip-sla-mpls-params)# path-discover`	IP SLA LSP ヘルス モニタ動作に対して LSP ディスカバリ オプションをイネーブルにし、LSP ディスカバリ パラメータ コンフィギュレーション サブモードを開始します。
ステップ 9	**hours-of-statistics-kept** *hours* 例： `Device(config-auto-ip-sla-mpls-lpd-params)# hours-of-statistics-kept 1`	（任意）LSP ヘルス モニタ動作用に LSP ディスカバリ グループ統計情報を維持する時間を設定します。
ステップ 10	**force-explicit-null** 例： `Device(config-auto-ip-sla-mpls-lpd-params)# force-explicit-null`	（任意）明示的な Null ラベルを LSP ヘルス モニタ動作のすべてのエコー要求パケットに追加します。
ステップ 11	**interval** *milliseconds* 例： `Device(config-auto-ip-sla-mpls-lpd-params)# interval 2`	（任意）LSP ヘルス モニタ動作用に LSP ディスカバリ プロセスの一部として送信される MPLS エコー要求の間隔を指定します。
ステップ 12	**lsp-selector-base** *ip-address* 例： `Device(config-auto-ip-sla-mpls-lpd-params)# lsp-selector-base 127.0.0.2`	（任意）LSP ヘルス モニタ動作の LSP ディスカバリ グループに属する LSP の選択に使用するベース IP アドレスを指定します。
ステップ 13	**maximum-sessions** *number* 例： `Device(config-auto-ip-sla-mpls-lpd-params)# maximum-sessions 2`	（任意）1 つの LSP ヘルス モニタ動作用に LSP ディスカバリを同時に処理できる BGP ネクスト ホップ ネイバーの最大数を指定します。 （注） このパラメータを設定するときには、デバイスの CPU に悪影響を及ぼさないように、細心の注意を払う必要があります。

	コマンドまたはアクション	目的
ステップ 14	**scan-period** *minutes* 例： `Device(config-auto-ip-sla-mpls-lpd-params)# scan-period 30`	（任意）LSP ヘルス モニタ動作用に LSP ディスカバリ プロセスが再開できるようになるまでの時間を設定します。
ステップ 15	**session-timeout** *seconds* 例： `Device(config-auto-ip-sla-mpls-lpd-params)# session-timeout 60`	（任意）LSP ヘルス モニタ動作の LSP ディスカバリ プロセスが個別の BGP ネクストホップ ネイバー向けの LSP ディスカバリ要求に対して応答を待つ時間を設定します。
ステップ 16	**timeout** *seconds* 例： `Device(config-auto-ip-sla-mpls-lpd-params)# timeout 4`	（任意）LSP ヘルス モニタ動作の LSP ディスカバリ プロセスがエコー要求パケットに対する応答を待つ時間を設定します。 （注） このパラメータを設定するときには、デバイスの CPU に悪影響を及ぼさないように、細心の注意を払う必要があります。
ステップ 17	**exit** 例： `Device(config-auto-ip-sla-mpls-lpd-params)# exit`	LSP ディスカバリ パラメータ コンフィギュレーション サブモードを終了し、MPLS パラメータ コンフィギュレーション モードに戻ります。
ステップ 18	**exit** 例： `Device(config-auto-ip-sla-mpls-params)# exit`	MPLS パラメータ コンフィギュレーション モードを終了し、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 19	**auto ip sla mpls-lsp-monitor reaction-configuration** *operation-number* **react lpd** {**lpd-group** [**retry** *number*] | **tree-trace**} [**action-type trapOnly**] 例： `Device(config)# auto ip sla mpls-lsp-monitor reaction-configuration 1 react lpd lpd-group retry 3 action-type trapOnly`	（任意）LSP ディスカバリがイネーブルの LSP ヘルス モニタ動作の予防的しきい値モニタリング パラメータを設定します。
ステップ 20	**ip sla logging traps** 例： `Device(config)# ip sla logging traps`	（任意）IP SLA トラップ通知に固有の SNMP システム ロギング メッセージの生成をイネーブルにします。
ステップ 21	**exit** 例：	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config)# exit`	

LSP ヘルス モニタ動作のスケジューリング

（注）
- LSP 検出プロセスは、送信元 PE デバイスのメモリや CPU に大きな影響を与える可能性があります。同時に稼働している IP SLA LSP ping 動作が多くなりすぎないように、スケジューリング パラメータを設定するときには、細心の注意が必要です。大規模な MPLS VPN に対しては、スケジュール期間を比較的大きな値に設定する必要があります。
- （新たに検出された BGP ネクスト ホップ ネイバーに対して）新たに作成された IP SLA 動作は、現在稼働している動作と同じ複数動作スケジュール期間に追加されます。同時に開始する動作が多くなりすぎないように、複数動作スケジューラは、それらの動作を、スケジュール期間にわたって均一に分散されるランダムな間隔で開始するようにスケジューリングします。

始める前に

- スケジュールされるすべての IP SLA 動作がすでに設定されている必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **auto ip sla mpls-lsp-monitor schedule** *operation-number* **schedule-period** *seconds* [**frequency** [*seconds*]] [**start-time** {**after** *hh* **:** *mm* **:** *ss* | *hh* **:** *mm*[**:** *ss*] [*month day* | *day month*] | **now** | **pending**}]
4. **exit**
5. **show ip sla configuration**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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。

	コマンドまたはアクション	目的
ステップ 3	**auto ip sla mpls-lsp-monitor schedule** *operation-number* **schedule-period** *seconds* [**frequency** [*seconds*]] [**start-time** {**after** *hh* **:** *mm* **:** *ss* | *hh* **:** *mm*[**:** *ss*] [*month day* | *day month*] | **now** | **pending**}] 例： `Device(config)# auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 start-time now`	LSP ヘルス モニタ動作のスケジューリング パラメータを設定します。
ステップ 4	**exit** 例： `Device(config)# exit`	特権 EXEC モードに戻ります。
ステップ 5	**show ip sla configuration** 例： `Device# show ip sla configuration`	（任意）IP SLA 設定の詳細を表示します。

トラブルシューティングのヒント

debug ip sla trace コマンドおよび **debug ip sla error** コマンドを使用すると、個々の IP SLA LSP ping 動作や LSP traceroute 動作に関する問題のトラブルシューティングに役立ちます。**debug ip sla mpls-lsp-monitor** コマンドを使用すると、IP SLA LSP ヘルス モニタ動作に関する問題のトラブルシューティングに役立ちます。

次の作業

個々の IP SLA 動作の結果を表示するには、**show ip sla statistics** コマンドと **show ip sla statistics aggregated** コマンドを使用します。サービス レベル契約の基準に対応するフィールドの出力を確認すると、サービス メトリックが許容範囲内であるかどうかを判断する役に立ちます。

IP SLA LSP ping 動作または LSP traceroute 動作の手動設定およびスケジューリング

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. 次のいずれかを実行します。
   - **mpls lsp ping ipv4** *destination-address destination-mask* [**force-explicit-null**] [**lsp-selector** *ip-address*] [**src-ip-addr** *source-address*] [**reply** {**dscp** *dscp-value* \| **mode** {**ipv4** \| **router-alert**}}]

- **mpls lsp trace ipv4** *destination-address destination-mask* [**force-explicit-null**] [**lsp-selector** *ip-address*] [**src-ip-addr** *source-address*] [**reply** {**dscp** *dscp-value* | **mode** {**ipv4** | **router-alert**}}]

5. **exp** *exp-bits*
6. **request-data-size** *bytes*
7. **secondary-frequency** {**connection-loss** | **timeout**} *frequency*
8. **tag** *text*
9. **threshold** *milliseconds*
10. **timeout** *milliseconds*
11. **ttl** *time-to-live*
12. **exit**
13. **ip sla reaction-configuration** *operation-number* [**react** *monitored-element*] [**threshold-type** {**never** | **immediate** | **consecutive** [*consecutive-occurrences*] | **xofy** [*x-value y-value*] | **average** [*number-of-probes*]}] [**threshold-value** *upper-threshold lower-threshold*] [**action-type** {**none** | **trapOnly** | **triggerOnly** | **trapAndTrigger**}]
14. **ip sla logging traps**
15. **ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh* **:** *mm*[**:** *ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh* **:** *mm* **:** *ss*}] [**ageout** *seconds*] [**recurring**]
16. **exit**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	**ip sla** *operation-number* 例： `Device(config)# ip sla 1`	IP SLA 動作の設定を開始し、IP SLA コンフィギュレーション モードに移行します。
ステップ 4	次のいずれかを実行します。 • **mpls lsp ping ipv4** *destination-address destination-mask* [**force-explicit-null**] [**lsp-selector** *ip-address*] [**src-ip-addr** *source-address*] [**reply** {**dscp** *dscp-value*	**mode** {**ipv4**	**router-alert**}}] • **mpls lsp trace ipv4** *destination-address destination-mask* [**force-explicit-null**] [**lsp-selector**	• 最初の例では、IP SLA 動作を LSP ping 動作として設定し、LSP ping コンフィギュレーション モードを開始します。 • 2 番目の例では、IP SLA 動作を LSP trace 動作として設定し、LSP trace コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

	ip-address] [**src-ip-addr** *source-address*] [**reply** {**dscp** *dscp-value* | **mode** {**ipv4** | **router-alert**}}]
	例：
	`Device(config-ip-sla)# mpls lsp ping ipv4 192.168.1.4 255.255.255.255 lsp-selector 127.1.1.1`
	例：
	`Device(config-ip-sla)# mpls lsp trace ipv4 192.168.1.4 255.255.255.255 lsp-selector 127.1.1.1`	

ステップ 5	**exp** *exp-bits* 例： `Device(config-sla-monitor-lspPing)# exp 5`	（任意）IP SLA 動作のエコー要求パケットのヘッダーの試験的フィールド値を指定します。 （注） LSP ping コンフィギュレーション モードは、この例と残りの手順で使用されます。注釈がある場合を除き、同じコマンドが LSP trace コンフィギュレーション モードでもサポートされています。
ステップ 6	**request-data-size** *bytes* 例： `Device(config-sla-monitor-lspPing)# request-data-size 200`	（任意）IP SLA 動作の要求パケットのプロトコル データ サイズを指定します。
ステップ 7	**secondary-frequency** {**connection-loss** | **timeout**} *frequency* 例： `Device(config-sla-monitor-lspPing)# secondary-frequency connection-loss 10`	（任意）より高い測定頻度（セカンダリ頻度）を設定します。応答条件時に IP SLA 動作の測定頻度がこの値に変化します。 • このコマンドは、IP SLA LSP ping 動作専用です。LSP trace コンフィギュレーション モードは、このコマンドをサポートしていません。
ステップ 8	**tag** *text* 例： `Device(config-sla-monitor-lspPing)# tag testgroup`	（任意）IP SLA 動作のユーザ指定 ID を作成します。
ステップ 9	**threshold** *milliseconds* 例： `Device(config-sla-monitor-lspPing)# threshold 6000`	（任意）IP SLA 動作によって作成されるネットワーク モニタリング統計情報を計算するための上限しきい値を設定します。

	コマンドまたはアクション	目的
ステップ 10	**timeout** *milliseconds* 例： `Device(config-sla-monitor-lspPing)# timeout 7000`	（任意）IP SLA 動作がその要求パケットからの応答を待機する時間を指定します。
ステップ 11	**ttl** *time-to-live* 例： `Device(config-sla-monitor-lspPing)# ttl 200`	（任意）IP SLA 動作のエコー要求パケットの最大ホップ カウントを指定します。
ステップ 12	**exit** 例： `Device(config-sla-monitor-lspPing)# exit`	LSP ping または LSP トレース コンフィギュレーション サブモードを終了し、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 13	**ip sla reaction-configuration** *operation-number* [**react** *monitored-element*] [**threshold-type** {**never** | **immediate** | **consecutive** [*consecutive-occurrences*] | **xofy** [*x-value y-value*] | **average** [*number-of-probes*]}] [**threshold-value** *upper-threshold lower-threshold*] [**action-type** {**none** | **trapOnly** | **triggerOnly** | **trapAndTrigger**}] 例： `Device(config)# ip sla reaction-configuration 1 react connectionLoss threshold-type consecutive 3 action-type traponly`	（任意）IP SLA の制御下のイベントに基づいて発生する特定のアクションを設定します。
ステップ 14	**ip sla logging traps** 例： `Device(config)# ip sla logging traps`	（任意）IP SLA トラップ通知に固有の SNMP システム ロギング メッセージの生成をイネーブルにします。
ステップ 15	**ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh* **:** *mm*[**:** *ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh* **:** *mm* **:** *ss*}] [**ageout** *seconds*] [**recurring**] 例： `Device(config)# ip sla schedule 1 start-time now`	IP SLA 動作のスケジューリング パラメータを設定します。
ステップ 16	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション サブモードを終了し、特権 EXEC モードに戻ります。

トラブルシューティングのヒント

debug ip sla trace コマンドおよび **debug ip sla error** コマンドを使用すると、個々の IP SLA LSP ping 動作や LSP traceroute 動作に関する問題のトラブルシューティングに役立ちます。

次の作業

個々の IP SLA 動作の結果を表示するには、**show ip sla statistics** コマンドと **show ip sla statistics aggregated** コマンドを使用します。サービス レベル契約の基準に対応するフィールドの出力を確認すると、サービス メトリックが許容範囲内であるかどうかを判断する役に立ちます。

LSP ヘルス モニタ動作の確認とトラブルシューティング

手順の概要

1. **debug ip sla error** [*operation-number*]
2. **debug ip sla mpls-lsp-monitor** [*operation-number*]
3. **debug ip sla trace** [*operation-number*]
4. **show ip sla mpls-lsp-monitor collection-statistics** [*group-id*]
5. **show ip sla mpls-lsp-monitor configuration** [*operation-number*]
6. **show ip sla mpls-lsp-monitor lpd operational-state** [*group-id*]
7. **show ip sla mpls-lsp-monitor neighbors**
8. **show ip sla mpls-lsp-monitor scan-queue** *operation-number*
9. **show ip sla mpls-lsp-monitor summary** [*operation-number* [**group** [*group-id*]]]
10. **show ip sla statistics** [*operation-number*] [**details**]
11. **show ip sla statistics aggregated** [*operation-number*] [**details**]
12. **show mpls discovery vpn**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**debug ip sla error** [*operation-number*] 例： `Device# debug ip sla error`	（任意）IP SLA 動作のランタイム エラーのデバッグ出力をイネーブルにします。
ステップ 2	**debug ip sla mpls-lsp-monitor** [*operation-number*] 例： `Device# debug ip sla mpls-lsp-monitor`	（任意）LSP ヘルス モニタ動作のデバッグ出力をイネーブルにします。
ステップ 3	**debug ip sla trace** [*operation-number*] 例： `Device# debug ip sla trace`	（任意）IP SLA 動作の実行をトレースするためのデバッグ出力をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	**show ip sla mpls-lsp-monitor collection-statistics** [*group-id*] 例： `Device# show ip sla mpls-lsp-monitor collection-statistics 100001`	（任意）LSP ヘルス モニタ動作の LSP ディスカバリ グループに属する IP SLA 動作の統計情報を表示します。 （注） このコマンドは、LSP ディスカバリ オプションがイネーブルの場合にのみ適用できます。
ステップ 5	**show ip sla mpls-lsp-monitor configuration** [*operation-number*] 例： `Device# show ip sla mpls-lsp-monitor configuration 1`	（任意）LSP ヘルス モニタ動作の設定を表示します。
ステップ 6	**show ip sla mpls-lsp-monitor lpd operational-state** [*group-id*] 例： `Device# show ip sla mpls-lsp-monitor lpd operational-state 100001`	（任意）LSP ヘルス モニタ動作に属する LSP ディスカバリ グループの動作ステータスを表示します。 （注） このコマンドは、LSP ディスカバリ オプションがイネーブルの場合にのみ適用できます。
ステップ 7	**show ip sla mpls-lsp-monitor neighbors** 例： `Device# show ip sla mpls-lsp-monitor neighbors`	（任意）LSP ヘルス モニタ動作によって検出された MPLS VPN BGP ネクスト ホップ ネイバーに関するルーティングおよび接続情報を表示します。
ステップ 8	**show ip sla mpls-lsp-monitor scan-queue** *operation-number* 例： `Device# show ip sla mpls-lsp-monitor scan-queue 1`	（任意）LSP ヘルス モニタ動作の特定の MPLS VPN に対する BGP ネクスト ホップ ネイバーの追加または削除に関する情報を表示します。
ステップ 9	**show ip sla mpls-lsp-monitor summary** [*operation-number* [**group** [*group-id*]]] 例： `Device# show ip sla mpls-lsp-monitor summary`	（任意）LSP ヘルス モニタ動作の BGP ネクスト ホップ ネイバーおよび LSP ディスカバリ グループの情報を表示します。 （注） このコマンドは、LSP ディスカバリ オプションがイネーブルの場合にのみ適用できます。
ステップ 10	**show ip sla statistics** [*operation-number*] [**details**] 例： `Device# show ip sla statistics 100001`	（任意）IP SLA のすべての動作または指定した動作の現在の動作ステータスおよび統計情報を表示します。

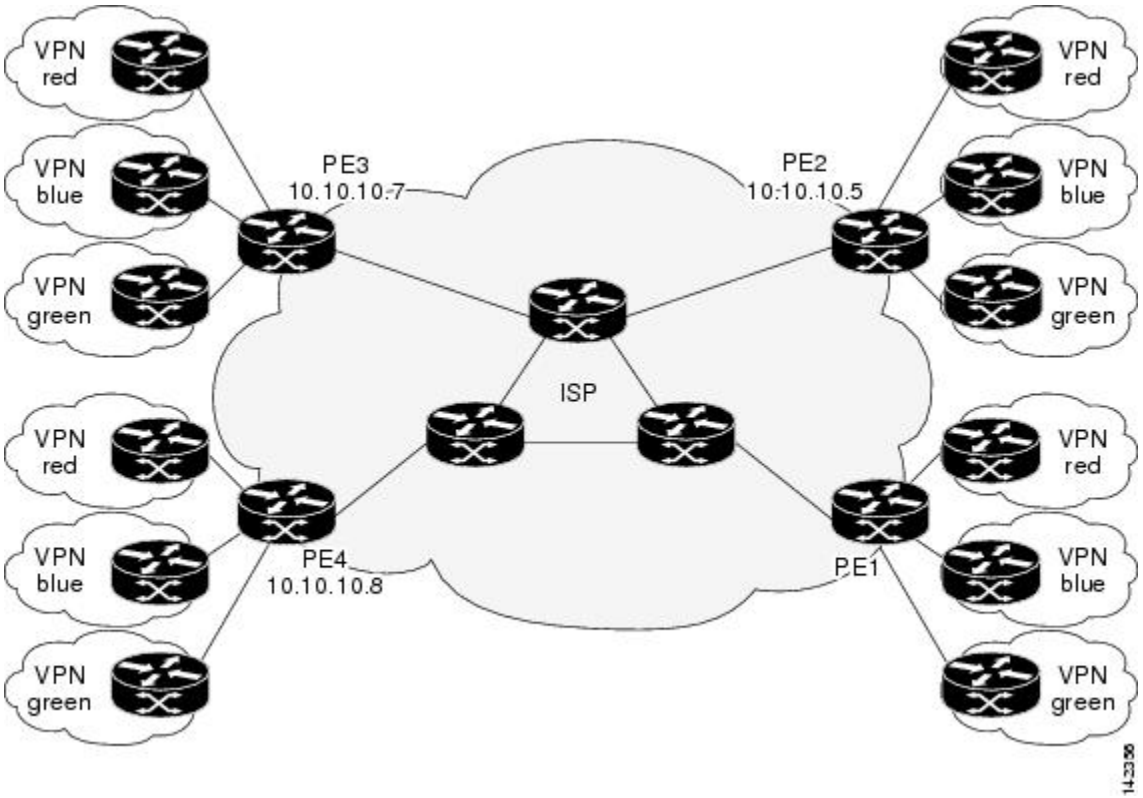
	コマンドまたはアクション	目的
		（注） このコマンドは、手動で設定された IP SLA 動作にのみ適用されます。
ステップ 11	**show ip sla statistics aggregated** [*operation-number*] [**details**] 例： `Device# show ip sla statistics aggregated 100001`	（任意）IP SLA のすべての動作または指定した動作の集約された統計エラーおよび分散情報を表示します。 （注） このコマンドは、手動で設定された IP SLA 動作にのみ適用されます。
ステップ 12	**show mpls discovery vpn** 例： `Device# show mpls discovery vpn`	（任意）MPLS VPN BGP ネクスト ホップ ネイバー探索プロセスに関するルーティング情報を表示します。

LSP ヘルス モニタの設定例

LSP ディスカバリなしの LSP ヘルス モニタの設定および検証例

次の図に、ISP 用の単純な VPN シナリオを示します。このネットワークは、3 つの VPN（red、blue、および green）に属している 4 台の PE デバイスとコア MPLS VPN で構成されます。デバイス PE1 から見ると、これらの VPN には、BGP ネクスト ホップ デバイス PE2（デバイス ID：10.10.10.5）、PE3（デバイス ID：10.10.10.7）、および PE4（デバイス ID：10.10.10.8）を経由してリモートで到達可能です。

図 *7: LSP* ヘルス モニタの例で使用されるネットワーク



次に、LSP ヘルス モニタを使用して PE 1（上の図を参照）上で動作パラメータ、予防的しきい値モニタリング、およびスケジューリング オプションを設定する例を示します。この例では、LSP ヘルス モニタ動作 1 に対して LSP ディスカバリ オプションがイネーブルになっています。動作 1 は、デバイス PE 1 に関連付けられたすべての VRF（red、blue、および green）で使用中のすべての BGP ネクスト ホップ ネイバー（PE2、PE3、および PE4）に対して IP SLA LSP ping 動作を自動的に作成するように設定されます。BGP ネクスト ホップ ネイバー プロセスがイネーブルにされ、有効ではなくなったルーティング エントリが BGP ネクスト ホップ ネイバー探索データベースから削除される間隔は 60 秒に設定されます。LSP ヘルス モニタがスキャン キューで BGP ネクスト ホップ ネイバーの更新をチェックする間隔は 1 分に設定されます。セカンダリ頻度オプションは、接続損失およびタイムアウトの両方のイベントでイネーブルになり、セカンダリ頻度は 10 秒に設定されます。接続損失イベントまたはタイムアウト イベントが 3 回連続して発生すると、予防的しきい値モニタリングの設定で指定したとおりに SNMP トラップ通知が送信されます。複数動作スケジューリングおよび IP SLA SNMP システム ロギング メッセージの生成がイネーブルにされます。

PE1 の設定

```
mpls discovery vpn interval 60
mpls discovery vpn next-hop
!
auto ip sla mpls-lsp-monitor 1
 type echo ipsla-vrf-all
 timeout 1000
```

```
 scan-interval 1
 secondary-frequency both 10
!
auto ip sla mpls-lsp-monitor reaction-configuration 1 react connectionLoss threshold-type
 consecutive 3 action-type trapOnly
auto ip sla mpls-lsp-monitor reaction-configuration 1 react timeout threshold-type
consecutive 3 action-type trapOnly
ip sla traps
snmp-server enable traps rtr
!
auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 start-time now
```

次に、PE1 での **show ip sla mpls-lsp-monitor configuration** コマンドの出力例を示します。

```
PE1# show ip sla mpls-lsp-monitor configuration 1
Entry Number : 1
Modification time   : *12:18:21.830 PDT Fri Aug 19 2005
Operation Type      : echo
Vrf Name            : ipsla-vrf-all
Tag                 :
EXP Value           : 0
Timeout(ms)         : 1000
Threshold(ms)       : 5000
Frequency(sec)      : Equals schedule period
LSP Selector        : 127.0.0.1
ScanInterval(min)   : 1
Delete Scan Factor  : 1
Operations List     : 100001-100003
Schedule Period(sec): 60
Request size        : 100
Start Time          : Start Time already passed
SNMP RowStatus      : Active
TTL value           : 255
Reply Mode          : ipv4
Reply Dscp Bits     :
Secondary Frequency : Enabled on Timeout
         Value(sec) : 10
Reaction Configs    :
    Reaction        : connectionLoss
    Threshold Type  : Consecutive
    Threshold Count : 3
    Action Type     : Trap Only
    Reaction        : timeout
    Threshold Type  : Consecutive
    Threshold Count : 3
    Action Type     : Trap Only
```

次に、PE1 での **show mpls discovery vpn** コマンドの出力例を示します。

```
PE1# show mpls discovery vpn
Refresh interval set to 60 seconds.
Next refresh in 46 seconds
Next hop 10.10.10.5 (Prefix: 10.10.10.5/32)
        in use by: red, blue, green
Next hop 10.10.10.7 (Prefix: 10.10.10.7/32)
        in use by: red, blue, green
Next hop 10.10.10.8 (Prefix: 10.10.10.8/32)
        in use by: red, blue, green
```

次に、PE1 での **show ip sla mpls-lsp-monitor neighbors** コマンドの出力例を示します。

```
PE1# show ip sla mpls-lsp-monitor neighbors
```

```
IP SLA MPLS LSP Monitor Database : 1
BGP Next hop 10.10.10.5 (Prefix: 10.10.10.5/32)  OK
  ProbeID: 100001 (red, blue, green)
BGP Next hop 10.10.10.7 (Prefix: 10.10.10.7/32)  OK
  ProbeID: 100002 (red, blue, green)
BGP Next hop 10.10.10.8 (Prefix: 10.10.10.8/32)  OK
  ProbeID: 100003 (red, blue, green)
```

次に、PE1 から PE4 への IP 接続が失われているときの **show ip sla mpls-lsp-monitor scan-queue 1** コマンドと **debug ip sla mpls-lsp-monitor** コマンドの出力例を示します。この出力は、PE4 に関連付けられている VPN（red、blue、および green）のそれぞれに対する接続損失が検出されたこと、およびその情報が LSP ヘルス モニタ スキャン キューに追加されたことを示しています。また、PE4 が有効な BGP ネクスト ホップ ネイバーではなくなっているので、PE4 の IP SLA 動作（Probe 10003）が削除されています。

```
PE1# show ip sla mpls-lsp-monitor scan-queue 1
Next scan Time after: 20 Secs
Next Delete scan Time after: 20 Secs
BGP Next hop    Prefix            vrf                              Add/Delete?
10.10.10.8      0.0.0.0/0         red                              Del(100003)
10.10.10.8      0.0.0.0/0         blue                             Del(100003)
10.10.10.8      0.0.0.0/0         green                            Del(100003)
PE1# debug ip sla mpls-lsp-monitor
IP SLAs MPLSLM debugging for all entries is on
*Aug 19 19:48: IP SLAs MPLSLM(1):Next hop 10.10.10.8 added in DeleteQ(1)
*Aug 19 19:49: IP SLAs MPLSLM(1):Removing vrf red from tree entry 10.10.10.8
*Aug 19 19:56: IP SLAs MPLSLM(1):Next hop 10.10.10.8 added in DeleteQ(1)
*Aug 19 19:56: IP SLAs MPLSLM(1):Next hop 10.10.10.8 added in DeleteQ(1)
*Aug 19 19:49: IP SLAs MPLSLM(1):Removing vrf blue from tree entry 10.10.10.8
*Aug 19 19:49: IP SLAs MPLSLM(1):Removing vrf green from tree entry 10.10.10.8
*Aug 19 19:49: IP SLAs MPLSLM(1):Removing Probe 100003
```

次に、PE1 から PE4 への IP 接続が復元されるときの **show ip sla mpls-lsp-monitor scan-queue 1** コマンドと **debug ip sla mpls-lsp-monitor** コマンドの出力例を示します。この出力は、PE4 に関連付けられている VPN（red、blue、および green）のそれぞれが検出されたこと、およびその情報が LSP ヘルス モニタ スキャン キューに追加されたことを示しています。また、PE4 が新たに検出された BGP ネクスト ホップ ネイバーになるので、PE4 の新しい IP SLA 動作（Probe 100005）が作成され、LSP ヘルス モニタ複数動作スケジュールに追加されています。PE4 は 3 つの VPN に属していますが、作成されている IP SLA 動作は 1 つだけです。

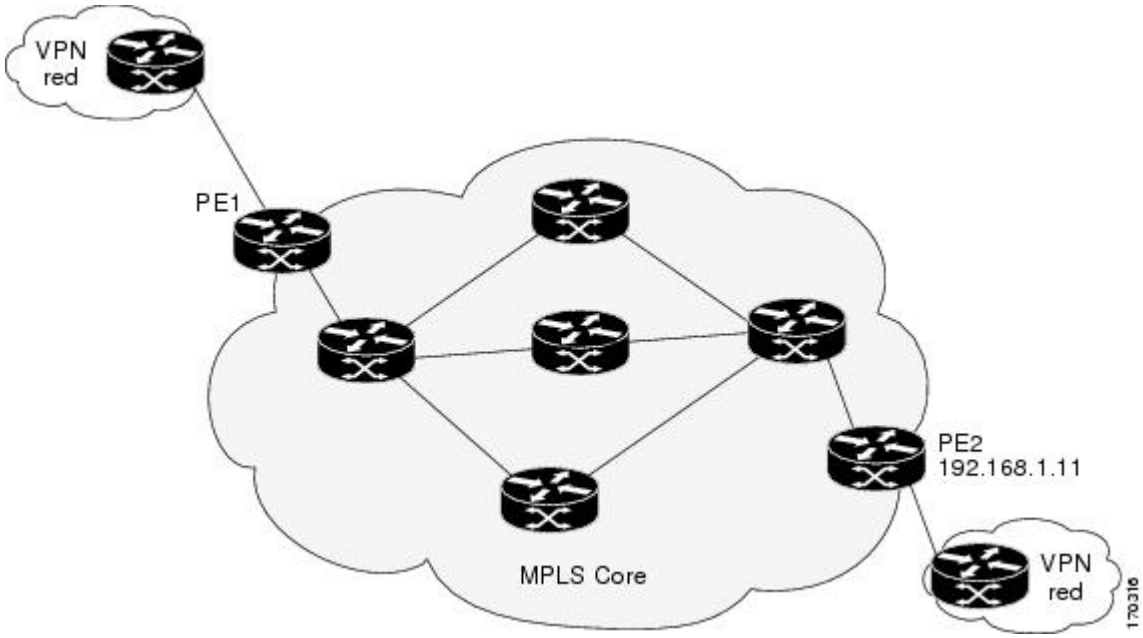
```
PE1# show ip sla mpls-lsp-monitor scan-queue 1
Next scan Time after: 23 Secs
Next Delete scan Time after: 23 Secs
BGP Next hop    Prefix            vrf                              Add/Delete?
10.10.10.8      10.10.10.8/32     red                              Add
10.10.10.8      10.10.10.8/32     blue                             Add
10.10.10.8      10.10.10.8/32     green                            Add
PE1# debug ip sla mpls-lsp-monitor
IP SLAs MPLSLM debugging for all entries is on
*Aug 19 19:59: IP SLAs MPLSLM(1):Next hop 10.10.10.8 added in AddQ
*Aug 19 19:59: IP SLAs MPLSLM(1):Next hop 10.10.10.8 added in AddQ
*Aug 19 19:59: IP SLAs MPLSLM(1):Next hop 10.10.10.8 added in AddQ
*Aug 19 19:59: IP SLAs MPLSLM(1):Adding vrf red into tree entry 10.10.10.8
*Aug 19 19:59: IP SLAs MPLSLM(1):Adding Probe 100005
*Aug 19 19:59: IP SLAs MPLSLM(1):Adding ProbeID 100005 to tree entry 10.10.10.8 (1)
*Aug 19 19:59: IP SLAs MPLSLM(1):Adding vrf blue into tree entry 10.10.10.8
*Aug 19 19:59: IP SLAs MPLSLM(1):Duplicate in AddQ 10.10.10.8
*Aug 19 19:59: IP SLAs MPLSLM(1):Adding vrf green into tree entry 10.10.10.8
```

```
*Aug 19 19:59: IP SLAs MPLSLM(1):Duplicate in AddQ 10.10.10.8
*Aug 19 19:59: IP SLAs MPLSLM(1):Added Probe(s) 100005 will be scheduled after 26 secs
over schedule period 60
```

LSP ディスカバリありの LSP ヘルス モニタの設定および検証例

次の図に、ISP 用の単純な VPN シナリオを示します。このネットワークは、red という名前の VPN に属している 2 台の PE デバイスとコア MPLS VPN で構成されます。デバイス PE1 から見て、デバイス PE2 に到達可能な等コスト マルチパスは 3 つあります。

図 *8 : LSP* ディスカバリありの *LSP* ヘルス モニタの例で使用されるネットワーク



次に、LSP ヘルス モニタを使用して PE 1（上の図を参照）上で動作パラメータ、予防的しきい値モニタリング、およびスケジューリング オプションを設定する例を示します。この例では、LSP ヘルス モニタ動作 100 に対して LSP ディスカバリ オプションがイネーブルにされます。動作 100 は、PE1 と PE2 の間のすべての等コスト マルチパスに対して IP SLA LSP ping 動作を自動的に作成するように設定されます。BGP ネクスト ホップ ネイバー プロセスがイネーブルにされ、有効ではなくなったルーティング エントリが BGP ネクスト ホップ ネイバー探索データベースから削除される間隔は 30 秒に設定されます。LSP ヘルス モニタがスキャン キューで BGP ネクスト ホップ ネイバーの更新をチェックする間隔は 1 分に設定されます。セカンダリ頻度オプションは、接続損失およびタイムアウトの両方のイベントでイネーブルになり、セカンダリ頻度は 5 秒に設定されます。エコー要求パケットの明示的な Null ラベル オプションがイネーブルにされます。LSP 再ディスカバリ期間は 3 分に設定されます。LSP ディスカバリ グループ ステータスが変化すると、予防的しきい値モニタリングの設定で指定したとおりに SNMP トラップ通知が送信されます。複数動作スケジューリングおよび IP SLA SNMP システム ロギング メッセージの生成がイネーブルにされます。

PE1 の設定

```
mpls discovery vpn next-hop
mpls discovery vpn interval 30
!
auto ip sla mpls-lsp-monitor 100
 type echo ipsla-vrf-all
 scan-interval 1
 secondary-frequency both 5
!
 path-discover
 force-explicit-null
 scan-period 3
!
auto ip sla mpls-lsp-monitor reaction-configuration 100 react lpd-group retry 3 action-type
 trapOnly
!
auto ip sla mpls-lsp-monitor schedule 100 schedule-period 30 start-time now
!
ip sla logging traps
snmp-server enable traps rtr
```

次に、PE1 での **show ip sla mpls-lsp-monitor configuration** コマンドの出力例を示します。

```
PE1# show ip sla mpls-lsp-monitor configuration
Entry Number : 100
Modification time   : *21:50:16.411 GMT Tue Jun 20 2006
Operation Type      : echo
Vrf Name            : ipsla-vrf-all
Tag                 :
EXP Value           : 0
Timeout(ms)         : 5000
Threshold(ms)       : 50
Frequency(sec)      : Equals schedule period
ScanInterval(min)   : 1
Delete Scan Factor  : 1
Operations List     : 100002
Schedule Period(sec): 30
Request size        : 100
Start Time          : Start Time already passed
SNMP RowStatus      : Active
TTL value           : 255
Reply Mode          : ipv4
Reply Dscp Bits     :
Path Discover       : Enable
    Maximum sessions          : 1
    Session Timeout(seconds)  : 120
    Base LSP Selector         : 127.0.0.0
    Echo Timeout(seconds)     : 5
    Send Interval(msec)       : 0
    Label Shimming Mode       : force-explicit-null
    Number of Stats Hours     : 2
    Scan Period(minutes)      : 3
Secondary Frequency : Enabled on Connection Loss and Timeout
         Value(sec) : 5
Reaction Configs    :
    Reaction        : Lpd Group
    Retry Number    : 3
    Action Type     : Trap Only
```

次に、PE1 での **show mpls discovery vpn** コマンドの出力例を示します。

```
PE1# show mpls discovery vpn
Refresh interval set to 30 seconds.
Next refresh in 4 seconds
Next hop 192.168.1.11 (Prefix: 192.168.1.11/32)
        in use by: red
```

次に、PE1 での **show ip sla mpls-lsp-monitor neighbors** コマンドの出力例を示します。

```
PE1# show ip sla mpls-lsp-monitor neighbors
IP SLA MPLS LSP Monitor Database : 100
BGP Next hop 192.168.1.11 (Prefix: 192.168.1.11/32)  OK Paths: 3
  ProbeID: 100001 (red)
```

次に、LSP ディスカバリ グループ 100001 に対する **show ip sla mpls-lsp-monitor lpd operational-state** コマンドの出力例を示します。

```
PE1# show ip sla mpls-lsp-monitor lpd operational-state
Entry number: 100001
MPLSLM Entry Number: 100
Target FEC Type: LDP IPv4 prefix
Target Address: 192.168.1.11
Number of Statistic Hours Kept: 2
Last time LPD Stats were reset: *21:21:18.239 GMT Tue Jun 20 2006
Traps Type: 3
Latest Path Discovery Mode: rediscovery complete
Latest Path Discovery Start Time: *21:59:04.475 GMT Tue Jun 20 2006
Latest Path Discovery Return Code: OK
Latest Path Discovery Completion Time(ms): 3092
Number of Paths Discovered: 3
Path Information :
Path   Outgoing   Lsp             Link  Conn  Adj             Downstream
Index  Interface  Selector        Type  Id    Addr            Label Stack     Status
1      Et0/0      127.0.0.8       90    0     10.10.18.30     21              OK
2      Et0/0      127.0.0.2       90    0     10.10.18.30     21              OK
3      Et0/0      127.0.0.1       90    0     10.10.18.30     21              OK
```

次に、LSP ディスカバリ グループ 100001 に対する **show ip sla mpls-lsp-monitor collection-statistics** コマンドの出力例を示します。

```
PE1# show ip sla mpls-lsp-monitor collection-statistics
Entry number: 100001
Start Time Index: *21:52:59.795 GMT Tue Jun 20 2006
Path Discovery Start Time: *22:08:04.507 GMT Tue Jun 20 2006
Target Destination IP address: 192.168.1.11
Path Discovery Status: OK
Path Discovery Completion Time: 3052
Path Discovery Minimum Paths: 3
Path Discovery Maximum Paths: 3
LSP Group Index: 100002
LSP Group Status: up
Total Pass: 36
Total Timeout: 0        Total Fail: 0
Latest Probe Status: 'up,up,up'
Latest Path Identifier: '127.0.0.8-Et0/0-21,127.0.0.2-Et0/0-21,127.0.0.1-Et0/0-21'
Minimum RTT: 280        Maximum RTT: 324        Average RTT: 290
```

次に、LSP ヘルス モニタ動作 100 に対する **show ip sla mpls-lsp-monitor summary** コマンドの出力例を示します。

```
PE1# show ip sla mpls-lsp-monitor summary 100
Index                    -  MPLS LSP Monitor probe index
Destination              -  Target IP address of the BGP next hop
Status                   -  LPD group status
LPD Group ID             -  Unique index to identify the LPD group
Last Operation Time      -  Last time an operation was attempted by
                            a particular probe in the LPD Group
Index  Destination     Status     LPD Group ID    Last Operation Time
100    192.168.1.11    up         100001          *22:20:29.471 GMT Tue Jun 20 2006
```

次に、LSP ディスカバリ グループ 100001 に対する **show ip sla mpls-lsp-monitor summary** コマンドの出力例を示します。

```
PE1#show ip sla mpls-lsp-monitor summary 100 group 100001
Group ID                 -  unique number to identify a LPD group
Lsp-selector             -  Unique 127/8 address used to identify a LPD
Last Operation status    -  Latest probe status
Last RTT                 -  Latest Round Trip Time
Last Operation Time      -  Time when the last operation was attempted
Group ID  Lsp-Selector    Status     Failures    Successes   RTT   Last Operation Time
100001    127.0.0.8       up         0           55          320   *22:20:29.471 GMT Tue
 Jun 20 2006
100001    127.0.0.2       up         0           55          376   *22:20:29.851 GMT Tue
 Jun 20 2006
100001    127.0.0.1       up         0           55          300   *22:20:30.531 GMT Tue
 Jun 20 2006
```

