IP SLA UDP ジッター動作の設定

この章では、IP サービス レベル契約（SLA）UDP ジッター動作を設定して、IPv4 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。この章では、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。

この章は、次の項で構成されています。

IP SLA UDP ジッタ動作に関する情報

IP SLA UDP ジッター動作では、Voice over IP（VoIP）、Video over IP、またはリアルタイム会議などのリアルタイム トラフィックのアプリケーションのネットワーク適合性を診断することができます。

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た場合、たとえば 10 ms 間隔で送信された場合、ネットワークが理想的に動作していれば、宛先は 10 ms 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、パケットの到着間隔は、10 ミリ秒より大きくなる場合も、10 ミリ秒より小さくなる場合もあります。この例を使用すると、正のジッタ値は、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 ms 間隔で到着する場合、正のジッターは 2 ms です。パケットが 8 ms 間隔で到着する場合、負のジッターは 2 ms です。VoIP など遅延に影響されやすいネットワークの場合、正のジッター値は望ましくなく、0 のジッター値が最適です。

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 ジッター動作では、以下を測定できます。

- 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ことがあるので（非対称）、方向別データを使用してネットワークの輻輳などの問題が発生している場所を簡単に特定できます。

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。UDP ジッター動作は、指定された頻度 F で、送信元スイッチからターゲット スイッチに、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。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 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。これらのパラメータはそれぞれ、次の表に示すように、ユーザーが設定できます。

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	**Default**	**コマンド**
パケット数（n）	10 パケット	**udp-jitter** コマンド、**numpackets** オプション
パケットあたりのペイロードサイズ（S）	32 バイト	**request-data-size** コマンド
パケット間隔（ミリ秒単位）（T）	20 ミリ秒	**udp-jitter** コマンド、interval オプション
動作を繰り返すまでの経過時間（秒単位）（F）	60 秒	**frequency**（**IP SLA**）コマンド

IP SLA UDP ジッター動作を構成するための前提条件

IP SLA UDP ジッター動作を構成するための前提条件は次のとおりです。

- 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。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場合はデータが返りますが、UDP ジッター動作による一方向遅延測定の場合は 0 の値が返ります。

- IP SLA アプリケーションを構成する前に、 **show ip sla application** コマンドを使用して、ソフトウェア イメージで目的の動作タイプがサポートされていることを確認してください。

UDP ジッター動作に関するガイドラインと制約事項

- キーワードが付いている**show**コマンド**internal**はサポートされていません。
- 一方向遅延（レイテンシ）測定では、マイクロ秒単位の測定はサポートされていません。ミリ秒などの他の測定単位はサポートされています。
- Cisco NX-OS リリース 10.6(1) 以降、IPv6 は UDP ジッター動作に対してサポートされています。UDP ジッター操作で接続先と送信元の両方に IPv6 アドレスを設定でき、IPv6 ベースのレスポンダによるこれらの操作の処理を有効にできます。

  このサポートにより、IPv6 のみのデータ センター ネットワークで、ファブリックに面したリンクのラウンドトリップ時間（RTT）と UDP ジッター メトリックを取得できます。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、接続を測定することで、IPv6 UDP の接続先を追跡し、VoIP やビデオ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分析できます。

  - IPv6 UDP ジッター動作では、トラフィック クラスはサポートされません。
  - データ検証を有効にしてIPv6 UDP ジッター動作を行うと、破損したパケットはIP SLA アプリケーションに到達する前に UDP レイヤでドロップされます。これは、ソケットの実装が IPv6 UDP チェックサムでゼロをサポートしていないために発生します。

IP SLA パケットの CoPP の構成

IP SLA 動作を大規模なスケールで使用する場合、IP SLA パケットのパススルーを許可する特定の CoPP 構成が必要になる場合があります。通常、このコントロール プレーン ポリシング（CoPP）設定は、IP SLA コントロール プレーンおよびデータ プレーン パケットがコントロール プレーン ポリシング メカニズムによってドロップされないようにするために、IP SLA送信者と受信側の両方のデバイスで必要です。IP SLA ではユーザー定義の UDP ポートを使用するため、コントロール プレーンへのすべての IP SLA パケットを許可する手段がありません。ただし、IP SLA が使用できる接続先/送信元ポートのそれぞれを指定することはできます。

IP SLA プローブ数の検証済みの拡張性に関する詳細については、*Cisco Nexus 9000 Series NX-OS Verified Scalability Guide*を参照してください。

以下に、IP SLA パケットのパススルーを許可する CoPP 構成例を示します。この例では、接続先ポートと送信元ポートが 6500 ～ 7000 の範囲であることを前提としています。この例では、「insert-before」が指定されていない場合、「class-default」の後に「copp-ipsla」が追加されます。

