



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 \(1 ページ\)](#)
- [LSP ヘルス モニタ動作の前提条件 \(2 ページ\)](#)
- [LSP ヘルス モニタ動作の制限事項 \(2 ページ\)](#)
- [LSP ヘルス モニタ動作に関する情報 \(2 ページ\)](#)
- [LSP ヘルス モニタ動作の設定方法 \(12 ページ\)](#)
- [LSP ヘルス モニタの設定例 \(27 ページ\)](#)
- [その他の参考資料 \(34 ページ\)](#)
- [LSP ヘルス モニタ動作に関する機能情報 \(36 ページ\)](#)

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 ルデバイスに対して新しい 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

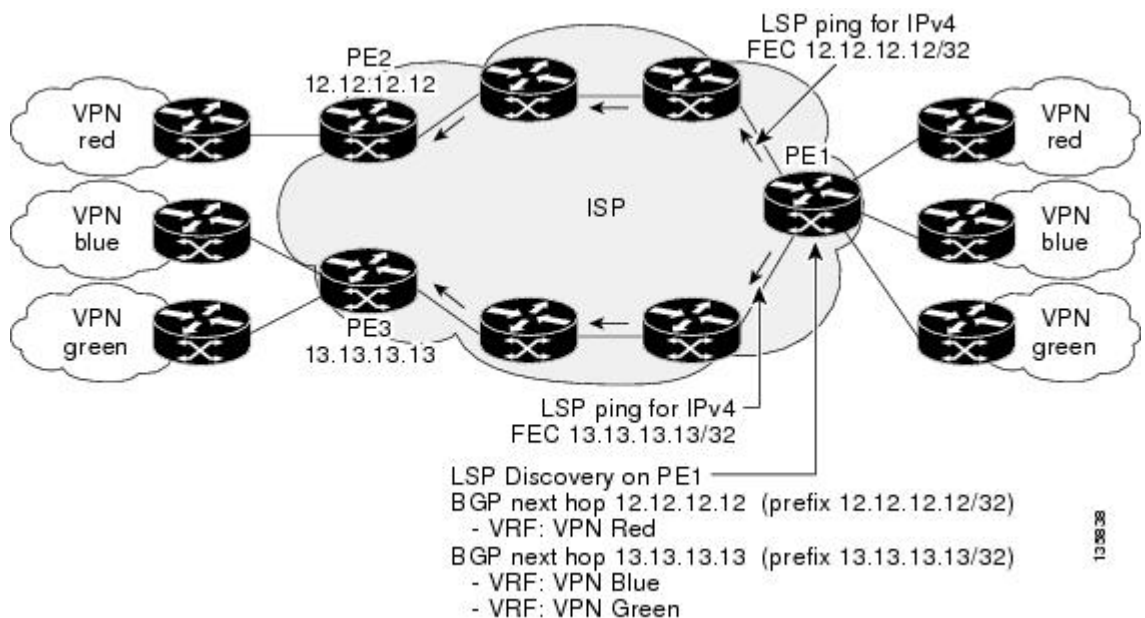
BGP ネクスト ホップ ネイバー探索プロセスは、送信元 PE デバイスに関連付けられているすべての VRF によって使用中の BGP ネクスト ホップ ネイバーを見つけるために使用されます。ほとんどの場合、これらのネイバーは PE デバイスです。

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

ティンク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 1: 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的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 マルチパスを一意的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。