IP SLA LSP ping 動作の手動設定の例

次に、IP SLA LSP ping 動作を手動で設定し、スケジューリングする例を示します。

```
ip sla 1
mpls lsp ping ipv4 192.168.1.4 255.255.255.255 lsp-selector 127.1.1.1
frequency 120
secondary-frequency timeout 30
!
ip sla reaction-configuration 1 react connectionLoss threshold-type consecutive 3
action-type trapOnly
ip sla reaction-configuration 1 react timeout threshold-type consecutive 3 action-type
trapOnly
ip sla logging traps
!
ip sla schedule 1 start-time now life forever
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
MPLS LSP ディスカバリ管理ツール	『*Multiprotocol Label Switching Configuration Guide*』の「MPLS EM-MPLS LSP Multipath Tree Trace」の章

関連項目	マニュアル タイトル
標準 IP アクセス リストの設定	『*Security Configuration Guide: Securing the Data Plane* guide』の「Access Control Lists」の章
IP SLA の複数動作スケジューリング	『*Cisco IOS P SLAs Configuration Guide*』の「Configuring Multioperation Scheduling of IP SLAs Operations」の章
IP SLA の予防的しきい値モニタリング	『*Cisco IOS IP SLAs Configuration Guide*』の「Configuring Proactive Threshold Monitoring of IP SLAs Operations」の章
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
Cisco IOS IP SLA コマンド	『Cisco IOS IP SLAs Command Reference』

標準

標準	タイトル
draft-ietf-mpls-lsp-ping-09.txt	『Detecting MPLS Data Plane Failures』
draft-ietf-mpls-oam-frmwk-03.txt	『A Framework for MPLS Operations and Management (OAM)』
draft-ietf-mpls-oam-requirements-06.txt	『OAM Requirements for MPLS Networks』

MIB

MIB	MIB のリンク
CISCO-RTTMON-MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

テクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

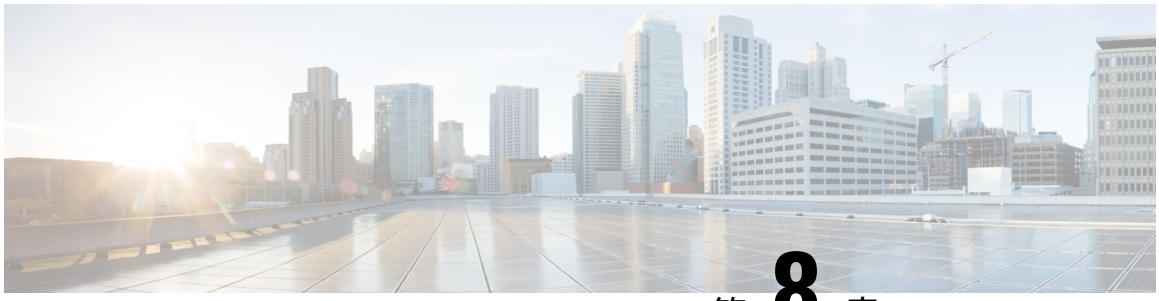
LSP ヘルス モニタ動作に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *15 : LSP* ヘルス モニタの機能情報

機能名	リリース	機能情報
IP SLA--LSP ヘルス モニタ		IP SLA LSP ヘルス モニタ機能により、レイヤ 3 MPLS VPN を予防的にモニタできます。
IP SLA--LSP ヘルス モニタ		この機能がすでに導入されていたソフトウェア リリースには、それ以前のリリースで導入されたコマンドライン インターフェイス（CLI）を置き換える新しい CLI が実装されました。
LSP ディスカバリありの IP SLA--LSP ヘルス モニタ		LSP ディスカバリ機能が追加されました。



第 8 章

VCCV 経由の MPLS 疑似回線用 IP SLA

このモジュールでは、疑似回線 ping 動作をスケジューリングし、SNMP トラップ経由でラウンドトリップ時間（RTT）、障害、および接続しきい値違反のモニタリングおよびアラートを提供するために、仮想回線接続検証（VCCV）によって MPLS 疑似回線（PWE3）用の IP サービス レベル契約（SLA）を設定する方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

VCCV を介した MPLS 擬似回線用 IP SLA に関する制限事項

LSP ディスカバリは、IP SLA VCCV 動作ではサポートされていません。

VCCV を介した MPLS 擬似回線用 IP SLA に関する情報

IP SLA VCCV 動作

IP SLA VCCV 動作は、MPLS ネットワーク経由の Pseudo-Wire Emulation Edge-to-Edge（PWE3）サービスに対する仮想回線接続性検証（VCCV）をサポートします。IP SLA VCCV 動作タイプは、**ping mpls pseudowire** コマンドに基づきます。このコマンドは、指定された宛先 PE ルータに一連の疑似回線 ping 動作を送信することにより、Any Transport over MPLS（AToM）仮想回線（VC）経由の MPLS LSP 接続をチェックします。

MPLS LSP 接続チェックが IP SLA VCCV 動作によって実行される場合（**pseudowire** キーワードを指定した **ping mpls** コマンドではない）、IP SLA 予防的しきい値モニタリング機能と複数動作スケジューリング機能を使用できます。

LSP ディスカバリ オプションは、IP SLA VCCV 動作をサポートしません。

LSP ヘルス モニタの予防的しきい値モニタリング

LSP ヘルス モニタの予防的しきい値モニタリング サポート機能では、ユーザ定義の応答条件（接続損失やタイムアウトなど）が満たされたときに、SNMP トラップ通知と Syslog メッセージをトリガーできます。LSP ヘルス モニタのしきい値モニタリング動作の設定方法は、標準的な IP SLA 動作の設定方法と同様です。

イネーブルにされた LSP ディスカバリ オプション

LSP ヘルス モニタの LSP ディスカバリ オプション動作がイネーブルにされている場合、次のいずれかのイベントが発生したときに SNMP トラップ通知を生成できます。

- 特定の BGP ネクスト ホップ ネイバーの LSP ディスカバリが失敗
- LSP ディスカバリ グループの動作ステータスが変化

特定の BGP ネクスト ホップ ネイバーに対する LSP ディスカバリが失敗する理由として、次のものが考えられます。

- BGP ネクスト ホップ ネイバーが LSP ディスカバリ要求に応答できる時間の期限切れ
- BGP ネクスト ホップ ネイバーに通じるすべてのパスに対してリターン コードが「Broken」または「Unexplorable」

次の表では、LSP ディスカバリ グループの動作ステータスが変化する条件を説明しています。LSP ディスカバリ グループの個々の IP SLA LSP ping 動作が実行されるたびに、戻りコードが生成されます。リターン コードの値と LSP ディスカバリ グループの現在のステータスに応じて、グループ ステータスは変化します。

表 *16 : LSP* ディスカバリ グループ ステータスが変化する条件

個々の IP SLA 動作のリターン コード	現在のグループ ステータス = UP	現在のグループ ステータス = PARTIAL	現在のグループ ステータス = DOWN
OK	グループ ステータスは変化しません。	グループ内のすべてのパスに対するリターン コードが OK の場合、グループ ステータスは UP に変化します。	グループ ステータスは PARTIAL に変化します。
Broken または Unexplorable	グループ ステータスは PARTIAL に変化します。	グループ内のすべてのパスに対するリターン コードが Broken または Unexplorable の場合、グループ ステータスは DOWN に変化します。	グループ ステータスは変化しません。

個々の IP SLA LSP ping 動作に対するリターン コードは、次のいずれかです。

- OK：LSP が正常に機能していることを示します。カスタマー VPN トラフィックは、このパスを経由して送信されます。
- Broken：LSP が壊れていることを示します。カスタマー VPN トラフィックは、このパスを経由して送信されず、場合によっては廃棄されます。
- Unexplorable：この PE ネイバーへの一部のパスが検出されていないことを示します。これは、LSP 上に中断がある場合や、LSP 選択に使用される 127/8 IP アドレスの数が足りなくなった場合になることがあります。

LSP ディスカバリ グループのステータスは、次のいずれかです。

- UNKNOWN：グループ ステータスがまだ決定されていないこと、およびグループに属しているパスが最初のテスト中であることを示します。この初期テストが完了すると、グループ ステータスは UP、PARTIAL、または DOWN に変化します。
- UP：グループ内のすべてのパスがアクティブで、動作の失敗は検出されていないことを示します。
- PARTIAL：グループ内のすべてではないが、1 つ以上のパスに対して動作の失敗が検出されていることを示します。
- DOWN：グループ内のすべてのパスに対して動作の失敗が検出されていることを示します。

セカンダリ頻度オプション

LSP ヘルス モニタ機能の導入により、セカンダリ頻度を指定できる新しいしきい値モニタリング パラメータが追加されています。特定のパスでセカンダリ頻度オプションが設定され、障害（接続損失やタイムアウトなど）が検出された場合、パスが再測定される頻度がセカンダリ頻度値（高速でのテスト）に増やされます。設定された応答条件が満たされると（連続する N 回

の接続損失、または連続する N 回のタイムアウトなど）、SNMP トラップおよび syslog メッセージが送信されて、測定頻度が元の頻度値に戻ります。

VCCM を介した MPLS 擬似回線用 IP SLA の設定方法

IP SLA VCCV 動作の手動設定とスケジューリング

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **mpls lsp ping pseudowire** *peer-ipaddr vc-id* [**source-ipaddr** *source-ipaddr*]
5. **exp** *exp-bits*
6. **frequency** *seconds*
7. **request-data-size** *bytes*
8. **secondary-frequency** {**both** | **connection-loss** | **timeout**} *frequency*
9. **tag** *text*
10. **threshold** *milliseconds*
11. **timeout** *milliseconds*
12. **exit**
13. **ip sla reaction-configuration** *operation-number* [**react** *monitored-element*] [**threshold-type** {**never** | **immediate** | **consecutive** [*consecutive-occurrences*] | **xofy** [*x-value y-value*] | **average** [*number-of-probes*]}] [**threshold-value** *upper-threshold lower-threshold*] [**action-type** {**none** | **trapOnly** | **triggerOnly** | **trapAndTrigger**}]
14. **ip sla logging traps**
15. **ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh* **:** *mm*[**:** *ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh* **:** *mm* **:** *ss*}] [**ageout** *seconds*] [**recurring**]
16. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `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。

	コマンドまたはアクション	目的
ステップ 3	**ip sla** *operation-number* 例： `Router(config)# ip sla 777`	IP SLA 動作の設定を開始し、IP SLA 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	**mpls lsp ping pseudowire** *peer-ipaddr vc-id* [**source-ipaddr** *source-ipaddr*] 例： `Router(config-ip-sla)# mpls lsp ping pseudowire 192.168.1.103 123 source-ipaddr 192.168.1.102`	IP SLA 動作を LSP 疑似配線 ping として設定し、VCCV コンフィギュレーション モードを開始します。
ステップ 5	**exp** *exp-bits* 例： 例： `Router(config-sla-vccv)# exp 5`	（任意）IP SLA 動作のエコー要求パケットのヘッダーの試験的フィールド値を指定します。
ステップ 6	**frequency** *seconds* 例： `Router(config-sla-vccv)# frequency 120`	（任意）指定した IP SLA 動作を繰り返す間隔を指定します。
ステップ 7	**request-data-size** *bytes* 例： `Router(config-sla-vccv)# request-data-size 200`	（任意）IP SLA 動作の要求パケットのプロトコル データ サイズを指定します。
ステップ 8	**secondary-frequency** {**both** | **connection-loss** | **timeout**} *frequency* 例： `Router(config-sla-vccv)# secondary-frequency connection-loss 10`	（任意）より高い測定頻度（セカンダリ頻度）を設定します。応答条件時に IP SLA 動作の測定頻度がこの値に変化します。
ステップ 9	**tag** *text* 例： `Router(config-sla-vccv)# tag testgroup`	（任意）IP SLA 動作のユーザ指定 ID を作成します。
ステップ 10	**threshold** *milliseconds* 例：	（任意）IP SLA 動作によって作成されるネットワーク モニタリング統計情報を計算するための上限しきい値を設定します。

	コマンドまたはアクション	目的
	例： `Router(config-sla-vccv)# threshold 6000`	
ステップ 11	**timeout** *milliseconds* 例： `Router(config-sla-vccv)# timeout 7000`	（任意）IP SLA 動作がその要求パケットからの応答を待機する時間を指定します。
ステップ 12	**exit** 例： `Router(config-sla-vccv)# exit`	VCCV コンフィギュレーション モードを終了し、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 13	**ip sla reaction-configuration** *operation-number* [**react** *monitored-element*] [**threshold-type** {**never** | **immediate** | **consecutive** [*consecutive-occurrences*] | **xofy** [*x-value y-value*] | **average** [*number-of-probes*]}] [**threshold-value** *upper-threshold lower-threshold*] [**action-type** {**none** | **trapOnly** | **triggerOnly** | **trapAndTrigger**}] 例： `Router(config)# ip sla reaction-configuration 777 react connectionLoss threshold-type consecutive 3 action-type traponly`	（任意）Cisco IOS IP SLA の制御下のイベントに基づいて発生する特定のアクションを設定します。
ステップ 14	**ip sla logging traps** 例： `Router(config)# ip sla logging traps`	（任意）IP SLA トラップ通知に固有の SNMP システム ロギング メッセージの生成をイネーブルにします。
ステップ 15	**ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh* **:** *mm*[**:** *ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh* **:** *mm* **:** *ss*}] [**ageout** *seconds*] [**recurring**] 例： `Router(config)# ip sla schedule 777 life forever start-time now`	IP SLA 動作のスケジューリング パラメータを設定します。
ステップ 16	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション サブモードを終了し、特権 EXEC モードに戻ります。

トラブルシューティングのヒント

debug ip sla trace コマンドおよび **debug ip sla error** コマンドを使用すると、VCCV 動作を介した個々の IP SLA PWE3 サービスに関する問題のトラブルシューティングに役立ちます。

次の作業

個々の IP SLA 動作の結果を表示するには、**show ip sla statistics** コマンドと **show ip sla statistics aggregated** コマンドを使用します。サービス レベル契約の基準に対応するフィールドの出力を確認すると、サービス メトリックが許容範囲内であるかどうかを判断する役に立ちます。

VCCM を介した MPLS 擬似回線用 IP SLA の設定例

IP SLA VCCV 動作の手動設定の例

次に、LSPヘルスモニタの予防的しきい値モニタリング機能および複数動作スケジューリング機能と組み合わせて IP SLA VCCV 動作を手動で設定する例を示します。

この例では、ID 123 の VC が、PE デバイスおよび IP アドレス 192.168.1.103 にあるそのピア間ですでに確立されています。

IP SLA VCCV 動作 777 は、動作パラメータと応答条件が設定された後、ただちに開始し、無期限に実行するようにスケジューリングされます。

```
ip sla 777
 mpls lsp ping pseudowire 192.168.1.103 123
  exp 5
  frequency 120
  secondary-frequency timeout 30
  tag testgroup
  threshold 6000
  timeout 7000
  exit
!
 ip sla reaction-configuration 777 react rtt threshold-value 6000 3000 threshold-type
immediate 3 action-type traponly
 ip sla reaction-configuration 777 react connectionLoss threshold-type immediate
action-type traponly
 ip sla reaction-configuration 777 react timeout threshold-type consecutive 3 action-type
 traponly
 ip sla logging traps
!
 ip sla schedule 777 life forever start-time now
 exit
```

RTT しきい値

threshold コマンドは、モニタされる疑似回線上で宣言される上昇しきい値の時間値として 6000 ミリ秒を設定しています。最初の **ip sla reaction-configuration** コマンドは、ラウンドトリップ時間が上限しきい値の 6000 ミリ秒または下限しきい値の 3000 ミリ秒に違反したら、ただちに SNMP ロギング トラップを送信するように指定しています。

接続の損失

2 番目の **ip sla reaction-configuration** コマンドは、モニタされる疑似回線に対して接続損失が発生したら、ただちに SNMP ロギング トラップを送信するように指定しています。

応答タイムアウト

timeout コマンドは、タイムアウトが宣言されるまでに VCCV 動作 777 が要求パケットの応答を待つ時間として 7000 秒を設定しています。**secondary-frequency** コマンドは、タイムアウトが発生したら、動作の繰り返しを 120 秒間隔（**frequency** コマンドを使用して指定された初期測定頻度）からより短い 30 秒間隔にして測定頻度を増やすように指定しています。3 番目の **ip sla reaction-configuration** コマンドは、3 回連続してタイムアウトが発生したら、SNMP ロギング トラップを送信するように指定しています。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
MPLS LSP ディスカバリ管理ツール	『*Multiprotocol Label Switching Configuration Guide*』の「MPLS EM-MPLS LSP Multipath Tree Trace」の章
標準 IP アクセス リストの設定	『*Security Configuration Guide: Securing the Data Plane* guide』の「Access Control Lists」の章
IP SLA の複数動作スケジューリング	『*Cisco IOS P SLAs Configuration Guide*』の「Configuring Multioperation Scheduling of IP SLAs Operations」の章
IP SLA の予防的しきい値モニタリング	『*Cisco IOS IP SLAs Configuration Guide*』の「Configuring Proactive Threshold Monitoring of IP SLAs Operations」の章
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
Cisco IOS IP SLA コマンド	『Cisco IOS IP SLAs Command Reference』

標準

標準	タイトル
draft-ietf-mpls-lsp-ping-09.txt	『Detecting MPLS Data Plane Failures』
draft-ietf-mpls-oam-frmwk-03.txt	『A Framework for MPLS Operations and Management (OAM)』
draft-ietf-mpls-oam-requirements-06.txt	『OAM Requirements for MPLS Networks』

MIB

MIB	MIB のリンク
CISCO-RTTMON-MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャセットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

テクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

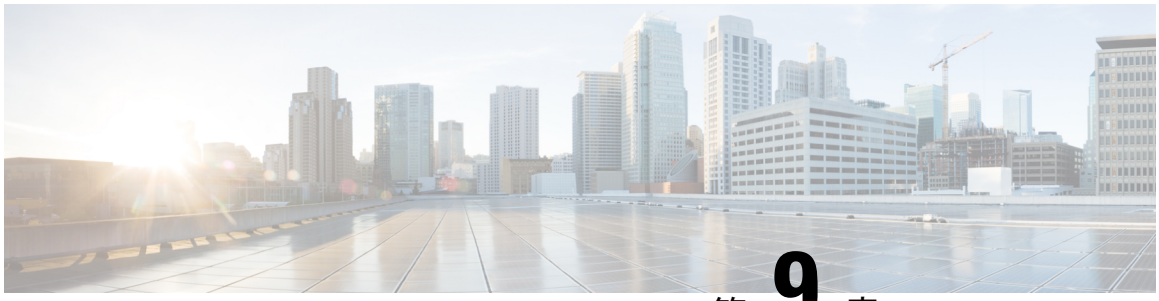
VCCM を介した MPLS PWE3 用 IP SLA の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *17 : VCCM* を介した *MPLS PWE3* 用 *IP SLA*

機能名	リリース	機能情報
VCCM 経由の MPLS 疑似回線（PWE3）用 IP SLA	12(33)SB 12.2(33)SRC 15.0(1)S Cisco IOS XE 3.1.0SG	MPLS ネットワーク経由の Pseudo-Wire Emulation Edge-to-Edge（PWE3）サービスに対する仮想回線接続性検証（VCCV）をサポートするために、IP SLA VCCV 動作が追加されました。



第 9 章

Metro-Ethernet 用 IP SLA の設定

このモジュールでは、サービス プロバイダー イーサネット ネットワークでネットワークのパフォーマンス メトリックを収集するように、Metro-Ethernet 用の IP サービス レベル契約（SLA）を設定する方法について説明します。IP SLA イーサネット動作で使用可能な統計情報の測定には、ラウンドトリップ時間、ジッタ（パケット間の遅延のばらつき）、パケット損失があります。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

Metro-Ethernet 用 IP SLA の前提条件

詳細なエラー レポーティングと診断情報を得るために、宛先デバイス上で IEEE 802.1ag 標準がサポートされていることが推奨されます。

Metro-Ethernet 用 IP SLA の制限事項

- メモリとパフォーマンスは、特定のイーサネット CFM メンテナンス ドメインおよびイーサネット仮想回線（EVC）または大量のメンテナンス エンドポイント（MEP）を持つ VLAN の影響を受ける場合があります。
- PW の冗長性の場合は、アクティブおよびバックアップ PW で 2 つの異なる CFM/Y1731 セッションが必要です。PW のスイッチオーバー後に、同じ mpid と Y1731 セッションが動作することは期待できません。
- Y1731 はポート mep ではサポートされません。
- CFM および Y1731 は、vpls のケースではサポートされず、タグなしの EFP でもサポートされていません。

Metro-Ethernet 用 IP SLA に関する情報

IP SLA イーサネット動作の基本

Metro-Ethernet 用 IP SLA により、IP SLA はイーサネット接続障害監理（CFM）機能と統合されます。イーサネット CFM は、サービス インスタンス単位のエンドツーエンド イーサネット レイヤ Operation, Administration, and Management（OAM）プロトコルです。

Metro-Ethernet 用 IP SLA 機能では、イーサネット CFM メンテナンス エンドポイント（MEP）間でイーサネット データ フレームを送受信することにより統計的な測定値を収集できます。IP SLA イーサネット動作のパフォーマンス メトリックは、送信元 MEP と宛先 MEP の間で測定されます。IP レイヤのパフォーマンス メトリックを提供する既存の IP SLA 動作とは異なり、IP SLA イーサネット動作はレイヤ 2 のパフォーマンス メトリックを提供します。

IP SLA イーサネット動作は、コマンドライン インターフェイス（CLI）または簡易ネットワーク管理プロトコル（SNMP）を使用して設定できます。

宛先 MEP 識別番号、メンテナンス ドメインの名前、および EVC または VLAN の識別子またはポート レベル オプションを指定することにより、個々のイーサネット ping 動作またはイーサネット ジッター動作を手動で設定できます。

また、特定のメンテナンス ドメインおよび EVC または VLAN 内のすべてのメンテナンス エンドポイントをイーサネット CFM データベースに照会する IP SLA 自動イーサネット動作（ping またはジッター）を設定するオプションもあります。IP SLA 自動イーサネット動作が設定されると、検出済みの MEP に基づいて個別のイーサネット ping 動作またはイーサネット ジッター動作が自動的に作成されます。自動イーサネット動作の稼働中にメンテナンス ドメインおよび EVC または VLAN に追加される適用可能な MEP に対してイーサネット ping 動作またはイーサネット ジッター動作を自動作成するために、IP SLA サブシステムとイーサネット CFM サブシステムの間には通知メカニズムが存在します。

Metro-Ethernet 用 IP SLA 機能では、IP SLA 動作の複数動作スケジューリングと、SNMP トラップ通知およびSyslogメッセージを使用した予防的しきい値違反モニタリングをサポートしています。

IP SLA イーサネット動作で測定された統計情報

IP SLA イーサネット動作でサポートされるネットワーク パフォーマンス メトリックは、既存の IP SLA 動作でサポートされるメトリックと同様です。IP SLA イーサネット ジッター動作でサポートされる統計的な測定値には次のものがあります。

- ラウンドトリップ時間の遅延
- 未処理のパケット
- パケット損失（ソースからターゲット、およびターゲットからソース）
- アウトオブシーケンス パケット、テールドロップされたパケット、および遅延パケット

Metro-Ethernet 用 IP SLA の設定方法

（注） 宛先デバイスで IP SLA Responder を設定する必要はありません。

送信元デバイスでのエンドポイント ディスカバリを伴う IP SLA 自動イーサネット動作の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla ethernet-monitor** *operation-number*
4. **type echo domain** *domain-name* {**evc** *evc-id* | **vlan** *vlan-id*} [**exclude-mpids** *mp-ids*]
5. **cos** *cos-value*
6. **owner** *owner-id*
7. **request-data-size** *bytes*
8. **tag** *text*
9. **threshold** *milliseconds*
10. **timeout** *milliseconds*
11. **end**
12. **show ip sla ethernet-monitor configuration** [*operation-number*]

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	**ip sla ethernet-monitor** *operation-number* 例： `Device(config)# ip sla ethernet-monitor 1`	IP SLA 自動イーサネット動作の設定を開始し、IP SLA イーサネット モニタ コンフィギュレーション モードに移行します。
ステップ 4	**type echo domain** *domain-name* {**evc** *evc-id* | **vlan** *vlan-id*} [**exclude-mpids** *mp-ids*] 例： `Device(config-ip-sla-ethernet-monitor)# type echo domain testdomain vlan 34`	• **domain** *domain-name*：作成したドメインの名前を指定します。 • **vlan***vlan-id*：1 つ以上のサービスプロバイダー VLAN ID を 1 ～ 4094 の範囲で指定します。2 つの VLAN ID をハイフンで区切って指定すると、その範囲の ID を指定できます。複数の VLAN ID をカンマで区切って指定することもできます。 • **exclude-mpids***mp-ids*：メンテナンス エンド ポイント ID（mpid）を入力します。ID は VLAN ごとに一意でなければいけません（サービス インスタンス）。指定できる範囲は 1 ～ 8191 です。 エコー動作の場合のみ：イーサネット ping 動作用の自動イーサネット動作を設定します。 （注） リリースによっては、**evc** *evc-id* キーワードと引数の組み合わせはこのコマンドで使用できない場合があります。
ステップ 5	**cos** *cos-value* 例： `Device(config-ip-sla-ethernet-params)# cos 2`	（任意）IP SLA イーサネット動作のサービス クラスを設定します。
ステップ 6	**owner** *owner-id* 例：	（任意）IP SLA 動作の簡易ネットワーク管理プロトコル（SNMP）所有者を設定します。

	コマンドまたはアクション	目的
	`Device(config-ip-sla-ethernet-params)# owner admin`	
ステップ 7	**request-data-size** *bytes* 例： `Device(config-ip-sla-ethernet-params)# request-data-size 64`	（任意）IP SLA イーサネット動作のデータ フレームのパディング サイズを設定します。 • IP SLA イーサネット ping 動作のデフォルト値は 66 バイトです。 • IP SLA イーサネット ジッター動作のデフォルト値は 51 バイトです。
ステップ 8	**tag** *text* 例： `Device(config-ip-sla-ethernet-params)# tag TelnetPollSever1`	（任意）IP SLA 動作のユーザ指定 ID を作成します。
ステップ 9	**threshold** *milliseconds* 例： `Device(config-ip-sla-ethernet-params)# threshold 10000`	（任意）IP SLA 動作によって作成されるネットワーク モニタリング統計情報を計算するための上限しきい値を設定します。
ステップ 10	**timeout** *milliseconds* 例： `Device(config-ip-sla-ethernet-params)# timeout 10000`	（任意）IP SLA 動作がその要求パケットからの応答を待機する時間を設定します。
ステップ 11	**end** 例： `Device(config-ip-sla-ethernet-params)# end`	特権 EXEC コンフィギュレーション モードを終了します。
ステップ 12	**show ip sla ethernet-monitor configuration** [*operation-number*] 例： `Device# show ip sla ethernet-monitor configuration 1`	（任意）すべての IP SLA 自動イーサネット動作または指定した自動イーサネット動作の構成時の設定を表示します。

次のタスク

トラップを生成する目的、または別の動作を開始する目的で、IP SLA 動作に予防的しきい値条件と反応トリガーを追加するには、「予防的しきい値モニタリングの設定」の項を参照してください。

送信元デバイスでの IP SLA イーサネット ping またはジッター動作の手動設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **ethernet echo mpid** *mp-id* **domain** *domain-name* {**evc** *evc-id* | **port** | **vlan** *vlan-id*}
5. **ethernet jitter mpid** *mp-id* **domain** *domain-name* {**evc** *evc-id* | **port** | **vlan** *vlan-id*} [**interval** *interframe-interval*] [**num-frames** *frames-number*]
6. **cos** *cos-value*
7. **frequency** *seconds*
8. **history** *history-parameter*
9. **owner** *owner-id*
10. **request-data-size** *bytes*
11. **tag** *text*
12. **threshold** *milliseconds*
13. **timeout** *milliseconds*
14. **end**
15. **show ip sla configuration** [*operation-number*]
16. **show ip sla application**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	**ip sla** *operation-number* 例： `Device(config)# ip sla 1`	IP SLA 動作の設定を開始し、IP SLA コンフィギュレーション モードに移行します。

	コマンドまたはアクション	目的
ステップ 4	**ethernet echo mpid** *mp-id* **domain** *domain-name* {**evc** *evc-id* | **port** | **vlan** *vlan-id*} 例： `Device(config-ip-sla)# ethernet echo mpid 23 domain testdomain vlan 34`	ping 動作専用：IP SLA 動作をイーサネット ping 動作として設定し、イーサネットエコーコンフィギュレーション モードを開始します。 （注） リリースによっては、**evc** evc-id キーワードと引数の組み合わせはこのコマンドで使用できない場合があります。
ステップ 5	**ethernet jitter mpid** *mp-id* **domain** *domain-name* {**evc** *evc-id* | **port** | **vlan** *vlan-id*} [**interval** *interframe-interval*] [**num-frames** *frames-number*] 例： `Device(config-ip-sla)# ethernet jitter mpid 23 domain testdomain evc testevc interval 20 num-frames 30`	ジッター動作専用：IP SLA 動作をイーサネットジッター動作として設定し、イーサネットジッターコンフィギュレーション モードを開始します。 （注） リリースによっては、**evc** evc-id キーワードと引数の組み合わせはこのコマンドで使用できない場合があります。
ステップ 6	**cos** *cos-value* 例： `Device(config-ip-sla-ethernet-echo)# cos 2`	（任意）IP SLA イーサネット動作のサービス クラスを設定します。 （注） これと残りの手順については、この例に示されている設定モードは、イーサネット エコー動作を設定するためのものです。ただし、コマンドはイーサネットジッターコンフィギュレーションモードで同じです。
ステップ 7	**frequency** *seconds* 例： `Device(config-ip-sla-ethernet-echo)# frequency 30`	（任意）指定した IP SLA 動作を繰り返す間隔を設定します。
ステップ 8	**history** *history-parameter* 例： `Device(config-ip-sla-ethernet-echo)# history hours-of-statistics-kept 3`	（任意）IP SLA 動作に関する統計履歴情報を収集するために使用するパラメータを指定します。
ステップ 9	**owner** *owner-id* 例： `Device(config-ip-sla-ethernet-echo)# owner admin`	（任意）IP SLA 動作の簡易ネットワーク管理プロトコル（SNMP）所有者を設定します。
ステップ 10	**request-data-size** *bytes* 例：	（任意）IP SLA イーサネット動作のデータ フレームのパディング サイズを設定します。

	コマンドまたはアクション	目的
	`Device(config-ip-sla-ethernet-echo)# request-data-size 64`	IP SLA イーサネット ping 動作のデフォルト値は 66 バイトです。IP SLA イーサネット ジッター動作のデフォルト値は 51 バイトです。
ステップ 11	**tag** *text* 例： `Device(config-ip-sla-ethernet-echo)# tag TelnetPollSever1`	（任意）IP SLA 動作のユーザ指定 ID を作成します。
ステップ 12	**threshold** *milliseconds* 例： `Device(config-ip-sla-ethernet-echo)# threshold 10000`	（任意）IP SLA 動作によって作成されるネットワーク モニタリング統計情報を計算するための上限しきい値を設定します。
ステップ 13	**timeout** *milliseconds* 例： `Device(config-ip-sla-ethernet-echo)# timeout 10000`	（任意）IP SLA 動作がその要求パケットからの応答を待機する時間を設定します。
ステップ 14	**end** 例： `Device(config-ip-sla-ethernet-echo)# end`	特権 EXEC モードに戻ります。
ステップ 15	**show ip sla configuration** [*operation-number*] 例： `Device# show ip sla configuration 1`	（任意）すべての IP SLA 動作または指定した IP SLA 動作に関する設定値を、すべてのデフォルト値を含めて表示します。
ステップ 16	**show ip sla application** 例： `Device# show ip sla application`	（任意）サポートされる IP SLA 機能に関するグローバル情報を表示します。

次のタスク

トラップを生成する目的、または別の動作を開始する目的で、IP SLA 動作に予防的しきい値条件と反応トリガーを追加するには、「予防的しきい値モニタリングの設定」の項を参照してください。

IP SLA 動作のスケジューリング

（注）
- スケジュールされるすべての IP SLA 動作がすでに設定されている必要があります。
- 複数動作スケジューラでランダム スケジューラ オプションを有効にしている場合を除き、動作グループにスケジュールされたすべての動作の頻度が同じでなければなりません。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかを実行します。
   - **ip sla ethernet-monitor schedule** *operation-number* **schedule-period** *seconds* [**frequency** [*seconds*]] [**start-time** {**after** *hh* **:** *mm* **:** *ss* | *hh* **:** *mm*[**:** *ss*] [*month day* | *day month*] | **now** | **pending**}]
   - **ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh* **:** *mm*[**:** *ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh* **:** *mm* **:** *ss*}] [**ageout** *seconds*] [**recurring**]
   - **ip sla group schedule** *group-operation-number operation-id-numbers* **schedule-period** *schedule-period-range* [**ageout** *seconds*] **frequency** *group-operation-frequency* [**life**{**forever** | *seconds*}] [**start-time**{*hh:mm*[*:ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh:mm:ss*}]
4. **exit**
5. **show ip sla group schedule**
6. **show ip sla configuration**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	次のいずれかを実行します。 • **ip sla ethernet-monitor schedule** *operation-number* **schedule-period** *seconds* [**frequency** [*seconds*]] [**start-time** {**after** *hh* **:** *mm* **:** *ss*	*hh* **:** *mm*[**:** *ss*] [*month day*	*day month*]	**now**	**pending**}] • **ip sla schedule** *operation-number* [**life** {**forever**	*seconds*}] [**start-time** {*hh* **:** *mm*[**:** *ss*] [*month day*		• 最初の例は、IP SLA 自動イーサネット動作のスケジューリング パラメータを設定する方法を示します。 • 2 番目の例は、個々の IP SLA 動作のスケジューリング パラメータを設定する方法を示します。

	コマンドまたはアクション	目的

	day month]	**pending**	**now**	**after** *hh* **:** *mm* **:** *ss*}] [**ageout** *seconds*] [**recurring**]
				• **ip sla group schedule** *group-operation-number operation-id-numbers* **schedule-period** *schedule-period-range* [**ageout** *seconds*] **frequency** *group-operation-frequency* [**life**{**forever**
					seconds}] [**start-time**{*hh:mm*[*:ss*] [*month day*	*day month*]	**pending**	**now**	**after** *hh:mm:ss*}]
									例：
									`Device(config)# ip sla ethernet-monitor schedule 10 schedule-period 60 start-time now`
									`Device(config)# ip sla schedule 1 start-time now life forever`
									`Device(config)# ip sla group schedule 1 3,4,6-9`
										• 3 番目の例は、複数動作スケジューラにスケジューリングされる IP SLA 動作グループ番号および動作番号の範囲を指定する方法を示します。

ステップ 4	**exit** **例**： `Device(config)# exit`	特権 EXEC モードを終了します。
ステップ 5	**show ip sla group schedule** **例**： `Device# show ip sla group schedule`	（任意）IP SLA グループ スケジュールの詳細を表示します。
ステップ 6	**show ip sla configuration** **例**： `Device# show ip sla configuration`	（任意）IP SLA 設定の詳細を表示します。

トラブルシューティングのヒント

debug ip sla trace コマンドおよび **debug ip sla error** コマンドを使用すると、個々の IP SLA イーサネット ping 動作やイーサネット ジッター動作に関する問題のトラブルシューティングに役立ちます。**debug ip sla ethernet-monitor** コマンドを使用すると、IP SLA 自動イーサネット動作に関する問題のトラブルシューティングに役立ちます。

次の作業

トラップを生成する目的（または別の動作を開始する目的）で、IP SLA 動作に予防的しきい値条件と反応トリガーを追加するには、「予防的しきい値モニタリングの設定」の項を参照してください。

operation)

IP SLA 動作の結果を表示し、内容を確認するには、**show ip sla statistics** コマンドを使用します。サービス レベル契約の基準に対応するフィールドの出力を確認し、サービス メトリックが許容範囲内であるかどうかを判断します。

Metro-Ethernet 用 IP SLA の設定例

エンドポイントディスカバリを伴うIP SLA自動イーサネット動作の例

次に、IP SLA 自動イーサネット動作の動作パラメータ、予防的しきい値モニタリング、およびスケジューリング オプションを示します。設定 A では、testdomain という名前のドメイン内で検出され、VLAN 識別番号が 34 のすべてのメンテナンス エンドポイントに対して IP SLA イーサネット ping 動作を自動的に作成するように、動作 10 が設定されます。設定 B では、testdomain という名前のドメイン内で検出され、EVC が testevc で識別されるすべてのメンテナンス エンドポイントに対して IP SLA イーサネット ping 動作を自動的に作成するように、動作 20 が設定されます。両方の設定において、接続損失イベントが 3 回連続して発生した場合、予防的しきい値モニタリングの設定では、SNMP トラップ通知が送信されるように指定されます。動作 10 および動作 20 のスケジュール期間は 60 秒で、両方の動作がただちに開始されるようにスケジューリングされます。

設定 A

```
ip sla ethernet-monitor 10
 type echo domain testdomain vlan 34
!
ip sla ethernet-monitor reaction-configuration 10 react connectionLoss threshold-type
consecutive 3 action-type trapOnly
!
ip sla ethernet-monitor schedule 10 schedule-period 60 start-time now
```

設定 B

```
ip sla ethernet-monitor 20
 type echo domain testdomain evc testevc
!
ip sla ethernet-monitor reaction-configuration 20 react connectionLoss threshold-type
consecutive 3 action-type trapOnly
!
ip sla ethernet-monitor schedule 20 schedule-period 60 start-time now
```

個々の IP SLA イーサネット ping 動作の例

次に、IP SLA イーサネット ping 動作の設定例を示します。設定 C では、メンテナンス エンドポイント識別番号が 23、メンテナンス ドメイン名が testdomain、VLAN 識別番号が 34 となっています。設定 D では、メンテナンス エンドポイント識別番号が 23、メンテナンス ドメイン名が testdomain、EVC が testevc と認識されています。両方の設定において、接続損失イベントが 3 回連続して発生した場合、予防的しきい値モニタリングの設定では、SNMP トラップ通知

が送信されるように指定されます。動作 1 と動作 5 は、ただちに開始するようにスケジューリングされます。

設定 C

```
ip sla 1
 ethernet echo mpid 23 domain testdomain vlan 34
!
ip sla reaction-configuration 1 react connectionLoss threshold-type consecutive 3
action-type trapOnly
!
ip sla schedule 1 start-time now
```

設定 D

```
ip sla 5
 ethernet echo mpid 23 domain testdomain evc testevc
!
ip sla reaction-configuration 5 react connectionLoss threshold-type consecutive 3
action-type trapOnly
!
ip sla schedule 5 start-time now
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
Cisco IOS IP SLA コマンド	『Cisco IOS IP SLAs Command Reference, All Releases』
Cisco IOS IP SLA：一般情報	『*Cisco IOS IP SLAs Configuration Guide*』の「Cisco IOS IP SLAs Overview」モジュール
IP SLA の複数動作スケジューリング	『*Cisco IOS P SLAs Configuration Guide*』の「Configuring Multioperation Scheduling of IP SLAs Operations」モジュール
IP SLA の予防的しきい値モニタリング	『*Cisco IOS IP SLAs Configuration Guide*』の「Configuring Proactive Threshold Monitoring of IP SLAs Operations」モジュール

MIB

MIB	MIB のリンク
CISCO-RTTMON-MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャセットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Metro-Ethernet 用 IP SLA の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *18 : Metro-Ethernet* 用 *IP SLA* の機能情報

機能名	リリース	機能情報
Metro-Ethernet 用 IP SLA		Metro-Ethernet 用 IP サービス レベル契約（SLA）機能を使用すると、イーサネットレイヤのネットワーク パフォーマンス メトリックを収集できます。IP SLA イーサネット動作で使用可能な統計情報の測定には、ラウンドトリップ時間、ジッタ（パケット間の遅延のばらつき）、パケット損失があります。

機能名	リリース	機能情報
IP SLA Metro-Ethernet 2.0（EVC）		Ethernet Virtual Circuit（EVC）のサポートが追加されました。
IP SLA Metro-Ethernet 3.0（CFM d8.1）		標準ベースの EOAM パフォーマンス モニタリング CFM ベース機能のサポートが追加されました。 Cisco IOS XE リリース 3.5S では、Cisco ASR 900 シリーズのサポートが追加されました。

第 10 章

IP SLA Metro-Ethernet 3.0（ITU-T Y.1731）動作の設定

このモジュールでは、イーサネットサービスの次のパフォーマンス測定値を収集するように、IP SLA Metro-Ethernet 3.0（ITU-T Y.1731）動作を設定する方法について説明します。

- イーサネット遅延
- イーサネット遅延変動
- イーサネット フレーム損失率

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

ITU-T Y.1731 動作の前提条件

Y.1731 パフォーマンス モニタリングが機能するためには、IEEE 準拠の接続障害監理（CFM）が設定され有効になっている必要があります。

（注） Y1731 はポート チャネル インターフェイスでサポートされます。

IP SLA Metro-Ethernet 3.0（ITU-T Y.1731）の制限事項

- IP SLA Metro-Ethernet 3.0（ITU-T Y.1731）動作に関するしきい値イベントのレポートおよびパフォーマンス統計情報の収集について SNMP がサポートされていません。

  SNMP は部分的にサポートされます。DM/LM の結果は、いくつかの属性についてポーリングすることができます。ただし、すべてのパラメータについての MIB サポートはありません。

- Continuity Check Message（CCM）ベースのデュアルエンド イーサネット フレーム損失の動作はサポートされていません。

- シングルエンドイーサネット動作では、パフォーマンス測定の統計情報は、送信者のイーサネット接続障害管理（CFM）メンテナンス エンド ポイント（MEP）が設定されているデバイスでのみ取得できます。

- フレームで設定された CoS 値が失われないように、L2 回線全体の EFPで **rewrite** を設定しないでください。Y.1731 フレームが特定の CoS 値でマークされている場合、CoS 値は保持されます。

- ルータ上のクロス接続による CFM は、 **control-word** が設定されている場合にのみ機能します。DM タイム スタンプを開始するには、リモート エンドのスイッチがオンになっていない場合は制御ワードのスイッチをオンにします。

- RX および TX のタイムスタンプのエラーを避けるために、Y1731 送信者は PTP マスターとし、Y1731 レスポンダは PTP スレーブとします。

- ローカル MEP はその過程の中で削除されるため、IM のオンライン挿入削除（OIR）またはルータのリロードの実行時に IP SLA Y1731 を再設定します。

- ルータのリロード後に **ip sla schedule** コマンドを発行すると、Y.1731 PM 測定値を設定するために遅延が観測される場合があります。

- dot1q タグには、サービス クラス（CoS）ビットが含まれています。これを IPSLA Y.1731 PM セッションで使用して、特定の CoS を持つパケットの遅延または損失をテストします。タグなしの EFP 上で EPM を使用する場合、この CoS はゼロ以外の値にすることはできません。

IP SLA Metro-Ethernet 3.0（ITU-T Y.1731）動作の設定方法

デュアルエンド イーサネット遅延または遅延変動動作の設定

記載されている順番でタスクを実行し、デュアルエンド動作を設定します。

（注） すでに設定済みのデュアルエンド動作で MEP 設定を削除するには、必ず設定時と逆の順序で MEP を削除してください。つまり、スケジューラを最初に削除してから、しきい値モニタリング設定を削除し、スケジューラを削除する前に送信元デバイスで送信者の MEP 設定、予防的しきい値モニタリング、および宛先デバイスで受信者の MEP 設定を削除します。

宛先デバイスでの受信者 MEP の設定

始める前に

一方向遅延または遅延変動を正確に測定するには、送信元デバイスと宛先デバイスとの間のクロック同期が必要です。送信元と宛先の両方のデバイスで、Precision Time Protocol（PTP）または Network Time Protocol（NTP）を設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **ethernet y1731 delay receive 1DM domain** *domain-name* {**evc** *evc-id* | **vlan** *vlan-id*} **cos** *cos* {**mpid** *source-mp-id* | **mac-address** *source-address*}
5. **aggregate interval** *seconds*
6. **distribution** {**delay** | **delay-variation**} **one-way** *number-of-bins boundary*[**,**...,*boundary*]
7. **frame offset** *offset-value*
8. **history interval** *intervals-stored*
9. **max-delay** *milliseconds*
10. **owner** *owner-id*
11. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `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 3	**ip sla** *operation-number* 例： `Router(config-term)# ip sla 501`	IP SLA 動作の設定を開始し、IP SLA 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	**ethernet y1731 delay receive 1DM domain** *domain-name* {**evc** *evc-id* | **vlan** *vlan-id*} **cos** *cos* {**mpid** *source-mp-id* | **mac-address** *source-address*} 例： `Router(config-ip-sla)# ethernet y1731 delay receive 1DM domain xxx evc yyy cos 3 mpid 101`	レスポンダで受信者の設定を開始し、IP SLA Y.1731 遅延コンフィギュレーションモードを開始します。 • このコマンドで設定された *source-mp-id* または *source-address* は、設定されている MEP での同等要素に対応します。 （注） CFM エラーがある場合は、mac-address を指定したセッションは非アクティブ化されません。
ステップ 5	**aggregate interval** *seconds* 例： `Router(config-sla-y1731-delay)# aggregate interval 900`	（任意）パフォーマンス測定が実施され、結果が保存される時間の長さを設定します。
ステップ 6	**distribution** {**delay** | **delay-variation**} **one-way** *number-of-bins boundary*[**,**...**,***boundary*] 例： `Router(config-sla-y1731-delay)# distribution delay-variation one-way 5 5000,10000,15000,20000,-1`	（任意）測定タイプを指定し、保持される統計情報配信の bin を設定します。
ステップ 7	**frame offset** *offset-value* 例： `Router(config-sla-y1731-delay)# frame offset 1`	（任意）遅延変動率を計算するための値を設定します。
ステップ 8	**history interval** *intervals-stored* 例： `Router(config-sla-y1731-delay)# history interval`	（任意）IP SLA イーサネット動作の有効期間中に保持する統計情報の配信数を設定します。

	コマンドまたはアクション	目的
	2	
ステップ 9	**max-delay** *milliseconds* 例： `Router(config-sla-y1731-delay)# max-delay 5000`	（任意）MEPがフレームを待つ時間を設定します。
ステップ 10	**owner** *owner-id* 例： `Router(config-sla-y1731-delay)# owner admin`	（任意）IP SLA 動作のオーナーを設定します。
ステップ 11	**end** 例： `Router(config-sla-y1731-delay)# end`	特権 EXEC モードに戻ります。