（注） 次の構成例は、プラットフォーム/ハードウェア タイプによって異なる場合があります。IP ACL および CoPP の設定の詳細については、『Cisco Nexus 9000 Series NX-OS Security Configuration Guide』を参照してください。

```
ip access-list acl-sla-allow
  10 remark ### ALLOW SLA control packets from 1.1.1.0/24
  20 permit udp 1.1.1.0/24 any eq 1967
  30 remark ### ALLOW SLA data packets from 1.1.1.0/24 using ports 6500-7000
  40 permit udp 1.1.1.0/24 any range 6500 7000

class-map type control-plane match-any copp-ipsla
  match access-group name acl-sla-allow

policy-map type control-plane Custom-copp-policy-strict
    class copp-ipsla insert-before Custom-copp-class-l2-default
    police cir 1500 kbps

control-plane
  service-policy input Custom-copp-policy-strict

switch# show policy-map interface control-plane | be copp-ipsla
    class-map copp-ipsla (match-any)
      match access-group name acl-sla-allow
      set cos 7
      police cir 1500 kbps , bc 32000 bytes
      module 1 :
        transmitted 0 bytes;
        dropped 0 bytes;

    class-map Custom-copp-class-l2-default (match-any)
      match access-group name Custom-copp-acl-mac-undesirable
      set cos 0
      police cir 400 kbps , bc 32000 bytes
      module 1 :
        transmitted 0 bytes;
        dropped 0 bytes;

    class-map class-default (match-any)
      set cos 0
      police cir 400 kbps , bc 32000 bytes
      module 1 :
        transmitted 122 bytes;
        dropped 0 bytes;
```

Netstack ポート範囲の一致

IP SLA は、ローカルのネットスタック ポート範囲内のポートのみを受け入れます。プローブの設定で使用される送信元ポートと接続先ポートは、SLA 送信側と SLA レスポンダでサポートされている netstack ポートと一致している必要があります。

以前のバージョンからバージョン 9.3(1) 以降のバージョンに ISSU を実行する場合は、SSH ポートなどのユーザー定義ポートの機能が次の表に記載されている範囲内にあることを確認してください。

表 *2 : ISSU* のポート範囲

バージョン	デフォルトのポート範囲
9.3(1)	Kstack ローカル ポート範囲（15001 ～ 58000） Netstack ローカル ポート範囲（58001 ～ 63535） nat ポート範囲（63536 ～ 65535）
9.3(2)	Kstack ローカル ポート範囲（15001 ～ 58000） Netstack ローカル ポート範囲（58001 ～ 63535） nat ポート範囲（63536 ～ 65535）
9.3(3) 以降	Kstack ローカル ポート範囲（15001 ～ 58000） Netstack ローカル ポート範囲（58001 ～ 60535） nat ポート範囲（60536 - 65535）

show sockets local-port-range コマンドを使用すれば コマンドは、送信側/応答側のポート範囲を表示します。

以下は、netstack ポート範囲を表示する例です。

```
switch# show sockets local-port-range

Kstack local port range (15001 - 22002)
Netstack local port range (22003 - 65535)
```

送信元デバイスでの UDP ジッター動作の設定およびスケジューリング

ここでは、UDP ジッター動作を構成し、スケジュールする方法について説明します。

宛先デバイスでの IP SLA レスポンダ の設定

この項では、接続先デバイスでレスポンダを設定する方法について説明します。

（注） レスポンダでは、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。レスポンダ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. **feature sla responder**
4. 次のいずれかを実行します。
   - **ip sla responder**

     Example: `switch(config)# ip sla responder`
   - **ip sla responder udp-echo ipaddress** *ip-address* **port** *port*

     Example: `switch(config)# ip sla responder udp-echo ipaddress 172.29.139.132 port 5000`
   - **ip sla responder udp-echo ipaddress** *ipv6-address* **port** *port*

     Example: `switch(config)# ip sla responder udp-echo ipaddress 2001:DB8::2 port 5000`
5. **exit**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `switch> enable`	特権 EXEC モードを有効にします。 プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `switch# 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	**feature sla responder** 例： `switch(config)# feature sla responder`	IP SLA のレスポンダ機能を有効にします。
ステップ 4	次のいずれかを実行します。	-

	コマンドまたはアクション	目的
	• **ip sla responder** *Example:* switch(config)# ip sla responder • **ip sla responder udp-echo ipaddress** *ip-address* **port** *port* *Example:* switch(config)# ip sla responder udp-echo ipaddress 172.29.139.132 port 5000 • **ip sla responder udp-echo ipaddress** *ipv6-address* **port** *port* *Example:* switch(config)# ip sla responder udp-echo ipaddress 2001:DB8::2 port 5000	• （任意）送信元からの制御メッセージに応じて、Cisco デバイスにおけるレスポンダ機能を一時的に有効にします。 • （任意）送信元でプロトコル制御が無効である場合にのみ必須です。指定された IP アドレスおよびポートでレスポンダ機能を永続的に有効にします。 制御は、デフォルトでイネーブルになります。
ステップ 5	**exit** 例： switch(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基本的なUDPジッター動作の設定およびスケジューリング