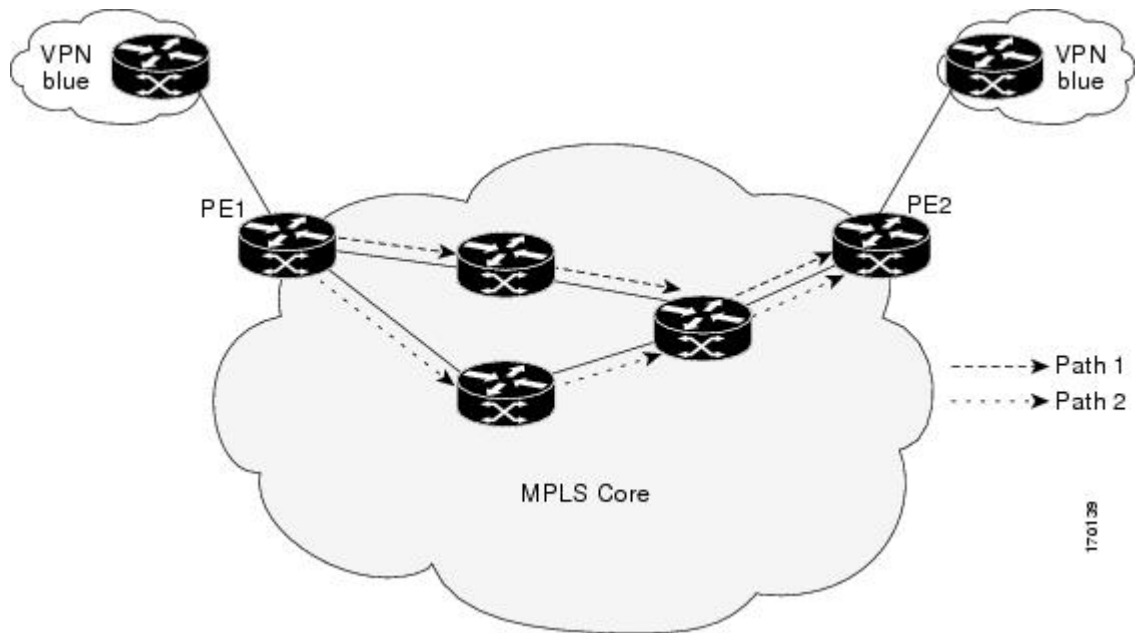


(注) 個別の LSP ヘルス モニタ動作に対し、ユーザは、同時に LSP ディスカバリを実行できる BGP ネクスト ホップ ネイバーの最大数を定義できます。

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、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。