次のタスク

トラップを生成するために予防的しきい値条件と反応トリガーを追加するには、『*IP SLA* コンフィギュレーション ガイド』の「予防的しきい値モニタリングの設定」モジュールを参照してください。

この MEP への予防的しきい値モニタリングの設定が完了したら、「IP SLA 動作のスケジューリング」の項を参照して動作をスケジューリングします。

発信元ルータでの送信者 MEP の設定

始める前に

- 一方向遅延または遅延変動を正確に測定するには、送信元デバイスと宛先デバイスとの間のクロック同期が必要です。送信元と宛先の両方のデバイスで、Precision Time Protocol（PTP）または Network Time Protocol（NTP）を設定します。
- 送信者 MEP を設定する前に、予防的しきい値モニタリングなどの受信者 MEP を設定してスケジュールする必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla operation-number**

4. **ethernet y1731 delay 1DM domain domain-name** { **evc** *evc-id* | **vlan** *vlan-id*} { **mpid** *target-mp-id* | **mac-address** *target-address*} **cos** *cos* {**source** { **mpid** *source-mp-id* | **mac-address** *source-address*}}
5. **aggregate interval** *seconds*
6. **frame interval** *milliseconds*
7. **frame size** *bytes*
8. **history interval** *intervals-stored*
9. **owner** *owner-id*
10. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `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 3	**ip sla operation-number** 例： `Router(config)# ip sla 500`	IP SLA 動作の設定を開始し、IP SLA 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	**ethernet y1731 delay 1DM domain domain-name** { **evc** *evc-id*	**vlan** *vlan-id*} { **mpid** *target-mp-id*	**mac-address** *target-address*} **cos** *cos* {**source** { **mpid** *source-mp-id*	**mac-address** *source-address*}} 例： `Router(config-ip-sla)# ethernet y1731 delay 1DM domain xxx evc yyy mpid 101 cos 3 source mpid 100`	デュアルエンド イーサネット遅延動作の設定を開始し、IP SLA Y.1731 遅延コンフィギュレーション モードを開始します。 （注） CFM エラーがある場合は、mac-address を指定したセッションは非アクティブ化されません。
ステップ 5	**aggregate interval** *seconds* 例： `Router(config-sla-y1731-delay)# aggregate interval 900`	（任意）パフォーマンス測定が実施され、結果が保存される時間の長さを設定します。

	コマンドまたはアクション	目的
ステップ 6	**frame interval** *milliseconds* 例： `Router(config-sla-y1731-delay)# frame interval 100`	（任意）連続フレーム間の間隔を設定します。
ステップ 7	**frame size** *bytes* 例： `Router(config-sla-y1731-delay)# frame size 64`	（任意）フレームのパディング サイズを設定します。
ステップ 8	**history interval** *intervals-stored* 例： `Router(config-sla-y1731-delay)# history interval 2`	（任意）IP SLA イーサネット動作の有効期間中に保持する統計情報の配信数を設定します。
ステップ 9	**owner** *owner-id* 例： `Router(config-sla-y1731-delay)# owner admin`	（任意）IP SLA 動作のオーナーを設定します。
ステップ 10	**end** 例： `Router(config-sla-y1731-delay)# end`	特権 EXEC モードに戻ります。

次のタスク

トラップを生成するために予防的しきい値条件と反応トリガーを追加するには、『*IP SLA* コンフィギュレーション ガイド』の「予防的しきい値モニタリングの設定」モジュールを参照してください。

この MEP への予防的しきい値モニタリングの設定が完了したら、「IP SLA 動作のスケジューリング」の項を参照して動作をスケジューリングします。

シングルエンドイーサネット遅延または遅延変動動作用の送信者MEPの設定

送信元デバイスで送信者 MEP を設定するには、次の作業を実行します。

始める前に

- 一方向遅延または遅延変動を正確に測定するには、送信元デバイスと宛先デバイスとの間のクロック同期が必要です。送信元と宛先の両方のデバイスで、Precision Time Protocol（PTP）または Network Time Protocol（NTP）を設定します。

（注） 宛先デバイスのリモート（ターゲット）MEP に関する情報を表示するには、**show ethernet cfm maintenance-points remote** コマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **ethernet y1731 delay** {**DMM** | **DMMv1**} [**burst**] **domain** *domain-name* { **evc** *evc-id* | **vlan** *vlan-id*} { **mpid** *target-mp-id* | **mac-address** *target-address*} **cos** *cos* {**source** { **mpid** *source-mp-id* | **mac-address** *source-address*}}
5. **clock sync**
6. **aggregate interval** *seconds*
7. **distribution** {**delay** | **delay-variation**} **one-way** *number-of-bins boundary*[**,**...,*boundary*]
8. **frame interval** *milliseconds*
9. **frame offset** *offset-value*
10. **frame size** *bytes*
11. **history interval** *intervals-stored*
12. **max-delay** *milliseconds*
13. **owner** *owner-id*
14. **end**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	**ip sla** *operation-number* 例：	IP SLA 動作の設定を開始し、IP SLA コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device(config-term)# ip sla 10`	
ステップ 4	**ethernet y1731 delay** {**DMM** | **DMMv1**} [**burst**] **domain** *domain-name* { **evc** *evc-id* | **vlan** *vlan-id*} { **mpid** *target-mp-id* | **mac-address** *target-address*} **cos** *cos* {**source** { **mpid** *source-mp-id* | **mac-address** *source-address*}} 例： `Device(config-ip-sla)# ethernet y1731 delay dmm domain xxx evc yyy mpid 101 cos 4 source mpid 100`	シングルエンド イーサネット遅延動作の設定を開始し、IP SLA Y.1731 遅延コンフィギュレーション モードを開始します。 • 同時動作を設定するには、このコマンドで **DMMv1** キーワードを使用します。各同時動作に前述の2つの手順を繰り返し、単一の IP SLA 動作番号に追加します。同時動作は、特定の EVC、CoS、およびリモート MEP の組み合わせ、または特定のマルチポイント EVC の複数の MEP に対してサポートされています。 （注） CFM エラーがある場合は、mac-address を指定したセッションは非アクティブ化されません。
ステップ 5	**clock sync** 例： `Device(config-sla-y1731-delay)# clock sync`	（任意）エンド ポイントが同期されており、一方向遅延測定を計算する動作が許可されていることを示します。
ステップ 6	**aggregate interval** *seconds* 例： `Device(config-sla-y1731-delay)# aggregate interval 900`	（任意）パフォーマンス測定が実施され、結果が保存される時間の長さを設定します。
ステップ 7	**distribution** {**delay** | **delay-variation**} **one-way** *number-of-bins boundary*[**,...,***boundary*] 例： `Device(config-sla-y1731-delay)# distribution delay-variation one-way 5 5000, 10000,15000,20000,-1`	（任意）測定タイプを指定し、保持される統計情報配信の bin を設定します。
ステップ 8	**frame interval** *milliseconds* 例： `Device(config-sla-y1731-delay)# frame interval 100`	（任意）連続フレーム間の間隔を設定します。

	コマンドまたはアクション	目的
ステップ 9	**frame offset** *offset-value* 例： `Device(config-sla-y1731-delay)# frame offset 1`	（任意）遅延変動値を計算するための値を設定します。
ステップ 10	**frame size** *bytes* 例： `Device(config-sla-y1731-delay)# frame size 32`	（任意）フレームのパディング サイズを設定します。
ステップ 11	**history interval** *intervals-stored* 例： `Device(config-sla-y1731-delay)# history interval 2`	（任意）IP SLA イーサネット動作の有効期間中に保持する統計情報の配信数を設定します。
ステップ 12	**max-delay** *milliseconds* 例： `Device(config-sla-y1731-delay)# max-delay 5000`	（任意）MEPがフレームを待つ時間を設定します。
ステップ 13	**owner** *owner-id* 例： `Device(config-sla-y1731-delay)# owner admin`	（任意）IP SLA 動作のオーナーを設定します。
ステップ 14	**end** 例： `Device(config-sla-y1731-delay)# end`	特権 EXEC モードに戻ります。

次のタスク

トラップを生成するために予防的しきい値条件と反応トリガーを追加するには、『*IP SLA* コンフィギュレーション ガイド』の「予防的しきい値モニタリングの設定」モジュールを参照してください。

この動作への予防的しきい値モニタリングの設定が完了したら、「IP SLA 動作のスケジューリング」の項を参照して動作をスケジューリングします。

シングルエンド イーサネット フレーム損失率動作用の送信者 MEP の設定

（注） 宛先デバイスのリモート（ターゲット）MEPに関する情報を表示するには、**show ethernet cfm maintenance-points remote** コマンドを使用します。

送信元デバイスで送信者 MEP を設定するには、次の作業を実行します。

始める前に

- サービス クラス（CoS）レベルのモニタリングは、動作の両端のデバイスで **monitor loss counter** コマンドを使用して、イーサネット フレーム損失動作に関連付けられている MEP で有効にする必要があります。コマンド情報については、『*Cisco IOS Carrier Ethernet Command Reference*』を参照してください。設定情報の詳細については、「IP SLA Metro-Ethernet 3.0（ITU-T Y.1731）動作の設定例」の項を参照してください。

（注） Cisco IOS Y.1731 を実装することで、CoS 値（CoS または集約 CoS の場合）に関係なく、EVC でフレームのフレーム損失をモニタリングできます。設定情報の詳細については、「IP SLA Metro-Ethernet 3.0（ITU-T Y.1731）動作の設定例」の項を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **ethernet y1731 loss** {**LMM** | **SLM**} [**burst**] **domain** *domain-name* { **evc** *evc-id* | **vlan** *vlan-id*} { **mpid** *target-mp-id* | **mac-address** *target-address*} **CoS** *CoS* {**source** { **mpid** *source-mp-id* | **mac-address** *source-address*}}
5. **aggregate interval** *seconds*
6. **availability algorithm** {**sliding-window** | **static-window**}
7. **frame consecutive** *value*
8. **frame interval** *milliseconds*
9. **history interval** *intervals-stored*
10. **owner** *owner-id*
11. **exit**
12. **exit**
13. **exit**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	**ip sla** *operation-number* 例： `Device(config-term)# ip sla 11`	IP SLA 動作の設定を開始し、IP SLA 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	**ethernet y1731 loss** {**LMM** | **SLM**} [**burst**] **domain** *domain-name* { **evc** *evc-id* | **vlan** *vlan-id*} { **mpid** *target-mp-id* | **mac-address** *target-address*} **CoS** *CoS* {**source** { **mpid** *source-mp-id* | **mac-address** *source-address*}} 例： `Device(config-ip-sla)# ethernet y1731 loss LMM domain xxx vlan 12 mpid 34 CoS 4 source mpid 23`	シングルエンド イーサネット フレーム損失率動作の設定を開始し、IP SLA Y.1731 損失コンフィギュレーション モードを開始します。 • 同時動作を設定するには、このコマンドで**SLM** キーワードを使用します。各同時動作を単一の IP SLA 動作番号に追加するよう設定するには、前述の 2 つの手順を繰り返します。同時動作は、特定の EVC、CoS、およびリモート MEP の組み合わせ、または特定のマルチポイント EVC の複数の MEP に対してサポートされています。 （注） CFM エラーがある場合は、mac-address を指定したセッションは非アクティブ化されません。
ステップ 5	**aggregate interval** *seconds* 例： `Device(config-sla-y1731-loss)# aggregate interval 900`	（任意）のパフォーマンス測定が実施され、結果が保存される時間の長さを設定します。
ステップ 6	**availability algorithm** {**sliding-window** | **static-window**} 例： `Device(config-sla-y1731-loss)# availability`	（任意）使用されるアベイラビリティ アルゴリズムを指定します。

	コマンドまたはアクション	目的
	`algorithm static-window`	
ステップ 7	**frame consecutive** *value* 例： `Device(config-sla-y1731-loss)# frame consecutive 10`	（任意）アベイラビリティまたは非アベイラビリティのステータスを判断するために使用される連続測定の数を指定します。
ステップ 8	**frame interval** *milliseconds* 例： `Device(config-sla-y1731-loss)# frame interval 100`	（任意）連続フレーム間の間隔を設定します。
ステップ 9	**history interval** *intervals-stored* 例： `Device(config-sla-y1731-loss)# history interval 2`	（任意）IP SLA イーサネット動作の有効期間中に保持する統計情報の配信数を設定します。
ステップ 10	**owner** *owner-id* 例： `Device(config-sla-y1731-delay)# owner admin`	（任意）IP SLA 動作のオーナーを設定します。
ステップ 11	**exit** 例： `Device(config-sla-y1731-delay)# exit`	IP SLA コンフィギュレーション モードを終了します。
ステップ 12	**exit** 例： `Device(config-ip-sla)# 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 13	**exit** 例： `Device(config)# exit`	特権 EXEC モードに戻ります。

次のタスク

この MEP の設定が完了したら、「IP SLA 動作のスケジューリング」の項を参照して動作をスケジューリングします。

IP SLA 動作のスケジューリング

始める前に

- スケジュールされるすべての IP サービス レベル契約（SLA）動作がすでに設定されている必要があります。
- 複数動作グループでスケジュールされたすべての動作の頻度が同じでなければなりません。
- 複数動作グループに追加する 1 つ以上の動作 ID 番号のリストは、カンマ（,）を含めて最大 125 文字に制限する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します。
   - **ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {[*hh*:*mm*:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**]
   - **ip sla group schedule** *group-operation-number operation-id-numbers* { **schedule-period** *schedule-period-range* | **schedule-together**} [**ageout** *seconds*] **frequency** *group-operation-frequency* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm* [:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm* [:*ss*]}]
4. **end**
5. **show ip sla group schedule**
6. **show ip sla configuration**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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。

	コマンドまたはアクション	目的

ステップ 3	次のいずれかのコマンドを入力します。
	• **ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {[*hh*:*mm*:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**]
	• **ip sla group schedule** *group-operation-number operation-id-numbers* { **schedule-period** *schedule-period-range* | **schedule-together**} [**ageout** *seconds*] **frequency** *group-operation-frequency* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm* [:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm* [:*ss*]}]
	例：
	`Device(config)# ip sla schedule 10 life forever start-time now`
	`Device(config)# ip sla group schedule 10 schedule-period frequency`
	`Device(config)# ip sla group schedule 1 3,4,6-9 life forever start-time now`
	`Device(config)# ip sla schedule 1 3,4,6-9 schedule-period 50 frequency range 80-100`
		• 個々の IP SLA 動作のスケジューリング パラメータを設定します。
		• 複数動作スケジューラ用に IP SLA 動作グループ番号と動作番号の範囲を指定します。

ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	**show ip sla group schedule** 例： `Device# show ip sla group schedule`	（任意）IP SLA グループ スケジュールの詳細を表示します。
ステップ 6	**show ip sla configuration** 例： `Device# show ip sla configuration`	（任意）IP SLA 設定の詳細を表示します。

IP SLA Metro-Ethernet 3.0（ITU-T Y.1731）動作の設定例

例：デュアルエンドイーサネット遅延動作

次に、デュアルエンドイーサネット遅延または遅延変動動作用の、レスポンダデバイスでの受信者 MEP の設定（デフォルト値を含む）の出力例を示します。

```
Device# show ip sla configuration 501

IP SLAs Infrastructure Engine-III
Entry number: 501
Owner: admin
Tag:
Operation timeout (milliseconds): 5000
Ethernet Y1731 Delay Operation
Frame Type: 1DM
Domain: xxx
ReceiveOnly: TRUE
Evc: yyy
Local Mpid: 101
CoS: 3
   Max Delay: 5000
Threshold (milliseconds): 5000
.
.
.
Statistics Parameters
  Aggregation Period: 900
  Frame offset: 1
  Distribution Delay One-Way:
   Number of Bins 10
   Bin Boundaries: 5000,10000,15000,20000,25000,30000,35000,40000,45000,-1
  Distribution Delay-Variation One-Way:
   Number of Bins 10
   Bin Boundaries: 5000,10000,15000,20000,25000,30000,35000,40000,45000,-1
History
  Number of intervals: 2
```

次に、デュアルエンドIP SLAイーサネット遅延または遅延変動動作用の、送信者MEPの設定（デフォルト値を含む）の出力例を示します。

```
Device# show ip sla configuration 500

IP SLAs Infrastructure Engine-III
Entry number: 500
Owner:
Tag:
Operation timeout (milliseconds): 5000
Ethernet Y1731 Delay Operation
Frame Type: 1DM
Domain: yyy
ReceiveOnly: FALSE
Evc: xxx
Target Mpid: 101
Source Mpid: 100
CoS: 3
```

```
   Request size (Padding portion): 64
   Frame Interval: 1000
Threshold (milliseconds): 5000
.
.
.
Statistics Parameters
  Aggregation Period: 900
  Frame offset: 1
History
  Number of intervals: 22
```

例：フレーム遅延とフレーム遅延変動の測定設定

次の出力例は、パフォーマンス モニタリング セッション サマリーを示します。

```
Device# show ethernet cfm pm session summary

Number of Configured Session : 2
Number of Active Session: 2
Number of Inactive Session: 0
```

次の出力例は、アクティブなパフォーマンス モニタリング セッションを示します。

```
Device# show ethernet cfm pm session active

Display of Active Session
--------------------------------------------------------------------------------
EPM-ID   SLA-ID    Lvl/Type/ID/Cos/Dir     Src-Mac-address Dst-Mac-address
--------------------------------------------------------------------------------
 0     10           3/BD-V/10/2/Down     d0c2.8216.c9d7  d0c2.8216.27a3
 1     11           3/BD-V/10/3/Down     d0c2.8216.c9d7  d0c2.8216.27a3
Total number of Active Session: 2
```

```
Device# show ethernet cfm pm session db 0

--------------------------------------------------------------------------------
      TX Time FWD                   RX Time FWD
      TX Time BWD                   RX Time BWD              Frame Delay
      Sec:nSec                      Sec:nSec                  Sec:nSec
--------------------------------------------------------------------------------
Session ID: 0
********************************************************************************
       234:526163572                 245:305791416
       245:306761904                 234:527134653            0:593
********************************************************************************
       235:528900628                 246:308528744
       246:309452848                 235:529825333            0:601
********************************************************************************
       236:528882716                 247:308511128
       247:309450224                 236:529822413            0:601
********************************************************************************
       237:526578788                 248:306207432
       248:307157936                 237:527529885            0:593
********************************************************************************
       238:527052156                 249:306681064
       249:307588016                 238:527959717            0:609
********************************************************************************
       239:526625044                 250:306254200
       250:307091888                 239:527463325            0:593
********************************************************************************
```

```
        240:528243204                 251:307872648
        251:308856880                 240:529228021           0:585
```

例：シングルエンド イーサネット遅延動作用の送信者 MEP

次に、シングルエンドIP SLAイーサネット遅延動作用の、送信者MEPの設定（デフォルト値を含む）の出力例を示します。

```
Router# show ip sla configuration 10

IP SLAs Infrastructure Engine-III
Entry number: 10
Owner:
Tag:
Operation timeout (milliseconds): 5000
Ethernet Y1731 Delay Operation
Frame Type: DMM
Domain: xxx
Vlan: yyy
Target Mpid: 101
Source Mpid: 100
CoS: 4
   Max Delay: 5000
   Request size (Padding portion): 64
   Frame Interval: 1000
   Clock: Not In Sync
Threshold (milliseconds): 5000
.
.
.
Statistics Parameters
  Aggregation Period: 900
  Frame offset: 1
  Distribution Delay Two-Way:
   Number of Bins 10
   Bin Boundaries: 5000,10000,15000,20000,25000,30000,35000,40000,45000,-1
  Distribution Delay-Variation Two-Way:
   Number of Bins 10
   Bin Boundaries: 5000,10000,15000,20000,25000,30000,35000,40000,45000,-1
History
  Number of intervals: 2
```

例：シングルエンド イーサネット フレーム損失動作用の送信者 MEP

次に、現在の開始時刻を設定した基本シングルエンドIP SLA イーサネット フレーム損失率動作における、送信者MEPの設定（デフォルト値を含む）の出力を示します。

```
Router# show ip sla configuration 11

IP SLAs Infrastructure Engine-III
Entry number: 11
Owner:
Tag:
Operation timeout (milliseconds): 5000
Ethernet Y1731 Loss Operation
Frame Type: LMM
```

```
Domain: xxx
Vlan: 12
Target Mpid: 34
Source Mpid: 23
CoS: 4
   Request size (Padding portion): 0
   Frame Interval: 1000
Schedule:
   Operation frequency (seconds): 60  (not considered if randomly scheduled)
   Next Scheduled Start Time: Start Time already passed
   Group Scheduled : FALSE
   Randomly Scheduled : FALSE
   Life (seconds): 3600
   Entry Ageout (seconds): never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): ActiveThreshold (milliseconds): 5000
Statistics Parameters
  Aggregation Period: 900
  Frame consecutive: 10
  Availability algorithm: static-window
History
  Number of intervals: 2
```

IP SLA Metro-Ethernet 3.0（ITU-T Y.1731）動作に関するその他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
Cisco IOS キャリア イーサネットのコマンド	『Cisco IOS Carrier Ethernet Command Reference』
Cisco IOS IP SLA コマンド	『Cisco IOS IP SLAs Command Reference』
イーサネット CFM	『*Cisco IOS* キャリア イーサネット コンフィギュレーション ガイド』の「サービス プロバイダー ネットワークでのイー サネット CFM の設定」モジュール

関連項目	マニュアル タイトル
Network Time Protocol（NTP）	『*Cisco IOS Network Management Configuration Guide*』の「Configuring NTP」モジュール
Cisco IOS IP SLA の予防的しきい値モニタリング	『*Cisco IOS IP SLAs Configuration Guide*』の「Configuring Proactive Threshold Monitoring of IP SLAs Operations」モジュール

標準および RFC

標準/RFC	タイトル
ITU-T Y.1731	『*OAM functions and mechanisms for Ethernet-based networks*』
このマニュアルに記載された機能によってサポートされている特定の RFC はありません。	--

MIB

MIB	MIB のリンク
• CISCO-IPSLA-ETHERNET-MIB • CISCO-RTTMON-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IP SLA Metro-Ethernet 3.0（ITU-T Y.1731）動作の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *19 : IP SLA Metro-Ethernet 3.0（ITU-T Y.1731）* の機能情報

機能名	リリース	機能情報
ETH-SLM（Y1731 のイーサネット合成損失測定）の IP SLA サポート		Y.1731 パフォーマンス モニタリング（PM）では、イーサネットのフレーム遅延、フレーム遅延変動、フレーム損失、フレーム スループット測定など、標準的なイーサネット PM 機能が提供されます。これらの測定は ITU-T Y-1731 標準で規定され、メトロ イーサネット フォーラム（MEF）標準グループによって認定されています。
既存の IPSLA MIB を介した Y1731 MIB サポート		SNMP を使用した IP SLA Metro-Ethernet 3.0（ITU-T Y.1731）動作に関するしきい値イベントのレポートおよびパフォーマンス統計情報の収集に対するサポートが追加されました。

第 11 章

IPSLA Y1731 オンデマンド動作および同時動作

このモジュールでは、設定権限のないユーザにリアルタイムのイーサネット サービス トラブルシューティングを有効にするために、IPSLA Y1731 SLM 機能拡張を設定する方法について説明します。この機能は、特権EXECモードで単一コマンドを発行することで実行可能なオンデマンド合成損失測定（SLM）動作をサポートしています。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

ITU-T Y.1731 動作の前提条件

Y.1731 パフォーマンス モニタリングが機能するためには、IEEE 準拠の接続障害監理（CFM）が設定され有効になっている必要があります。

（注） Y1731 はポート チャネル インターフェイスでサポートされます。

IP SLA Y.1731 オンデマンド動作に関する制約事項

- SNMP は、オンデマンド動作に関するしきい値イベントのレポートおよびパフォーマンス統計情報の収集についてサポートされていません。
- オンデマンド動作の統計情報は保存されず、統計情報の履歴と集約機能によってサポートされていません。

IP SLA Y.1731 オンデマンド動作および同時動作に関する情報

IPSLA Y1731 SLM 機能拡張

IPSLA Y1731 SLM 機能拡張機能でのオンデマンド IP SLA 合成損失測定（SLM）動作によって、ユーザは、設定アクセスせずに、イーサネット サービスのリアルタイム トラブルシューティングを実行できます。オンデマンド動作には、動作を即座に作成して実行するダイレクトモードと、以前に設定された動作を開始して実行する参照モードの2つの動作モードがあります。

- ダイレクトモードでは、単一コマンドを使用して、ある範囲のサービス クラス（CoS）値がバックグラウンドで即座に実行されるように複数の疑似動作を作成することができます。特権 EXEC モードで単一コマンドを使用して、ダイレクト オンデマンド動作に対しフレーム サイズ、間隔、頻度、および期間を指定できます。コマンドを発行した後、ダイレクト オンデマンド動作が即座に開始および実行されます。
- 参照モードでは、1 つ以上のすでに設定済みの動作を、異なる CoS 値を使用して異なる宛先、または同じ宛先に対して開始できます。特権 EXEC コマンドを発行すると、予防的動作の実行中であってもバックグラウンドで起動および動作する疑似版の予防的動作が作成されます。

- オンデマンド動作が完了すると、統計的な出力がコンソールに表示されます。オンデマンド動作の統計情報は保存されず、統計情報の履歴と集約機能によってサポートされません。
- オンデマンド動作が完了し、統計情報が処理されると、ダイレクトおよび参照オンデマンド動作は削除されます。予防的動作は削除されず、参照モードで再び実行するために引き続き使用可能です。

同時動作は、すべてが同じ動作 ID 番号で設定され同時に実行する動作のグループで構成されます。同時動作は、特定のイーサネット仮想回線（EVC）、CoS、およびリモート メンテナンス エンド ポイント（MEP）の組み合わせ、または遅延や損失測定の場合は特定のマルチポイント EVC の複数の MEP に対してサポートされています。同時イーサネット フレーム遅延測定（ETH-DM）の合成フレームが動作中に送信されることを指定するために、新しいキーワードが適切なコマンドに追加されました。

IPSLA Y.1731 SLM 機能拡張機能では、同時動作、一方向デュアルエンド、シングルエンド遅延および遅延変動動作、シングルエンド損失動作に対するバースト モードもサポートしています。集約インターバル中に PDU 送信のバーストをサポートするために、新しいキーワードが適切なコマンドに追加されました。監視対象のサービスの最大値は 30 分ごとに 50 で、平均は 2 時間ごとに 25 サービスです。

IP SLA Y.1731 オンデマンド動作および同時動作の設定方法

送信者 MEP でのダイレクト オンデマンド動作の設定

始める前に

サービス クラス（CoS）レベルのモニタリングは、動作の両端のデバイスで **monitor loss counter** コマンドを使用して、イーサネット フレーム損失動作に関連付けられている MEP で有効にする必要があります。コマンド情報については、『*Cisco IOS Carrier Ethernet Command Reference*』を参照してください。設定情報の詳細については、「IP SLA Metro-Ethernet 3.0（ITU-T Y.1731）動作の設定例」の項を参照してください。

（注） Cisco IOS Y.1731 を実装することで、CoS 値（CoS または集約 CoS の場合）に関係なく、EVC でフレーム損失をモニタリングできます。設定情報の詳細については、「IP SLA Metro-Ethernet 3.0（ITU-T Y.1731）動作の設定例」の項を参照してください。

手順の概要

1. **enable**

2. **ip sla on-demand ethernet** {**DMMv1** | **SLM**} **domain** *domain-name* { **evc** *evc-id* | **vlan** *vlan-id*} { **mpid** *target-mp-id* | **mac-address** *target-address*} **cos** *cos* {**source** { **mpid** *source-mp-id* | **mac-address** *source-address*}} {**continuous** [**interval** *milliseconds*] | **burst** [**interval** *milliseconds*] [**number** *number-of-frames*] [**frequency** *seconds*]} [**size** *bytes*] **aggregation** *seconds* { **duration** *seconds* | **max** *number-of-packets*}

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**ip sla on-demand ethernet** {**DMMv1**	**SLM**} **domain** *domain-name* { **evc** *evc-id*	**vlan** *vlan-id*} { **mpid** *target-mp-id*	**mac-address** *target-address*} **cos** *cos* {**source** { **mpid** *source-mp-id*	**mac-address** *source-address*}} {**continuous** [**interval** *milliseconds*]	**burst** [**interval** *milliseconds*] [**number** *number-of-frames*] [**frequency** *seconds*]} [**size** *bytes*] **aggregation** *seconds* { **duration** *seconds*	**max** *number-of-packets*} 例： `Device# ip sla on-demand ethernet SLM domain xxx vlan 12 mpid 34 cos 4 source mpid 23 continuous aggregation 10 duration 60`	ダイレクトモードでオンデマンド動作を作成し、実行します。 • 同時オンデマンド動作を作成して実行するには、**DMMv1** キーワードを使用してこのコマンドを設定します。 • 動作の終了後に、統計出力がコンソールに投稿されます。 • 実行する各オンデマンド動作にこの手順を繰り返します。 • オンデマンド動作が完了し、統計情報が処理されると、動作は削除されます。

送信者 MEP での参照オンデマンド動作の設定

（注） オンデマンド動作が完了し、統計情報が処理されると、オンデマンドバージョンの動作は削除されます。

始める前に

- 参照されるシングルエンドおよび同時イーサネット遅延、または遅延変動、およびフレーム損失動作を設定する必要があります。『*IP SLA* コンフィギュレーション ガイド』の「IP SLA Metro-Ethernet 3.0（ITU-T Y.1731）動作の設定」モジュールを参照してください。

手順の概要

1. **enable**

2. **ip sla on-demand ethernet** [**dmmv1** | **slm**] *operation-number* { **duration** *seconds* | **max** *number-of-packets*

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**ip sla on-demand ethernet** [**dmmv1**	**slm**] *operation-number* { **duration** *seconds*	**max** *number-of-packets* 例： `Device# ip sla on-demand ethernet slm 11 duration 38`	バックグラウンドで参照されている動作の偽の動作を作成し、実行します。 • 動作の終了後に、統計出力がコンソールに投稿されます。 • 実行する各オンデマンド動作にこの手順を繰り返します。

送信者 MEP での IP SLA Y.1731 同時動作の設定

同時イーサネット遅延、遅延変動、およびフレーム損失動作を設定するには、『IP SLA コンフィギュレーション ガイド』の「IP SLA Metro-Ethernet 3.0（ITU-T Y.1731）動作の設定」モジュールを

参照してください。

IP SLA Y.1731 オンデマンド動作および同時動作の設定例

例：ダイレクト モードのオンデマンド動作

```
Device# ip sla on-demand ethernet SLM domain xxx vlan 10 mpid 3 cos 1 source mpid 1
continuous aggregation 35 duration 38

Loss Statistics for Y1731 Operation 2984884426
Type of operation: Y1731 Loss Measurement
Latest operation start time: *20:17:41.535 PST Wed May 16 2012
Latest operation return code: OK
Distribution Statistics:


Interval 1
 Start time:  *20:17:41.535 PST Wed May 16 2012
 End time:  *20:18:16.535 PST Wed May 16 2012
 Number of measurements initiated: 35
 Number of measurements completed: 35
 Flag: OK
```

```
Forward
  Number of Observations 3
  Available indicators: 0
  Unavailable indicators: 3
  Tx frame count: 30
  Rx frame count: 30
    Min/Avg/Max - (FLR % ): 0:9/000.00%/0:9
  Cumulative - (FLR % ): 000.00%
  Timestamps forward:
    Min - *20:18:10.586 PST Wed May 16 2012
    Max - *20:18:10.586 PST Wed May 16 2012
Backward
  Number of Observations 3
  Available indicators: 0
  Unavailable indicators: 3
  Tx frame count: 30
  Rx frame count: 30
    Min/Avg/Max - (FLR % ): 0:9/000.00%/0:9
  Cumulative - (FLR % ): 000.00%
  Timestamps backward:
    Min - *20:18:10.586 PST Wed May 16 2012
    Max - *20:18:10.586 PST Wed May 16 2012
Loss Statistics for Y1731 Operation 2984884426
Type of operation: Y1731 Loss Measurement
Latest operation start time: *20:17:41.535 PST Wed May 16 2012
Latest operation return code: OK
Distribution Statistics:


Interval 1
 Start time:  *20:17:41.535 PST Wed May 16 2012
 End time:  *20:18:16.535 PST Wed May 16 2012
 Number of measurements initiated: 35
 Number of measurements completed: 35
 Flag: OK

Forward
  Number of Observations 3
  Available indicators: 0
  Unavailable indicators: 3
  Tx frame count: 30
  Rx frame count: 30
    Min/Avg/Max - (FLR % ): 0:9/000.00%/0:9
  Cumulative - (FLR % ): 000.00%
  Timestamps forward:
    Min - *20:18:10.586 PST Wed May 16 2012
    Max - *20:18:10.586 PST Wed May 16 2012
Backward
  Number of Observations 3
  Available indicators: 0
  Unavailable indicators: 3
  Tx frame count: 30
  Rx frame count: 30
    Min/Avg/Max - (FLR % ): 0:9/000.00%/0:9
  Cumulative - (FLR % ): 000.00%
  Timestamps backward:
    Min - *20:18:10.586 PST Wed May 16 2012
    Max - *20:18:10.586 PST Wed May 16 2012
```

例：参照モードのオンデマンド動作

```
Device(config)# ip sla 11
Device(config-ip-sla)# ethernet y1731 loss SLM domain xxx vlan 10 mpid 3 cos 1 source
mpid 1
Device(config-sla-y1731-loss)# end
Device# ip sla on-demand ethernet slm 11 duration 38

Loss Statistics for Y1731 Operation 2984884426
Type of operation: Y1731 Loss Measurement
Latest operation start time: *20:17:41.535 PST Wed May 16 2012
Latest operation return code: OK
Distribution Statistics:


Interval 1
 Start time:  *20:17:41.535 PST Wed May 16 2012
 End time:  *20:18:16.535 PST Wed May 16 2012
 Number of measurements initiated: 35
 Number of measurements completed: 35
 Flag: OK

Forward
  Number of Observations 3
  Available indicators: 0
  Unavailable indicators: 3
  Tx frame count: 30
  Rx frame count: 30
    Min/Avg/Max - (FLR % ): 0:9/000.00%/0:9
  Cumulative - (FLR % ): 000.00%
  Timestamps forward:
    Min - *20:18:10.586 PST Wed May 16 2012
    Max - *20:18:10.586 PST Wed May 16 2012
Backward
  Number of Observations 3
  Available indicators: 0
  Unavailable indicators: 3
  Tx frame count: 30
  Rx frame count: 30
    Min/Avg/Max - (FLR % ): 0:9/000.00%/0:9
  Cumulative - (FLR % ): 000.00%
  Timestamps backward:
    Min - *20:18:10.586 PST Wed May 16 2012
    Max - *20:18:10.586 PST Wed May 16 2012
Loss Statistics for Y1731 Operation 2984884426
Type of operation: Y1731 Loss Measurement
Latest operation start time: *20:17:41.535 PST Wed May 16 2012
Latest operation return code: OK
Distribution Statistics:


Interval 1
 Start time:  *20:17:41.535 PST Wed May 16 2012
 End time:  *20:18:16.535 PST Wed May 16 2012
 Number of measurements initiated: 35
 Number of measurements completed: 35
 Flag: OK

Forward
  Number of Observations 3
  Available indicators: 0
  Unavailable indicators: 3
```

```
  Tx frame count: 30
  Rx frame count: 30
    Min/Avg/Max - (FLR % ): 0:9/000.00%/0:9
  Cumulative - (FLR % ): 000.00%
  Timestamps forward:
    Min - *20:18:10.586 PST Wed May 16 2012
    Max - *20:18:10.586 PST Wed May 16 2012
Backward
  Number of Observations 3
  Available indicators: 0
  Unavailable indicators: 3
  Tx frame count: 30
  Rx frame count: 30
    Min/Avg/Max - (FLR % ): 0:9/000.00%/0:9
  Cumulative - (FLR % ): 000.00%
  Timestamps backward:
    Min - *20:18:10.586 PST Wed May 16 2012
    Max - *20:18:10.586 PST Wed May 16 2012
```

IP SLA 再設定シナリオ

IP SLA 再設定シナリオ

IP SLA は、以下のシナリオの場合には再設定する必要があります。

- **service instance ethernet** コマンドを使用して、インターフェイスでイーサネット サービス インスタンスがディセーブルになっている。
- **no cfm mep domain** *domain-name* **mpid** *mpid* コマンドを使用して、ローカル MEP が削除されている。
- **default interface** コマンドを使用して、インターフェイスの設定がデフォルト値にリセットされている。
- **no interface** コマンドを使用して、インターフェイスの設定が削除されている。
- **no ethernet cfm global** および **no ethernet cfm ieee** コマンドを使用して、イーサネット接続障害管理（CFM）の展開がディセーブルになっている。

IP SLA Y.1731 オンデマンド動作および同時動作に関するその他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
Cisco IOS キャリア イーサネットのコマンド	『Cisco IOS Carrier Ethernet Command Reference』
Cisco IOS IP SLA コマンド	『Cisco IOS IP SLAs Command Reference』
ITU-T Y.1731 用イーサネット CFM	『*Carrier Ethernet Configuration Guide*』の「ITU-T Y.1731 Performance Monitoring in a Service Provider Network」モジュール
イーサネット動作	『*IP SLA* コンフィギュレーション ガイド』の「IP SLA Metro-Ethernet 3.0（ITU-T Y.1731）動作の設定」モジュール
Network Time Protocol（NTP）	『*Network Management Configuration Guide*』の「Configuring NTP」モジュール

標準および RFC

標準/RFC	タイトル
ITU-T Y.1731	『*OAM functions and mechanisms for Ethernet-based networks*』

MIB

MIB	MIB のリンク
• CISCO-IPSLA-ETHERNET-MIB • CISCO-RTTMON-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャセットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

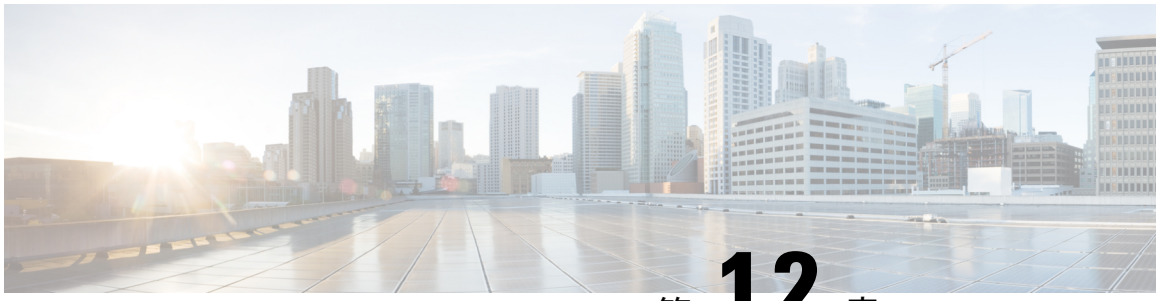
IP SLA Y.1731 オンデマンド動作および同時動作に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *20 : IP SLA Y.1731* オンデマンド動作および同時動作に関する機能情報

機能名	リリース	機能情報
IPSLA Y1731 SLM 機能拡張		この機能拡張により、ネットワークのイーサネット サービスのトラブルシューティング目的で、以前にスケジュールされた動作から独立して、オンデマンド合成損失測定（SLM）動作を実行できます。 次のコマンドが導入または変更されました。**ethernet y1731 delay**、**ethernet y1737 loss**、**ip sla on-demand ethernet**



第 12 章

IP SLA UDP エコー動作の設定

このモジュールでは、IP サービス レベル契約（SLA）ユーザデータグラム プロトコル（UDP）エコー動作を設定して、シスコ デバイスと IPv4 または IPv6 を使用するデバイスとのエンドツーエンド応答時間をモニタする方法について説明します。UDP エコーの精度は、宛先シスコデバイスで Cisco IP SLA Responder を使用することによって向上します。このモジュールでは、UDP エコー動作の結果を表示して分析し、UDP アプリケーションのパフォーマンスを測定する方法についても説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

IP SLA UDP エコー動作に関する制約事項

RFC 862 のエコー プロトコルをサポートするネットワーキング デバイスであれば使用できますが、シスコのネットワーキング デバイスを宛先デバイスとして使用することを推奨します。

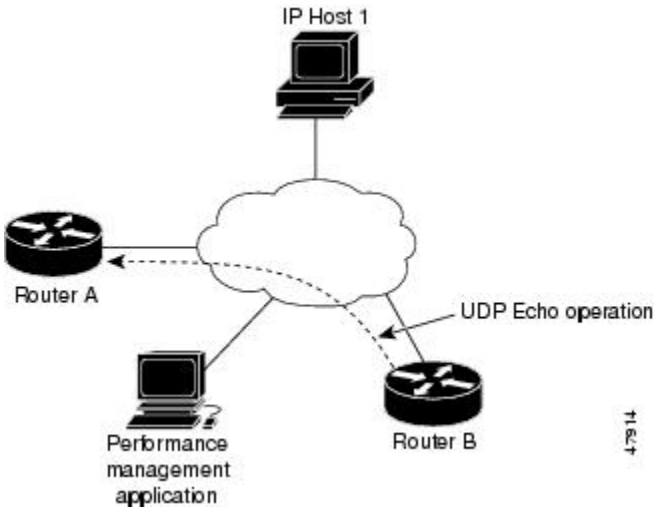
IP SLA UDP エコー動作に関する情報

UDP エコー動作

UDP エコー動作は、シスコ デバイスと IP を使用するデバイスとの間でエンドツーエンド応答時間を測定します。UDP は、多くの IP サービスで使用されるトランスポート層（レイヤ 4）インターネット プロトコルです。UDP エコーは応答時間を測定し、エンドツーエンドの接続をテストするために使用されます。

次の図では、デバイス A が IP SLA Responder として設定され、デバイス B が送信元 IP SLA デバイスとして設定されています。

図 *9 : UDP* エコー動作



デバイス B から宛先デバイス（デバイス A）に UDP エコー要求メッセージを送信してから、デバイス A からの UDP エコー応答を受信するまでの時間を測定することで、応答時間（ラウンドトリップ時間）が算出されます。UDP エコーの精度は、デバイス A（宛先のシスコ デバイス）で IP SLA レスポンダを使用することによって向上します。宛先デバイスがシスコ デバイスの場合、IP SLA は指定した任意のポート番号に UDP データグラムを送信します。シスコ デバイスを使用する場合、UDP エコー動作における IP SLA Responder の使用は任意です。シスコ以外のデバイスに IP SLA Responder を設定することはできません。

ラウンドトリップ遅延時間を測定し、シスコおよびシスコ以外のデバイス両方への接続をテストすることによって、ビジネスクリティカルなアプリケーションに関する問題をトラブルシューティングする際に、UDP エコー動作の結果が役立つことがあります。

IP SLA UDP エコー動作の設定方法

宛先デバイスでの IP SLA Responder の設定

（注） Responderでは、送信元に対して固定ポートを設定しないでください。Responderが送信元に対して固定ポートを設定すると、パケットが正常に（タイムアウトまたはパケット損失の問題が発生せずに）送信されたとしても、ジッター値はゼロになります。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します。
   - **ip sla responder**
   - **ip sla responder udp-echo ipaddress** *ip-address* **port** *port***vrf** *vrf*
4. **end**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	次のいずれかのコマンドを入力します。
	• **ip sla responder**
	• **ip sla responder udp-echo ipaddress** *ip-address* **port** *port***vrf** *vrf*
	例：
	`Device(config)# ip sla responder`
	`Device(config)# ip sla responder udp-echo ipaddress 192.0.2.132 port 5000 vrf vrf1`
		（任意）送信元からの制御メッセージに応じて、シスコ デバイスにおける IP SLA Responder 機能を一時的にイネーブルにします。
		（任意：送信元でプロトコル制御がディセーブルである場合にのみ必須です。）指定の IP アドレス、ポート、および VRF で、IP SLA Responder の機能をイネーブルにします。
		• プロトコル制御は、デフォルトでイネーブルになっています。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

