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。

• IP SLA に関する情報 （1 ページ）

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。

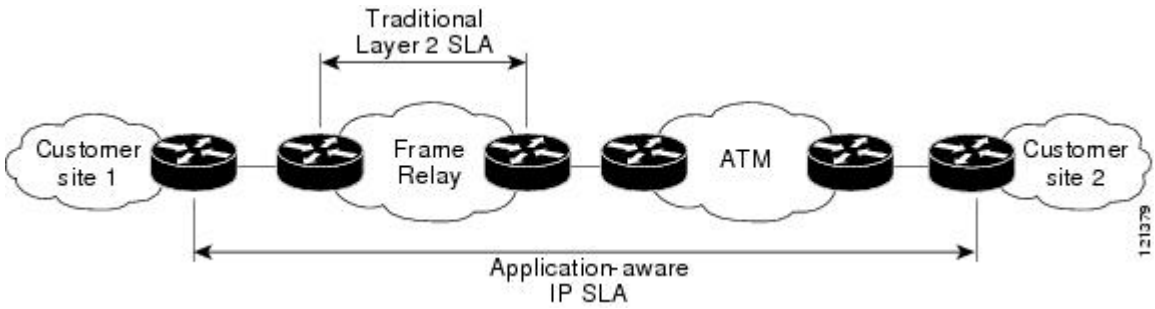
IP SLA 動作によって収集されたデータに基づく SNMP 通知により、パフォーマンスが指定したレベルを下回った場合や問題が修正された場合に、ルータはアラートを受信できます。IP SLA は、外部ネットワーク管理システム（NMS）アプリケーションとシスコ デバイス上で実行されている IP SLA 動作との間のインタラクションに Cisco RTTMON MIB を使用します。IP SLA 機能から参照されるオブジェクト変数の詳細については、Cisco MIB Web サイトから入手できる CISCO-RTTMON-MIB.my ファイルのテキストを参照してください。

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

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、ASR 920、および NCS 520 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。

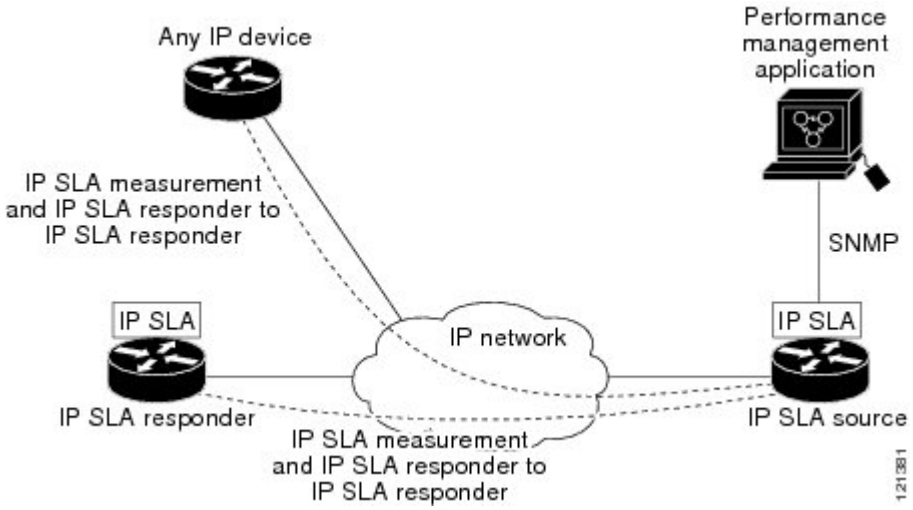
IP SLA を使用したネットワーク パフォーマンスの測定

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

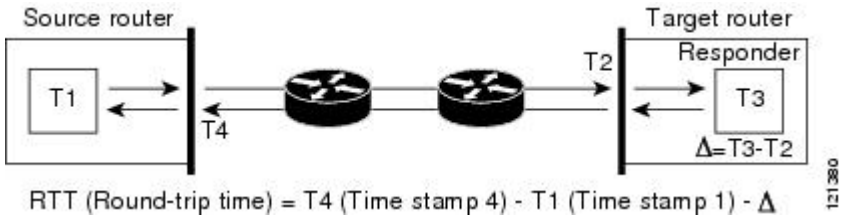
デバイスは、他のハイ プライオリティ プロセスがあるために、着信パケットの処理に数十ミリ秒かかることがあります。テストパケットに対する応答は、処理されるのを待ちながらキューに入っていることがあるため、この遅延によって応答時間は変化します。この場合、応答時間は正しいネットワーク遅延を反映しません。IP SLA は送信元デバイスとターゲット デバイス（IP SLA Responder が使用されている場合）の処理遅延を最小化し、正しいラウンドトリップ時間を識別します。IP SLA テスト パケットは、タイム スタンプによって処理遅延を最小化します。

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。