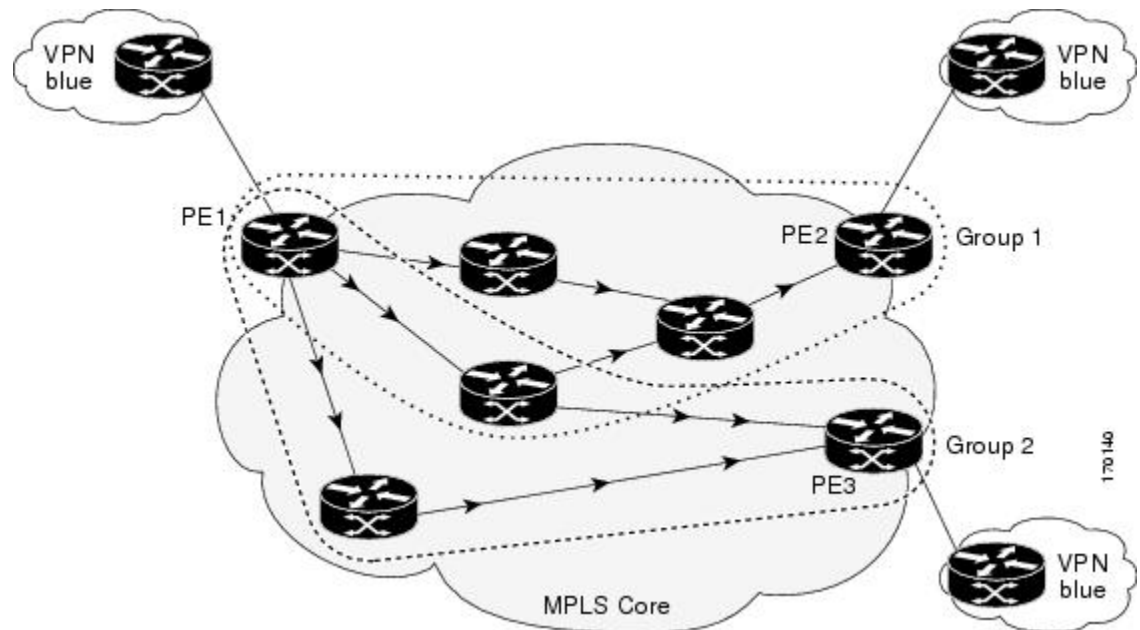
図 2: 単純な VPN の LSP ディスカバリ



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 3: 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のネットワークのオペ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 機能で使用す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 1: 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 : <pre>Device> enable</pre>	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 : <pre>Device# configure terminal</pre>	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 : <pre>Device(config)# mpls discovery vpn next-hop</pre>	（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 : <pre>Device(config)# mpls discovery vpn interval 120</pre>	（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 : <pre>Device(config)# auto ip sla mpls-lsp-monitor 1</pre>	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 : <pre>Device(config-auto-ip-sla-mpls)# type echo ipsla-vrf-all</pre> 例 : <pre>Device(config-auto-ip-sla-mpls)# type pathEcho ipsla-vrf-all</pre>	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 <i>minutes</i> 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 <i>factor</i> 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 <i>exp-bits</i> 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 <i>ip-address</i> 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 <i>dscp-value</i> 例 : <pre>Device(config-auto-ip-sla-mpls-params)# reply-dscp-bits 5</pre>	(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 { <i>ipv4</i> <i>router-alert</i> } 例 : <pre>Device(config-auto-ip-sla-mpls-params)# reply-mode router-alert</pre>	(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 <i>bytes</i> 例 : <pre>Device(config-auto-ip-sla-mpls-params)# request-data-size 200</pre>	(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 { <i>both</i> <i>connection-loss</i> <i>timeout</i> } <i>frequency</i> 例 : <pre>Device(config-auto-ip-sla-mpls-params)# secondary-frequency connection-loss 10</pre>	(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 <i>text</i> 例 : <pre>Device(config-auto-ip-sla-mpls-params)# tag testgroup</pre>	(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 <i>milliseconds</i> 例 : <pre>Device(config-auto-ip-sla-mpls-params)# threshold 6000</pre>	(任意) IPSLA 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 <i>milliseconds</i> 例 : <pre>Device(config-auto-ip-sla-mpls-params)# timeout 7000</pre>	(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 <i>time-to-live</i> 例 : <pre>Device(config-auto-ip-sla-mpls-params)# ttl 200</pre>	(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 : <pre>Device(config-auto-ip-sla-mpls-params)# exit</pre>	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 <i>operation-number</i> react { connectionLoss timeout } [action-type option] [threshold-type {consecutive [occurrences] immediate never}] 例 : <pre>Device(config)# auto ip sla mpls-lsp-monitor reaction-configuration 1 react connectionLoss action-type trapOnly threshold-type consecutive 3</pre>	(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 : <pre>Device(config)# exit</pre>	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** **lsp** {**lsp-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 <i>seconds</i> 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 <i>operation-number</i> 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 : <pre>Device(config-auto-ip-sla-mpls)# type echo ipsla-vrf-all</pre>	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 : <pre>Device(config-auto-ip-sla-mpls-params)# path-discover</pre>	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 : <pre>Device(config-auto-ip-sla-mpls-lpd-params)# hours-of-statistics-kept 1</pre>	(任意) LSP ヘルス モニタ動作に 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 : <pre>Device(config-auto-ip-sla-mpls-lpd-params)# force-explicit-null</pre>	(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 : <pre>Device(config-auto-ip-sla-mpls-lpd-params)# interval 2</pre>	(任意) LSP ヘルス モニタ動作に 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 : <pre>Device(config-auto-ip-sla-mpls-lpd-params)# lsp-selector-base 127.0.0.2</pre>	(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 : <pre>Device(config-auto-ip-sla-mpls-lpd-params)# maximum-sessions 2</pre>	(任意) 1 つの LSP ヘルス モニタ動作に 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 <i>minutes</i> 例 : <pre>Device(config-auto-ip-sla-mpls-lpd-params)# scan-period 30</pre>	(任意) LSP ヘルス モニタ動作に 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 <i>seconds</i> 例 : <pre>Device(config-auto-ip-sla-mpls-lpd-params)# session-timeout 60</pre>	(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 <i>seconds</i> 例 : <pre>Device(config-auto-ip-sla-mpls-lpd-params)# timeout 4</pre>	(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 : <pre>Device(config-auto-ip-sla-mpls-lpd-params)# exit</pre>	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 : <pre>Device(config-auto-ip-sla-mpls-params)# exit</pre>	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 <i>operation-number</i> react lpd {lpd-group [retry number] tree-trace} [action-type trapOnly] 例 : <pre>Device(config)# auto ip sla mpls-lsp-monitor reaction-configuration 1 react lpd lpd-group retry 3 action-type trapOnly</pre>	(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 : <pre>Device(config)# ip sla logging traps</pre>	(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 <i>operation-number</i> schedule-period <i>seconds</i> [frequency [<i>seconds</i>]] [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 <i>operation-number</i> 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 <i>destination-address destination-mask</i> [force-explicit-null] [lsp-selector <i>ip-address</i>] [src-ip-addr <i>source-address</i>] [reply { dscp <i>dscp-value</i> mode { ipv4 router-alert }}] • mpls lsp trace ipv4 <i>destination-address destination-mask</i> [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
	<i>ip-address</i>] [src-ip-addr <i>source-address</i>] [reply {dscp <i>dscp-value</i> mode {ipv4 router-alert}}] 例 : <pre>Device(config-ip-sla)# mpls lsp ping ipv4 192.168.1.4 255.255.255.255 lsp-selector 127.1.1.1</pre> 例 : <pre>Device(config-ip-sla)# mpls lsp trace ipv4 192.168.1.4 255.255.255.255 lsp-selector 127.1.1.1</pre>	
ステップ 5	exp <i>exp-bits</i> 例 : <pre>Device(config-sla-monitor-lspPing)# exp 5</pre>	(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 <i>bytes</i> 例 : <pre>Device(config-sla-monitor-lspPing)# request-data-size 200</pre>	(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} <i>frequency</i> 例 : <pre>Device(config-sla-monitor-lspPing)# secondary-frequency connection-loss 10</pre>	(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 <i>text</i> 例 : <pre>Device(config-sla-monitor-lspPing)# tag testgroup</pre>	(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 <i>milliseconds</i> 例 : <pre>Device(config-sla-monitor-lspPing)# threshold 6000</pre>	(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 <i>milliseconds</i> 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 <i>time-to-live</i> 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	LSPping 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 <i>operation-number</i> [react <i>monitored-element</i>] [threshold-type { never immediate consecutive [<i>consecutive-occurrences</i>] xofy [<i>x-value</i> <i>y-value</i>] average [<i>number-of-probes</i>]}] [threshold-value <i>upper-threshold</i> <i>lower-threshold</i>] [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 <i>operation-number</i> [life { forever <i>seconds</i> }] [start-time { <i>hh : mm[: ss]</i> [<i>month</i> <i>day</i> <i>day</i> <i>month</i>] pending now after <i>hh : mm : ss</i> }] [ageout <i>seconds</i>] [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 <i>[operation-number]</i> 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 <i>[operation-number]</i> 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 <i>[operation-number]</i> 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 <i>[group-id]</i> 例 : <pre>Device# show ip sla mpls-lsp-monitor collection-statistics 100001</pre>	(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 <i>[operation-number]</i> 例 : <pre>Device# show ip sla mpls-lsp-monitor configuration 1</pre>	(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 <i>[group-id]</i> 例 : <pre>Device# show ip sla mpls-lsp-monitor lpd operational-state 100001</pre>	(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 : <pre>Device# show ip sla mpls-lsp-monitor neighbors</pre>	(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 <i>operation-number</i> 例 : <pre>Device# show ip sla mpls-lsp-monitor scan-queue 1</pre>	(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 <i>[operation-number [group [group-id]]]</i> 例 : <pre>Device# show ip sla mpls-lsp-monitor summary</pre>	(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 <i>[operation-number] [details]</i> 例 : <pre>Device# show ip sla statistics 100001</pre>	(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。