送信元デバイスでの UDP エコー動作の設定

次のいずれかの作業のみを実行します。

送信元デバイスでの基本 UDP エコー動作の設定

始める前に

IP SLA Responder を使用する場合は、このタスクを開始する前に「宛先デバイスでの IP SLA Responder の設定」の項を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **udp-echo** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*} **source-port** *port-number*] [**control** {**enable** | **disable**}]
5. **data-pattern** *hex value*
6. **frequency** *seconds*
7. **end**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	**ip sla** *operation-number* 例： `Device(config)# ip sla 10`	IP SLA 動作の設定を開始し、IP SLA コンフィギュレーション モードに移行します。

	コマンドまたはアクション	目的
ステップ 4	**udp-echo** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*} **source-port** *port-number*] [**control** {**enable** | **disable**}] 例： `Device(config-ip-sla)# udp-echo 172.29.139.134 5000`	UDP エコー動作を定義し、IP SLA UDP コンフィギュレーション モードを開始します。 • 送信元デバイスとターゲットデバイスの両方で IP SLA 制御プロトコルをディセーブルにする場合のみ **control disable** キーワードの組み合わせを使用します。
ステップ 5	**data-pattern** *hex value* 例： `Device(config-ip-sla-udp)# data-pattern FFFFFFFF`	（任意）データ パターンの 16 進数値を設定します。 指定できる範囲は 0 ～ FFFFFFFF です。
ステップ 6	**frequency** *seconds* 例： `Device(config-ip-sla-udp)# frequency 30`	（任意）指定した IP SLA 動作を繰り返す間隔を設定します。
ステップ 7	**end** 例： `Device(config-ip-sla-udp)# end`	特権 EXEC モードに戻ります。

次のタスク

トラップを生成する目的、または別の動作を開始する目的で、IP SLA 動作に予防的しきい値条件と反応トリガーを追加するには、「予防的しきい値モニタリングの設定」の項を参照してください。

送信元デバイスでのオプション パラメータを使用した UDP エコー動作の設定

始める前に

この動作で IP SLA Responder を使用している場合、宛先デバイスで Responder を設定する必要があります。「宛先デバイスでの IP SLA Responder の設定」を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **udp-echo** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*} **source-port** *port-number*] [**control** {**enable** | **disable**}]
5. **history buckets-kept** *size*
6. **data-pattern** *hex-pattern*

7. **history distributions-of-statistics-kept** *size*
8. **history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*]
9. **history filter** {**none** | **all** | **overThreshold** | **failures**}
10. **frequency** *seconds*
11. **history hours-of-statistics-kept** *hours*
12. **history lives-kept** *lives*
13. **owner** *owner-id*
14. **request-data-size** *bytes*
15. **history statistics-distribution-interval** *milliseconds*
16. **tag** *text*
17. **threshold** *milliseconds*
18. **timeout** *milliseconds*
19. 次のいずれかを実行します。
    - **tos** *number*
    - **traffic-class** *number*
20. **flow-label** *number*
21. **verify-data**
22. **exit**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	**ip sla** *operation-number* 例： `Device(config)# ip sla 10`	IP SLA 動作の設定を開始し、IP SLA コンフィギュレーション モードに移行します。
ステップ 4	**udp-echo** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*} **source-port** *port-number*] [**control** {**enable** | **disable**}] 例： `Device(config-ip-sla)# udp-echo 172.29.139.134 5000`	UDP エコー動作を定義し、IP SLA UDP コンフィギュレーション モードを開始します。 • 送信元デバイスとターゲット デバイスの両方で IP SLA 制御プロトコルをディセーブルにする場合のみ **control disable** キーワードの組み合わせを使用します。

	コマンドまたはアクション	目的
ステップ 5	**history buckets-kept** *size* 例： `Device(config-ip-sla-udp)# history buckets-kept 25`	（任意）IP SLA 動作のライフタイム中に保持する履歴バケット数を設定します。
ステップ 6	**data-pattern** *hex-pattern* 例： `Device(config-ip-sla-udp)# data-pattern`	（任意）データ破損のテストのために IP SLA 動作のデータ パターンを指定します。
ステップ 7	**history distributions-of-statistics-kept** *size* 例： `Device(config-ip-sla-udp)# history distributions-of-statistics-kept 5`	（任意）IP SLA 動作中にホップ単位で保持する統計情報の配信数を設定します。
ステップ 8	**history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*] 例： `Device(config-ip-sla-udp)# history enhanced interval 900 buckets 100`	（任意）IP SLA 動作に対する拡張履歴収集をイネーブルにします。
ステップ 9	**history filter** {**none** | **all** | **overThreshold** | **failures**} 例： `Device(config-ip-sla-udp)# history filter failures`	（任意）IP SLA 動作の履歴テーブルに格納する情報のタイプを定義します。
ステップ 10	**frequency** *seconds* 例： `Device(config-ip-sla-udp)# frequency 30`	（任意）指定した IP SLA 動作を繰り返す間隔を設定します。
ステップ 11	**history hours-of-statistics-kept** *hours* 例： `Device(config-ip-sla-udp)# history hours-of-statistics-kept 4`	（任意）IP SLA 動作の統計情報を保持する時間数を設定します。
ステップ 12	**history lives-kept** *lives* 例： `Device(config-ip-sla-udp)# history lives-kept 2`	（任意）IP SLA 動作の履歴テーブルに格納するライフ数を設定します。

	コマンドまたはアクション	目的
ステップ 13	**owner** *owner-id* 例： `Device(config-ip-sla-udp)# owner admin`	（任意）IP SLA 動作の簡易ネットワーク管理プロトコル（SNMP）所有者を設定します。
ステップ 14	**request-data-size** *bytes* 例： `Device(config-ip-sla-udp)# request-data-size 64`	（任意）IP SLA 動作の要求パケットのペイロードにおけるプロトコル データ サイズを設定します。
ステップ 15	**history statistics-distribution-interval** *milliseconds* 例： `Device(config-ip-sla-udp)# history statistics-distribution-interval 10`	（任意）IP SLA 動作で維持する各統計情報の配信間隔を設定します。
ステップ 16	**tag** *text* 例： `Device(config-ip-sla-udp)# tag TelnetPollServer1`	（任意）IP SLA 動作のユーザ指定 ID を作成します。
ステップ 17	**threshold** *milliseconds* 例： `Device(config-ip-sla-udp)# threshold 10000`	（任意）IP SLA 動作によって作成されるネットワーク モニタリング統計情報を計算するための上限しきい値を設定します。
ステップ 18	**timeout** *milliseconds* 例： `Device(config-ip-sla-udp)# timeout 10000`	（任意）IP SLA 動作がその要求パケットからの応答を待機する時間を設定します。

ステップ 19	次のいずれかを実行します。
	• **tos** *number*
	• **traffic-class** *number*
	例：
	`Device(config-ip-sla-jitter)# tos 160`
	例：
	`Device(config-ip-sla-jitter)# traffic-class 160`
		（任意）IPv4 ネットワークに限り、IP SLA 動作の IPv4 ヘッダーの ToS バイトを定義します。
		または
		（任意）IPv6 ネットワークに限り、サポートされている IP 動作に対する IPv6 ヘッダーのトラフィック クラス バイトを定義します。

	コマンドまたはアクション	目的
ステップ 20	**flow-label** *number* 例： `Device(config-ip-sla-udp)# flow-label 112233`	（任意）IPv6 ネットワークに限り、サポートされている IP SLA 動作に対する IPv6 ヘッダーのフローラベル フィールドを定義します。
ステップ 21	**verify-data** 例： `Device(config-ip-sla-udp)# verify-data`	（任意）IP SLA 動作が各応答パケットに対してデータ破壊の有無をチェックするようにします。
ステップ 22	**exit** 例： `Device(config-ip-sla-udp)# exit`	UDP コンフィギュレーション サブモードを終了し、グローバル コンフィギュレーション モードに戻ります。

次のタスク

トラップを生成する目的、または別の動作を開始する目的で、IP SLA 動作に予防的しきい値条件と反応トリガーを追加するには、「予防的しきい値モニタリングの設定」の項を参照してください。

IP SLA 動作のスケジューリング

始める前に

- スケジュールされるすべての IP サービス レベル契約（SLA）動作がすでに設定されている必要があります。
- 複数動作グループでスケジュールされたすべての動作の頻度が同じでなければなりません。
- 複数動作グループに追加する 1 つ以上の動作 ID 番号のリストは、カンマ（,）を含めて最大 125 文字に制限する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します。
   - **ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {[*hh*:*mm*:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**]
   - **ip sla group schedule** *group-operation-number operation-id-numbers* { **schedule-period** *schedule-period-range* | **schedule-together**} [**ageout** *seconds*] **frequency** *group-operation-frequency* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm* [:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm* [:*ss*]}]

4. **end**
5. **show ip sla group schedule**
6. **show ip sla configuration**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	次のいずれかのコマンドを入力します。
	• **ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {[*hh*:*mm*:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**]
	• **ip sla group schedule** *group-operation-number operation-id-numbers* { **schedule-period** *schedule-period-range* | **schedule-together**} [**ageout** *seconds*] **frequency** *group-operation-frequency* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm* [:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm* [:*ss*]}]
	例：
	`Device(config)# ip sla schedule 10 life forever start-time now`
	`Device(config)# ip sla group schedule 10 schedule-period frequency`
	`Device(config)# ip sla group schedule 1 3,4,6-9 life forever start-time now`
	`Device(config)# ip sla schedule 1 3,4,6-9 schedule-period 50 frequency range 80-100`
		• 個々の IP SLA 動作のスケジューリング パラメータを設定します。
		• 複数動作スケジューラ用に IP SLA 動作グループ番号と動作番号の範囲を指定します。

ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**show ip sla group schedule** 例： `Device# show ip sla group schedule`	（任意）IP SLA グループ スケジュールの詳細を表示します。
ステップ 6	**show ip sla configuration** 例： `Device# show ip sla configuration`	（任意）IP SLA 設定の詳細を表示します。

トラブルシューティングのヒント

- IP サービス レベル契約（SLA）動作が実行中でなく、統計情報が生成されていない場合は、設定に **verify-data** コマンドを追加して（IP SLA コンフィギュレーション モードで設定）、データ検証をイネーブルにします。データ検証をイネーブルにすると、各動作の応答で破損の有無がチェックされます。通常の動作時に **verify-data** コマンドを使用すると、不要なオーバーヘッドがかかるので注意してください。
- IP SLA 動作に関する問題をトラブルシューティングするには、**debug ip sla trace** コマンドと **debug ip sla error** コマンドを使用します。

次の作業

トラップを生成する目的（または別の動作を開始する目的）で、IPサービス レベル契約（SLA）動作に予防的しきい値条件と反応トリガーを追加するには、「予防的しきい値モニタリングの設定」の項を参照してください。

IP SLA UDP エコー動作の設定例

UDP エコー動作の設定例

次に、ただちに開始され、無期限に実行されるUDPエコーのIP SLA動作タイプを設定する例を示します。

```
ip sla 5
 udp-echo 172.29.139.134 5000
 frequency 30
 request-data-size 160
 tos 128
 timeout 1000
 tag FLL-RO
ip sla schedule 5 life forever start-time now
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
Cisco IOS IP SLA コマンド	『Cisco IOS IP SLAs Command Reference』

標準および RFC

標準/RFC	タイトル
RFC 862	Echo Protocol

MIB

MIB	MIB のリンク
CISCO-RTTMON-MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャセットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

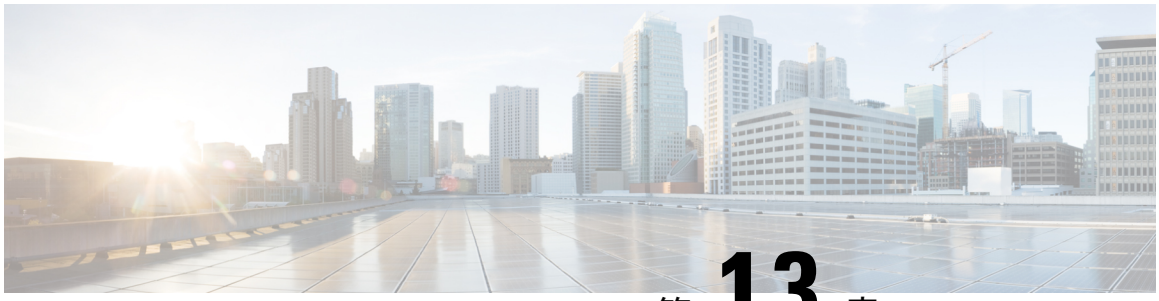
IP SLA UDP エコー動作に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *21 : IP SLA UDP* エコー動作に関する機能情報

機能名	リリース	機能情報
IP SLA：UDP エコー動作		Cisco IOS IP SLA ユーザ データグラム プロトコル（UDP）ジッター動作を使用すると、UDP トラフィックを伝送するネットワーク内におけるラウンドトリップ遅延、一方向遅延、一方向ジッター、一方向パケット損失、および接続を測定できます。
IPv6：IP SLA（UDP ジッター、UDP エコー、ICMP エコー、TCP 接続）		IPv6 ネットワークでの動作を可能にするためにサポートが追加されました。



第 13 章

IP SLA HTTP 動作の設定

このモジュールでは、シスコ デバイスと HTTP サーバの間で Web ページを取得するための応答時間をモニタするように、IP サービス レベル契約（SLA）HTTP 動作を設定する方法について説明します。IP SLA HTTP 動作は、通常の GET 要求とカスタマー RAW 要求の両方をサポートします。また、このモジュールでは、HTTP 動作の結果を表示および分析して HTTP サーバのパフォーマンスを調べる方法についても説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

IP SLA HTTP 動作の制約事項

- IP SLA HTTP 動作は HTTP/1.0 だけをサポートします。
- HTTP/1.1 は、HTTP RAW 要求を含むすべての IP SLA HTTP 動作でサポートされません。

IP SLA HTTP 動作に関する情報

HTTP 動作

HTTP 動作は、シスコ デバイスと HTTP サーバの間で Web ページを取得するためのラウンドトリップ時間（RTT）を測定します。HTTP サーバ応答時間の測定は次の 3 つの RTT から構成されます。

- DNS ルックアップ：ドメイン名ルックアップの実行に要する RTT。
- TCP 接続：HTTP サーバへの TCP 接続の実行に要する RTT。
- HTTP トランザクション時間：要求を送信し、HTTP サーバからの応答の取得に要する RTT。この動作はホーム HTML ページだけを取得します。

DNS 動作が最初に実行され、DNS RTT が測定されます。ドメイン名が見つかったら、適切な HTTP サーバに対する TCP 接続動作が実行され、この動作の RTT が測定されます。最後の動作は HTTP 要求であり、HTTP サーバからホーム HTML ページを取得するのに要する RTT が測定されます。もうひとつ別の測定が行われ、これは Time To First Byte と呼ばれます。Time To First Byte によって、TCP 接続動作の開始から HTTP 動作により取得された最初の HTML バイトを検出するまでの時間が測定されます。総 HTTP RTT は、DNS RTT、TCP 接続 RTT、および HTTP RTT の合計です。

GET 要求の場合、IP SLA は指定された URL に基づいて要求の形式を設定します。RAW の場合、IP SLA は HTTP 要求の内容全体を必要とします。RAW 要求が設定された場合は、raw コマンドが HTTP RAW コンフィギュレーション モードで指定されます。RAW 要求は柔軟であり、認証などのフィールドの制御を可能にします。HTTP 要求はプロキシサーバを経由して行うことができます。

HTTP 動作の結果は、Web ページの取得に要する RTT を調べることにより Web サーバのパフォーマンス レベルをモニタする場合に役に立ちます。

HTTP エラーとは関係なく、IP SLA は正常に動作します。現時点では、エラーコードが判別され、戻りコードが 200 以外の場合にのみ IP SLA HTTP 操作がダウンします。

（注） SLA プローブがダウンするのは、SLA が TCP 接続を確立できない場合、またはリモート サーバから HTTP 要求に対する応答を受信できない場合のみです。

IP SLA HTTP 動作の設定方法

送信元デバイスでの HTTP GET 動作の設定

（注） この動作には、送信先デバイスの IP SLA Responder は必要ありません。

次のいずれかの作業のみを実行します。

送信元デバイスでの基本 HTTP GET 動作の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **http** {**get** | **raw**} *url* [**name-server** *ip-address*] [**version** *version-number*] [**source-ip** {*ip-address* | *hostname*}] [**source-port** *port-number*] [**cache** {**enable** | **disable**}] [**proxy** *proxy-url*]
5. **frequency** *seconds*
6. **end**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	**ip sla** *operation-number* 例： `Device(config)# ip sla 10`	IP SLA 動作の設定を開始し、IP SLA コンフィギュレーション モードに移行します。
ステップ 4	**http** {**get**	**raw**} *url* [**name-server** *ip-address*] [**version** *version-number*] [**source-ip** {*ip-address*	*hostname*}] [**source-port** *port-number*] [**cache** {**enable**	**disable**}] [**proxy** *proxy-url*]	HTTP 動作を定義し、IP SLA コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	例： `Device(config-ip-sla)# http get http://198.133.219.25`	
ステップ 5	**frequency** *seconds* 例： `Device(config-ip-sla-http)# frequency 90`	（任意）指定した IP SLA HTTP 動作を繰り返す間隔を設定します。IP SLA HTTP 動作のデフォルトの最小頻度値は 60 秒です。
ステップ 6	**end** 例： `Device(config-ip-sla-http)# end`	特権 EXEC モードに戻ります。

送信元デバイスでのオプション パラメータを使用した HTTP GET 動作の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **http** {**get** | **raw**} *url* [**name-server** *ip-address*] [**version** *version-number*] [**source-ip** {*ip-address* | *hostname*}] [**source-port** *port-number*] [**cache** {**enable** | **disable**}] [**proxy** *proxy-url*]
5. **history distributions-of-statistics-kept** *size*
6. **frequency** *seconds*
7. **history hours-of-statistics-kept** *hours*
8. **http-raw-request**
9. **owner** *owner-id*
10. **history statistics-distribution-interval** *milliseconds*
11. **tag** *text*
12. **threshold** *milliseconds*
13. **timeout** *milliseconds*
14. **tos** *number*
15. **end**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
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	**ip sla** *operation-number* 例： `Device(config)# ip sla 10`	IP SLA 動作の設定を開始し、IP SLA コンフィギュレーション モードに移行します。
ステップ 4	**http** {**get** | **raw**} *url* [**name-server** *ip-address*] [**version** *version-number*] [**source-ip** {*ip-address* | *hostname*}] [**source-port** *port-number*] [**cache** {**enable** | **disable**}] [**proxy** *proxy-url*] 例： `Device(config-ip-sla)# http get http://198.133.219.25`	HTTP 動作を定義し、IP SLA コンフィギュレーション モードを開始します。
ステップ 5	**history distributions-of-statistics-kept** *size* 例： `Device(config-ip-sla-http)# history distributions-of-statistics-kept 5`	（任意）IP SLA 動作中にホップ単位で保持する統計情報の配信数を設定します。
ステップ 6	**frequency** *seconds* 例： `Device(config-ip-sla-http)# frequency 90`	（任意）指定した IP SLA HTTP 動作を繰り返す間隔を設定します。IP SLA HTTP 動作のデフォルトの最小頻度値は 60 秒です。
ステップ 7	**history hours-of-statistics-kept** *hours* 例： `Device(config-ip-sla-http)# history hours-of-statistics-kept 4`	（任意）IP SLA 動作の統計情報を保持する時間数を設定します。
ステップ 8	**http-raw-request** 例： `Device(config-ip-sla-http)# http-raw-request`	（任意）IP SLA HTTP 動作の GET 要求のオプションを明示的に指定します。
ステップ 9	**owner** *owner-id* 例： `Device(config-ip-sla-http)# owner admin`	（任意）IP SLA 動作の簡易ネットワーク管理プロトコル（SNMP）所有者を設定します。
ステップ 10	**history statistics-distribution-interval** *milliseconds* 例： `Device(config-ip-sla-http)# history statistics-distribution-interval 10`	（任意）IP SLA 動作で維持する各統計情報の配信間隔を設定します。
ステップ 11	**tag** *text* 例：	（任意）IP SLA 動作のユーザ指定 ID を作成します。

	コマンドまたはアクション	目的
	`Device(config-ip-sla-http)# tag TelnetPollServer1`	
ステップ 12	**threshold** *milliseconds* 例： `Device(config-ip-sla-http)# threshold 10000`	（任意）IP SLA 動作によって作成されるネットワーク モニタリング統計情報を計算するための上限しきい値を設定します。
ステップ 13	**timeout** *milliseconds* 例： `Device(config-ip-sla-http)# timeout 10000`	（任意）IP SLA 動作がその要求パケットからの応答を待機する時間を設定します。
ステップ 14	**tos** *number* 例： `Device(config-ip-sla-http)# tos 160`	（任意）IP SLA 動作の IP ヘッダー内のタイプ オブ サービス（ToS）バイトを定義します。
ステップ 15	**end** 例： `Device(config-ip-sla-http)# end`	特権 EXEC モードに戻ります。

送信元デバイスでの HTTP RAW 動作の設定

（注） この動作には、送信先デバイスの IP SLA Responder は必要ありません。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **http** {**get** | **raw**} *url* [**name-server** *ip-address*] [**version** *version-number*] [**source-ip** {*ip-address* | *hostname*}] [**source-port** *port-number*] [**cache** {**enable** | **disable**}] [**proxy** *proxy-url*]
5. **http-raw-request**
6. 必要な HTTP 1.0 コマンド構文を入力します。
7. **end**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
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	**ip sla** *operation-number* 例： `Device(config)# ip sla 10`	IP SLA 動作の設定を開始し、IP SLA コンフィギュレーション モードに移行します。
ステップ 4	**http** {**get** | **raw**} *url* [**name-server** *ip-address*] [**version** *version-number*] [**source-ip** {*ip-address* | *hostname*}] [**source-port** *port-number*] [**cache** {**enable** | **disable**}] [**proxy** *proxy-url*] 例： `Device(config-ip-sla)# http raw http://198.133.219.25`	HTTP 動作を定義します。
ステップ 5	**http-raw-request** 例： `Device(config-ip-sla)# http-raw-request`	HTTP RAW コンフィギュレーション モードを開始します。
ステップ 6	必要な HTTP 1.0 コマンド構文を入力します。 例： `Device(config-ip-sla-http)# GET /en/US/hmpgs/index.html HTTP/1.0\r\n\r\n`	必要なすべての HTTP 1.0 コマンドを入力します。
ステップ 7	**end** 例： `Device(config-ip-sla-http)# end`	特権 EXEC モードに戻ります。

IP SLA 動作のスケジューリング

始める前に

- スケジュールされるすべての IP サービス レベル契約（SLA）動作がすでに設定されている必要があります。
- 複数動作グループでスケジュールされたすべての動作の頻度が同じでなければなりません。
- 複数動作グループに追加する 1 つ以上の動作 ID 番号のリストは、カンマ（,）を含めて最大 125 文字に制限する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します。
   - **ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {[*hh*:*mm*:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**]
   - **ip sla group schedule** *group-operation-number operation-id-numbers* { **schedule-period** *schedule-period-range* | **schedule-together**} [**ageout** *seconds*] **frequency** *group-operation-frequency* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm* [:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm* [:*ss*]}]
4. **end**
5. **show ip sla group schedule**
6. **show ip sla configuration**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	次のいずれかのコマンドを入力します。 • **ip sla schedule** *operation-number* [**life** {**forever**	*seconds*}] [**start-time** {[*hh*:*mm*:*ss*] [*month day*	*day month*]	**pending**	**now**	**after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**] • **ip sla group schedule** *group-operation-number operation-id-numbers* { **schedule-period** *schedule-period-range*	**schedule-together**} [**ageout** *seconds*] **frequency** *group-operation-frequency* [**life** {**forever**	*seconds*}] [**start-time** {*hh*:*mm* [:*ss*] [*month day*	*day month*]	**pending**	**now**	**after** *hh*:*mm* [:*ss*]}] 例： `Device(config)# ip sla schedule 10 life forever start-time now` `Device(config)# ip sla group schedule 10 schedule-period frequency`	• 個々の IP SLA 動作のスケジューリング パラメータを設定します。 • 複数動作スケジューラ用に IP SLA 動作グループ番号と動作番号の範囲を指定します。

	コマンドまたはアクション	目的

	`Device(config)# ip sla group schedule 1 3,4,6-9 life forever start-time now`
	
	`Device(config)# ip sla schedule 1 3,4,6-9 schedule-period 50 frequency range 80-100`	

ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	**show ip sla group schedule** 例： `Device# show ip sla group schedule`	（任意）IP SLA グループ スケジュールの詳細を表示します。
ステップ 6	**show ip sla configuration** 例： `Device# show ip sla configuration`	（任意）IP SLA 設定の詳細を表示します。

トラブルシューティングのヒント

- IP サービス レベル契約（SLA）動作が実行中でなく、統計情報が生成されていない場合は、設定に **verify-data** コマンドを追加して（IP SLA コンフィギュレーション モードで設定）、データ検証をイネーブルにします。データ検証をイネーブルにすると、各動作の応答で破損の有無がチェックされます。通常の動作時に **verify-data** コマンドを使用すると、不要なオーバーヘッドがかかるので注意してください。
- IP SLA 動作に関する問題をトラブルシューティングするには、**debug ip sla trace** コマンドと **debug ip sla error** コマンドを使用します。

次の作業

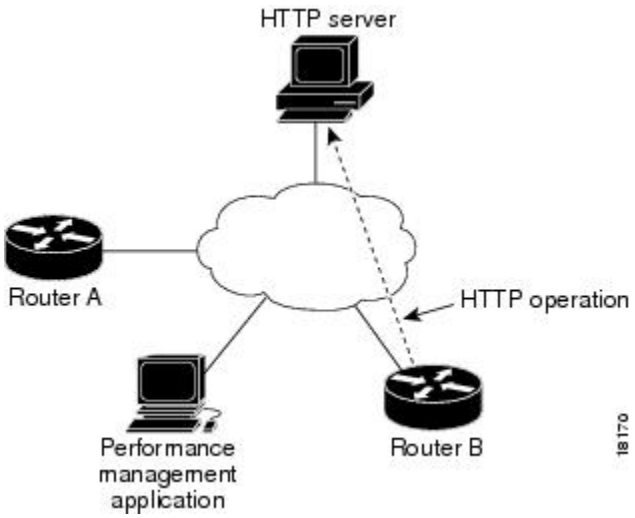
トラップを生成する目的（または別の動作を開始する目的）で、IP サービス レベル契約（SLA）動作に予防的しきい値条件と反応トリガーを追加するには、「予防的しきい値モニタリングの設定」の項を参照してください。

IP SLA HTTP 動作の設定例

HTTP GET 動作の設定例

次に、動作番号 8 を作成し、HTTP GET 動作として設定する例を示します。送信先 URL IP アドレスは www.cisco.com の Web サイトを表します。次の図は HTTP GET 動作を示しています。

図 *10 : HTTP* 動作



デバイス B の設定

```
ip sla 8
 http get url http://198.133.219.25
!
ip sla schedule 8 start-time now
```

HTTP RAW 動作の設定例

次に、HTTP RAW 動作を設定する例を示します。RAW コマンドを使用するには、IP SLA コンフィギュレーション モードで **http-raw-request** コマンドを使用して HTTP RAW コンフィギュレーション モードを開始します。IP SLA HTTP RAW コンフィギュレーション モードは（config-ip-sla-http）ルータ プロンプトによって示されます。

```
ip sla 8
 http raw url http://198.133.219.25
 http-raw-request
 GET /en/US/hmpgs/index.html HTTP/1.0\r\n
 \r\n
 end
ip sla schedule 8 life forever start-time now
```

プロキシ サーバ経由での HTTP RAW 動作の設定例

次に、プロキシ サーバを経由して HTTP RAW 動作を設定する例を示します。プロキシ サーバは www.proxy.cisco.com であり、HTTP サーバは www.yahoo.com です。

```
ip sla 8
 http raw url http://www.proxy.cisco.com
 http-raw-request
 GET http://www.yahoo.com HTTP/1.0\r\n
 \r\n
 end
ip sla schedule 8 life forever start-time now
```

認証による HTTP RAW 動作の設定例

次に、HTTP RAW 動作を認証により設定する例を示します。

```
ip sla 8
 http raw url http://site-test.cisco.com
 http-raw-request
 GET /lab/index.html HTTP/1.0\r\n
 Authorization: Basic btNpdGT4biNvoZe=\r\n
 \r\n
 end
ip sla schedule 8 life forever start-time now
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
Cisco IOS IP SLA コマンド	『Cisco IOS IP SLAs Command Reference』

標準および RFC

標準/RFC	タイトル
この機能によりサポートされる新規または変更された標準やRFCはありません。またこの機能による既存の標準のサポートに変更はありません。	--

MIB

MIB	MIB のリンク
CISCO-RTTMON-MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャセットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IP SLA HTTP 動作の機能情報

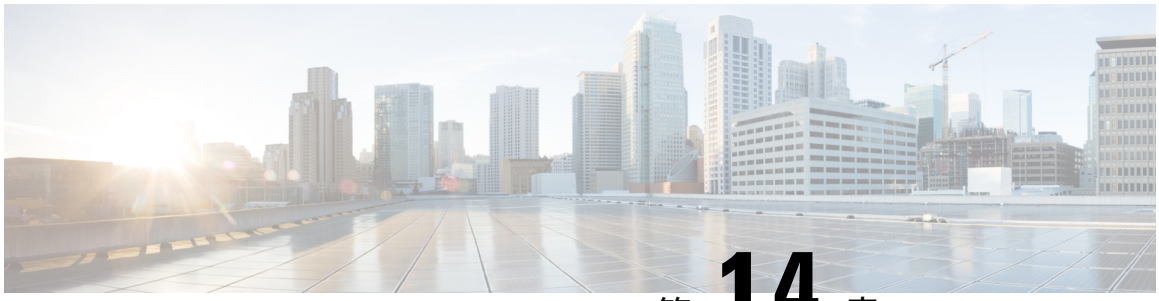
次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *22 : IP SLA HTTP* 動作の機能情報

機能名	リリース	機能情報
IP SLA HTTP 動作		Cisco IOS IP SLA ハイパーテキスト転送プロトコル（HTTP）動作を使用すると、Web ページを取得する場合のシスコ デバイスと HTTP サーバの間のネットワーク応答時間を測定できます。

機能名	リリース	機能情報
IPSLA 4.0 - IP v6 phase2		IPv6 ネットワークでの動作を可能にするためにサポートが追加されました。次のコマンドが導入または変更されました。**http (IP SLA)**、**show ip sla configuration**、**show ip sla summary**
IP SLAs VRF Aware 2.0		TCP 接続、FTP、HTTP および DNS クライアント動作タイプに対する IP SLA VRF 対応機能のサポートが追加されました。



第 14 章

IP SLA TCP 接続動作の設定

このモジュールでは、Cisco ルータと IPv4 または IPv6 を使用するデバイスの間の、TCP 接続動作の実行に要する応答時間を測定するように、IP サービス レベル契約（SLA）の TCP 接続動作を設定する方法について説明します。TCP 接続の精度は、宛先の Cisco ルータに IP SLA Responder を使用することによって向上します。このモジュールでは、TCP 接続動作の結果を表示して分析し、ネットワーク内のサーバおよびホストへの接続回数が、IP サービス レベルにどのように影響する可能性があるかを判断する方法についても説明します。TCP 接続動作は、特定のアプリケーションに使用するサーバの応答時間の測定やサーバの可用性の接続テストに役立ちます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

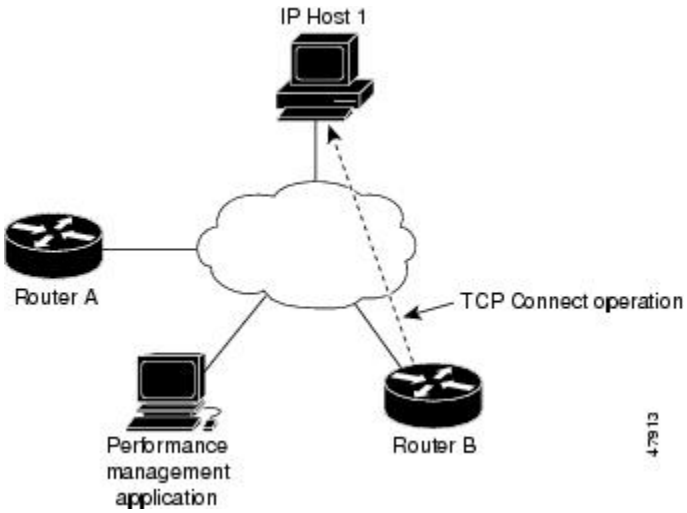
IP SLA TCP 接続動作に関する情報

TCP 接続動作

IP SLA TCP 接続動作は、シスコ デバイスと IP を使用するデバイスの間の TCP 接続動作の実行に要する応答時間を測定します。TCP は、信頼性の高い全二重データ伝送を行うトランスポート層（レイヤ4）インターネットプロトコルです。宛先デバイスは、IP を使用する任意のデバイスまたは IP SLA Responder になります。

次の図では、デバイス B が送信元 IP SLA デバイスとして設定され、IP ホスト 1 を宛先デバイスとする TCP 接続動作が設定されています。

図 *11 : TCP* 接続動作



接続応答時間は、デバイス B から IP ホスト 1 に TCP 要求メッセージを送信してから、IP ホスト 1 からの応答を受信するまでの時間を測定して算出されます。

TCP 接続の精度は、宛先のシスコ デバイスに IP SLA Responder を使用することによって向上します。宛先デバイスがシスコデバイスの場合、IP SLA は指定した任意のポート番号への TCP 接続を実行します。宛先が Cisco IP ホストでない場合は、既知の宛先ポート番号を指定する必要があります（たとえば、FTP には 21、Telnet には 23、HTTP サーバには 80 を指定）。

シスコ デバイスを使用する場合、TCP 接続動作に IP SLA Responder を使用するかどうかは任意です。シスコ以外のデバイスに IP SLA Responder を設定することはできません。

TCP 接続は、仮想回線の可用性またはアプリケーションの可用性をテストするために使用します。Telnet、SQL、および他のタイプの接続をシミュレーションすることによってサーバおよびアプリケーションの接続パフォーマンスをテストすると、IP サービス レベルの確認に役立ちます。

IP SLA TCP 接続動作の設定方法

宛先デバイスでの IP SLA Responder の設定

始める前に

IP SLA Responder を使用する場合は、応答側として使用するネットワーキング デバイスがシスコ デバイスであり、そのデバイスにネットワークを介して接続できることを確認します。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかを実行します。
   - **ip sla responder**
   - **ip sla responder tcp-connect ipaddress** *ip-address* **port** *port* **vrf** *vrf*
4. **exit**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	次のいずれかを実行します。
	• **ip sla responder**
	• **ip sla responder tcp-connect ipaddress** *ip-address* **port** *port* **vrf** *vrf*
	例：
	`Device(config)# ip sla responder`
	例：
	`Device(config)# ip sla responder tcp-connect ipaddress 172.29.139.132 port 5000 vrf vrf1`
		（任意）送信元からの制御メッセージに応じて、シスコ デバイスにおける IP SLA Responder 機能を一時的にイネーブルにします。
		または
		（任意）送信元デバイスでプロトコル制御が明示的にディセーブルである場合にのみ必須です。指定の IP アドレスとポートおよび VRF で IP SLA Responder 機能を永続的にイネーブルにします。
		• 制御は、デフォルトでイネーブルになります。

	コマンドまたはアクション	目的
ステップ 4	**exit** 例： `Device(config)# exit`	（任意）グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

送信元デバイスでの TCP 接続動作の設定およびスケジューリング

次のいずれかの作業のみを実行します。

前提条件

IP SLA Responder を使用する場合は、このタスクを開始する前に「宛先デバイスでの IP SLA Responder の設定」の項を完了してください。

送信元デバイスでの基本 TCP 接続動作の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **tcp-connect** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*} **source-port** *port-number*] [**control** {**enable** | **disable**}]
5. **frequency** *seconds*
6. **end**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	**ip sla** *operation-number* 例： `Device(config)# ip sla 10`	IP SLA 動作の設定を開始し、IP SLA コンフィギュレーション モードに移行します。

	コマンドまたはアクション	目的
ステップ 4	**tcp-connect** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*} **source-port** *port-number*] [**control** {**enable** | **disable**}] 例： `Device(config-ip-sla)# tcp-connect 172.29.139.132 5000`	TCP 接続動作を定義し、IP SLA TCP コンフィギュレーション モードを開始します。 • 送信元デバイスとターゲットデバイスの両方で IP SLA 制御プロトコルをディセーブルにする場合のみ **control disable** キーワードの組み合わせを使用します。
ステップ 5	**frequency** *seconds* 例： `Device(config-ip-sla-tcp)# frequency 30`	（任意）指定した IP SLA 動作を繰り返す間隔を設定します。
ステップ 6	**end** 例： `Device(config-ip-sla-tcp)# 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。

送信元デバイスでのオプション パラメータを使用した TCP 接続動作の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **tcp-connect** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*} **source-port** *port-number*] [**control** {**enable** | **disable**}]
5. **history buckets-kept** *size*
6. **history distributions-of-statistics-kept** *size*
7. **history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*]
8. **history filter** {**none** | **all** | **overThreshold** | **failures**}
9. **frequency** *seconds*
10. **history hours-of-statistics-kept** *hours*
11. **history lives-kept** *lives*
12. **owner** *owner-id*
13. **history statistics-distribution-interval** *milliseconds*
14. **tag** *text*
15. **threshold** *milliseconds*
16. **timeout** *milliseconds*
17. 次のいずれかを実行します。
    - **tos** *number*
    - **traffic-class** *number*
18. **flow-label** *number*

19. **exit**
20. **show ip sla configuration** [*operation-number*]

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	**ip sla** *operation-number* 例： `Device(config)# ip sla 10`	IP SLA 動作の設定を開始し、IP SLA コンフィギュレーション モードに移行します。
ステップ 4	**tcp-connect** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*} **source-port** *port-number*] [**control** {**enable** | **disable**}] 例： `Device(config-ip-sla)# tcp-connect 172.29.139.132 5000`	TCP 接続動作を定義し、IP SLA TCP コンフィギュレーション モードを開始します。 • 送信元デバイスとターゲット デバイスの両方で IP SLA 制御プロトコルをディセーブルにする場合のみ **control disable** キーワードの組み合わせを使用します。
ステップ 5	**history buckets-kept** *size* 例： `Device(config-ip-sla-tcp)# history buckets-kept 25`	（任意）IP SLA 動作のライフタイム中に保持する履歴バケット数を設定します。
ステップ 6	**history distributions-of-statistics-kept** *size* 例： `Device(config-ip-sla-tcp)# history distributions-of-statistics-kept 5`	（任意）IP SLA 動作中にホップ単位で保持する統計情報の配信数を設定します。
ステップ 7	**history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*] 例： `Device(config-ip-sla-tcp)# history enhanced interval 900 buckets 100`	（任意）IP SLA 動作に対する拡張履歴収集をイネーブルにします。
ステップ 8	**history filter** {**none** | **all** | **overThreshold** | **failures**} 例：	（任意）IP SLA 動作の履歴テーブルに格納する情報のタイプを定義します。

	コマンドまたはアクション	目的
	`Device(config-ip-sla-tcp)# history filter failures`	
ステップ 9	**frequency** *seconds* 例： `Device(config-ip-sla-tcp)# frequency 30`	（任意）指定した IP SLA 動作を繰り返す間隔を設定します。
ステップ 10	**history hours-of-statistics-kept** *hours* 例： `Device(config-ip-sla-tcp)# history hours-of-statistics-kept 4`	（任意）IP SLA 動作の統計情報を保持する時間数を設定します。
ステップ 11	**history lives-kept** *lives* 例： `Device(config-ip-sla-tcp)# history lives-kept 2`	（任意）IP SLA 動作の履歴テーブルに格納するライフ数を設定します。
ステップ 12	**owner** *owner-id* 例： `Device(config-ip-sla-tcp)# owner admin`	（任意）IP SLA 動作の簡易ネットワーク管理プロトコル（SNMP）所有者を設定します。
ステップ 13	**history statistics-distribution-interval** *milliseconds* 例： `Device(config-ip-sla-tcp)# history statistics-distribution-interval 10`	（任意）IP SLA 動作で維持する各統計情報の配信間隔を設定します。
ステップ 14	**tag** *text* 例： `Device(config-ip-sla-tcp)# tag TelnetPollServer1`	（任意）IP SLA 動作のユーザ指定 ID を作成します。
ステップ 15	**threshold** *milliseconds* 例： `Device(config-ip-sla-tcp)# threshold 10000`	（任意）IP SLA 動作によって作成されるネットワーク モニタリング統計情報を計算するための上限しきい値を設定します。
ステップ 16	**timeout** *milliseconds* 例： `Device(config-ip-sla-tcp)# timeout 10000`	（任意）IP SLA 動作がその要求パケットからの応答を待機する時間を設定します。
ステップ 17	次のいずれかを実行します。 • **tos** *number* • **traffic-class** *number* 例： `Device(config-ip-sla-jitter)# tos 160`	（任意）IPv4 の場合：IP SLA 動作の IPv4 ヘッダーに ToS バイトを定義します。 または （任意）IPv6 の場合：サポートされている IP SLA 動作に対する IPv6 ヘッダーにトラフィック クラス バイトを定義します。

	コマンドまたはアクション	目的
	例： `Device(config-ip-sla-jitter)# traffic-class 160`	
ステップ 18	**flow-label** *number* 例： `Device(config-ip-sla-tcp)# flow-label 112233`	（任意）IPv6 の場合：サポートされている IP SLA 動作に対する IPv6 ヘッダーにフロー ラベル フィールドを定義します。
ステップ 19	**exit** 例： `Device(config-ip-sla-tcp)# exit`	TCP コンフィギュレーション サブモードを終了し、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 20	**show ip sla configuration** [*operation-number*] 例： `Device# show ip sla configuration 10`	（任意）すべての IP SLA 動作または指定した IP SLA 動作に関する設定値を、すべてのデフォルト値を含めて表示します。

IP SLA 動作のスケジューリング

始める前に

- スケジュールされるすべての IP サービス レベル契約（SLA）動作がすでに設定されている必要があります。
- 複数動作グループでスケジュールされたすべての動作の頻度が同じでなければなりません。
- 複数動作グループに追加する 1 つ以上の動作 ID 番号のリストは、カンマ（,）を含めて最大 125 文字に制限する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します。
   - **ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {[*hh*:*mm*:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**]
   - **ip sla group schedule** *group-operation-number operation-id-numbers* { **schedule-period** *schedule-period-range* | **schedule-together**} [**ageout** *seconds*] **frequency** *group-operation-frequency* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm* [:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm* [:*ss*]}]
4. **end**
5. **show ip sla group schedule**
6. **show ip sla configuration**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	次のいずれかのコマンドを入力します。
	• **ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {[*hh*:*mm*:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**]
	• **ip sla group schedule** *group-operation-number operation-id-numbers* { **schedule-period** *schedule-period-range* |**schedule-together**} [**ageout** *seconds*] **frequency** *group-operation-frequency* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm* [:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm* [:*ss*]}]
	例：
	`Device(config)# ip sla schedule 10 life forever start-time now`
	`Device(config)# ip sla group schedule 10 schedule-period frequency`
	`Device(config)# ip sla group schedule 1 3,4,6-9 life forever start-time now`
	`Device(config)# ip sla schedule 1 3,4,6-9 schedule-period 50 frequency range 80-100`
		• 個々の IP SLA 動作のスケジューリング パラメータを設定します。
		• 複数動作スケジューラ用に IP SLA 動作グループ番号と動作番号の範囲を指定します。

ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	**show ip sla group schedule** 例： `Device# show ip sla group schedule`	（任意）IP SLA グループ スケジュールの詳細を表示します。

	コマンドまたはアクション	目的
ステップ 6	**show ip sla configuration** 例： `Device# show ip sla configuration`	（任意）IP SLA 設定の詳細を表示します。

トラブルシューティングのヒント

- IP サービス レベル契約（SLA）動作が実行中でなく、統計情報が生成されていない場合は、設定に **verify-data** コマンドを追加して（IP SLA コンフィギュレーション モードで設定）、データ検証をイネーブルにします。データ検証をイネーブルにすると、各動作の応答で破損の有無がチェックされます。通常の動作時に **verify-data** コマンドを使用すると、不要なオーバーヘッドがかかるので注意してください。
- IP SLA 動作に関する問題をトラブルシューティングするには、**debug ip sla trace** コマンドと **debug ip sla error** コマンドを使用します。

次の作業

トラップを生成する目的（または別の動作を開始する目的）で、IPサービス レベル契約（SLA）動作に予防的しきい値条件と反応トリガーを追加するには、「予防的しきい値モニタリングの設定」の項を参照してください。

IP SLA TCP 接続動作の設定例

TCP 接続動作の設定例

次に、「IP SLA TCP 接続動作に関する情報」の項の図「TCP 接続動作」に示されているように、デバイス B から IP ホスト 1（IP アドレス 10.0.0.1）の Telnet ポート（TCP ポート 23）への TCP 接続動作を設定する例を示します。動作は、ただちに開始されるようにスケジューリングされます。この例では、送信元（デバイスB）で制御プロトコルがディセーブルになっています。IP SLA は制御プロトコルを使用して、ターゲット ポートを一時的にイネーブルにするように IP SLA Responder に通知します。このアクションにより、Responder は TCP 接続動作に応答できます。この例では、ターゲットがシスコ デバイスではなく、既知の TCP ポートが使用されているため、制御メッセージを送信する必要はありません。

デバイス A（デバイス ターゲット）の設定

```
configure terminal
 ip sla responder tcp-connect ipaddress 10.0.0.1 port 23
```

デバイス B（送信元デバイス）の設定

```
ip sla 9
 tcp-connect 10.0.0.1 23 control disable
 frequency 30
 tos 128
 timeout 1000
 tag FLL-RO
ip sla schedule 9 start-time now
```

次に、特定のポート（ポート 23）を使用し、IP SLA Responder を使用せずに TCP 接続動作を設定する例を示します。動作は、ただちに開始され、無期限に実行するようスケジューリングされます。

```
ip sla 9
 tcp-connect 173.29.139.132 21 control disable
 frequency 30
ip sla schedule 9 life forever start-time now
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
Cisco IOS IP SLA コマンド	『Cisco IOS IP SLAs Command Reference, All Releases』
Cisco IOS IP SLA：一般情報	『*Cisco IOS IP SLAs Configuration Guide*』の「Cisco IOS IP SLAs Overview」モジュール
IP SLA の複数動作スケジューリング	『*Cisco IOS P SLAs Configuration Guide*』の「Configuring Multioperation Scheduling of IP SLAs Operations」モジュール
IP SLA の予防的しきい値モニタリング	『*Cisco IOS IP SLAs Configuration Guide*』の「Configuring Proactive Threshold Monitoring of IP SLAs Operations」モジュール

MIB

MIB	MIB のリンク
CISCO-RTTMON-MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャセットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

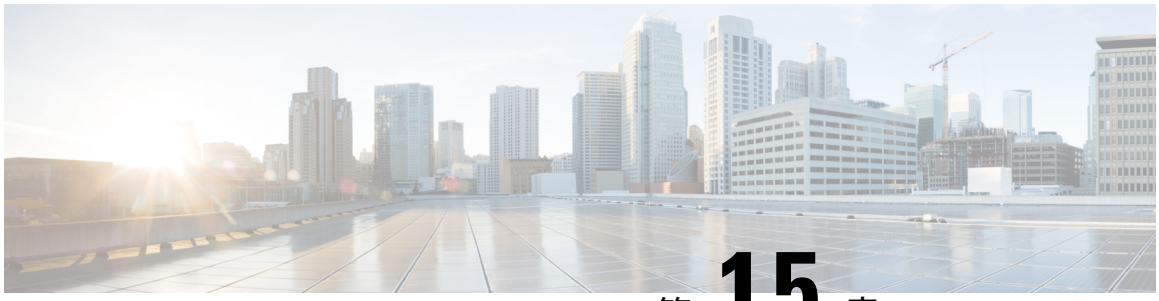
IP SLA TCP 接続動作の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *23 : IP SLA TCP* 接続動作の機能情報

機能名	リリース	機能情報
IP SLA TCP 接続動作		Cisco IOS IP SLA の伝送制御プロトコル（TCP）接続動作を使用すると、シスコ デバイスと IP を使用するその他のデバイスの間の、TCP 接続動作の実行に要するネットワーク応答時間を測定できます。
IPv6：IP SLA（UDP ジッタ、UDP エコー、ICMP エコー、TCP 接続）		IPv6 ネットワークでの動作を可能にするためにサポートが追加されました。
IP SLAs VRF Aware 2.0		TCP 接続、FTP、HTTP および DNS クライアント動作タイプに対する IP SLA VRF 対応機能のサポートが追加されました。



第 15 章

Cisco IP SLA ICMP ジッター動作の設定

このモジュールでは、Cisco IOS デバイス（送信元）とその他の IP デバイス（宛先）の間でネットワーク パフォーマンスに関する統計情報を収集するための ICMP パケットのストリームを生成するように Cisco IOS IP サービス レベル契約（SLA）インターネット制御メッセージ プロトコル（ICMP）ジッター動作を設定する方法について説明します。宛先デバイスは、サーバやワークステーションなどの ICMP をサポートする任意のネットワーク デバイスです。IP SLA ICMP ジッター動作で使用可能な統計測定値には、遅延、ラウンドトリップ時間、ジッター（パケット間の遅延のばらつき）、およびパケット損失が含まれます。IP SLA ICMP ジッター動作には、宛先デバイスの IP SLA Responder は必要ありません。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

IP SLA ICMP ジッター動作に関する制約事項

- Cisco IOS-XR デバイスは ICMP タイムスタンプをサポートしていないため、これらのデバイスへのすべての ICMP ジッター動作は失敗します。
- IP SLA UserDatagramProtocol（UDP）ジッター動作と比較すると、IP SLA ICMP ジッター動作は、シスコ以外の宛先デバイスによって提供される測定の精度を判断できないので、測定精度が低くなる可能性があります。
- ICMP パケットは音声テクノロジーをサポートしていないため、IP SLA ICMP ジッター動作は、平均オピニオン評点（MOS）、Calculated Planning Impairment Factor（ICPIF）、または概算伝送評価係数（R）反応設定機能をサポートしていません。

IP SLA ICMP ジッター動作に関する情報

IP SLA ICMP ジッター動作の利点

IP SLA ICMP ジッター動作機能の主な利点は次のとおりです。

- ICMP を使用した、シスコデバイス（送信元）と他の IP デバイス（宛先）間のエンドツーエンドのパフォーマンス測定。
- Simple Network Management Protocol（SNMP）トラップ通知および syslog メッセージによる予防的しきい値違反モニタリング。

IP SLA ICMP ジッター動作によって測定された統計情報

IP SLA ICMP ジッター動作では、次の統計情報測定をサポートしています。

- ジッター（ソースからターゲット、およびターゲットからソース）
- 遅延（送信元から宛先へ、宛先から送信元へ）
- ラウンドトリップ時間の遅延
- パケット損失
- 継続的なパケット損失
- アウトオブシーケンスパケット（送信元から宛先へ、宛先から送信元へ、およびラウンドトリップ）
- 遅延パケット

IP SLA ICMP ジッターは、2 つの ICMP タイム スタンプ メッセージ、ICMP タイムスタンプ リクエスト（タイプ 13）および ICMP タイムスタンプ応答（タイプ 14）を使用して、ジッター、

パケット損失、および遅延を提供します。IP SLA ICMP ジッター動作は、ICMP エコーは ICMP エコー要求および応答（ping）を使用するという点で、IP SLA ICMP エコー動作と異なります。RFC 792 に完全に準拠しているデバイス、インターネット制御メッセージプロトコルは、宛先で IP SLA Responder を必要とすることなく、タイム スタンプ メッセージに応答できる必要があります。

（注） Cisco IOS デバイスは、RFC 792 のタイムスタンプ要求および応答をサポートしていますが、Cisco IOS-XR デバイスはこれをサポートしていません。

ICMP API は、インターフェイスから設定可能な数の要求メッセージ パケットを送信します。要求で受信されたデータ（タイム スタンプ）は、別のタイム スタンプとともに返信メッセージパケットで返されます。すべてのパケットには、発信（送信）タイムスタンプ、受信タイムスタンプ、および送信（返信）タイプスタンプの 3 つのタイム スタンプが含まれています。

IP SLA は、それらのタイム スタンプを利用して、2 つの連続するパケットの到着間遅延と出発間遅延の差に基づいて、各方向のジッターを計算します。差が正であれば、正のジッターでカウントされます。負の値は、負のジッターでカウントされます。パスは異なるもの（非対称）にできるので、送信元から宛先へ、および宛先から送信元へのデータ パスの個別の測定を使用して、ネットワークの問題を識別できます。

各 ICMP パケットには、送信者のシーケンスから受信されたパケット数をカウントするために使用されるシーケンス番号がヘッダー内に含まれています。シーケンス番号と受信タイムスタンプはともに、送信元から宛先へのパスでアウトオブシーケンス パケットを計算するために使用できます。パケットの受信タイム スタンプが次のパケットのタイム スタンプよりも大きい場合は、最初のパケットが送信元から宛先へのパスで不適切に配信されました。宛先から送信元へのパスには、同じ方法を適用できます。送信元から宛先へのパスでパケットに問題がある場合は、宛先から送信元へのパスでも問題がある場合を除き、送信者に正しく返されないことに注意してください。

内部または予期しないエラーが原因でパケットを送信できない場合、またはパケットを含む timerwheel スロットが見つからないため、スキップされたパケットとしてカウントされます。このメトリックは、統計情報が送信されたパケットだけで測定されるため、非常に重要です。

すべてのタイムアウトになったパケットは、パケット損失に考慮されます。連続的なパケット損失は、連続してドロップされたパケットの数をカウントおよび追加することで計算されます。連続的なパケット損失は、最小の連続的なパケット ドロップおよび最大の連続的なパケット ドロップとして報告されます。

他のすべての統計情報は、UDP ジッター動作と同じロジックを使用して計算されます。

IP SLA ICMP ジッター動作の設定方法

IP SLA 動作のスケジューリング

始める前に

- スケジュールされるすべての IP サービス レベル契約（SLA）動作がすでに設定されている必要があります。
- 複数動作グループでスケジュールされたすべての動作の頻度が同じでなければなりません。
- 複数動作グループに追加する 1 つ以上の動作 ID 番号のリストは、カンマ（,）を含めて最大 125 文字に制限する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します。
   - **ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {[*hh*:*mm*:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**]
   - **ip sla group schedule** *group-operation-number operation-id-numbers* { **schedule-period** *schedule-period-range* | **schedule-together**} [**ageout** *seconds*] **frequency** *group-operation-frequency* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm* [:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm* [:*ss*]}]
4. **end**
5. **show ip sla group schedule**
6. **show ip sla configuration**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	次のいずれかのコマンドを入力します。	• 個々の IP SLA 動作のスケジューリング パラメータを設定します。

	コマンドまたはアクション	目的

	• **ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {[*hh*:*mm*:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**]
	• **ip sla group schedule** *group-operation-number operation-id-numbers* { **schedule-period** *schedule-period-range* |**schedule-together**} [**ageout** *seconds*] **frequency** *group-operation-frequency* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm* [:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm* [:*ss*]}]
	例：
	`Device(config)# ip sla schedule 10 life forever start-time now`
	`Device(config)# ip sla group schedule 10 schedule-period frequency`
	`Device(config)# ip sla group schedule 1 3,4,6-9 life forever start-time now`
	`Device(config)# ip sla schedule 1 3,4,6-9 schedule-period 50 frequency range 80-100`
		• 複数動作スケジューラ用に IP SLA 動作グループ番号と動作番号の範囲を指定します。

ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	**show ip sla group schedule** 例： `Device# show ip sla group schedule`	（任意）IP SLA グループ スケジュールの詳細を表示します。
ステップ 6	**show ip sla configuration** 例： `Device# show ip sla configuration`	（任意）IP SLA 設定の詳細を表示します。

トラブルシューティングのヒント

• IP サービス レベル契約（SLA）動作が実行中でなく、統計情報が生成されていない場合は、設定に **verify-data** コマンドを追加して（IP SLA コンフィギュレーション モードで設定）、データ検証をイネーブルにします。データ検証をイネーブルにすると、各動作の応答で破損の有無がチェックされます。通常の動作時に **verify-data** コマンドを使用すると、不要なオーバーヘッドがかかるので注意してください。

- IP SLA 動作に関する問題をトラブルシューティングするには、**debug ip sla trace** コマンドと **debug ip sla error** コマンドを使用します。

次の作業

トラップを生成する目的（または別の動作を開始する目的）で、IPサービス レベル契約（SLA）動作に予防的しきい値条件と反応トリガーを追加するには、「予防的しきい値モニタリングの設定」の項を参照してください。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Cisco IOS IP SLA コマンド	『IP SLAs Command Reference』
Cisco IOS IP SLA：一般情報	『*Cisco IOS IP SLAs Configuration Guide*』の「Cisco IOS IP SLAs Overview」の章

標準

標準	タイトル
この機能でサポートされる新規の規格または変更された規格はありません。また、既存の規格のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
• CISCO-RTTMON-MIB • CISCO-RTTMON-ICMP-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 792	インターネット制御メッセージプロトコル（*ICMP*）

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

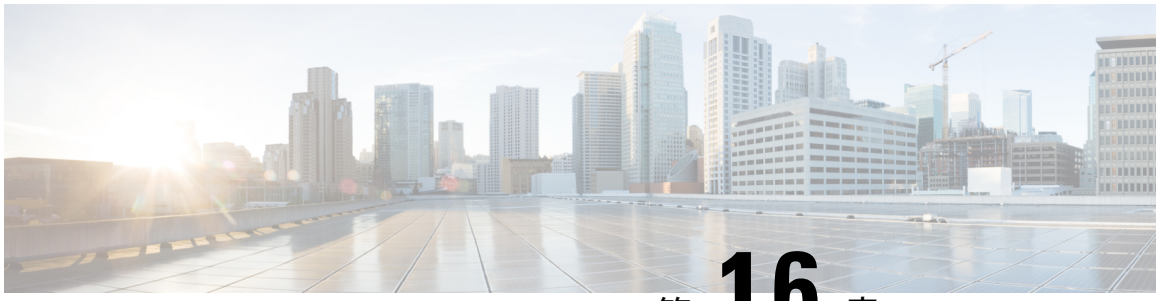
IP SLA - ICMP ジッター動作の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *24 : IP SLA - ICMP* ジッター動作の機能情報

機能名	リリース	機能情報
IP SLA ICMP ジッター動作		Cisco IOS IP サービス レベル契約（SLA）インターネット制御メッセージ プロトコル（ICMP）ジッター動作では、Cisco IOS デバイス（送信元）とその他の IP デバイス（宛先）の間でネットワーク パフォーマンスに関する統計情報を収集するための ICMP パケットのストリームを生成できます。IP SLA ICMP ジッター動作で使用可能な統計測定値には、遅延、ラウンドトリップ時間、ジッター（パケット間の遅延のばらつき）、およびパケット損失が含まれます。



第 16 章

IP SLA ICMP エコー動作の設定

このモジュールでは、Cisco ルータと IPv4 または IPv6 を使用するデバイスの間のエンドツーエンド応答時間をモニタするように、IP サービス レベル契約（SLA）インターネット制御メッセージプロトコル（ICMP）エコー動作を設定する方法について説明します。ICMP エコーは、ネットワーク接続問題のトラブルシューティングに役立ちます。また、このモジュールでは、ネットワークの IP 接続の実行状況を判別するために ICMP エコー動作の結果がどのように表示され、分析されるかについても説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

IP SLA ICMP エコー動作に関する制約事項

RFC 862 のエコー プロトコルをサポートするネットワーキング デバイスであれば使用できますが、シスコのネットワーキングデバイスを宛先デバイスとして使用することを推奨します。

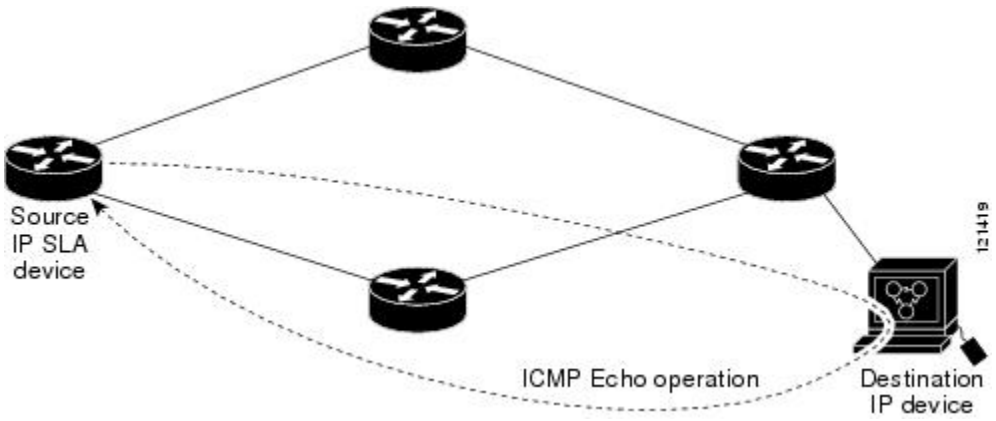
IP SLA ICMP エコー動作に関する情報

ICMP エコー動作

ICMP エコー動作は、Cisco ルータと IP を使用する任意のデバイスの間のエンドツーエンド応答時間を測定します。応答時間は、ICMP エコー要求メッセージを宛先に送信してから ICMP エコー応答を受信するまでの時間を測定して算出されます。

次の図では、ICMP エコー動作は ping を使用して送信元 IP SLA デバイスと宛先 IP デバイスの間の応答時間を測定します。多くのお客様が、応答時間の測定に IP SLA ICMP ベース動作、社内 ping テスト、または ping ベース専用プローブを使用しています。

図 *12 : ICMP* エコー動作



IP SLA ICMP エコー動作と ICMP ping テストは同じ IETF 仕様に準拠しているので、どちらの方法でも同じ応答時間が得られます。

IP SLA ICMP エコー動作の設定方法

ICMP エコー動作の設定

（注） 宛先デバイスで IP SLA Responder を設定する必要はありません。

次のいずれかの作業を実行します。

送信元デバイスでの基本 ICMP エコー動作の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **icmp-echo** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*} | **source-interface** *interface-name*]
5. **frequency** *seconds*
6. **end**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	**ip sla** *operation-number* 例： `Device(config)# ip sla 6`	IP SLA 動作の設定を開始し、IP SLA コンフィギュレーション モードに移行します。
ステップ 4	**icmp-echo** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*} | **source-interface** *interface-name*] 例： `Device(config-ip-sla)# icmp-echo 172.29.139.134`	ICMP エコー動作を定義し、IP SLA ICMP エコー コンフィギュレーション モードを開始します。
ステップ 5	**frequency** *seconds* 例： `Device(config-ip-sla-echo)# frequency 300`	（任意）指定した IP SLA 動作を繰り返す間隔を設定します。
ステップ 6	**end** 例： `Device(config-ip-sla-echo)# end`	特権 EXEC モードに戻ります。

次のタスク

トラップを生成する目的、または別の動作を開始する目的で、IP SLA 動作に予防的しきい値条件と反応トリガーを追加するには、「予防的しきい値モニタリングの設定」の項を参照してください。

オプション パラメータを使用した ICMP エコー動作の設定

このタスクは、送信元デバイスで実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **icmp-echo** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*} | **source-interface** *interface-name*]
5. **data-pattern** *hex value*
6. **history buckets-kept** *size*
7. **history distributions-of-statistics-kept** *size*
8. **history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*]
9. **history filter** {**none** | **all** | **overThreshold** | **failures**}
10. **frequency** *seconds*
11. **history hours-of-statistics-kept** *hours*
12. **history lives-kept** *lives*
13. **owner** *owner-id*
14. **request-data-size** *bytes*
15. **history statistics-distribution-interval** *milliseconds*
16. **tag** *text*
17. **threshold** *milliseconds*
18. **timeout** *milliseconds*
19. 次のいずれかを実行します。
    - **tos** *number*
    - **traffic-class** *number*
20. **flow-label** *number*
21. **verify-data**
22. **vrf** *vrf-name*
23. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	`Device> enable`	
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	**ip sla** *operation-number* 例： `Device(config)# ip sla 6`	IP SLA 動作の設定を開始し、IP SLA コンフィギュレーション モードに移行します。
ステップ 4	**icmp-echo** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*} | **source-interface** *interface-name*] 例： `Device(config-ip-sla)# icmp-echo 172.29.139.134 source-ip 172.29.139.132`	エコー動作を定義し、IP SLA エコー コンフィギュレーション モードを開始します。
ステップ 5	**data-pattern** *hex value* 例： `Device(config-ip-sla-echo)# data pattern FFFFFFFF`	（任意）データ パターンの 16 進数値を設定します。 指定できる範囲は 0 ～ FFFFFFFF です。
ステップ 6	**history buckets-kept** *size* 例： `Device(config-ip-sla-echo)# history buckets-kept 25`	（任意）IP SLA 動作のライフタイム中に保持する履歴バケット数を設定します。
ステップ 7	**history distributions-of-statistics-kept** *size* 例： `Device(config-ip-sla-echo)# history distributions-of-statistics-kept 5`	（任意）IP SLA 動作中にホップ単位で保持する統計情報の配信数を設定します。
ステップ 8	**history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*] 例： `Device(config-ip-sla-echo)# history enhanced interval 900 buckets 100`	（任意）IP SLA 動作に対する拡張履歴収集をイネーブルにします。
ステップ 9	**history filter** {**none** | **all** | **overThreshold** | **failures**} 例：	（任意）IP SLA 動作の履歴テーブルに格納する情報のタイプを定義します。

	コマンドまたはアクション	目的
	`Device(config-ip-sla-echo)# history filter failures`	
ステップ 10	**frequency** *seconds* 例： `Device(config-ip-sla-echo)# frequency 30`	（任意）指定した IP SLA 動作を繰り返す間隔を設定します。
ステップ 11	**history hours-of-statistics-kept** *hours* 例： `Device(config-ip-sla-echo)# history hours-of-statistics-kept 4`	（任意）IP SLA 動作の統計情報を保持する時間数を設定します。
ステップ 12	**history lives-kept** *lives* 例： `Device(config-ip-sla-echo)# history lives-kept 5`	（任意）IP SLA 動作の履歴テーブルに格納するライフ数を設定します。
ステップ 13	**owner** *owner-id* 例： `Device(config-ip-sla-echo)# owner admin`	（任意）IP SLA 動作の簡易ネットワーク管理プロトコル（SNMP）所有者を設定します。
ステップ 14	**request-data-size** *bytes* 例： `Device(config-ip-sla-echo)# request-data-size 64`	（任意）IP SLA 動作の要求パケットのペイロードにおけるプロトコル データ サイズを設定します。
ステップ 15	**history statistics-distribution-interval** *milliseconds* 例： `Device(config-ip-sla-echo)# history statistics-distribution-interval 10`	（任意）IP SLA 動作で維持する各統計情報の配信間隔を設定します。
ステップ 16	**tag** *text* 例： `Device(config-ip-sla-echo)# tag TelnetPollServer1`	（任意）IP SLA 動作のユーザ指定 ID を作成します。
ステップ 17	**threshold** *milliseconds* 例： `Device(config-ip-sla-echo)# threshold 10000`	（任意）IP SLA 動作によって作成されるネットワーク モニタリング統計情報を計算するための上限しきい値を設定します。

	コマンドまたはアクション	目的
ステップ 18	**timeout** *milliseconds* 例： `Device(config-ip-sla-echo)# timeout 10000`	（任意）IP SLA 動作がその要求パケットからの応答を待機する時間を設定します。

ステップ 19	次のいずれかを実行します。
	• **tos** *number*
	• **traffic-class** *number*
	例：
	`Device(config-ip-sla-jitter)# tos 160`
	例：
	`Device(config-ip-sla-jitter)# traffic-class 160`
		（任意）IPv4 ネットワークに限り、IP SLA 動作の IPv4 ヘッダーの ToS バイトを定義します。
		または
		（任意）IPv6 ネットワークに限り、サポートされている IP 動作に対する IPv6 ヘッダーのトラフィック クラス バイトを定義します。

ステップ 20	**flow-label** *number* 例： `Device(config-ip-sla-echo)# flow-label 112233`	（任意）IPv6 ネットワークに限り、サポートされている IP SLA 動作に対する IPv6 ヘッダーのフローラベル フィールドを定義します。
ステップ 21	**verify-data** 例： `Device(config-ip-sla-echo)# verify-data`	（任意）IP SLA 動作が各応答パケットに対してデータ破壊の有無をチェックするようにします。
ステップ 22	**vrf** *vrf-name* 例： `Device(config-ip-sla-echo)# vrf vpn-A`	（任意）IP SLA 動作を使用して、マルチプロトコル ラベル スイッチング（MPLS）バーチャル プライベート ネットワーク（VPN）内をモニタリングできるようにします。
ステップ 23	**end** 例： `Device(config-ip-sla-echo)# end`	特権 EXEC モードに戻ります。

次のタスク

トラップを生成する目的、または別の動作を開始する目的で、IP SLA 動作に予防的しきい値条件と反応トリガーを追加するには、「予防的しきい値モニタリングの設定」の項を参照してください。

IP SLA 動作のスケジューリング

始める前に

- スケジュールされるすべての IP サービス レベル契約（SLA）動作がすでに設定されている必要があります。
- 複数動作グループでスケジュールされたすべての動作の頻度が同じでなければなりません。
- 複数動作グループに追加する 1 つ以上の動作 ID 番号のリストは、カンマ（,）を含めて最大 125 文字に制限する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します。
   - **ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {[*hh*:*mm*:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**]
   - **ip sla group schedule** *group-operation-number operation-id-numbers* { **schedule-period** *schedule-period-range* | **schedule-together**} [**ageout** *seconds*] **frequency** *group-operation-frequency* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm* [:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm* [:*ss*]}]
4. **end**
5. **show ip sla group schedule**
6. **show ip sla configuration**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	次のいずれかのコマンドを入力します。 • **ip sla schedule** *operation-number* [**life** {**forever**	*seconds*}] [**start-time** {[*hh*:*mm*:*ss*] [*month day*	*day month*]	**pending**	**now**	**after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**]	• 個々の IP SLA 動作のスケジューリング パラメータを設定します。 • 複数動作スケジューラ用に IP SLA 動作グループ番号と動作番号の範囲を指定します。

	コマンドまたはアクション	目的

	• **ip sla group schedule** *group-operation-number operation-id-numbers* { **schedule-period** *schedule-period-range* | **schedule-together**} [**ageout** *seconds*] **frequency** *group-operation-frequency* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm* [:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm* [:*ss*]}]
	例：
	`Device(config)# ip sla schedule 10 life forever start-time now`
	`Device(config)# ip sla group schedule 10 schedule-period frequency`
	`Device(config)# ip sla group schedule 1 3,4,6-9 life forever start-time now`
	`Device(config)# ip sla schedule 1 3,4,6-9 schedule-period 50 frequency range 80-100`	

ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	**show ip sla group schedule** 例： `Device# show ip sla group schedule`	（任意）IP SLA グループ スケジュールの詳細を表示します。
ステップ 6	**show ip sla configuration** 例： `Device# show ip sla configuration`	（任意）IP SLA 設定の詳細を表示します。

トラブルシューティングのヒント

- IP サービス レベル契約（SLA）動作が実行中でなく、統計情報が生成されていない場合は、設定に **verify-data** コマンドを追加して（IP SLA コンフィギュレーション モードで設定）、データ検証をイネーブルにします。データ検証をイネーブルにすると、各動作の応答で破損の有無がチェックされます。通常の動作時に **verify-data** コマンドを使用すると、不要なオーバーヘッドがかかるので注意してください。
- IP SLA 動作に関する問題をトラブルシューティングするには、**debug ip sla trace** コマンドと **debug ip sla error** コマンドを使用します。

次の作業

トラップを生成する目的（または別の動作を開始する目的）で、IPサービス レベル契約（SLA）動作に予防的しきい値条件と反応トリガーを追加するには、「予防的しきい値モニタリングの設定」の項を参照してください。

IP SLA ICMP エコー動作の設定例

ICMP エコー動作の設定例

次に、ただちに開始され、無期限に実行される ICMP エコーの IP SLA 動作タイプを設定する例を示します。

```
ip sla 6
 icmp-echo 172.29.139.134 source-ip 172.29.139.132
 frequency 300
 request-data-size 28
 tos 160
 timeout 2000
 tag SFO-RO
ip sla schedule 6 life forever start-time now
```

IP SLA ICMP エコー動作に関するその他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IP SLA コマンド	『Cisco IOS IP SLAs Command Reference』
Cisco IP SLA に関する情報	『*IP SLA* コンフィギュレーション ガイド』の「Cisco IOS IP SLA の概要」モジュール

標準および RFC

標準/RFC	タイトル
RFC 862	Echo Protocol

MIB

MIB	MIB のリンク
CISCO-RTTMON-MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャセットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IP SLA ICMP エコー動作の機能情報

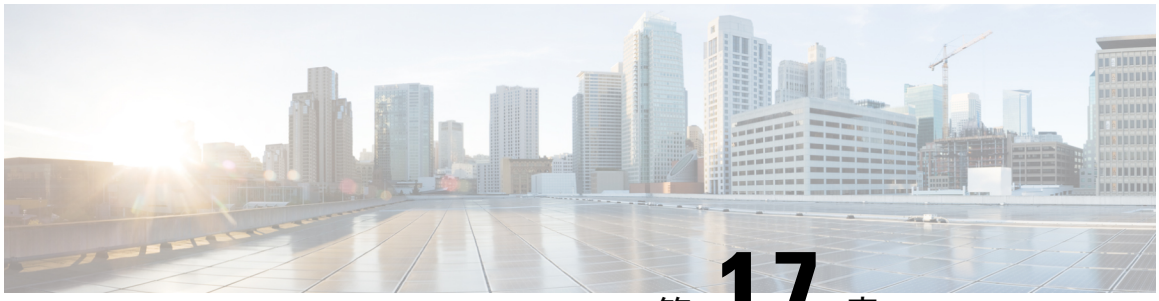
次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *25 : IP SLA ICMP* エコー動作の機能情報

機能名	リリース	機能情報
IP SLA ICMP エコー動作		Cisco IOS IP SLA インターネット制御メッセージ プロトコル（ICMP）エコー動作を使用すると、シスコデバイスと IP を使用するその他のデバイスの間のエンドツーエンドのネットワーク応答時間を測定できます。

機能名	リリース	機能情報
IPv6：IP SLA（UDP ジッタ、UDP エコー、ICMP エコー、TCP 接続）		IPv6ネットワークでの動作を可能にするためにサポートが追加されました。



第 17 章

IP SLA ICMP パス エコー動作の設定

このモジュールでは、シスコ デバイスと IP を使用する他のデバイスの間のエンドツーエンドおよびホップバイホップの応答時間をモニタするように、IP サービス レベル契約（SLA）のインターネット制御メッセージ プロトコル（ICMP）パス エコー動作を設定する方法について説明します。ICMP パス エコーは、ネットワークの可用性を判断するため、また、ネットワークの接続問題をトラブルシューティングするために役立ちます。ICMP パス エコー動作の結果を表示し、分析することで、ICMP の実行状態を判断できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

IP SLA ICMP パス エコー動作に関する制約事項

RFC 862 のエコー プロトコルをサポートするネットワーキング デバイスであれば使用できますが、シスコのネットワーキング デバイスを宛先デバイスとして使用することを推奨します。

IP SLA ICMP パス エコー動作に関する情報

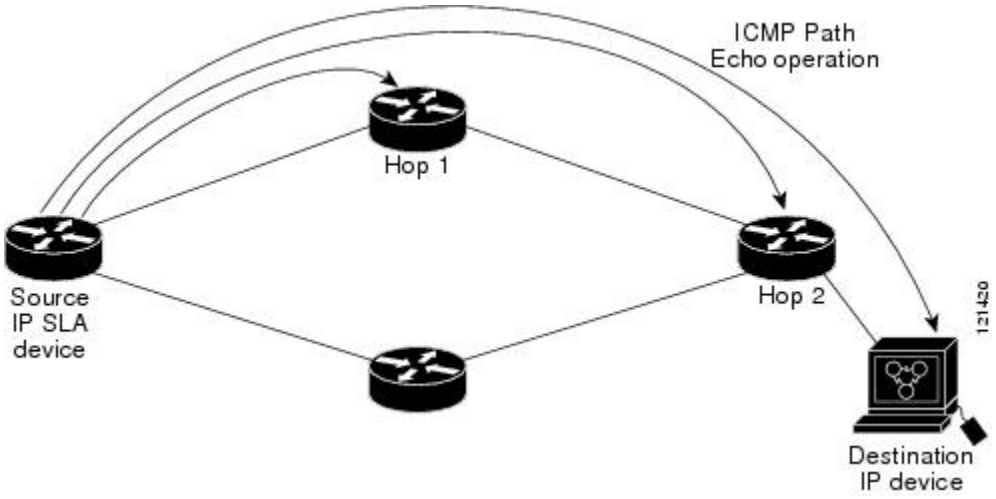
ICMP パス エコー動作

デバイス上の ICMP パス エコー パフォーマンスをモニタするには、IP SLA ICMP パス エコー動作を使用します。ICMP パス エコー動作は、シスコ デバイスと IP を使用する他のデバイスとの間でエンドツーエンドおよびホップバイホップの応答時間を測定します。ICMP パス エコーは、ネットワークの可用性を判断するため、また、ネットワークの接続問題をトラブルシューティングするために役立ちます。

IP SLA ICMP パス エコー動作は、IP SLA 動作が宛先に到達するためにたどるパスに沿った各ホップの統計情報を記録します。ICMP パス エコー動作では、traceroute 機能を使用してパスを検出することにより、シスコ デバイスとネットワーク上の IP デバイスの間のこのホップバイホップ応答時間が判断されます。

次の図では、送信元 IP SLA デバイスは、traceroute を使用して宛先 IP デバイスへのパスを検出します。その後、ping を使用して、送信元 IP SLA デバイスと、宛先 IP デバイスへのパス中の以降の各ホップの間の応答時間が測定されます。

図 *13 : ICMP* パス エコー動作



応答時間と可用性に関して記録された統計情報を使用することで、ICMP パス エコー動作では、ボトルネックを引き起こしているパス上のホップを識別できます。

IP SLA ICMP パス エコー動作の設定方法

送信元デバイスでの ICMP パス エコー動作の設定

（注） この動作には、送信先デバイスの IP SLA Responder は必要ありません。

次のいずれかの作業のみを実行します。

送信元デバイスでの基本 ICMP パス エコー動作の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-id*
4. **path-echo** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*}]
5. **frequency** *seconds*
6. **end**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	**ip sla** *operation-id* 例： `Device(config)# ip sla 7`	設定されている動作用に ID 番号を指定し、IP SLA 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	**path-echo** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*}] 例： `Device(config-ip-sla)# path-echo 172.29.139.134`	パス エコー動作を定義し、IP SLA パス エコー コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**frequency** *seconds* 例： `Device(config-ip-sla-pathEcho)# frequency 30`	（任意）指定した IP SLA 動作を繰り返す間隔を設定します。
ステップ 6	**end** 例： `Device(config-ip-sla-pathEcho)# end`	特権 EXEC モードに戻ります。

例

次に、30 秒以内に開始され、5 分間実行する IP SLA ICMP パス エコー動作番号 7 の設定例を示します。

```
ip sla 7
 path-echo 172.29.139.134
 frequency 30
!
ip sla schedule 7 start-time after 00:00:30 life 300
```

送信元デバイスでのオプション パラメータを使用した ICMP パス エコー動作の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **path-echo** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*}]
5. **history buckets-kept** *size*
6. **history distributions-of-statistics-kept** *size*
7. **history filter** {**none** | **all** | **overThreshold** | **failures**}
8. **frequency** *seconds*
9. **history hours-of-statistics-kept** *hours*
10. **history lives-kept** *lives*
11. **owner** *owner-id*
12. **paths-of-statistics-kept** *size*
13. **request-data-size** *bytes*
14. **samples-of-history-kept** *samples*
15. **history statistics-distribution-interval** *milliseconds*
16. **tag** *text*
17. **threshold** *milliseconds*
18. **timeout** *milliseconds*
19. **tos** *number*

20. **verify-data**
21. **vrf** *vrf-name*
22. **end**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	**ip sla** *operation-number* 例： `Device(config)# ip sla 10`	IP SLA 動作の設定を開始し、IP SLA コンフィギュレーション モードに移行します。
ステップ 4	**path-echo** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*}] 例： `Device(config-ip-sla)# path-echo 172.29.139.134`	パス エコー動作を定義し、IP SLA パス エコー コンフィギュレーション モードを開始します。
ステップ 5	**history buckets-kept** *size* 例： `Device(config-ip-sla-pathEcho)# history buckets-kept 25`	（任意）IP SLA 動作のライフタイム中に保持する履歴バケット数を設定します。
ステップ 6	**history distributions-of-statistics-kept** *size* 例： `Device(config-ip-sla-pathEcho)# history distributions-of-statistics-kept 5`	（任意）IP SLA 動作中にホップ単位で保持する統計情報の配信数を設定します。
ステップ 7	**history filter** {**none** | **all** | **overThreshold** | **failures**} 例： `Device(config-ip-sla-pathEcho)# history filter failures`	（任意）IP SLA 動作の履歴テーブルに格納する情報のタイプを定義します。

	コマンドまたはアクション	目的
ステップ 8	**frequency** *seconds* 例： `Device(config-ip-sla-pathEcho)# frequency 30`	（任意）指定した IP SLA 動作を繰り返す間隔を設定します。
ステップ 9	**history hours-of-statistics-kept** *hours* 例： `Device(config-ip-sla-pathEcho)# history hours-of-statistics-kept 4`	（任意）IP SLA 動作の統計情報を保持する時間数を設定します。
ステップ 10	**history lives-kept** *lives* 例： `Device(config-ip-sla-pathEcho)# history lives-kept 5`	（任意）IP SLA 動作の履歴テーブルに格納するライフ数を設定します。
ステップ 11	**owner** *owner-id* 例： `Device(config-ip-sla-pathEcho)# owner admin`	（任意）IP SLA 動作の簡易ネットワーク管理プロトコル（SNMP）所有者を設定します。
ステップ 12	**paths-of-statistics-kept** *size* 例： `Device(config-ip-sla-pathEcho)# paths-of-statistics-kept 3`	（任意）IP SLA 動作の統計情報を保持するパス数（時間単位）を設定します。
ステップ 13	**request-data-size** *bytes* 例： `Device(config-ip-sla-pathEcho)# request-data-size 64`	（任意）IP SLA 動作の要求パケットのペイロードにおけるプロトコル データ サイズを設定します。
ステップ 14	**samples-of-history-kept** *samples* 例： `Device(config-ip-sla-pathEcho)# samples-of-history-kept 10`	（任意）IP SLA 動作の履歴テーブルに格納するエントリ数（バケット単位）を設定します。
ステップ 15	**history statistics-distribution-interval** *milliseconds* 例： `Device(config-ip-sla-pathEcho)# history statistics-distribution-interval 10`	（任意）IP SLA 動作で維持する各統計情報の配信間隔を設定します。

	コマンドまたはアクション	目的
ステップ 16	**tag** *text* 例： `Device(config-ip-sla-pathEcho)# tag TelnetPollServer1`	（任意）IP SLA 動作のユーザ指定 ID を作成します。
ステップ 17	**threshold** *milliseconds* 例： `Device(config-ip-sla-pathEcho)# threshold 10000`	（任意）IP SLA 動作によって作成されるネットワーク モニタリング統計情報を計算するための上限しきい値を設定します。
ステップ 18	**timeout** *milliseconds* 例： `Device(config-ip-sla-pathEcho)# timeout 10000`	（任意）IP SLA 動作がその要求パケットからの応答を待機する時間を設定します。
ステップ 19	**tos** *number* 例： `Device(config-ip-sla-pathEcho)# tos 160`	（任意）IP SLA 動作の IP ヘッダー内のタイプ オブ サービス（ToS）バイトを定義します。
ステップ 20	**verify-data** 例： `Device(config-ip-sla-pathEcho)# verify-data`	（任意）IP SLA 動作が各応答パケットに対してデータ破壊の有無をチェックするようにします。
ステップ 21	**vrf** *vrf-name* 例： `Device(config-ip-sla-pathEcho)# vrf vpn-A`	（任意）IP SLA 動作を使用して、マルチプロトコル ラベル スイッチング（MPLS）バーチャル プライベート ネットワーク（VPN）内をモニタリングできるようにします。
ステップ 22	**end** 例： `Device(config-ip-sla-pathEcho)# end`	特権 EXEC モードに戻ります。

IP SLA 動作のスケジューリング

始める前に

- スケジュールされるすべての IP サービス レベル契約（SLA）動作がすでに設定されている必要があります。
- 複数動作グループでスケジュールされたすべての動作の頻度が同じでなければなりません。

- 複数動作グループに追加する 1 つ以上の動作 ID 番号のリストは、カンマ（,）を含めて最大 125 文字に制限する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します。
   - **ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {[*hh*:*mm*:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**]
   - **ip sla group schedule** *group-operation-number operation-id-numbers* { **schedule-period** *schedule-period-range* | **schedule-together**} [**ageout** *seconds*] **frequency** *group-operation-frequency* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm* [:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm* [:*ss*]}]
4. **end**
5. **show ip sla group schedule**
6. **show ip sla configuration**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	次のいずれかのコマンドを入力します。 • **ip sla schedule** *operation-number* [**life** {**forever**	*seconds*}] [**start-time** {[*hh*:*mm*:*ss*] [*month day*	*day month*]	**pending**	**now**	**after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**] • **ip sla group schedule** *group-operation-number operation-id-numbers* { **schedule-period** *schedule-period-range*	**schedule-together**} [**ageout** *seconds*] **frequency** *group-operation-frequency* [**life** {**forever**	*seconds*}] [**start-time** {*hh*:*mm* [:*ss*] [*month day*	*day month*]	**pending**	**now**	**after** *hh*:*mm* [:*ss*]}] 例： `Device(config)# ip sla schedule 10 life forever start-time now`	• 個々の IP SLA 動作のスケジューリング パラメータを設定します。 • 複数動作スケジューラ用に IP SLA 動作グループ番号と動作番号の範囲を指定します。

	コマンドまたはアクション	目的

	`Device(config)# ip sla group schedule 10 schedule-period frequency`
	
	`Device(config)# ip sla group schedule 1 3,4,6-9 life forever start-time now`
	
	`Device(config)# ip sla schedule 1 3,4,6-9 schedule-period 50 frequency range 80-100`	

ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	**show ip sla group schedule** 例： `Device# show ip sla group schedule`	（任意）IP SLA グループ スケジュールの詳細を表示します。
ステップ 6	**show ip sla configuration** 例： `Device# show ip sla configuration`	（任意）IP SLA 設定の詳細を表示します。

トラブルシューティングのヒント

- IP サービス レベル契約（SLA）動作が実行中でなく、統計情報が生成されていない場合は、設定に **verify-data** コマンドを追加して（IP SLA コンフィギュレーション モードで設定）、データ検証をイネーブルにします。データ検証をイネーブルにすると、各動作の応答で破損の有無がチェックされます。通常の動作時に **verify-data** コマンドを使用すると、不要なオーバーヘッドがかかるので注意してください。
- IP SLA 動作に関する問題をトラブルシューティングするには、**debug ip sla trace** コマンドと **debug ip sla error** コマンドを使用します。

次の作業

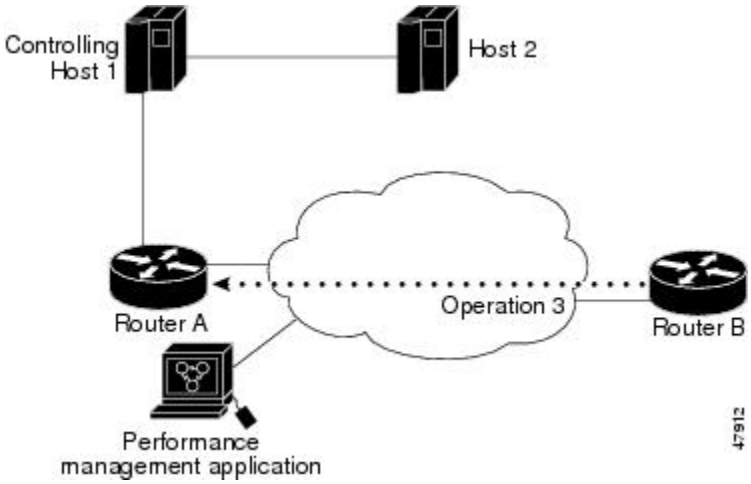
トラップを生成する目的（または別の動作を開始する目的）で、IPサービス レベル契約（SLA）動作に予防的しきい値条件と反応トリガーを追加するには、「予防的しきい値モニタリングの設定」の項を参照してください。

IP SLA ICMP パス エコー動作の設定例

ICMP パス エコー動作の設定例

次に、30 秒後に開始され、5 分間実行される ICMP パス エコーの IP SLA 動作タイプを設定する例を示します。次の図は、ICMP パス エコー動作を示しています。

図 *14 : ICMP* パス エコー動作



次の例では、IP/ICMP を使用してデバイス B からデバイス A へのパス エコー動作（ip sla 3）を設定します。この動作は、（1 回目を 0 秒として）25 秒以内に 3 回試行されます。

デバイス B の設定