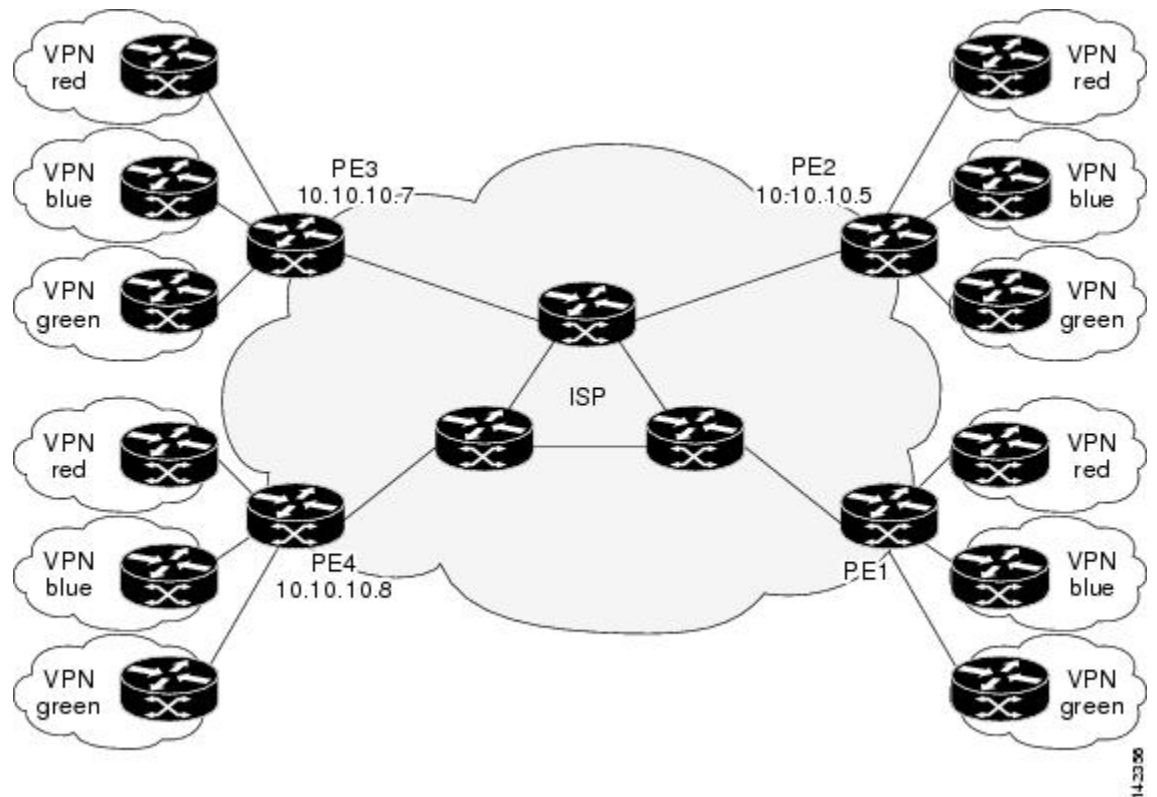
	コマンドまたはアクション	目的
		(注) このコマンドは、手動で設定された IP SLA 動作にのみ適用されます。
ステップ 11	show ip sla statistics aggregated [operation-number] [details] 例 : Device# show ip sla statistics aggregated 100001	(任意) IP SLA のすべての動作または指定した動作の集約された統計エラーおよび分散情報を表示します。 (注) このコマンドは、手動で設定された IP SLA 動作にのみ適用されます。
ステップ 12	show mpls discovery 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 4: LSP ヘルス モニタの例で使用するネットワーク