```
ip sla 3
 path-echo 172.29.139.134
 frequency 10
 tag SGN-RO
 timeout 1000
ip sla schedule 3 life 25
```

IP SLA ICMP エコー動作に関するその他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IP SLA コマンド	『Cisco IOS IP SLAs Command Reference』

関連項目	マニュアル タイトル
Cisco IP SLA に関する情報	『*IP SLA* コンフィギュレーション ガイド』の「Cisco IOS IP SLA の概要」モジュール

標準および RFC

標準/RFC	タイトル
RFC 862	Echo Protocol

MIB

MIB	MIB のリンク
CISCO-RTTMON-MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

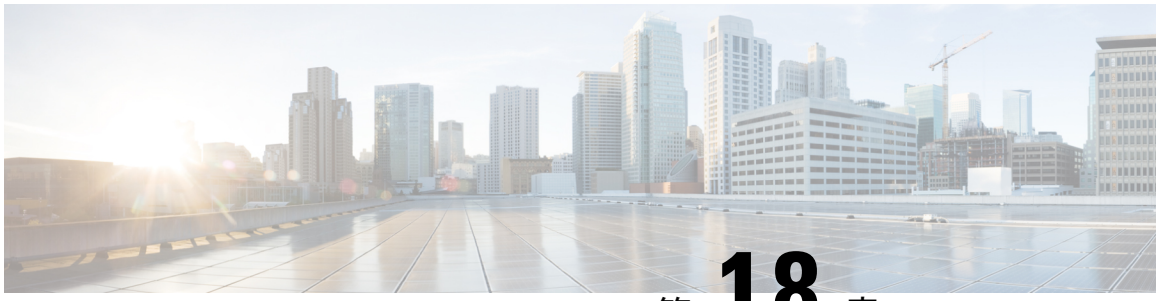
IP SLA ICMP パス エコー動作の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *26 : IP SLA ICMP* パス エコー動作の機能情報

機能名	リリース	機能情報
IP SLA ICMP パス エコー動作	12.2(31)SB2 12.2(33)SRB1 12.2(33)SXH 12.3(14)T Cisco IOS XE Release 2.1 15.0(1)S Cisco IOS XE 3.1.0SG	Cisco IOS IP SLA インターネット制御メッセージ プロトコル（ICMP）パス エコー動作を使用すると、シスコ デバイスと IP を使用するその他のデバイスの間のエンドツーエンドおよびホップバイホップのネットワーク応答時間を測定できます。
IP SLA 4.0 - IP v6 phase2	15.2(3)T Cisco IOS XE Release 3.7S 15.1(2)SG Cisco IOS XE Release 3.4SG	IPv6 ネットワークでの動作を可能にするためにサポートが追加されました。 次のコマンドが導入または変更されました。**path-echo**（(IP SLA）、**show ip sla configuration**、**show ip sla summary**



第 18 章

IP SLA ICMP パス ジッター動作の設定

このマニュアルでは、ホップバイホップ ジッター（パケット間の遅延のばらつき）をモニタするために、IP サービス レベル契約（SLA）インターネット制御メッセージプロトコル（ICMP）パス ジッター動作を設定する方法について説明します。このマニュアルでは、パス ジッター動作を使用して収集されたデータを表示し、Cisco コマンドを使用してこれらのデータを分析する方法についても説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

ICMP パス ジッター動作の前提条件

- IP SLA アプリケーションを設定する前に、**show ip sla application** コマンドを使用して、ご使用のソフトウェア イメージでサポートされている動作タイプを確認してください。

- 他の IP SLA 動作とは異なって、パス ジッタ動作の中間デバイスまたはターゲット デバイスのいずれにおいても IP SLA Responder をイネーブルにする必要はありません。ただし、IP SLA Responder を有効にすると、動作の効率が向上する可能性があります。

ICMP パス ジッター動作の制限事項

- IP SLA - ICMP パス ジッターは ICMP ベースです。ICMP ベースの動作は、送信元の処理遅延を補うことはできますが、ターゲットの処理遅延を補うことはできません。より確実なモニタリングおよび検証を行う場合は、IP SLA UDP ジッター動作を使用することをお勧めします。
- ICMP には、デバイス上での処理時間をパケットに組み込む機能がないため、IP SLA - ICMP パス ジッター動作を使用して取得されたジッター値は概算になります。ターゲット デバイスが ICMP パケットのプライオリティを最高に設定しない場合、デバイスは正常に応答しません。ICMP パフォーマンスは、デバイス上のプライオリティ キューイング設定および ping 応答にも影響される場合があります。
- パス ジッター動作では、時間単位の統計情報およびホップ情報はサポートされていません。
- ICMP パス ジッタ動作は、他の IP SLA 動作とは異なり、RTTMON MIB ではサポートされません。パス ジッター動作は、Cisco コマンド以外では設定できません。統計情報は、**show ip sla** コマンドを使用しなければ返されません。
- ジッター動作には大量のデータが含まれるため、IP SLA - パス ジッターでは IP SLA 履歴機能（統計情報の履歴バケット）はサポートされていません。
- 次のコマンドはパス ジッター コンフィギュレーション モードで使用できますが、パス ジッター動作には適用しないでください。
  - **history buckets-kept**
  - **history distributions-of-statistics-kept**
  - **history enhanced**
  - **history filter**
  - **history hours-of-statistics-kept**
  - **history lives-kept**
  - **history statistics-distribution-interval**
  - **samples-of-history-kept**
  - **lsr-path**
  - **tos**
  - **threshold**
  - **verify-data**

IP SLA ICMP パス ジッター動作に関する情報

ICMP パス ジッター動作

IP SLA - ICMP パス ジッターは、IP ネットワーク内のホップバイホップ ジッター、パケット損失、および遅延測定統計情報を提供します。パス ジッター動作は、一方向データの総計と往復データの総計を提供する標準的な UDP ジッター動作とは異なる機能を果たします。

ICMP パス ジッター動作は、標準的な UDP ジッター動作を補完するものとして使用できます。たとえば、UDP ジッター動作から得られた結果が予期しない遅延や高いジッター値を示すことがあります。この場合に ICMP パス ジッター動作を使用すると、ネットワーク パスのトラブルシューティングを行い、伝送パス沿いの特定のセグメントでトラフィックが渋滞していないかどうかを確認できます。

ICMP パス ジッタ動作は、まず traceroute ユーティリティを使用して送信元から宛先までのホップバイホップ IP ルートを検出し、次に ICMP エコーを使用して、パス沿いの各ホップの応答時間、パケット損失、およびジッタの概算値を測定します。ICMP はラウンドトリップ時間しか提供しないため、IP SLA - ICMP パス ジッターを使用して取得されたジッター値は概算値になります。

ICMP パス ジッター動作は、送信元デバイスから指定した宛先デバイスまでの IP パスをトレースし、次にそのトレース パス沿いの各ホップに *N* 個のエコー プローブを *T* ミリ秒間隔で送信します。動作全体は、*F* 秒ごとに 1 回の頻度で繰り返されます。次に示すように、属性はユーザ設定可能です。

パス ジッタ動作パラメータ	デフォルト	設定方法
エコー プローブの数（*N*）	10 エコー	**path-jitter** コマンド、 **num-packets** オプション
エコー プローブ間隔（ミリ秒単位）（*T*）	20 ミリ秒	**path-jitter** コマンド、 **interval** オプション （注） 動作の頻度と動作の間隔は異なります。
動作の繰り返し頻度（*F*）	60 秒に 1 回	**frequency** コマンド

IP SLA ICMP パス ジッター動作の設定方法

宛先デバイスでの IP SLA Responder の設定

（注） IP SLA Responder は、パス ジッター動作のターゲット デバイスまたは中間デバイスでは必要ありません。ただし、IP SLA Responder を有効にすると、動作の効率性を向上できます。

始める前に

レスポンダとして使用するネットワーキング デバイスがシスコ デバイスであり、そのデバイスにネットワークを介して接続できる必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla responder**
4. **exit**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	**ip sla responder** 例： 例： `Device(config)# ip sla responder`	（任意）送信元からの制御メッセージに応じて、シスコ デバイスにおける IP SLA Responder 機能を一時的にイネーブルにします。 • 制御は、デフォルトでイネーブルになります。
ステップ 4	**exit** 例：	（任意）グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config)# exit`	

送信元デバイスでの ICMP パス ジッター動作の設定

この項の次のいずれかの手順のみを実行します。

基本的な ICMP パス ジッター動作の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **path-jitter** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*}] [**num-packets** *packet-number*] [**interval** *milliseconds*] [**targetOnly**]
5. **frequency** *seconds*
6. **end**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	**ip sla** *operation-number* 例： `Device(config)# ip sla 10`	IP SLA 動作の設定を開始し、IP SLA コンフィギュレーション モードに移行します。
ステップ 4	**path-jitter** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*}] [**num-packets** *packet-number*] [**interval** *milliseconds*] [**targetOnly**] 例： `Device(config-ip-sla)# path-jitter 172.31.1.129 source-ip 10.2.30.1 num-packets 12 interval 22`	ICMP パス ジッター動作を設定するための IP SLA パス ジッター コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**frequency** *seconds* 例： `Device(config-ip-sla-pathJitter)# frequency 30`	（任意）指定した IP SLA 動作を繰り返す間隔を設定します。
ステップ 6	**end** 例： `Device(config-ip-sla-pathJitter)# end`	特権 EXEC モードに戻ります。

例

次の例では、**targetOnly** キーワードを使用してホップバイホップ測定を回避します。コマンドのこのバージョンを使用した場合、エコープローブは宛先のみに送信されます。

```
Device(config)# ip sla 1
Device(config-ip-sla)# path-jitter 172.17.246.20 num-packets 50 interval 30 targetOnly
```

追加パラメータを指定した ICMP パス ジッター動作の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **path-jitter** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*}] [**num-packets** *packet-number*] [**interval** *milliseconds*] [**targetOnly**]
5. **frequency** *seconds*
6. **owner** *owner-id*
7. **request-data-size** *bytes*
8. **tag** *text*
9. **timeout** *milliseconds*
10. **vrf** *vrf-name*
11. **end**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
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	**ip sla** *operation-number* 例： `Device(config)# ip sla 10`	IP SLA 動作の設定を開始し、IP SLA コンフィギュレーション モードに移行します。
ステップ 4	**path-jitter** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*}] [**num-packets** *packet-number*] [**interval** *milliseconds*] [**targetOnly**] 例： `Device(config-ip-sla)# path-jitter 172.31.1.129 source-ip 10.2.30.1 num-packets 12 interval 22`	ICMP パス ジッター動作を定義するための IP SLA パス ジッター コンフィギュレーション モードを開始します。
ステップ 5	**frequency** *seconds* 例： `Device(config-ip-sla-pathJitter)# frequency 30`	（任意）指定した IP SLA 動作を繰り返す間隔を設定します。
ステップ 6	**owner** *owner-id* 例： `Device(config-ip-sla-pathJitter)# owner admin`	（任意）IP SLA 動作の簡易ネットワーク管理プロトコル（SNMP）所有者を設定します。
ステップ 7	**request-data-size** *bytes* 例： `Device(config-ip-sla-pathJitter)# request-data-size 64`	（任意）IP SLA 動作の要求パケットのペイロードにおけるプロトコル データ サイズを設定します。
ステップ 8	**tag** *text* 例： `Device(config-ip-sla-pathJitter)# tag TelnetPollServer1`	（任意）IP SLA 動作のユーザ指定 ID を作成します。
ステップ 9	**timeout** *milliseconds* 例： `Device(config-ip-sla-pathJitter)# timeout 10000`	（任意）IP SLA 動作がその要求パケットからの応答を待機する時間を設定します。

	コマンドまたはアクション	目的
ステップ 10	**vrf** *vrf-name* 例： `Device(config-ip-sla-pathJitter)# vrf vpn-A`	（任意）IP SLA 動作を使用して、マルチプロトコル ラベル スイッチング（MPLS）バーチャル プライベート ネットワーク（VPN）内をモニタリングできるようにします。
ステップ 11	**end** 例： `Device(config-ip-sla-pathJitter)# end`	特権 EXEC モードに戻ります。

IP SLA 動作のスケジューリング

始める前に

- スケジュールされるすべての IP サービス レベル契約（SLA）動作がすでに設定されている必要があります。
- 複数動作グループでスケジュールされたすべての動作の頻度が同じでなければなりません。
- 複数動作グループに追加する 1 つ以上の動作 ID 番号のリストは、カンマ（,）を含めて最大 125 文字に制限する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します。
   - **ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {[*hh*:*mm*:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**]
   - **ip sla group schedule** *group-operation-number operation-id-numbers* { **schedule-period** *schedule-period-range* | **schedule-together**} [**ageout** *seconds*] **frequency** *group-operation-frequency* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm* [:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm* [:*ss*]}]
4. **end**
5. **show ip sla group schedule**
6. **show ip sla configuration**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	`Device> enable`	
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	次のいずれかのコマンドを入力します。
	• **ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {[*hh*:*mm*:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**]
	• **ip sla group schedule** *group-operation-number operation-id-numbers* { **schedule-period** *schedule-period-range* |**schedule-together**} [**ageout** *seconds*] **frequency** *group-operation-frequency* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm* [:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm* [:*ss*]}]
	例：
	`Device(config)# ip sla schedule 10 life forever start-time now`
	`Device(config)# ip sla group schedule 10 schedule-period frequency`
	`Device(config)# ip sla group schedule 1 3,4,6-9 life forever start-time now`
	`Device(config)# ip sla schedule 1 3,4,6-9 schedule-period 50 frequency range 80-100`
		• 個々の IP SLA 動作のスケジューリング パラメータを設定します。
		• 複数動作スケジューラ用に IP SLA 動作グループ番号と動作番号の範囲を指定します。

ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	**show ip sla group schedule** 例： `Device# show ip sla group schedule`	（任意）IP SLA グループ スケジュールの詳細を表示します。
ステップ 6	**show ip sla configuration** 例： `Device# show ip sla configuration`	（任意）IP SLA 設定の詳細を表示します。

トラブルシューティングのヒント

- IP サービス レベル契約（SLA）動作が実行中でなく、統計情報が生成されていない場合は、設定に **verify-data** コマンドを追加して（IP SLA コンフィギュレーション モードで設定）、データ検証をイネーブルにします。データ検証をイネーブルにすると、各動作の応答で破損の有無がチェックされます。通常の動作時に **verify-data** コマンドを使用すると、不要なオーバーヘッドがかかるので注意してください。
- IP SLA 動作に関する問題をトラブルシューティングするには、**debug ip sla trace** コマンドと **debug ip sla error** コマンドを使用します。

次の作業

トラップを生成する目的（または別の動作を開始する目的）で、IPサービス レベル契約（SLA）動作に予防的しきい値条件と反応トリガーを追加するには、「予防的しきい値モニタリングの設定」の項を参照してください。

IP SLA ICMP パス ジッター動作の設定例

パス ジッター動作の設定例

次に、ICMPパス ジッター動作が設定されている場合の出力例を示します。パス ジッター動作は時間単位の統計情報およびホップ情報をサポートしていないので、パス ジッター動作の **show ip sla statistics** コマンドの出力では、最初のホップの統計情報のみが表示されます。

次に、ICMP パス ジッター動作が設定されている場合の出力例を示します。

```
Device# configure terminal
Device(config)# ip sla 15011
Device(config-sla-monitor)# path-jitter 10.222.1.100 source-ip 10.222.3.100 num-packets
 20
Device(config-sla-monitor-pathJitter)# frequency 30
Device(config-sla-monitor-pathJitter)# exit
Device(config)# ip sla schedule 15011 life forever start-time now
Device(config)# exit
Device# show ip sla statistics 15011
Round Trip Time (RTT) for       Index 15011
        Latest RTT: 1 milliseconds
Latest operation start time: 15:37:35.443 EDT Mon Jun 16 2008
Latest operation return code: OK
---- Path Jitter Statistics ----
Hop IP 10.222.3.252:
Round Trip Time milliseconds:
        Latest RTT: 1 ms
        Number of RTT: 20
        RTT Min/Avg/Max: 1/1/3 ms
Jitter time milliseconds:
        Number of jitter: 2
        Jitter Min/Avg/Max: 2/2/2 ms
Packet Values:
        Packet Loss (Timeouts): 0
```

```
        Out of Sequence: 0
        Discarded Samples: 0
Operation time to live: Forever
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
Cisco IOS IP SLA コマンド	『Cisco IOS IP SLA コマンド リファレンス』

標準および RFC

標準/RFC	タイトル
RFC 1889[4]	『*RTP: A Transport Protocol for Real-Time Applications*』（「Estimating the Interarrival Jitter」の項を参照）

[4] 表示されている RFC は、サポートを主張するものではありません（参考までに表示します）。

MIB

MIB	MIB のリンク
パス ジッタ動作に関する MIB サポートはありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

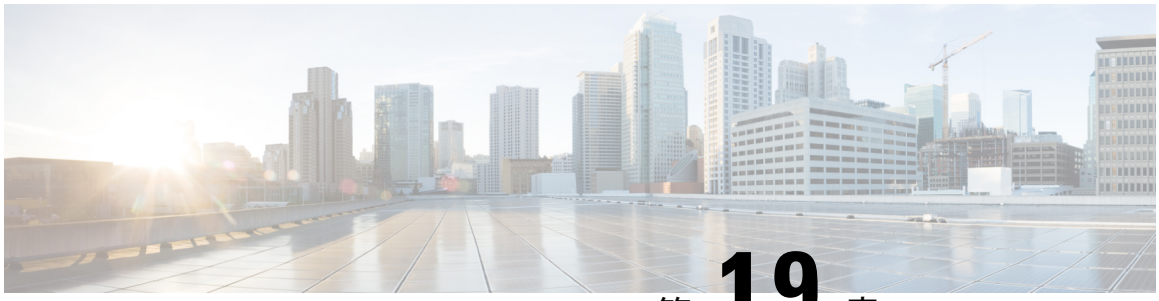
IP SLA ICMP パス ジッター動作の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *27 : IP SLA ICMP* パス ジッター動作の機能情報

機能名	リリース	機能情報
IP SLA パス ジッター動作		Cisco IOS IP SLA インターネット制御メッセージ プロトコル（ICMP）パス ジッター動作を使用すると、ホップバイホップ ジッタ（パケット間の遅延の分散）を測定できます。
IPSLA 4.0 - IP v6 phase2		IPv6 ネットワークでの動作を可能にするためにサポートが追加されました。 次のコマンドが導入または変更されました。**path- jitter**、**show ip sla configuration**、**show ip sla summary**



第 19 章

IP SLA FTP 動作の設定

このモジュールでは、シスコ デバイスと FTP サーバの間でファイルを取得するための応答時間を測定するように、IP サービス レベル契約（SLA）ファイル転送プロトコル（FTP）動作を設定する方法について説明します。IP SLA FTP 動作は FTP GET 要求だけをサポートします。また、このモジュールでは、FTP 動作の結果を表示および分析してネットワークの容量を調べる方法についても説明します。FTP 動作は FTP サーバのパフォーマンスをトラブルシューティングするためにも使用できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

IP SLA FTP 動作の制約事項

IP SLA FTP 動作は FTP GET（ダウンロード）要求だけをサポートします。

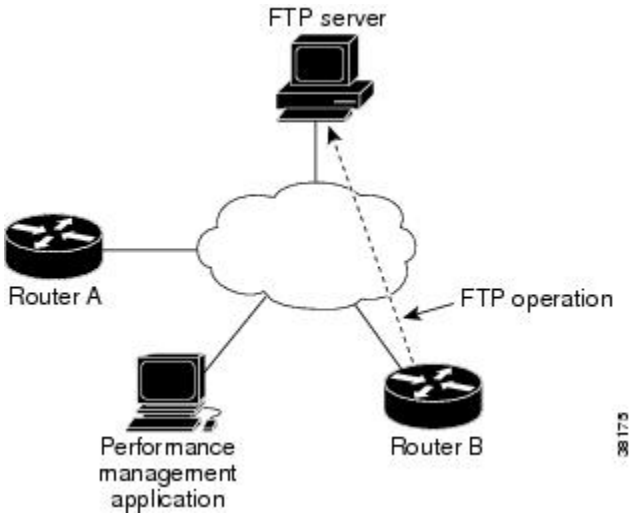
IP SLA FTP 動作に関する情報

FTP 動作

FTP 動作は、シスコ デバイスと FTP サーバの間でファイルを取得するためのラウンドトリップ時間（RTT）を測定します。FTP は、伝送制御プロトコル（TCP）/IP プロトコル スタックの一部であるアプリケーション プロトコルであり、ネットワーク ノード間でファイルを転送するために使用されます。

以下の図では、デバイス B が送信元 IP SLA デバイスとして設定され、宛先デバイスを FTP サーバとする FTP 動作が設定されています。

図 *15 : FTP* 動作



接続応答時間は、TCP 上で FTP を使用してリモート FTP サーバからデバイス B にファイルをダウンロードするのに要する時間を測定して算出されます。この動作は IP SLA Responder を使用しません。

（注） FTP ポート（ポート 21）に接続する際の応答時間をテストするには、IP SLA TCP 接続動作を使用します。

アクティブ FTP 転送モードとパッシブ FTP 転送モードの両方がサポートされます。パッシブモードはデフォルトでイネーブルになります。FTPGET（ダウンロード）動作タイプだけがサポートされます。FTP GET 動作に指定された URL は次のいずれかの形式である必要があります。

- ftp://ユーザ名:パスワード@ホスト/ファイル名
- ftp://ホスト/ファイル名

ユーザ名とパスワードが指定されていない場合のデフォルト値は、それぞれ anonymous と test です。

FTP は大量のデータ トラフィックを伝送するため、ネットワークのパフォーマンスに影響を与えることがあります。大きなファイルを取得する IP SLA FTP 動作の結果を使用してネットワークの能力を調べることができます。ただし、FTP 動作は多くの帯域幅を消費するため、大きなファイルを取得する際は注意してください。また、FTP 動作は、ファイルの取得に要する RTT を調べることにより FTP サーバのパフォーマンス レベルを測定します。

IP SLA FTP 動作の設定方法

送信元デバイスでの FTP 動作の設定

（注） 宛先デバイスで IP SLA Responder を設定する必要はありません。

次のいずれかの作業を実行します。

送信元デバイスでの基本 FTP 動作の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **ftp get** *url* [**source-ip** {*ip-address* | *hostname*}] [**mode** {**passive** | **active**}
5. **frequency** *seconds*
6. **end**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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。

	コマンドまたはアクション	目的
ステップ 3	**ip sla** *operation-number* 例： `Device(config)# ip sla 10`	IP SLA 動作の設定を開始し、IP SLA コンフィギュレーション モードに移行します。
ステップ 4	**ftp get** *url* [**source-ip** {*ip-address* | *hostname*}] [**mode** {**passive** | **active**} 例： `Device(config-ip-sla)# ftp get ftp://username:password@hostip/test.cap`	FTP 動作を定義し、IP SLA FTP コンフィギュレーション モードを開始します。
ステップ 5	**frequency** *seconds* 例： `Device(config-ip-sla-ftp)# frequency 30`	（任意）指定した IP SLA 動作を繰り返す間隔を設定します。
ステップ 6	**end** 例： `Device(config-ip-sla-ftp)# exit`	特権 EXEC モードに戻ります。

送信元デバイスでのオプション パラメータを使用した FTP 動作の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **ftp get** *url* [**source-ip** {*ip-address* | *hostname*}] [**mode** {**passive** | **active**}
5. **history buckets-kept** *size*
6. **history distributions-of-statistics-kept** *size*
7. **history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*]
8. **history filter** {**none** | **all** | **overThreshold** | **failures**}
9. **frequency** *seconds*
10. **history hours-of-statistics-kept** *hours*
11. **history lives-kept** *lives*
12. **owner** *owner-id*
13. **history statistics-distribution-interval** *milliseconds*
14. **tag** *text*
15. **threshold** *milliseconds*
16. **timeout** *milliseconds*
17. **end**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	**ip sla** *operation-number* 例： `Device(config)# ip sla 10`	IP SLA 動作の設定を開始し、IP SLA コンフィギュレーション モードに移行します。
ステップ 4	**ftp get** *url* [**source-ip** {*ip-address* | *hostname*}] [**mode** {**passive** | **active**} 例： `Device(config-ip-sla)# ftp get ftp://username:password@hostip/filename`	FTP 動作を定義し、IP SLA FTP コンフィギュレーション モードを開始します。
ステップ 5	**history buckets-kept** *size* 例： `Device(config-ip-sla-ftp)# history buckets-kept 25`	（任意）IP SLA 動作のライフタイム中に保持する履歴バケット数を設定します。
ステップ 6	**history distributions-of-statistics-kept** *size* 例： `Device(config-ip-sla-ftp)# history distributions-of-statistics-kept 5`	（任意）IP SLA 動作中にホップ単位で保持する統計情報の配信数を設定します。
ステップ 7	**history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*] 例： `Device(config-ip-sla-ftp)# history enhanced interval 900 buckets 100`	（任意）IP SLA 動作に対する拡張履歴収集をイネーブルにします。
ステップ 8	**history filter** {**none** | **all** | **overThreshold** | **failures**} 例： `Device(config-ip-sla-ftp)# history filter failures`	（任意）IP SLA 動作の履歴テーブルに格納する情報のタイプを定義します。

	コマンドまたはアクション	目的
ステップ 9	**frequency** *seconds* 例： `Device(config-ip-sla-ftp)# frequency 30`	（任意）指定した IP SLA 動作を繰り返す間隔を設定します。
ステップ 10	**history hours-of-statistics-kept** *hours* 例： `Device(config-ip-sla-ftp)# history hours-of-statistics-kept 4`	（任意）IP SLA 動作の統計情報を保持する時間数を設定します。
ステップ 11	**history lives-kept** *lives* 例： `Device(config-ip-sla-ftp)# history lives-kept 5`	（任意）IP SLA 動作の履歴テーブルに格納するライフ数を設定します。
ステップ 12	**owner** *owner-id* 例： `Device(config-ip-sla-ftp)# owner admin`	（任意）IP SLA 動作の簡易ネットワーク管理プロトコル（SNMP）所有者を設定します。
ステップ 13	**history statistics-distribution-interval** *milliseconds* 例： `Device(config-ip-sla-ftp)# history statistics-distribution-interval 10`	（任意）IP SLA 動作で維持する各統計情報の配信間隔を設定します。
ステップ 14	**tag** *text* 例： `Device(config-ip-sla-ftp)# tag TelnetPollServer1`	（任意）IP SLA 動作のユーザ指定 ID を作成します。
ステップ 15	**threshold** *milliseconds* 例： `Device(config-ip-sla-ftp)# threshold 10000`	（任意）IP SLA 動作によって作成されるネットワーク モニタリング統計情報を計算するための上限しきい値を設定します。
ステップ 16	**timeout** *milliseconds* 例： `Device(config-ip-sla-ftp)# timeout 10000`	（任意）IP SLA 動作がその要求パケットからの応答を待機する時間を設定します。
ステップ 17	**end** 例： `Device(config-ip-sla-ftp)# end`	特権 EXEC モードに戻ります。

IP SLA 動作のスケジューリング

始める前に

- スケジュールされるすべての IP サービス レベル契約（SLA）動作がすでに設定されている必要があります。
- 複数動作グループでスケジュールされたすべての動作の頻度が同じでなければなりません。
- 複数動作グループに追加する 1 つ以上の動作 ID 番号のリストは、カンマ（,）を含めて最大 125 文字に制限する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します。
   - **ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {[*hh*:*mm*:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**]
   - **ip sla group schedule** *group-operation-number operation-id-numbers* { **schedule-period** *schedule-period-range* | **schedule-together**} [**ageout** *seconds*] **frequency** *group-operation-frequency* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm* [:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm* [:*ss*]}]
4. **end**
5. **show ip sla group schedule**
6. **show ip sla configuration**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	次のいずれかのコマンドを入力します。 • **ip sla schedule** *operation-number* [**life** {**forever**	*seconds*}] [**start-time** {[*hh*:*mm*:*ss*] [*month day*	*day month*]	**pending**	**now**	**after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**]	• 個々の IP SLA 動作のスケジューリング パラメータを設定します。 • 複数動作スケジューラ用に IP SLA 動作グループ番号と動作番号の範囲を指定します。

	コマンドまたはアクション	目的

	• **ip sla group schedule** *group-operation-number operation-id-numbers* { **schedule-period** *schedule-period-range* | **schedule-together**} [**ageout** *seconds*] **frequency** *group-operation-frequency* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm* [:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm* [:*ss*]}]
	例：
	`Device(config)# ip sla schedule 10 life forever start-time now`
	`Device(config)# ip sla group schedule 10 schedule-period frequency`
	`Device(config)# ip sla group schedule 1 3,4,6-9 life forever start-time now`
	`Device(config)# ip sla schedule 1 3,4,6-9 schedule-period 50 frequency range 80-100`	

ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	**show ip sla group schedule** 例： `Device# show ip sla group schedule`	（任意）IP SLA グループ スケジュールの詳細を表示します。
ステップ 6	**show ip sla configuration** 例： `Device# show ip sla configuration`	（任意）IP SLA 設定の詳細を表示します。

トラブルシューティングのヒント

- IP サービス レベル契約（SLA）動作が実行中でなく、統計情報が生成されていない場合は、設定に **verify-data** コマンドを追加して（IP SLA コンフィギュレーション モードで設定）、データ検証をイネーブルにします。データ検証をイネーブルにすると、各動作の応答で破損の有無がチェックされます。通常の動作時に **verify-data** コマンドを使用すると、不要なオーバーヘッドがかかるので注意してください。
- IP SLA 動作に関する問題をトラブルシューティングするには、**debug ip sla trace** コマンドと **debug ip sla error** コマンドを使用します。

次の作業

トラップを生成する目的（または別の動作を開始する目的）で、IP サービス レベル契約（SLA）動作に予防的しきい値条件と反応トリガーを追加するには、「予防的しきい値モニタリングの設定」の項を参照してください。

IP SLA FTP 動作の設定例

例：FTP 動作の設定

次に、「IP SLA FTP 動作に関する情報」の項の図「FTP 動作」に示されているように、デバイス B から FTP サーバへの FTP 動作を設定する例を示します。この動作は、毎日午前 1 時 30 分に開始するようにスケジュールされています。この例では、test.cap という名前のファイルが、ホスト（cisco.com）からパスワード abc を使用してアクティブ モードの FTP により取得されます。

デバイス B の設定

```
ip sla 10
 ftp get ftp://user1:abc@test.cisco.com/test.cap mode active
 frequency 20
 tos 128
 timeout 40000
 tag FLL-FTP
ip sla schedule 10 start-time 01:30:00 recurring
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IP SLA コマンド	『*IP SLAs Command Reference*』

標準

標準	タイトル
ITU-T G.711 u-law および G.711 a-law	『Pulse code modulation (PCM) of voice frequencies』
ITU-T G.729A	『Reduced complexity 8 kbit/s CS-ACELP speech codec』

MIB

MIB	MIB のリンク
CISCO-RTTMON-MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

テクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

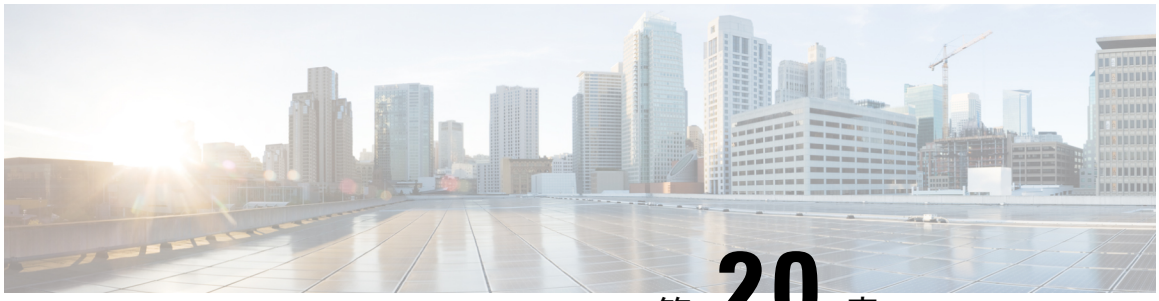
IP SLA FTP 動作の設定に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *28 : IP SLA FTP* 動作の機能情報

機能名	リリース	機能情報
IP SLA：FTP 動作	12.2(31)SB2 12.2(33)SRB1 12.2(33)SXH 12.3(14)T Cisco IOS XE Release 2.1 15.0(1)S Cisco IOS XE Release 3.1.0SG	IP SLA ファイル転送プロトコル（FTP）動作を使用すると、シスコ デバイスと FTP サーバの間でファイルを取得するためのネットワーク応答時間を測定できます。
IPSLA 4.0 - IP v6 phase2	15.2(3)T 15.2(4)S Cisco IOS XE リリース XE 3.7S 15.1(2)SG Cisco IOS XE Release 3.4SG	IPv6 ネットワークでの動作を可能にするためにサポートが追加されました。 次のコマンドが導入または変更されました。**ftp get**（(IP SLA）、**show ip sla configuration**、**show ip sla summary**
IP SLAs VRF Aware 2.0	12.4(2)T 15.1(1)S 15.1(1)SY Cisco IOS XE Release 3.8S	TCP 接続、FTP、HTTP および DNS クライアント動作タイプに対する IP SLA VRF 対応機能のサポートが追加されました。



第 20 章

IP SLA DNS 動作の設定

このモジュールでは、DNS要求を送信するのに要する時間と応答を受信するのに要する時間の差異を測定するために、IP サービス レベル契約（SLA）ドメイン ネーム システム（DNS）動作を設定する方法について説明します。また、このモジュールでは、DNS動作の結果を表示および分析して DNS サーバまたは Web サーバのパフォーマンスを決定する重要な要因となる DNS ルックアップ時間を調べる方法についても説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

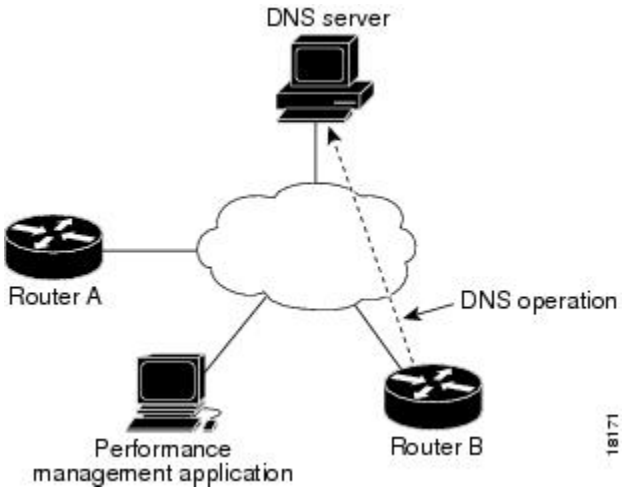
IP SLA DNS 動作に関する情報

DNS の動作

DNS 動作では、DNS 要求を送信するのに要する時間と、応答を受信するのに要する時間の差異を測定します。DNS は、ネットワーク ノードの名前をアドレスに変換するためにインターネットで使用されます。IP SLA DNS 動作は、ホスト名を指定した場合は IP アドレスを問い合わせ、IP アドレスを指定した場合はホスト名を問い合わせます。

以下の図では、デバイス B が送信元 IP SLA デバイスとして設定され、宛先デバイスを DNS サーバとする DNS 動作が設定されています。

図 *16 : DNS* の動作



要求を DNS サーバに送信するのに要する時間とデバイス B が応答を受信するのに要する時間の差異を測定することにより、接続応答時間が算出されます。得られた DNS ルックアップ時間は、DNS のパフォーマンスの分析に役立ちます。DNS ルックアップ時間が短いと、Web サーバ アクセスが高速になります。

IP SLA DNS 動作の設定方法

送信元デバイスでの IP SLA DNS 動作の設定

（注） 宛先デバイスで IP SLA Responder を設定する必要はありません。

次のいずれかの作業を実行します。

送信元デバイスでの基本 DNS 動作の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **dns** {*destination-ip-address* | *destination-hostname*} **name-server** *ip-address* [**source-ip** {*ip-address* | *hostname*} **source-port** *port-number*]
5. **frequency** *seconds*
6. **end**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	**ip sla** *operation-number* 例： `Device(config)# ip sla 10`	IP SLA 動作の設定を開始し、IP SLA コンフィギュレーション モードに移行します。
ステップ 4	**dns** {*destination-ip-address* | *destination-hostname*} **name-server** *ip-address* [**source-ip** {*ip-address* | *hostname*} **source-port** *port-number*] 例： `Device(config-ip-sla)# dns host1 name-server 172.20.2.132`	DNS 動作を定義し、IP SLA DNS コンフィギュレーション モードを開始します。
ステップ 5	**frequency** *seconds* 例： `Device(config-ip-sla-dns)# frequency 60`	（任意）指定した IP SLA 動作を繰り返す間隔を設定します。
ステップ 6	**end** 例： `Device(config-ip-sla-dns)# end`	特権 EXEC モードに戻ります。

送信元デバイスでのオプション パラメータを使用した DNS 動作の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **dns** {*destination-ip-address* | *destination-hostname*} **name-server** *ip-address* [**source-ip** {*ip-address* | *hostname*} **source-port** *port-number*]
5. **history buckets-kept** *size*
6. **history distributions-of-statistics-kept** *size*
7. **history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*]
8. **history filter** {**none** | **all** | **overThreshold** | **failures**}
9. **frequency** *seconds*
10. **history hours-of-statistics-kept** *hours*
11. **history lives-kept** *lives*
12. **owner** *owner-id*
13. **history statistics-distribution-interval** *milliseconds*
14. **tag** *text*
15. **threshold** *milliseconds*
16. **timeout** *milliseconds*
17. **end**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	**ip sla** *operation-number* 例： `Device(config)# ip sla 10`	IP SLA 動作の設定を開始し、IP SLA コンフィギュレーション モードに移行します。
ステップ 4	**dns** {*destination-ip-address* | *destination-hostname*} **name-server** *ip-address* [**source-ip** {*ip-address* | *hostname*} **source-port** *port-number*] 例：	DNS 動作を定義し、IP SLA DNS コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device(config-ip-sla)# dns host1 name-server 172.20.2.132`	
ステップ 5	**history buckets-kept** *size* 例： `Device(config-ip-sla-dns)# history buckets-kept 25`	（任意）IP SLA 動作のライフタイム中に保持する履歴バケット数を設定します。
ステップ 6	**history distributions-of-statistics-kept** *size* 例： `Device(config-ip-sla-dns)# history distributions-of-statistics-kept 5`	（任意）IP SLA 動作中にホップ単位で保持する統計情報の配信数を設定します。
ステップ 7	**history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*] 例： `Device(config-ip-sla-dns)# history enhanced interval 900 buckets 100`	（任意）IP SLA 動作に対する拡張履歴収集をイネーブルにします。
ステップ 8	**history filter** {**none** | **all** | **overThreshold** | **failures**} 例： `Device(config-ip-sla-dns)# history filter failures`	（任意）IP SLA 動作の履歴テーブルに格納する情報のタイプを定義します。
ステップ 9	**frequency** *seconds* 例： `Device(config-ip-sla-dns)# frequency 30`	（任意）指定した IP SLA 動作を繰り返す間隔を設定します。
ステップ 10	**history hours-of-statistics-kept** *hours* 例： `Device(config-ip-sla-dns)# history hours-of-statistics-kept 4`	（任意）IP SLA 動作の統計情報を保持する時間数を設定します。
ステップ 11	**history lives-kept** *lives* 例： `Device(config-ip-sla-dns)# history lives-kept 5`	（任意）IP SLA 動作の履歴テーブルに格納するライフ数を設定します。
ステップ 12	**owner** *owner-id* 例：	（任意）IP SLA 動作の簡易ネットワーク管理プロトコル（SNMP）所有者を設定します。

	コマンドまたはアクション	目的
	`Device(config-ip-sla-dns)# owner admin`	
ステップ 13	**history statistics-distribution-interval** *milliseconds* 例： `Device(config-ip-sla-dns)# history statistics-distribution-interval 10`	（任意）IP SLA 動作で維持する各統計情報の配信間隔を設定します。
ステップ 14	**tag** *text* 例： `Device(config-ip-sla-dns)# tag TelnetPollServer1`	（任意）IP SLA 動作のユーザ指定 ID を作成します。
ステップ 15	**threshold** *milliseconds* 例： `Device(config-ip-sla-dns)# threshold 10000`	（任意）IP SLA 動作によって作成されるネットワーク モニタリング統計情報を計算するための上限しきい値を設定します。
ステップ 16	**timeout** *milliseconds* 例： `Device(config-ip-sla-dns)# timeout 10000`	（任意）IP SLA 動作がその要求パケットからの応答を待機する時間を設定します。
ステップ 17	**end** 例： `Device(config-ip-sla-dns)# end`	特権 EXEC モードに戻ります。

IP SLA 動作のスケジューリング

始める前に

- スケジュールされるすべての IP サービス レベル契約（SLA）動作がすでに設定されている必要があります。
- 複数動作グループでスケジュールされたすべての動作の頻度が同じでなければなりません。
- 複数動作グループに追加する 1 つ以上の動作 ID 番号のリストは、カンマ（,）を含めて最大 125 文字に制限する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します。

- **ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {[*hh*:*mm*:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**]
- **ip sla group schedule** *group-operation-number operation-id-numbers* { **schedule-period** *schedule-period-range* | **schedule-together**} [**ageout** *seconds*] **frequency** *group-operation-frequency* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm* [:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm* [:*ss*]}]

4. **end**
5. **show ip sla group schedule**
6. **show ip sla configuration**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	次のいずれかのコマンドを入力します。 • **ip sla schedule** *operation-number* [**life** {**forever**	*seconds*}] [**start-time** {[*hh*:*mm*:*ss*] [*month day*	*day month*]	**pending**	**now**	**after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**] • **ip sla group schedule** *group-operation-number operation-id-numbers* { **schedule-period** *schedule-period-range*	**schedule-together**} [**ageout** *seconds*] **frequency** *group-operation-frequency* [**life** {**forever**	*seconds*}] [**start-time** {*hh*:*mm* [:*ss*] [*month day*	*day month*]	**pending**	**now**	**after** *hh*:*mm* [:*ss*]}] 例： `Device(config)# ip sla schedule 10 life forever start-time now` `Device(config)# ip sla group schedule 10 schedule-period frequency` `Device(config)# ip sla group schedule 1 3,4,6-9 life forever start-time now` `Device(config)# ip sla schedule 1 3,4,6-9 schedule-period 50 frequency range 80-100`	• 個々の IP SLA 動作のスケジューリング パラメータを設定します。 • 複数動作スケジューラ用に IP SLA 動作グループ番号と動作番号の範囲を指定します。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	**show ip sla group schedule** 例： `Device# show ip sla group schedule`	（任意）IP SLA グループ スケジュールの詳細を表示します。
ステップ 6	**show ip sla configuration** 例： `Device# show ip sla configuration`	（任意）IP SLA 設定の詳細を表示します。

トラブルシューティングのヒント

- IP サービス レベル契約（SLA）動作が実行中でなく、統計情報が生成されていない場合は、設定に **verify-data** コマンドを追加して（IP SLA コンフィギュレーション モードで設定）、データ検証をイネーブルにします。データ検証をイネーブルにすると、各動作の応答で破損の有無がチェックされます。通常の動作時に **verify-data** コマンドを使用すると、不要なオーバーヘッドがかかるので注意してください。
- IP SLA 動作に関する問題をトラブルシューティングするには、**debug ip sla trace** コマンドと **debug ip sla error** コマンドを使用します。

次の作業

トラップを生成する目的（または別の動作を開始する目的）で、IPサービス レベル契約（SLA）動作に予防的しきい値条件と反応トリガーを追加するには、「予防的しきい値モニタリングの設定」の項を参照してください。

IP SLA DNS 動作の設定例

DNS 動作の設定例

以下に、「DNS 動作」の項の図「DNS 動作」に示されているように、デバイス B から DNS サーバ（IP アドレス 172.20.2.132）への DNS 動作を設定する例を示します。動作は、ただちに開始されるようにスケジューリングされます。この例では、ターゲット アドレスはホスト名であり、DNS 動作はホスト名 host1 に関連付けられた IP アドレスを DNS サーバに問い合わせます。DNS サーバでの設定は必要ありません。

デバイス B の設定

```
ip sla 11
 dns host1 name-server 172.20.2.132
 frequency 50
 timeout 8000
 tag DNS-Test
ip sla schedule 11 start-time now
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
Cisco IOS IP SLA コマンド	『Cisco IOS IP SLAs Command Reference, All Releases』
Cisco IOS IP SLA：一般情報	『*Cisco IOS IP SLAs Configuration Guide*』の「Cisco IOS IP SLAs Overview」モジュール
IP SLA の複数動作スケジューリング	『*Cisco IOS P SLAs Configuration Guide*』の「Configuring Multioperation Scheduling of IP SLAs Operations」モジュール
IP SLA の予防的しきい値モニタリング	『*Cisco IOS IP SLAs Configuration Guide*』の「Configuring Proactive Threshold Monitoring of IP SLAs Operations」モジュール

MIB

MIB	MIB のリンク
CISCO-RTTMON-MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャセットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IP SLA DNS 動作の設定に関する機能情報

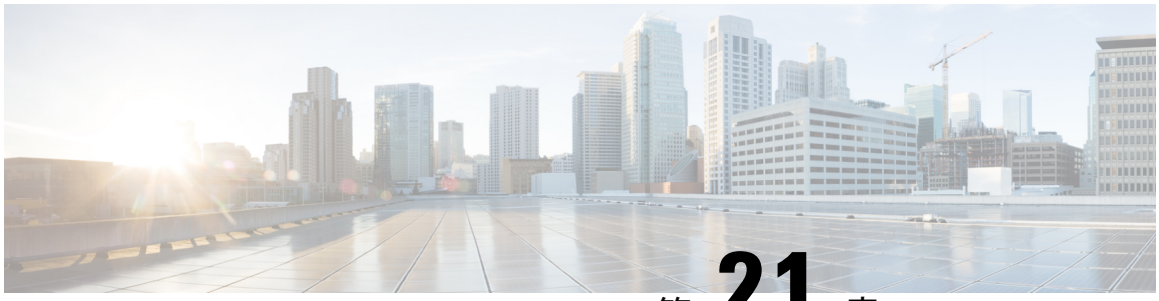
次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *29 : IP SLA - DNS* 動作の機能情報

機能名	リリース	機能情報
IP SLA - DNS 動作	12.2(31)SB2 12.2(33)SRB1 12.2(33)SXH 12.3(14)T Cisco IOS XE Release 2.1 15.0(1)S Cisco IOS XE 3.1.0SG	IP SLA ドメイン ネーム システム（DNS）動作機能を使用すると、DNS 要求の送信に要する時間と応答の受信に要する時間の差異を測定できます。
IPSLA 4.0 - IP v6 phase2	15.2(3)T Cisco IOS XE Release 3.7S 15.1(2)SG Cisco IOS XE Release 3.4SG	IPv6 ネットワークでの動作を可能にするためにサポートが追加されました。次のコマンドが導入または変更されました。**dns (IP SLA)**、**show ip sla configuration**、**show ip sla summary**

機能名	リリース	機能情報
IP SLAs VRF Aware 2.0	12.4(2)T 15.1(1)S 15.1(1)SY Cisco IOS XE Release 3.8S	TCP 接続、FTP、HTTP および DNS クライアント動作タイプに対する IP SLA VRF 対応機能のサポートが追加されました。



第 21 章

IP SLA DHCP 動作の設定

このモジュールでは、シスコ デバイスと DHCP サーバの間で IP アドレスを取得するための応答時間を測定するように、IP サービス レベル契約（SLA）の動的ホスト制御プロトコル（DHCP）のプローブを設定する方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

IP SLA DHCP 動作に関する情報

DHCP の動作

DHCPには、ホストが必要としなくなったアドレスを再使用できように、IPアドレスを動的に割り当てるためのメカニズムが備わっています。DHCP 動作では、DHCP サーバを検出して

リースされた IP アドレスを取得するまでのラウンドトリップ時間（RTT）を測定します。この動作が終わると、IP SLA はリースした IP アドレスを解放します。

RTT 情報を使用して、DHCP のパフォーマンス レベルを判断できます。

DHCP の動作には 2 つのモードがあります。デフォルトでは、DHCP 動作は、デバイス上のすべての使用可能な IP インターフェイスの検出パケットを送信します。デバイスに特定のサーバが設定されている場合、検出パケットは指定の DHCP サーバにのみ送信されます。

IP SLA DHCP リレー エージェントのオプション

DHCP リレー エージェントとは、クライアントとサーバ間で DHCP パケットを転送するホストです。リレーエージェントは、同一の物理サブネット上にないクライアントとサーバ間で要求および応答を転送するために使用されます。リレー エージェント転送は、IP デバイスの通常の転送とは異なります。通常の転送では、IPパケットがネットワーク間である程度透過的にスイッチングされます。リレーエージェントはDHCPメッセージを受信すると、新規のDHCPメッセージを生成して別のインターフェイスに送信します。

IP SLA DHCP 動作の設定方法

（注） 宛先デバイスで IP SLA Responder を設定する必要はありません。

送信元デバイスでの DHCP 動作の設定

次のいずれかの作業を実行します。

基本的な DHCP 動作の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **dhcp** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*}]
5. **frequency** *seconds*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	`Device> enable`	• パスワードを入力します（要求された場合）。
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	**ip sla** *operation-number* 例： `Device(config)# ip sla 10`	IP SLA 動作の設定を開始し、IP SLA コンフィギュレーション モードに移行します。
ステップ 4	**dhcp** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*}] 例： `Device(config-ip-sla)# dhcp 10.10.10.3`	DHCP 動作を定義し、IP SLA DHCP コンフィギュレーション モードを開始します。
ステップ 5	**frequency** *seconds* 例： `Device(config-ip-sla-dhcp)# frequency 30`	（任意）指定した IP SLA 動作を繰り返す間隔を設定します。
ステップ 6	**end** 例： `Device(config-ip-sla-dhcp)# end`	特権 EXEC モードに戻ります。

オプション パラメータを使用した DHCP 動作の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **dhcp** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*}]
5. **history buckets-kept** *size*
6. **history distributions-of-statistics-kept** *size*
7. **history filter** {**none** | **all** | **overThreshold** | **failures**}
8. **frequency** *seconds*
9. **history hours-of-statistics-kept** *hours*
10. **history lives-kept** *lives*
11. **owner** *owner-id*
12. **history statistics-distribution-interval** *milliseconds*
13. **tag** *text*

14. **threshold** *milliseconds*
15. **timeout** *milliseconds*
16. **end**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	**ip sla** *operation-number* 例： `Device(config)# ip sla 10`	IP SLA 動作の設定を開始し、IP SLA コンフィギュレーション モードに移行します。
ステップ 4	**dhcp** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*}] 例： `Device(config-ip-sla)# dhcp 10.10.10.3`	DHCP 動作を定義し、IP SLA DHCP コンフィギュレーション モードを開始します。
ステップ 5	**history buckets-kept** *size* 例： `Device(config-ip-sla-dhcp)# history buckets-kept 25`	（任意）IP SLA 動作のライフタイム中に保持する履歴バケット数を設定します。
ステップ 6	**history distributions-of-statistics-kept** *size* 例： `Device(config-ip-sla-dhcp)# history distributions-of-statistics-kept 5`	（任意）IP SLA 動作中にホップ単位で保持する統計情報の配信数を設定します。
ステップ 7	**history filter** {**none** | **all** | **overThreshold** | **failures**} 例： `Device(config-ip-sla-dhcp)# history filter failures`	（任意）IP SLA 動作の履歴テーブルに格納する情報のタイプを定義します。
ステップ 8	**frequency** *seconds* 例：	（任意）指定した IP SLA 動作を繰り返す間隔を設定します。

	コマンドまたはアクション	目的
	`Device(config-ip-sla-dhcp)# frequency 30`	
ステップ 9	**history hours-of-statistics-kept** *hours* 例： `Device(config-ip-sla-dhcp)# history hours-of-statistics-kept 4`	（任意）IP SLA 動作の統計情報を保持する時間数を設定します。
ステップ 10	**history lives-kept** *lives* 例： `Device(config-ip-sla-dhcp)# history lives-kept 5`	（任意）IP SLA 動作の履歴テーブルに格納するライフ数を設定します。
ステップ 11	**owner** *owner-id* 例： `Device(config-ip-sla-dhcp)# owner admin`	（任意）IP SLA 動作の簡易ネットワーク管理プロトコル（SNMP）所有者を設定します。
ステップ 12	**history statistics-distribution-interval** *milliseconds* 例： `Device(config-ip-sla-dhcp)# history statistics-distribution-interval 10`	（任意）IP SLA 動作で維持する各統計情報の配信間隔を設定します。
ステップ 13	**tag** *text* 例： `Device(config-ip-sla-dhcp)# tag TelnetPollServer1`	（任意）IP SLA 動作のユーザ指定 ID を作成します。
ステップ 14	**threshold** *milliseconds* 例： `Device(config-ip-sla-dhcp)# threshold 10000`	（任意）IP SLA 動作によって作成されるネットワーク モニタリング統計情報を計算するための上限しきい値を設定します。
ステップ 15	**timeout** *milliseconds* 例： `Device(config-ip-sla-dhcp)# timeout 10000`	（任意）IP SLA 動作がその要求パケットからの応答を待機する時間を設定します。
ステップ 16	**end** 例： `Device(config-ip-sla-dhcp)# end`	特権 EXEC モードに戻ります。

IP SLA 動作のスケジューリング

始める前に

- スケジュールされるすべての IP サービス レベル契約（SLA）動作がすでに設定されている必要があります。
- 複数動作グループでスケジュールされたすべての動作の頻度が同じでなければなりません。
- 複数動作グループに追加する 1 つ以上の動作 ID 番号のリストは、カンマ（,）を含めて最大 125 文字に制限する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します。
   - **ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {[*hh*:*mm*:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**]
   - **ip sla group schedule** *group-operation-number operation-id-numbers* { **schedule-period** *schedule-period-range* | **schedule-together**} [**ageout** *seconds*] **frequency** *group-operation-frequency* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm* [:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm* [:*ss*]}]
4. **end**
5. **show ip sla group schedule**
6. **show ip sla configuration**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	次のいずれかのコマンドを入力します。 • **ip sla schedule** *operation-number* [**life** {**forever**	*seconds*}] [**start-time** {[*hh*:*mm*:*ss*] [*month day*	*day month*]	**pending**	**now**	**after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**]	• 個々の IP SLA 動作のスケジューリング パラメータを設定します。 • 複数動作スケジューラ用に IP SLA 動作グループ番号と動作番号の範囲を指定します。

	コマンドまたはアクション	目的

	• **ip sla group schedule** *group-operation-number operation-id-numbers* { **schedule-period** *schedule-period-range* | **schedule-together**} [**ageout** *seconds*] **frequency** *group-operation-frequency* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm* [:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm* [:*ss*]}]
	例：
	`Device(config)# ip sla schedule 10 life forever start-time now`
	`Device(config)# ip sla group schedule 10 schedule-period frequency`
	`Device(config)# ip sla group schedule 1 3,4,6-9 life forever start-time now`
	`Device(config)# ip sla schedule 1 3,4,6-9 schedule-period 50 frequency range 80-100`	

ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	**show ip sla group schedule** 例： `Device# show ip sla group schedule`	（任意）IP SLA グループ スケジュールの詳細を表示します。
ステップ 6	**show ip sla configuration** 例： `Device# show ip sla configuration`	（任意）IP SLA 設定の詳細を表示します。

トラブルシューティングのヒント

- IP サービス レベル契約（SLA）動作が実行中でなく、統計情報が生成されていない場合は、設定に **verify-data** コマンドを追加して（IP SLA コンフィギュレーション モードで設定）、データ検証をイネーブルにします。データ検証をイネーブルにすると、各動作の応答で破損の有無がチェックされます。通常の動作時に **verify-data** コマンドを使用すると、不要なオーバーヘッドがかかるので注意してください。
- IP SLA 動作に関する問題をトラブルシューティングするには、**debug ip sla trace** コマンドと **debug ip sla error** コマンドを使用します。

次の作業

トラップを生成する目的（または別の動作を開始する目的）で、IPサービス レベル契約（SLA）動作に予防的しきい値条件と反応トリガーを追加するには、「予防的しきい値モニタリングの設定」の項を参照してください。

IP SLA DHCP 動作の設定例

IP SLA DHCP 動作の設定例

次の例では、IP SLA 動作番号 12 が、DHCP サーバ 172.16.20.3 に対してイネーブルである DHCP 動作として設定されています。DHCP オプション 82 は回線 ID を指定するために使用されることに注意してください。

デバイス B の設定

```
ip dhcp-server 172.16.20.3
!
ip sla 12
 dhcp 10.10.10.3
 frequency 30
 timeout 5000
 tag DHCP_Test
!
ip sla schedule 12 start-time now
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
Cisco IOS IP SLA コマンド	『Cisco IOS IP SLAs Command Reference, All Releases』
Cisco IOS IP SLA：一般情報	『*Cisco IOS IP SLAs Configuration Guide*』の「Cisco IOS IP SLAs Overview」モジュール
IP SLA の複数動作スケジューリング	『*Cisco IOS P SLAs Configuration Guide*』の「Configuring Multioperation Scheduling of IP SLAs Operations」モジュール
IP SLA の予防的しきい値モニタリング	『*Cisco IOS IP SLAs Configuration Guide*』の「Configuring Proactive Threshold Monitoring of IP SLAs Operations」モジュール

MIB

MIB	MIB のリンク
CISCO-RTTMON-MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャセットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

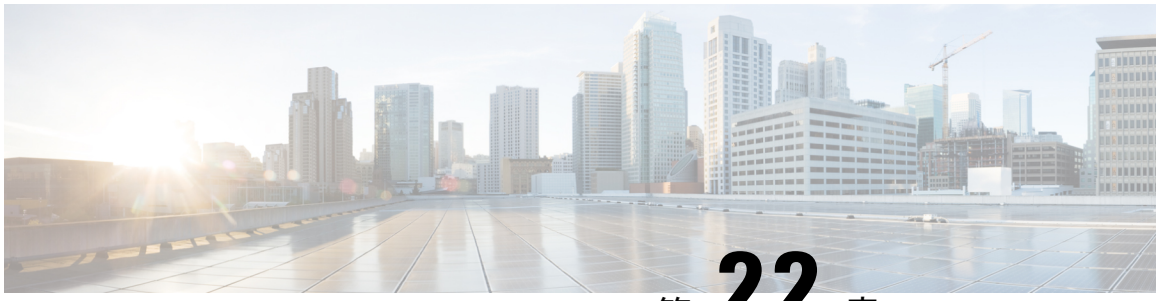
IP SLA DHCP 動作の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *30 : IP SLA DHCP* 動作の機能情報

機能名	リリース	機能情報
IP SLA DHCP プローブ		IP SLA の動的ホスト制御プロトコル（DHCP）プローブ機能を使用すると、シスコ デバイスと DHCP サーバの間で IP アドレスを取得するためのネットワーク応答時間をスケジューリングし、測定できます。



第 22 章

IP SLA 複数動作スケジューラの設定

このマニュアルでは、IP サービス レベル契約（SLA）複数動作スケジューラ機能を使用して複数の動作を一度にスケジューリングする方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

IP SLA 複数動作スケジューラの制限事項

no ip sla group schedule および **ip sla group schedule** コマンドはコンフィギュレーション ファイルでは連続して使用せず、実行コンフィギュレーションにコピーします。これにより、サービス レベル契約（SLA）のプローブの一部がダウンします。

IP SLA 複数動作スケジューラの前提条件

- グループをスケジューリングする前に、IP SLA 動作をグループに含める設定を行う。
- 1 つのグループとしてスケジュールする IP SLA 動作を決定する。
- ネットワーク トラフィック タイプとネットワーク管理ステーションを特定する。
- ネットワークのトポロジおよびデバイスのタイプを特定する。
- 各動作に対するテストの頻度を決定する。

IP SLA 複数動作スケジューラに関する情報

IP SLA 複数動作スケジューラ

IP SLA 動作の通常のスケジューリングでは、一度に 1 つの動作をスケジューリングできます。IP SLA 動作が何千もある大規模なネットワークでネットワーク パフォーマンスをモニタする場合、通常のスケジューリング（各動作を個別にスケジューリング）は、非効率的であり、時間がかかります。

複数動作のスケジューリングでは、コマンドライン インターフェイス（CLI）または CISCO RTTMON-MIB による単一のコマンドを使用して、複数の IP SLA 動作をスケジューリングすることができます。この機能では、これらの動作を均等な時間間隔で実行するようにスケジューリングすることで、IP SLA モニタリング トラフィックの量を制御できます。スケジューリングされる動作 ID 番号、およびすべての IP SLA 動作が開始されなければならない時間の範囲を指定する必要があります。この機能は、指定したタイム フレームにおいて等間隔で自動的に IP SLA 動作を分散します。動作の間隔（開始間隔）が計算されて、動作が開始されます。このように IP SLA 動作を分散することで、CPU の使用を最小限に抑えることが可能になり、それによりネットワークのスケーラビリティが向上します。

IP SLA 複数動作スケジューリング機能では、次の設定パラメータを使用して、複数の IP SLA 動作を 1 つのグループとしてスケジュールできます。

- グループ動作番号：スケジューリングされる IP SLA 動作のグループ設定またはグループ スケジュール番号。
- 動作 ID 番号：スケジューリングされる動作グループの IP SLA 動作 ID 番号のリスト。
- スケジュール期間：IP SLA 動作グループがスケジューリングされる時間。
- エージアウト：情報をアクティブに収集していないときに、メモリ内に動作を維持する時間。デフォルトでは、動作はメモリに永久に保持されます。

- 頻度：各 IP SLA 動作が再開されるまでの時間。頻度オプションを指定すると、グループに属しているすべての動作の動作頻度が上書きされます。頻度オプションが指定されていない場合、各動作の頻度は、スケジュール期間の値に設定されます。
- ライフ：動作が情報をアクティブに収集する時間。動作は、無期限に実行されるように設定することもできます。デフォルトでは、動作のライフタイムは 1 時間です。
- 開始時間：動作が情報の収集を開始する時間。すぐに動作を開始するように指定するか、時間、分、秒、日、月を使用して、絶対的な開始時刻に動作を開始するように指定できます。

IP SLA 複数動作スケジューリング機能では、中断なしで実行できる最大動作数をスケジューリングします。ただし、この機能は、すでに実行されている IP SLA 動作や、設定されていないため存在しない動作はスキップします。動作の総数は、不明またはすでに実行されている動作の数に関係なく、コマンドで指定された動作の数に基づいて計算されます。IP SLA 複数動作スケジューリング機能では、アクティブな動作および不明な動作の数を示すメッセージが表示されます。ただし、これらのメッセージが表示されるのは、設定されていないまたはすでに実行されている動作をスケジューリングした場合だけです。

複数の IP SLA 動作をスケジュールする場合の主な利点は、スケジュールされた期間にわたって動作を均一に分散することで、ネットワークの負荷が低減されることです。この分散はより一貫したモニタリングのカバレッジを実現するのに役立ちます。このシナリオの例として、60 秒のスケジュール期間の中の同じ 1 秒の間隔中に 60 個の動作が開始される場合を考えてみます。60 個すべての動作が開始した後にネットワークの障害が 30 秒間発生した場合、それらの動作が再び開始される時間（この障害後の 30 秒以内）になる前にネットワークが復旧すると、この障害は 60 個のいずれの動作でも検出されません。一方、60 個の動作が 60 秒のスケジュール期間にわたって 1 秒間隔で均等に分散された場合は、一部の動作でこのネットワーク障害が検出されます。逆に、60 個すべての動作がアクティブな場合にネットワーク障害が発生すると、60 個のすべての動作は失敗し、障害は実際よりも重大である可能性があることが示されます。

同じタイプの動作では、IP SLA 複数動作スケジューリングに同じ頻度を使用してください。頻度を指定しない場合、デフォルトの頻度はスケジュール期間と同じになります。スケジュール期間は、指定されたすべての動作が実行される必要がある期間です。

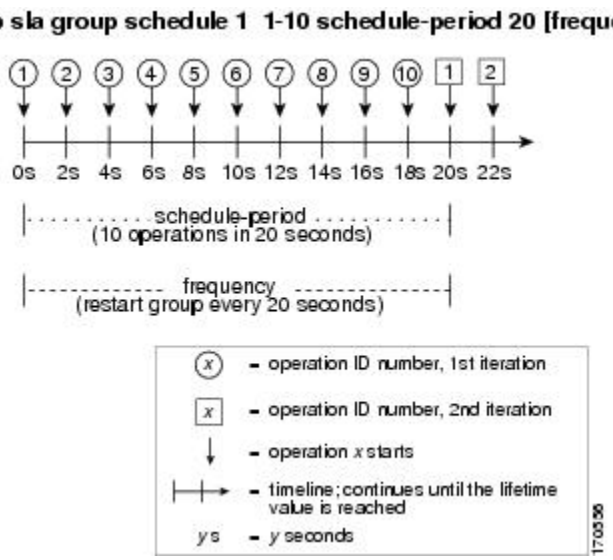
次の各項では、スケジュール期間と頻度の値の相互関係を中心に説明します。開始時間やライフタイムなどの他の値は説明に含まれていません。

IP SLA 複数動作スケジューリングのデフォルトの動作

IP SLA 複数動作スケジューリング機能では、複数の IP SLA 動作を 1 つのグループとしてスケジューリングできます。

次の図に、動作 1 から動作 10 を含む動作グループ 1 のスケジューリングを示します。動作グループ 1 のスケジュール期間は 20 秒です。したがって、このグループ内のすべての動作が 20 秒の期間内に等間隔で開始されます。デフォルトでは、頻度は、設定されたスケジュール期間と同じ値に設定されます。次の図に示すように、頻度はデフォルトで 20 に設定されるため、頻度を設定するかどうかは任意です。

図 *17:* スケジュール期間が頻度と等しい：デフォルトの動作



この例では、動作グループ 1 内の最初の動作（動作 1）が 0 秒に開始します。動作グループ 1 内の 10 個すべての動作（動作 1 ～ 10）が、20 秒のスケジュール期間内に開始される必要があります。各 IP SLA 動作の開始時間は、スケジュール期間を動作の数で割ることにより（20 秒が 10 個の動作で割られる）、スケジュール期間にわたって均等に分散されます。したがって、各動作は前の操作の 2 秒後に開始されます。

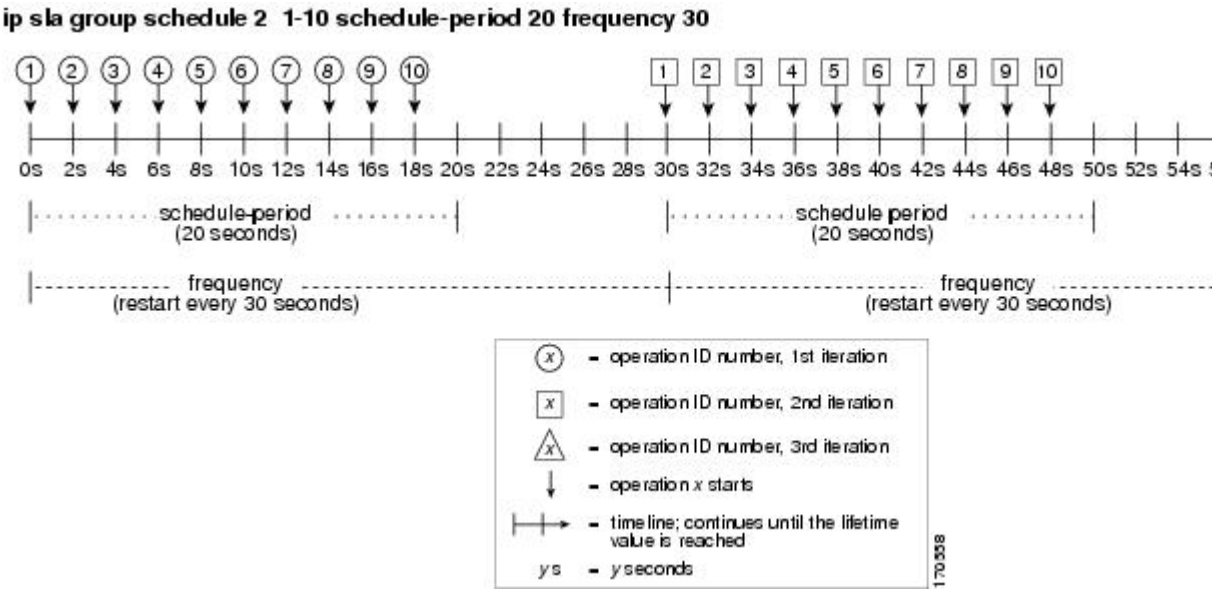
頻度は、動作グループが再開されるまで（繰り返されるまで）の経過時間です。頻度が指定されていない場合、その頻度は、スケジュール期間の値に設定されます。上に示した例では、動作グループ 1 が 20 秒ごとに繰り返し開始されます。この設定では、指定されたスケジュール期間にわたって動作の最適な分割（間隔）が得られています。

スケジュール期間が頻度よりも小さい場合の IP SLA 複数動作スケジューリング

頻度の値は、スケジュール グループが再開されるまでに経過する時間です。スケジュール期間が頻度よりも小さい場合は、開始される動作のない期間ができます。

次の図に、動作グループ 2 内の動作 1 から動作 10 のスケジューリングを示します。動作グループ 2 のスケジュール期間は 20 秒、頻度は 30 秒です。

図 *18 :* スケジュール期間が頻度よりも小さい場合



この例では、動作グループ 2 内の最初の動作（動作 1）が 0 秒に開始します。動作グループ 2 内の 10 個すべての動作（動作 1 ～ 10）が、20 秒のスケジュール期間内に開始される必要があります。各 IP SLA 動作の開始時間は、スケジュール期間を動作の数で割ることにより（20 秒が 10 個の動作で割られる）、スケジュール期間にわたって均等に分散されます。したがって、各動作は前の操作の 2 秒後に開始されます。

動作グループ 2 の最初の繰り返しでは、動作 1 が 0 秒で開始され、最後の動作（動作 10）が 18 秒で開始されます。ただし、グループの頻度が 30 秒に設定されているため、動作グループの各動作は 30 秒ごとに再開されます。したがって、19 秒から 29 秒までの時間に開始する動作が存在しないため、18 秒の後に 10 秒の隙間が生じます。よって、動作グループ 2 の 2 番めの繰り返しは 30 秒に開始します。動作グループ 2 内の 10 個すべての動作は、設定された 20 秒のスケジュール期間内に均等に分散された間隔で開始しなければならないので、動作グループ 2 内の最後の動作（動作 10）は常に最初の動作（動作 1）の 18 秒後に開始します。

上の図に示すように、次のイベントが発生します。

- 0 秒において、動作グループ 2 内の最初の動作（動作 1）が開始されます。
- 18 秒の時点で、動作グループ 2 内の最後の動作（動作 10）が開始されます。したがって、動作グループ 1 の最初の繰り返し（スケジュール期間）がここで終わります。
- 19 ～ 29 秒に開始される動作はありません。
- 30 秒において、動作グループ 2 内の最初の動作（動作 1）が再び開始されます。動作グループ 2 の 2 番めの繰り返しがここから始まります。
- 48 秒において（2 番めの繰り返しが始まってから 18 秒後）、動作グループ 2 内の最後の動作（動作 10）が開始され、動作グループ 2 の 2 番めの繰り返しが終わります。
- 60 秒の時点で、動作グループ 2 の 3 番めの繰り返しが開始されます。

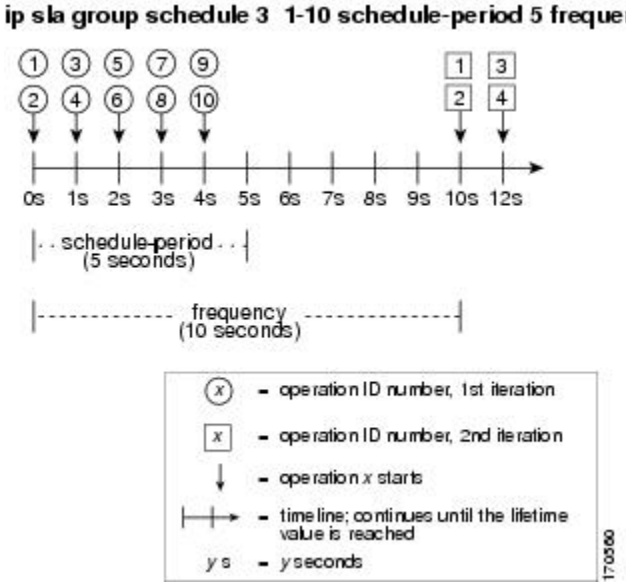
このプロセスは、動作グループ2のライフタイムが終わるまで続きます。ライフタイムの値は設定可能です。動作グループのデフォルトのライフタイムは無期限です。

IP SLA 動作の数がスケジュール期間よりも大きい場合の複数動作スケジューリング

グループ動作内の IP SLA 動作の開始の最小間隔は、1 秒です。そのため、複数スケジューリングされる動作の数がスケジュール期間よりも大きいと、IP SLA 複数動作スケジューリング機能は、同じ1秒間隔内で複数の動作が開始するようにスケジューリングします。スケジューリングされる動作の数が1秒間隔に均等に分割されない場合は、スケジュール期間の開始時に動作が均等に分割され、余った動作は最後の 1 秒の間隔で開始します。

次の図に、動作グループ3内の動作1から動作10のスケジューリングを示します。動作グループ 3 のスケジュール期間は 5 秒、頻度は 10 秒です。

図 *19 : IP SLA* 動作の数がスケジュール期間よりも大きい場合：均一な分散



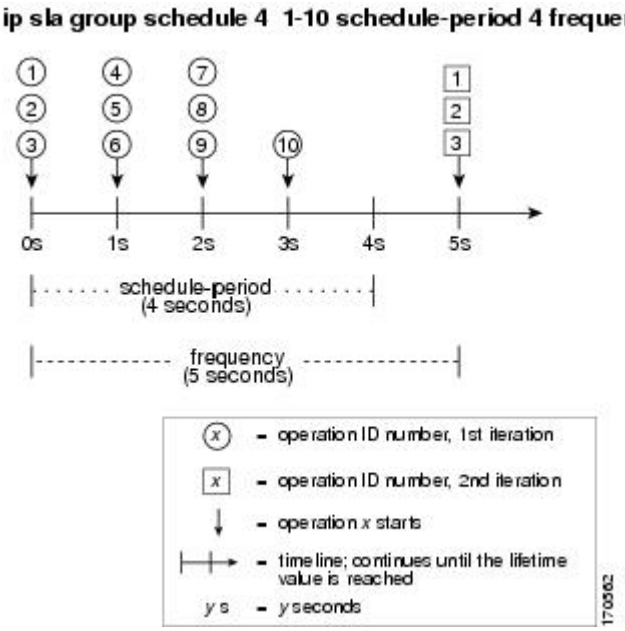
この例では、スケジュール期間を動作の数で割ると、各 IP SLA 動作の開始時間が 1 秒未満になります（5 秒が 10 個の動作で割られて、0.5 秒毎に 1 動作になる）。グループ動作内の IP SLA 動作の開始の最小間隔は 1 秒なので、IP SLA 複数動作スケジューリング機能は、動作の数をスケジュール期間で割ることにより（10 個の動作が 5 秒で割られる）、各 1 秒間隔で開始しなければならない動作の数を代わりに計算します。そのため、上の図に示すように、2 つの動作が 1 秒ごとに開始されます。

この例では頻度が 10 に設定されるので、動作グループ 3 の各繰り返しは、前の繰り返しの開始から 10 秒後に始まります。ただし、繰り返しの間に 5 秒の隙間があるため、この分散は最適なものではありません。

スケジューリングされる動作の数が1秒間隔に均等に分割されない場合は、スケジュール期間の開始時に動作が均等に分割され、余った動作は最後の 1 秒の間隔で開始します。

次の図に、動作グループ4内の動作1から動作10のスケジューリングを示します。動作グループ 4 のスケジュール期間は 4 秒、頻度は 5 秒です。

図 *20 : IP SLA* 動作の数がスケジュール期間よりも大きい場合：不均一な分散



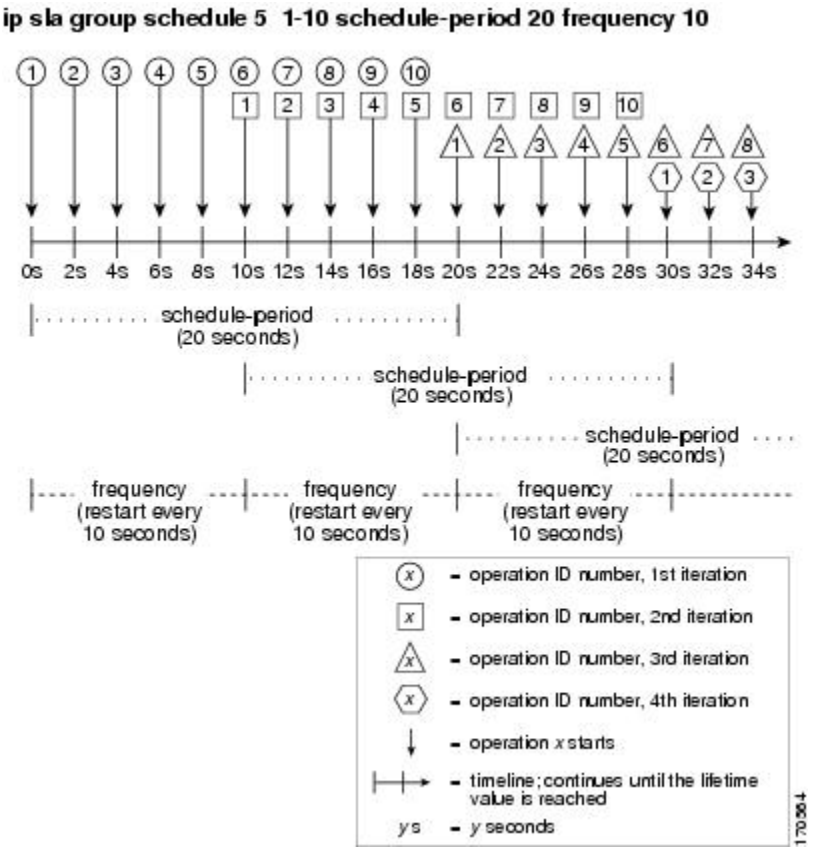
この例では、IP SLA 複数動作スケジューリング機能が、動作の数をスケジュール期間で割ることにより、各1秒間隔で開始しなければならない動作の数を計算します（10個の動作が4秒で割られて、1 秒毎に 2.5 動作になる）。動作の数は 1 秒間隔に均等に分割されないため、この数は、最後の1秒間隔で開始される残りの動作とともに、次の整数に丸められます（上の図を参照）。

スケジュール期間が頻度よりも大きい場合の IP SLA 複数動作スケジューリング

頻度の値は、スケジュールグループが再開されるまでに経過する時間です。スケジュール期間が頻度よりも大きい場合は、動作グループのある繰り返し内の動作が、その後の繰り返しの動作と重なる期間ができます。

次の図に、動作グループ5内の動作1から動作10のスケジューリングを示します。動作グループ 5 のスケジュール期間は 20 秒、頻度は 10 秒です。

図 *21 :* スケジュール期間が頻度よりも大きい場合の *IP SLA* グループ スケジューリング



この例では、動作グループ 5 内の最初の動作（動作 1）が 0 秒に開始します。動作グループ 5 内の 10 個すべての動作（動作 1 ～ 10）が、20 秒のスケジュール期間内に開始される必要があります。各 IP SLA 動作の開始時間は、スケジュール期間を動作の数で割ることにより（20 秒が 10 個の動作で割られる）、スケジュール期間にわたって均等に分散されます。したがって、各動作は前の操作の 2 秒後に開始されます。

動作グループ 5 の最初の繰り返しでは、動作 1 が 0 秒に開始し、動作 10（動作グループ内の最後の動作）は 18 秒に開始します。動作グループは 10 秒ごとに再開するように設定されているため（**frequency 10**）、動作グループ 5 の 2 番めの繰り返しは、最初の繰り返しの完了前である 10 秒に再び開始します。したがって、10 ～ 18 秒の期間中、最初の繰り返しの動作 6 ～ 10 が 2 番目の繰り返しの動作 1 ～ 5 と重なって実行されます（前の図を参照）。同様に、20 ～ 28 秒の期間中、2 番めの繰り返しの動作 6 ～ 10 は、3 番めの繰り返しの動作 1 ～ 5 と重なります。

この例では、動作 1 と動作 6 の開始時間は、同じ 2 秒の間隔内になりますが、厳密に同じ時間になる必要はありません。

動作の数をスケジュール期間よりも大きく設定することで、複数の動作が同じ 1 秒の間隔内で開始するように設定できるので、ここで説明されている設定は推奨されません。詳細については、「IP SLA 動作の数がスケジュール期間よりも大きい場合の複数動作スケジューリング」の項を参照してください。

IP SLA ランダム スケジューラ

IP SLA ランダム スケジューラ機能は、既存の IP SLA 複数動作スケジューリング機能の拡張です。IP SLA 複数動作スケジューリング機能を使用すると、複数の IP SLA 動作を、指定された期間にわたって均一に分散された間隔で開始し、指定された頻度で再開するように簡単にスケジューリングできます。IP SLA ランダム スケジューラ機能を使用すると、複数の IP SLA 動作を、指定された期間にわたって均一に分散されたランダムな間隔で開始し、指定された頻度の範囲内に均一に分散されたランダムな頻度で再開するようにスケジューリングできるようになります。ランダム スケジューリングにより、ネットワーク パフォーマンスを評価するための統計的なメトリックが改善されます。

（注） IP SLA ランダム スケジューラ機能は、パケット間のランダム性が考慮されないため、RFC2330 に準拠していません。

IP SLA ランダム スケジューラ オプションは、デフォルトではディセーブルです。ランダム スケジューラ オプションをイネーブルにするには、グローバル コンフィギュレーション モードでグループ スケジュールを設定するときに、頻度範囲を設定する必要があります。動作のグループは、指定された頻度範囲の均一に分散されたランダムな頻度で再開されます。頻度の範囲を設定する場合は、次のガイドラインが適用されます。

- 頻度の範囲の開始値は、グループ動作のすべての動作のタイムアウト値よりも大きい値にする必要があります。
- 頻度の範囲の開始値は、スケジュール期間（グループ動作がスケジューリングされる時間）よりも大きい値にする必要があります。このガイドラインを順守することで、同じ動作が、スケジュール期間内に複数回スケジューリングされることがなくなります。

ランダム スケジューラ オプションがイネーブルである場合は、次のガイドラインが適用されます。

- グループ動作の個々の動作は、均一に分散されて、スケジュール期間にランダムな間隔で開始されます。
- 動作のグループは、指定された頻度範囲の均一に分散されたランダムな頻度で再開されます。
- グループ動作の各動作開始の最小間隔は、100 ミリ秒（0.1 秒）です。ランダム スケジューラ オプションがディセーブルの場合、最小間隔は 1 秒です。
- 特定の時間に開始されるようにスケジューリングできるのは、1 つの動作だけです。ランダム スケジューラ オプションがディセーブルの場合、複数の動作を同じ時間に開始できます。
- 最初の動作は常にスケジュール期間の 0 ミリ秒に開始されます。
- グループ動作の各動作が開始される順序はランダムです。

IP SLA 複数動作スケジューラの設定方法

複数の IP SLA 動作のスケジューリング

（注）
- スケジュールされるすべての IP SLA 動作がすでに設定されている必要があります。
- 複数動作グループでスケジュールされたすべての動作の頻度が同じでなければなりません。
- 複数動作グループに追加される 1 つ以上の動作 ID 番号のリストは、カンマ（,）を含めて最大 125 文字に制限されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla group schedule** *group-operation-number operation-id-numbers* **schedule-period** *schedule-period-range* [**ageout** *seconds*] [**frequency** *group-operation-frequency*] [**life**{**forever** | *seconds*}] [**start-time**{*hh:mm*[*:ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh:mm:ss*}]
4. **exit**
5. **show ip sla group schedule**
6. **show ip sla configuration**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	**ip sla group schedule** *group-operation-number operation-id-numbers* **schedule-period** *schedule-period-range* [**ageout** *seconds*] [**frequency** *group-operation-frequency*] [**life**{**forever**	*seconds*}] [**start-time**{*hh:mm*[*:ss*] [*month day*	*day month*]	**pending**	**now**	**after** *hh:mm:ss*}] 例：	スケジューリングされる IP SLA 動作グループ番号と動作番号の範囲をグローバル コンフィギュレーション モードで指定します。

	コマンドまたはアクション	目的
	`Device(config)# ip sla group schedule 1 3,4,6-9 schedule-period 50 frequency range 80-100`	
ステップ 4	**exit** 例： `Device(config)# exit`	特権 EXEC モードに戻ります。
ステップ 5	**show ip sla group schedule** 例： `Device# show ip sla group schedule`	（任意）IP SLA グループ スケジュールの詳細を表示します。
ステップ 6	**show ip sla configuration** 例： `Device# show ip sla configuration`	（任意）IP SLA 設定の詳細を表示します。

IP SLA ランダム スケジューラのイネーブル化

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla group schedule** *group-operation-number operation-id-numbers* **schedule-period** *seconds* [**ageout** *seconds*] [**frequency** [*seconds*| **range** *random-frequency-range*]] [**life**{**forever** | *seconds*}] [**start-time**{*hh:mm*[*:ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh:mm:ss*}]
4. **exit**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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。

	コマンドまたはアクション	目的
ステップ 3	**ip sla group schedule** *group-operation-number operation-id-numbers* **schedule-period** *seconds* [**ageout** *seconds*] [**frequency** [*seconds*| **range** *random-frequency-range*]] [**life**{**forever** | *seconds*}] [**start-time**{*hh:mm*[*:ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh:mm:ss*}] 例： `Device(config)# ip sla group schedule 2 1-3 schedule-period 50 frequency range 80-100`	IP SLA 動作のグループのスケジューリング パラメータを指定します。 • IP SLA ランダム スケジューラ オプションをイネーブルにするには、**frequency range** *random-frequency-range* キーワードおよび引数を設定する必要があります。
ステップ 4	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IP SLA 複数動作スケジューリングの確認

手順の概要

1. **show ip sla statistics**
2. **show ip sla group schedule**
3. **show ip sla configuration**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show ip sla statistics** 例： `Device# show ip sla statistics`	（任意）IP SLA 動作の詳細を表示します。
ステップ 2	**show ip sla group schedule** 例： `Device# show ip sla group schedule`	（任意）IP SLA グループ スケジュールの詳細を表示します。
ステップ 3	**show ip sla configuration** 例： `Device# show ip sla configuration`	（任意）IP SLA 設定の詳細を表示します。

例

複数の IP SLA 動作のスケジューリングが完了した後は、適切な **show** コマンドを使用して、最新の動作の詳細情報を確認できます。

次に、動作グループ 1 内の IP SLA 動作 1 ～ 20 を、60 秒のスケジュール期間と 1200 秒の寿命値でスケジューリングする例を示します。デフォルトにより、頻度はスケジュール期間と同じです。この例では、開始間隔は 3 秒になります（スケジュール期間を動作の数で割った値）。