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

```

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

```

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ため、PE4 の IP SLA 動作 (Probe 100003) 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 **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 ネイバーになるため、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

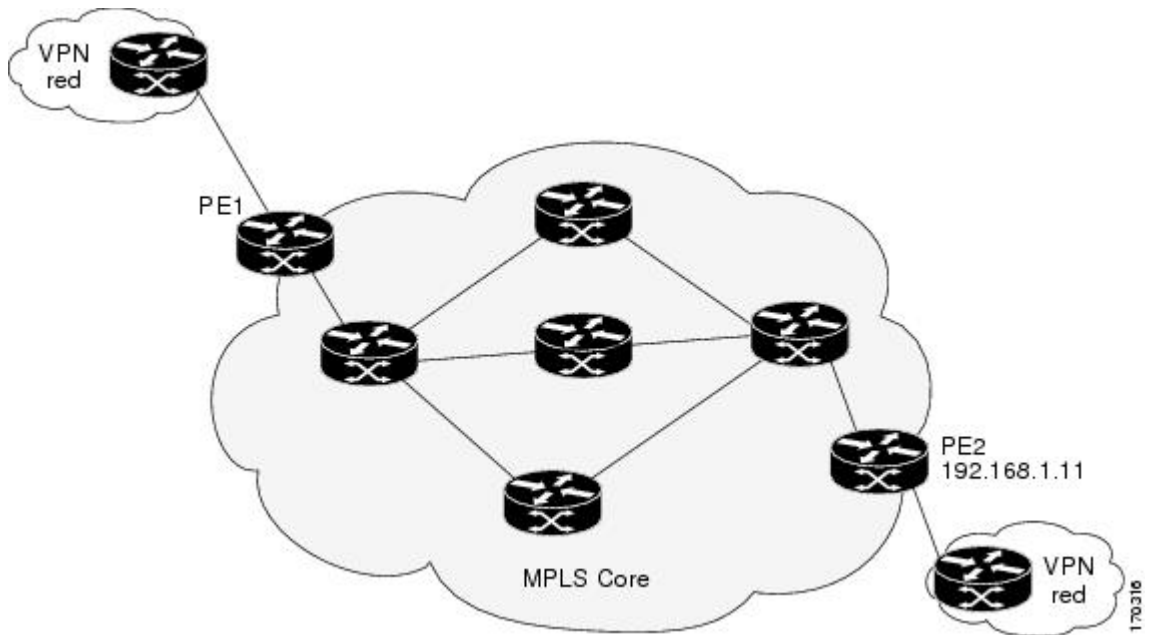
```

```
*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 5: LSP ディスカバリありの LSP ヘルス モニタの例で使用するネットワーク



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わると、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 Index	Outgoing Interface	Lsp Selector	Link Type	Conn Id	Adj Addr	Downstream 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
MPLSLSP ディスカバリ管理ツール	『 <i>Multiprotocol Label Switching Configuration Guide</i> 』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 2: 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。