```
Device# ip sla group schedule 1 1-20 schedule-period 60 life 1200
```

次に、スケジューリングされた複数 IP SLA 動作の詳細を、**show ip sla group schedule** コマンドを使用して表示する例を示します。

```
Device# show ip sla group schedule
Group Entry Number: 1
Probes to be scheduled: 1-20
Total number of probes: 20
Schedule period: 60
Group operation frequency: Equals schedule period
Status of entry (SNMP RowStatus): Active
Next Scheduled Start Time: Start Time already passed
Life (seconds): 1200
Entry Ageout (seconds): never
```

次に、スケジューリングされた複数 IP SLA 動作の詳細を、**show ip sla configuration** コマンドを使用して表示する例を示します。この例の最後の行には、IP SLA 動作が複数スケジューリングされていること（TRUE）が示されています。

```
Device# show ip sla configuration 1
Entry number: 1
Owner:
Tag:
Type of operation to perform: udpEcho
Target address: 10.2.31.121
Source address: 0.0.0.0
Target port: 9001
Source port: 0
Request size (ARR data portion): 16
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Data pattern:
Vrf Name:
Control Packets: enabled
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Life (seconds): 1200
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Threshold (milliseconds): 5000
Number of statistic hours kept: 2
Number of statistic distribution buckets kept: 1
Statistic distribution interval (milliseconds): 20
Enhanced History:
```

```
Number of history Lives kept: 0
Number of history Buckets kept: 15
History Filter Type: None
Group Scheduled : TRUE
```

次に、等間隔でスケジューリングされた複数 IP SLA 動作の最新の動作開始時間を、**show ip sla statistics** コマンドを使用して表示する例を示します。

```
Device# show ip sla statistics | include Latest operation start time
Latest operation start time: *03:06:21.760 UTC Tue Oct 21 2003
Latest operation start time: *03:06:24.754 UTC Tue Oct 21 2003
Latest operation start time: *03:06:27.751 UTC Tue Oct 21 2003
Latest operation start time: *03:06:30.752 UTC Tue Oct 21 2003
Latest operation start time: *03:06:33.754 UTC Tue Oct 21 2003
Latest operation start time: *03:06:36.755 UTC Tue Oct 21 2003
Latest operation start time: *03:06:39.752 UTC Tue Oct 21 2003
Latest operation start time: *03:06:42.753 UTC Tue Oct 21 2003
Latest operation start time: *03:06:45.755 UTC Tue Oct 21 2003
Latest operation start time: *03:06:48.752 UTC Tue Oct 21 2003
Latest operation start time: *03:06:51.753 UTC Tue Oct 21 2003
Latest operation start time: *03:06:54.755 UTC Tue Oct 21 2003
Latest operation start time: *03:06:57.752 UTC Tue Oct 21 2003
Latest operation start time: *03:07:00.753 UTC Tue Oct 21 2003
Latest operation start time: *03:07:03.754 UTC Tue Oct 21 2003
Latest operation start time: *03:07:06.752 UTC Tue Oct 21 2003
Latest operation start time: *03:07:09.752 UTC Tue Oct 21 2003
Latest operation start time: *03:07:12.753 UTC Tue Oct 21 2003
Latest operation start time: *03:07:15.755 UTC Tue Oct 21 2003
Latest operation start time: *03:07:18.752 UTC Tue Oct 21 2003
```

IP SLA 複数動作スケジューラの設定例

複数の IP SLA 動作のスケジューリングの例

以下に、20 秒のスケジュール期間で動作グループ 1 の IP SLA 動作 1 ～ 10 をスケジュールする例を示します。デフォルトにより、頻度はスケジュール期間と同じです。

```
Device# ip sla group schedule 1 1-10 schedule-period 20
```

次に、スケジューリングされた複数 IP SLA 動作の詳細を、**show ip sla group schedule** コマンドを使用して表示する例を示します。この例の最後の行には、IP SLA 動作が複数スケジューリングされていること（TRUE）が示されています。

```
Device# show ip sla group schedule
Multi-Scheduling Configuration:
Group Entry Number: 1
Probes to be scheduled: 1-10
Schedule period :20
Group operation frequency: 20
Multi-scheduled: TRUE
```

IP SLA ランダム スケジューラのイネーブル化の例

次に、IP SLA 動作 1 ～ 3 をグループ（グループ 2 として指定）としてスケジューリングする例を示します。この例では、動作は、50秒のスケジュール期間にわたって均一に分散されたランダムな間隔で開始するようにスケジューリングされます。最初の動作は、ただちに開始されるようにスケジューリングされます。間隔は、プローブが呼び出されるたびに、指定された範囲から毎回選択されます。ランダム スケジューラ オプションがイネーブルになり、動作のグループが再開する均一に分散されたランダムな頻度は、80 ～ 100 秒の範囲内で選択されます。

```
ip sla group schedule 2 1-3 schedule-period 50 frequency range 80-100 start-time now
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
Cisco IOS IP SLA コマンド	『Cisco IOS IP SLAs Command Reference, All Releases』
Cisco IOS IP SLA：一般情報	『*Cisco IOS IP SLAs Configuration Guide*』の「Cisco IOS IP SLAs Overview」モジュール
IP SLA の複数動作スケジューリング	『*Cisco IOS P SLAs Configuration Guide*』の「Configuring Multioperation Scheduling of IP SLAs Operations」モジュール
IP SLA の予防的しきい値モニタリング	『*Cisco IOS IP SLAs Configuration Guide*』の「Configuring Proactive Threshold Monitoring of IP SLAs Operations」モジュール

MIB

MIB	MIB のリンク
CISCO-RTTMON-MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャセットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

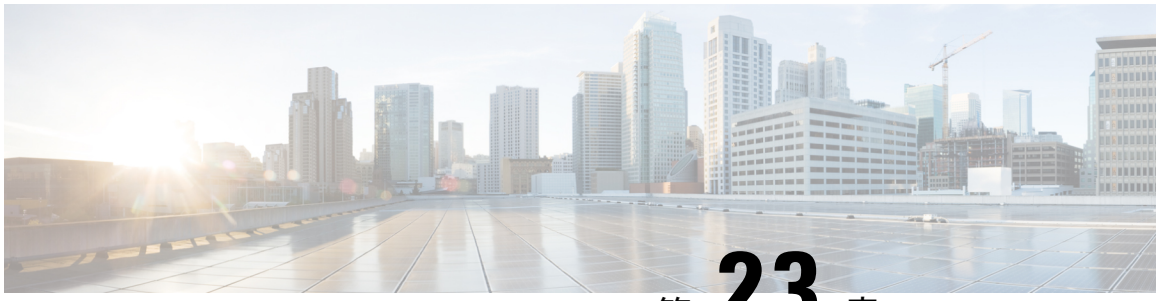
IP SLA 複数動作スケジューラに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *31 : IP SLA* 複数動作スケジューリングに関する機能情報

機能名	リリース	機能情報
IP SLA 複数動作スケジューラ		IP SLA 複数動作スケジューラ機能を使用すると、単一のコマンドを使用して複数の IP SLA 動作をスケジューリングできるため、スケーラビリティの高いインフラストラクチャが IP SLA に提供されます。
IP SLA ランダム スケジューラ		IP SLA ランダム スケジューラ機能を使用すると、複数の IP SLA 動作を、指定された期間にわたって均一に分散されたランダムな間隔で開始し、指定された頻度の範囲内に均一に分散されたランダムな頻度で再開するようにスケジューリングできます。



第 23 章

IP SLA 動作の予防的しきい値モニタリングの設定

このマニュアルでは、しきい値および反応トリガーを使用した IP サービス レベル契約（SLA）の予防的モニタリング機能について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

予防的しきい値モニタリングに関する情報

IP SLA 反応の設定

IP SLA の反応は、モニタリング対象の値が指定のレベルを超えるか、下回った場合、または、タイムアウトや接続損失などのモニタリング対象のイベントが発生した場合にトリガーされる

ように設定します。IP SLAによって測定された反応の設定が高すぎたり、低すぎたりすると、IP SLA では、ネットワーク管理アプリケーションへの通知を生成したり、より多くのデータを収集する別の IP SLA 動作をトリガーしたりすることがあります。

IP SLA 動作がトリガーされると、（トリガーされた）ターゲット動作が開始し、トリガーする動作の条件に関する知識がなくても独立して動作し続けます。ターゲット動作は、ターゲット動作に設定されたライフタイム値で指定されたとおり、そのライフが期限切れになるまで続行されます。ターゲット動作は、存続期間が終了するまで、再度トリガーされることはありません。

Cisco IOS リリース 15.2(3) 以降のリリースでは、（トリガーされた）ターゲット動作は条件クリアイベントまで動作します。その後、ターゲット動作は段階的に停止し、ターゲット動作の状態がアクティブから保留中に変わり、再度トリガーできるようになります。

IP SLA 動作によってサポートされる反応

各 IP SLA 動作にサポートされる反応を次の表に示します。

表 *32 : IP SLA* 動作によってサポートされる反応設定

反応	ICMP エコー	Path エコー	UDP ジッター	UDP エコー	TCP 接続	DHCP	DLSW	ICMP ジッター	DNS	フレームリレー
Failure	Y	--	Y	Y	Y	Y	--	Y	Y	--
RTT	Y	Y	--	Y	Y	Y	Y	--	Y	Y
RTTAvg	--	--	Y	--	--	--	--	Y	--	--
timeout	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
connectionLoss	--	--	Y	Y	Y	--	--	--	--	
verifyError	--	--	Y	Y	--	--	--	Y	--	Y
jitterSDAvg	--	--	Y	--	--	--		Y	--	--
jitterAvg	--	--	Y	--	--	--	--	Y	--	--
packetLateArrival	--	--	Y	--	--	--	--	Y	--	--
packetOutOfSequence	--	--	Y	--	--	--	--	Y	--	--
MaxOfPostiveSD	--	--	Y	--	--	--		Y	--	--
MaxOfNegativeSD	--	--	Y	--	--	--	--	Y	--	--
MaxOfPostiveDS	--	--	Y	--	--	--	--	Y	--	--
MaxOfNegativeDS	--	--	Y	--	--	--	--	Y	--	--
MOS	--	--	Y	--	--	--		--	--	--
ICPIF	--	--	Y	--	--	--	--	--	--	--

反応	ICMP エコー	Path エコー	UDP ジッター	UDP エコー	TCP 接続	DHCP	DLSW	ICMP ジッター	DNS	フレームリレー
PacketLossDS	--	--	Y	--	--	--	--	--	--	--
PacketLossSD	--	--	Y	--	--	--	--	--	--	--
PacketMIA	--	--	Y	--	--	--		--	--	--
iaJitterDS	--	--	--	--	--	--	--	--	--	--
frameLossDS	--	--	--	--	--	--	--	--	--	--
mosLQDSS	--	--	--	--	--	--	--	--	--	--
mosCQDS	--	--	--	--	--	--	--	--	--	--
rfactorDS	--	--	--	--	--	--	--	--	--	--
iaJitterSD	--	--	--	--	--	--	--	--	--	--
successivePacketLoss	--	--	--	--	--	--	--	Y	--	--
MaxOfLatencyDS	--	--	--	--	--	--	--	Y	--	--
MaxOfLatencySD	--	--	--	--	--	--	--	Y	--	--
LatencyDS	--	--	--	--	--	--	--	Y	--	--
LatencySD	--	--	--	--	--	--	--	Y	--	--
packetLoss	--	--	--	--	--	--	--	Y	--	--

表 *33 : IP SLA* 動作によってサポートされる反応設定

反応	HTTP	SLM	RTP	FTP	Lsp トレース	Post 遅延	パス ジッター	LSP ping	ゲートキーパーの登録
Failure	--	--	--	--	--	--	--	--	--
RTT	Y	Y	Y	Y	Y	Y	Y	Y	Y
RTTAvg	--	--	--	--	--	--	--	--	--
timeout	Y	Y	Y	Y	--	Y	Y	Y	Y
connectionLoss	Y		Y	Y	Y	--	--	Y	--
verifyError	--	--	--	--	--	--	--	--	--
jitterSDAvg	--	--	--	--	--	--	Y	--	--
jitterAvg	--	--	--	--	--	--	Y	--	--
packetLateArrival	--	--	--	--	--	--	Y	--	--

反応	HTTP	SLM	RIP	FTP	Lsp トレース	Post 遅延	パス ジッター	LSP ping	ゲートキーパーの登録
packetOutOfSequence	--	--	--	--	--	--	Y	--	--
MaxOfPostiveSD	--	--	--	--	--	--	Y	--	--
MaxOfNegativeSD	--	--	--	--	--	--	Y	--	--
MaxOfPostiveDS	--	--	--	--	--	--	Y	--	--
MaxOfNegativeDS	--	--	--	--	--	--	Y	--	--
MOS	--	--	--	--	--	--	--	--	--
ICPIF	--	--	--	--	--	--	--	--	--
PacketLossDS	--	--	Y	--	--	--	--	--	--
PacketLossSD	--	--	Y	--	--	--	--	--	--
PacketMIA	--	--	Y	--	--	--	--	--	--
iaJitterDS	--	--	Y	--	--	--	--	--	--
frameLossDS	--	--	Y	--	--	--	--	--	--
mosLQDSS	--	--	Y	--	--	--	--	--	--
mosCQDS	--	--	Y	--	--	--	--	--	--
rfactorDS	--	--	Y						
iaJitterSD	--	--	Y	--	--	--	--	--	--
successivePacketLoss	--	--	--	--	--	--	--	--	--
MaxOfLatencyDS	--	--	--	--	--	--	--	--	--
MaxOfLatencySD	--	--	--	--	--	--	--	--	--
LatencyDS	--	--	--	--	--	--	--	--	--
LatencySD	--	--	--	--	--	--	--	--	--
packetLoss	--	--	--	--	--	--	--	--	--

IP SLA しきい値モニタリングおよび通知

IP SLA は、ほとんどの IP SLA 動作に関する平均ジッタ、単方向の遅延、双方向のラウンドトリップ時間（RTT）、および接続などのパフォーマンス パラメータについての予防的しきい値モニタリングおよび通知をサポートします。予防的モニタリング機能は、単方向ジッター、単

方向のパケット損失、および単方向 VoIP 音声品質スコアリングを含む重要な VoIP 関連パラメータの反応しきい値を設定するためのオプションを提供します。

IP SLA の通知は、トリガーされた応答として設定されます。パケット損失、ジッター、平均動作スコア（MOS）統計情報は、IP SLA ジッター動作に固有です。通知はいずれかの方向（送信元から宛先、および宛先から送信元）の違反、またはパケット損失およびジッターの範囲外 RTT 値に対して生成できます。RTT 値が指定したしきい値を上回るか下回ると、トラップなどのイベントがトリガーされます。

応答条件が発生した場合、IP SLA ではシステム ロギング（syslog）メッセージを生成できます。システム ロギング メッセージは、CISCO-RTTMON-MIB を使用して簡易ネットワーク管理プロトコル（SNMP）トラップ（通知）として送信できます。IP SLA の SNMP トラップは、CISCO-RTTMON-MIB および CISCO-SYSLOG-MIB でサポートされます。

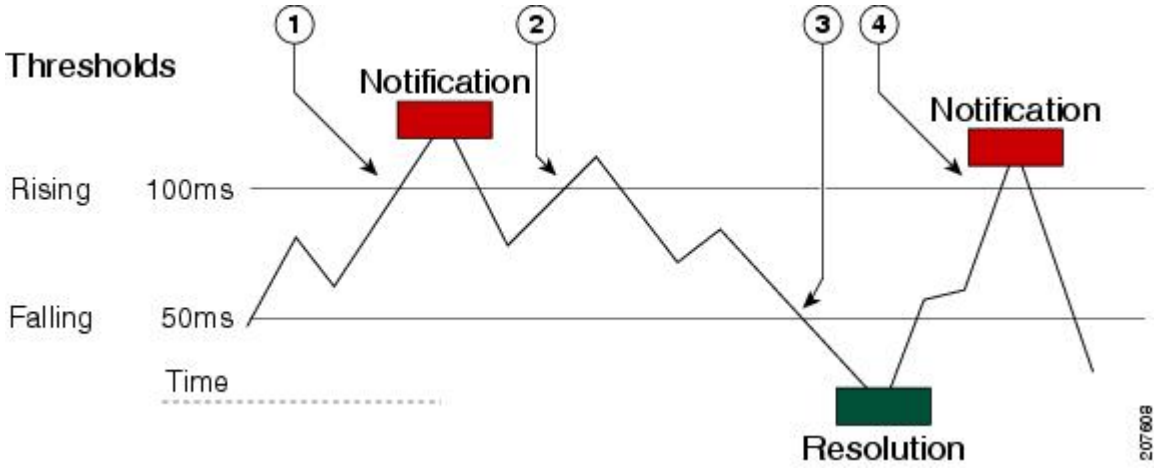
CISCO-SYSLOG-MIB の重大度レベルは、SyslogSeverity INTEGER {emergency(1), alert(2), critical(3), error(4), warning(5), notice(6), info(7), debug(8)} のように定義されます。

ソフトウェアのシステム ロギング プロセスに対しては、異なる重大度レベル値が定義されます。Cisco ソフトウェアのシステム ロギング プロセスに対する重大度レベルは、{emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), informational (6), debugging (7)} のように定義されます。

IP SLA しきい値違反は、Cisco システム ロギング プロセス内ではレベル 6（informational）としてロギングされますが、CISCO-SYSLOG-MIB からはレベル 7（info）トラップとして送信されます。

通知は、しきい値違反が発生するたびに発行されるわけではありません。次の図に、モニタリング対象要素が上限しきい値を超えたときに発生するトリガー反応の流れを示します。最初に上昇しきい値を超えたときに、イベントが送信され、通知が発行されます。後続のしきい値超過通知は、モニタリング対象の値が上昇しきい値を再び超える前に下限しきい値を下回った場合に限り発行されます。

図 *22 : IP SLA* のトリガーされた反応条件およびしきい値超過通知



1	最初に上昇しきい値を超えたときに、イベントが送信され、しきい値超過通知が発行されます。

2	上昇しきい値の超過違反が連続して発生しても、追加の通知は発行されません。
3	モニタリング対象の値が下限しきい値を下回っています。
4	上昇しきい値を超えたときに別のしきい値超過通知が発行されているのは、モニタリング対象の値が最初に下限しきい値を下回った後だけです。

（注） また、モニタリング対象の要素が下限しきい値を最初に下回った時点で（3）、下限しきい値超過通知が発行されます。前述のように、下限しきい値超過違反に対する後続の通知が発行されるのは、上昇しきい値を超えた後で、モニタリング対象の値が下限しきい値を再び下回った場合に限られます。

ジッター動作に対する RTT 反応

ジッター動作に対する RTT 反応は、動作の最後にのみトリガーされます。これには、平均リターントリップ時間（RTTAvg）値とマッチングされる、リターントリップ時間の最新値（LatestRTT）が使用されます。

ジッター動作に対する RTT の SNMP トラップは、動作全体の平均リターントリップ時間（RTTAvg）値に基づいており、動作中に送信される個々のパケットの RTT 値は含まれません。たとえば、平均がしきい値を下回っている場合、実際には最大で半数のパケットがしきい値を上回っている可能性がありますが、あくまでも動作全体に対する値であるため、このような詳細は通知には含まれません。

RTTAvg しきい値違反に対しては、syslog メッセージだけがサポートされています。syslog メッセージは、CISCO-RTTMON-MIB から送信されます。

予防的しきい値モニタリングの設定方法

予防的しきい値モニタリングの設定

この作業は、トラップを生成したり、別の動作を開始したりするためのしきい値および反応トリガーを設定する場合に実行します。

始める前に

- 違反条件を満たした場合に開始される IP SLA 動作を設定する必要があります。

（注）
- ジッター動作に対する RTT 反応は、動作の最後にのみトリガーされます。これには、リターントリップ時間の最新値（LatestRTT）が使用されます。
- ジッター動作に対する RTT の SNMP トラップは、動作全体に対するリターントリップ時間の平均値（RTTAvg）のみに基づいており、動作中に送信された個々のパケットのリターントリップ時間値は含まれません。RTTAvg しきい値違反に対しては、syslog メッセージだけがサポートされています。
- ジッター動作中の RTT 違反には、syslog メッセージだけがサポートされます。
- ジッター動作中以外の RTT 違反には、SNMP トラップだけがサポートされます。
- timeout、connectionLoss、または verifyError 以外の非 RTT 違反には、syslog メッセージのみがサポートされます。
- SNMP トラップと syslog メッセージの両方がサポートされているのは、timeout、connectionLoss、または verifyError 違反のみです。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla reaction-configuration** *operation-number* **react** *monitored-element* [**action-type** *option*] [**threshold-type** {**average** [*number-of-measurements*] | **consecutive** [*occurrences*] | **immediate** | **never** | **xofy** [*x-value y-value*]}] [**threshold-value** *upper-threshold lower-threshold*]
4. **ip sla reaction-trigger** *operation-number target-operation*
5. **ip sla logging traps**
6. 次のいずれかを実行します。
   - **snmp-server enable traps rtr**
   - **snmp-server enable traps syslog**
7. **snmp-server host** {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]
8. **exit**
9. **show ip sla reaction- configuration** [*operation-number*]
10. **show ip sla reaction- trigger** [*operation-number*]

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例：	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。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 3	**ip sla reaction-configuration** *operation-number* **react** *monitored-element* [**action-type** *option*] [**threshold-type** {**average** [*number-of-measurements*] | **consecutive** [*occurrences*] | **immediate** | **never** | **xofy** [*x-value y-value*]}] [**threshold-value** *upper-threshold lower-threshold*] 例： `Device(config)# ip sla reaction-configuration 10 react jitterAvg threshold-type immediate threshold-value 5000 3000 action-type trapAndTrigger`	指定したしきい値違反に基づいて実行されるアクション（SNMP トラップまたは IP SLA トリガー）を設定します。
ステップ 4	**ip sla reaction-trigger** *operation-number target-operation* 例： `Device(config)# ip sla reaction-trigger 10 2`	（任意）違反条件が満たされた場合に、別の IP SLA 動作を開始します。 • **ip sla reaction-configuration** コマンドを **trapAndTrigger** キーワードまたは **triggerOnly** キーワードを指定して設定した場合にのみ必須です。
ステップ 5	**ip sla logging traps** 例： `Device(config)# ip sla logging traps`	（任意）CISCO-RTTMON-MIB からの IP SLA syslog メッセージをイネーブルにします。

ステップ 6	次のいずれかを実行します。
	• **snmp-server enable traps rtr**
	• **snmp-server enable traps syslog**
	例：
	`Device(config)# snmp-server enable traps rtr`
	例：
	`Device(config)# snmp-server enable traps syslog`
		• （任意）最初の例は、CISCO-RTTMON-MIB トラップを生成するようにシステムを有効にする方法を示しています。
		• （任意）2 番目の例は、CISCO-SYSLOG-MIB トラップを生成するようにシステムを有効にする方法を示しています。

ステップ 7	**snmp-server host** {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*] 例： `Device(config)# snmp-server host 10.1.1.1 public syslog`	（任意）リモートホストにトラップを送信します。 • **snmp-server enable traps** コマンドを設定した場合に必須です。

	コマンドまたはアクション	目的
ステップ 8	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 9	**show ip sla reaction- configuration** [*operation-number*] 例： `Device# show ip sla reaction-configuration 10`	（任意）予防的しきい値モニタリングの設定を表示します。
ステップ 10	**show ip sla reaction- trigger** [*operation-number*] 例： `Device# show ip sla reaction-trigger 2`	（任意）トリガーされるターゲット動作の設定ステータスおよび動作状態を表示します。

予防的しきい値モニタリングの設定例

IP SLA 反応の設定例

次の例では、MOS 値が 4.9（最高品質）を超えたとき、または 2.5（低品質）を下回ったときに SNMP ロギング トラップを送信するよう、IP SLA 動作 10 が設定されます。

```
Device(config)# ip sla reaction-configuration 10 react mos threshold-type immediate
threshold-value 490 250 action-type trapOnly
```

次に、**ip sla reaction-configuration** コマンドのデフォルト設定の例を示します。

```
Device# show ip sla reaction-configuration 1
Entry number: 1
Reaction Configuration not configured
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ip sla reaction-configuration 1
Device(config)# do show ip sla reaction-configuration 1
Entry number: 1
Reaction: rtt
Threshold Type: Never
Rising (milliseconds): 5000
Falling (milliseconds): 3000
Threshold Count: 5
Threshold Count2: 5
Action Type: None
```

IP SLA 反応設定の確認例

次の例では、出力内の Reaction: 値に示されているとおり、複数のモニタリング対象要素が IP SLA 動作（1）に対して設定されています。

```
Device# show ip sla reaction-configuration

Entry Number: 1
Reaction: RTT
Threshold type: Never
Rising (milliseconds): 5000
Falling (milliseconds): 3000
Threshold Count: 5
Threshold Count2: 5
Action Type: None
Reaction: jitterDSAvg
Threshold type: average
Rising (milliseconds): 5
Falling (milliseconds): 3
Threshold Count: 5
Threshold Count2: 5
Action Type: triggerOnly
Reaction: jitterDSAvg
Threshold type:  immediate
Rising (milliseconds): 5
Falling (milliseconds): 3
Threshold Count: 5
Threshold Count2: 5
Action Type: trapOnly
Reaction: PacketLossSD
Threshold type:  immediate
Rising (milliseconds): 5
Threshold Falling (milliseconds): 3
Threshold Count: 5
Threshold Count2: 5
Action Type: trapOnly
```

SNMP 通知のトリガー例

次に、RTT または VoIP MOS のしきい値に違反した場合に、10.1.1.1 のリモート ホストに CISCO-SYSLOG-MIB トラップが送信されるように、予防的しきい値モニタリングを設定する例を示します。

```
! Configure the operation on source.
Device(config)# ip sla 1

Device(config-ip-sla)# udp-jitter 10.1.1.1 3000 codec g711alaw
Device(config-ip-sla-jitter)# exit

Device(config)# ip sla schedule 1 start now life forever

! Configure thresholds and reactions.
Device(config)# ip sla reaction-configuration 1 react rtt threshold-type immediate
threshold-value 3000 2000 action-type trapOnly

Device(config)# ip sla reaction-configuration 1 react MOS threshold-type consecutive 4
threshold-value 390 220 action-type trapOnly
```

```
Device(config)# ip sla logging traps

! The following command sends traps to the specified remote host.
Device(config)# snmp-server host 10.1.1.1 version 2c public syslog

! The following command is needed for the system to generate CISCO-SYSLOG-MIB traps.
Device(config)# snmp-server enable traps syslog
```

次に示すシステム ロギング メッセージの例は、IP SLA しきい値違反通知が Cisco システム ロギング プロセスでレベル 6（informational）として生成されることを示しています。

```
3d18h:%RTT-6-SAATHRESHOLD:RTR(11):Threshold exceeded for MOS
```

次の例は、同じ違反に対する CISCO-SYSLOG-MIB からの SNMP 通知であり、レベル 7（info）の通知となっています。

```
3d18h:SNMP:V2 Trap, reqid 2, errstat 0, erridx 0
 sysUpTime.0 = 32613038
 snmpTrapOID.0 = ciscoSyslogMIB.2.0.1
 clogHistoryEntry.2.71 = RTT
 clogHistoryEntry.3.71 = 7
 clogHistoryEntry.4.71 = SAATHRESHOLD
 clogHistoryEntry.5.71 = RTR(11):Threshold exceeded for MOS
 clogHistoryEntry.6.71 = 32613037
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
Cisco IOS IP SLA コマンド	『Cisco IOS IP SLAs Command Reference』

MIB

MIB	MIB のリンク
• CISCO-RTTMON-MIB • CISCO-SYSLOG-MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

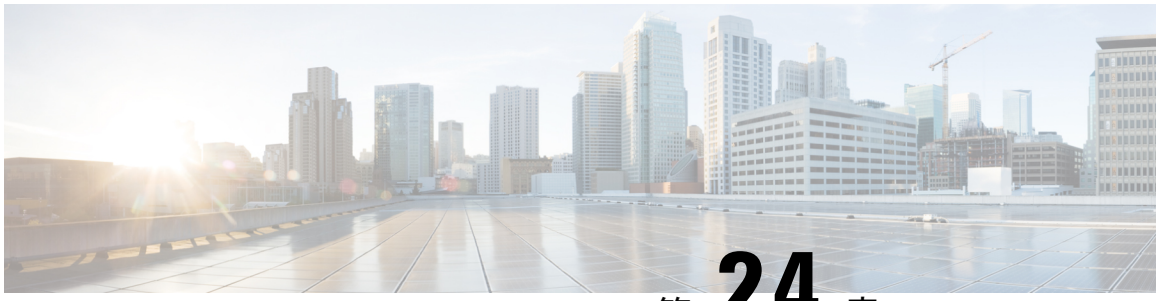
IP SLA 予防的しきい値モニタリングに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *34 : IP SLA* 予防的しきい値モニタリングに関する機能情報

機能名	リリース	機能情報
IP SLA - 反応しきい値		Cisco IOS IP SLA 予防的しきい値モニタリング機能を使用すると、特定の測定対象ネットワーク条件に反応するように IP SLA の動作を設定できます。
IP SLA - VoIP トラップ		IP SLA - VoIP トラップ機能には、単方向ジッター、単方向のパケット損失、および単方向 VoIP 音声品質スコアリング（MOS スコア）などの重要な VoIP 関連パラメータの反応しきい値を設定するための新しい機能が含まれています。
IP SLA の追加のしきい値トラップ		IP SLA 反応しきい値モニタリング用のこの機能拡張には、方向ごとの平均ジッター、方向ごとのパケット損失、最大の正負ジッター、および平均オピニオン評点（MOS）トラップが含まれています。この機能では、IP SLA 内の一方向遅延ジッター、パケット損失および遅延トラップも可能になり、アクション到着および遅延到着の紛失によるパケット損失のトラップも含まれています。



第 24 章

IP SLA TWAMP Responder

このモジュールでは、ネットワーク上のシスコ デバイスとシスコ以外の TWAMP 制御デバイス間の IP パフォーマンスを測定するために、シスコ デバイスで IETF Two-Way Active Measurement Protocol（TWAMP）Responder を設定する方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

IP SLA TWAMP Responder の前提条件

IP SLA TWAMP Responder が機能するには、TWAMP 制御クライアントとセッション送信元をネットワークに設定する必要があります。

IP SLA TWAMP Responder の制限事項

- IP SLA TWAMP Responder v1.0 では、TWAMP サーバとセッション リフレクタは、同一のシスコ デバイスに設定する必要があります。
- タイム スタンプは、管理インターフェイスを介して入出力する TWAMP テストパケットではサポートされません。
- タイム スタンプは、ルーティングされていないインターフェイスや BDI インターフェイスではサポートされません。
- タイム スタンプは、MPLS/VPLS インターフェイスではサポートされません。
- TWAMP クライアントおよびセッション送信側はサポートされていません。
- 1 つの TWAMP 応答側 に対して最大 9 個のセッション送信側を設定できます。
- TWAMP 光モードはサポートされていません。

IP SLA TWAMP Responder に関する情報

TWAMP

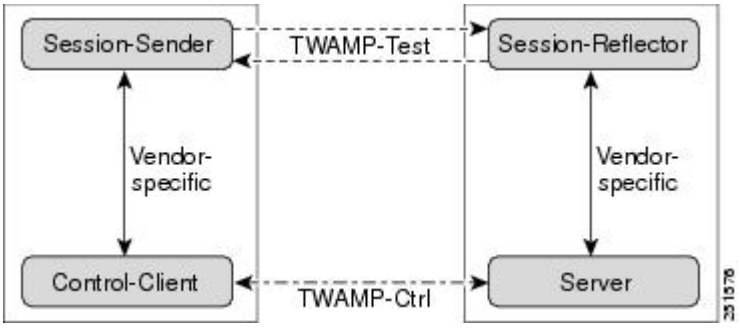
IETF Two-Way Active Measurement Protocol（TWAMP）は、TWAMP プロトコルをサポートする 2 つのデバイス間でのラウンドトリップ ネットワーク パフォーマンスの測定に関する規格を定めたものです。TWAMP 制御プロトコルは、パフォーマンス測定セッションを設定するために使用されます。TWAMP テストプロトコルは、パフォーマンス測定プローブを送受信するために使用されます。

TWAMP アーキテクチャは、モニタリング セッションの開始とパケットの交換に関与する次の 4 つの論理エンティティで構成されます。

- 制御クライアントは、TWAMP テストセッションをセットアップし、開始および停止を行います。
- セッション送信元は、セッション リフレクタに送信される TWAMP テスト パケットをインスタンス化します。
- セッション リフレクタは、TWAMP テスト パケットの受信時に、測定パケットを反映します。セッション リフレクタは、TWAMP 内のパケット統計情報を収集しません。
- TWAMP サーバは、1 つ以上の TWAMP セッションを管理するエンド システムで、エンドポイント内のセッションごとのポートを設定することもできます。サーバは TCP ポート 135 でリッスンします。セッション リフレクタとサーバは、IP SLA 動作で TWAMP Responder を構成します。

TWAMP は柔軟性の異なるエンティティを定義しますが、単一デバイスでロールの論理的なマージも可能にし、実装が容易になります。次の図に、TWAMP アーキテクチャを構成する 4 つのエンティティを示します。

図 *23 : TWAMP* のアーキテクチャ

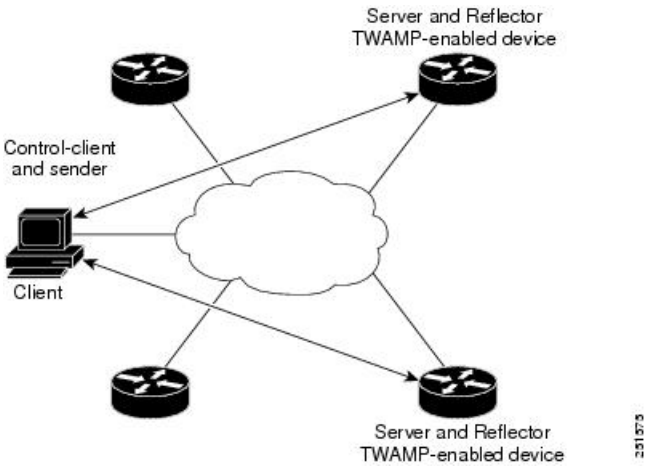


IP SLA TWAMP Responder v1.0

TWAMP Responder は、TWAMP をサポートする別のデバイスでコントロール クライアントおよびセッション送信元と相互運用します。IP SLA TWAMP Responder v1.0 機能では、Responder を構成するセッション リフレクタおよび TWAMP サーバは、同じデバイス上に設置する必要があります。

次の図では、1 つのデバイスがコントロール クライアントおよびセッション送信元（TWAMP 制御デバイス）で、他の 2 つのデバイスが IP SLA TWAMP Responder として設定されたシスコ デバイスです。各 IP SLA TWAMP Responder は、TWAMP サーバおよびセッション リフレクタの両方として機能します。

図 *24 :* 基本的な *TWAMP* 展開での *IP SLA TWAMP Responder*



IP SLA TWAMP Responder の設定方法

（注） 送信側（T1、T4）と受信側（T3、T2）のタイム スタンプはソフトウェアではなくハードウェアによって実行されるため、実際の Cisco IOS XE Everest 16.6.1 のジッタおよび遅延測定の精度が向上します。

TWAMP サーバの設定

（注） IP SLA TWAMP Responder v1.0 では、TWAMP サーバとセッション リフレクタは、同一のデバイスに設定されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla server twamp**
4. **port** *port-number*
5. **timer inactivity** *seconds*
6. **end**

手順の詳細

ステップ 1 **enable**

例：

```
Device> enable
```

特権 EXEC モードをイネーブルにします。

- パスワードを入力します（要求された場合）。

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 **ip sla server twamp**

例：

```
Device(config)#  ip sla server twamp
```

デバイスを TWAMP サーバとして設定し、TWAMP サーバ 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 **port** *port-number*

例：

```
Device(config-twamp-srvr)# port 9000
```

（任意）TWAMP サーバが接続および制御要求を受信するために使用するポートを設定します。

ステップ 5 **timer inactivity** *seconds*

例：

```
Device(config-twamp-srvr)# timer inactivity 300
```

（任意）TWAMP 制御セッションの非アクティビティ タイマーを設定します。

ステップ 6 **end**

例：

```
Device(config-twamp-srvr)# end
```

特権 EXEC モードに戻ります。

セッション リフレクタの設定

（注） IP SLA TWAMP Responder v1.0 では、TWAMP サーバとセッション リフレクタは、同一のデバイスに設定されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla responder twamp**
4. **timeout** *seconds*
5. **end**

手順の詳細

ステップ 1 **enable**

例：

```
Device> enable
```

特権 EXEC モードをイネーブルにします。

- パスワードを入力します（要求された場合）。

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 **ip sla responder twamp**

例：

```
Device(config)# ip sla responder twamp
```

デバイスを TWAMP Responder として設定し、TWAMP リフレクタ 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 **timeout** *seconds*

例：

```
Device(config-twamp-ref)#  timeout 300
```

（任意）TWAMP テスト セッションの非アクティビティ タイマーを設定します。

ステップ 5 **end**

例：

```
Device(config-twamp-ref)# end
```

特権 EXEC モードに戻ります。

IP SLA TWAMP レスポンダの設定例

IP SLA TWAMP Responder v1.0 の例

次の例と部分的な出力は、同一のシスコ デバイスで IP SLA TWAMP Responder v1.0 用の TWAMP サーバとセッション リフレクタを設定する方法を示します。この設定では、ポート 862 は TWAMP サーバが接続および制御要求を受信するために使用する（デフォルト）ポートです。サーバ リスナーのデフォルト ポートは、RFC 指定のポートで、必要に応じて再設定できます。

（注） IP SLA TWAMP Responder が機能するには、制御クライアントとセッション送信元をネットワークに設定する必要があります。

```
Device> enable
Device# configure terminal
Device(config)#  ip sla server twamp
Device(config-twamp-srvr)#  exit
Device(config)#  ip sla responder twamp
Device(config-twamp-ref)# end
Device> show running-config
.
.
.
ip sla responder
ip sla responder twamp
ip sla server twamp
port 862
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IP SLA コマンド	『Cisco IOS IP SLAs Command Reference』

標準および RFC

標準/RFC	タイトル
RFC 5357	『*Two-Way Active Measurement Protocol (TWAMP)*』
RFC 4656	『*One-way Active Measurement Protocol (OWAMP)*』

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IP SLA TWAMP Responder の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *35 : IP SLA TWAMP Responder* の機能情報

機能名	リリース	機能情報
IP SLA TWAMP Responder v1.0		この機能によって、ネットワーク上の IP SLA TWAMP Responder とシスコ以外の TWAMP 制御デバイス間のラウンドトリップ パフォーマンスを測定するために、シスコデバイスに TWAMP サーバとセッション リフレクタを設定できます。 次のコマンドが導入または変更されました。**ip sla responder twamp**、**ip sla server twamp**、**port (twamp)**、**show ip sla standards**、**show ip sla twamp connection**、**show ip sla twamp session**、**show ip sla twamp standards**、**timer inactivity**、**timeout (twamp)** .