ここでは、送信元デバイスでの基本 UDP ジッター動作を設定およびスケジュールする方法について説明します。

ヒント
- IP SLA 動作が実行せず、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 構成モードで設定）、データ検証を有効にします。イネーブルになると、各動作の応答が破損していないかどうか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 動作に関する問題のトラブルシューティングを行うには、**debug ip sla sender trace** コマンドと **debug ip sla sender error** コマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **feature sla sender**
4. **ip sla** *operation-number*
5. **udp-jitter** {*destination-ip-address* | *destination-ipv6-address* | *destination-hostname*} *destination-port* [**source-ip** {*source-ip-address* | *source-ipv6-address* | *hostname*}] [**sourceport**

port-number] [**control** { **enable**| **disable**}] [**num-packets** *number-of-packets*] [**interval** *interpacket-interval*]

6. **frequency** *seconds*
7. **exit**
8. **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**]
9. **exit**
10. **show ip sla configuration** [*operation-number*]

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `switch# enable`	特権 EXEC モードを有効にします。 プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `switch# 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	**feature sla sender** 例： `switch(config)# feature sla sender`	IP SLA 動作機能を有効にします。
ステップ 4	**ip sla** *operation-number* 例： `switch(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 5	**udp-jitter** {*destination-ip-address* | *destination-ipv6-address* | *destination-hostname*} *destination-port* [**source-ip** {*source-ip-address* | *source-ipv6-address* | *hostname*}] [**sourceport** *port-number*] [**control** { **enable**| **disable**}] [**num-packets** *number-of-packets*] [**interval** *interpacket-interval*]
	例：
	（IPv4 アドレス）
	`switch(config-ip-sla)# udp-jitter 172.29.139.134 5000`
	例：
	（IPv6 アドレス）
	`switch(config-ip-sla)# udp-jitter 2001:DB8::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。
		送信元スイッチとターゲット スイッチの両方で IP SLA 制御プロトコルを無効にする場合のみ、**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 6	**frequency** *seconds* 例： `switch(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	**exit** 例： `switch(config-ip-sla-jitter)# exit`	UDP ジッタ 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 8	**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： `switch(config)# ip sla schedule 5 start-time now life forever`	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。
ステップ 9	**exit** 例： `switch(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。
ステップ 10	**show ip sla configuration** [*operation-number*] 例： `switch# 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

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、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。

追加特性を指定したUDPジッター動作の設定およびスケジューリング

ここでは、追加特性を使用して UDP ジッター動作を設定し、スケジュールする方法について説明します。

- UDP ジッター動作には大量のデータが含まれるので、以下のコマンド群は UDP ジッター動作ではサポートされず、そのため 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）はサポートされません：**history buckets-kept**、**history filter**、**historylives-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** を使用してより大きな値を構成する*hours* グローバル構成を使用しても、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。

ヒント

- IP SLA 動作が実行されておらず、統計を生成していない場合は、 **verify-data** コマンドを動作の構成に追加して（IP SLA 構成モードで設定）、データ検証を有効にします。イネーブルになると、各動作の応答が破損していないかどうか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。
- **debug ip sla sender trace** コマンドを使用し、 および **debug ip sla sender error** IP SLA 動作に関する問題をトラブルシューティングするコマンドです。

始める前に

送信元デバイスで UDP ジッタ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 NX-OS 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、「接続先デバイスでの 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. **feature sla sender**
4. **ip sla** *operation-number*
5. **udp-jitter** {*destination-ip-address* | *destination-ipv6-address* | *destination-hostname*} *destination-port* [**source-ip** {*source-ip-address* | *source-ipv6-address* | *hostname*}] [**source-port** *port-number*] [**control** {**enable** | **disable**}] [**num-packets***number-of-packets*] [**interval** *interpacket-interval*]
6. **history distributions-of-statistics-kept** *size*
7. **history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*]
8. **frequency** *seconds*
9. **history hours-of-statistics-kept** *hours*
10. **owner** *owner-id*
11. **request-data-size** *bytes*
12. **history statistics-distribution-interval** *milliseconds*
13. **tag** *text*
14. **threshold** *milliseconds*
15. **timeout** *milliseconds*
16. **tos** *number*
17. **verify-data**

18. **vrf** *vrf-name*
19. **exit**
20. **ip sla schedule** *operation-number* [**life** {**forever**| *seconds*}] [**start-time** {*hh*:*mm*[:*ss*] [*monthday* | *daymonth*] | **pending** | **now** | **after***hh*:*mm*:*ss*}] [**ageout***seconds*] [**recurring**]
21. **exit**
22. **show ip sla configuration** [*operation-number*]

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードを有効にします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Switch# 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	**feature sla sender** 例： `switch(config)# feature sla sender`	IP SLA 動作機能を有効にします。
ステップ 4	**ip sla** *operation-number* 例： `Switch(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 5	**udp-jitter** {*destination-ip-address* | *destination-ipv6-address* | *destination-hostname*} *destination-port* [**source-ip** {*source-ip-address* | *source-ipv6-address* | *hostname*}] [**source-port** *port-number*] [**control** {**enable** | **disable**}] [**num-packets***number-of-packets*] [**interval** *interpacket-interval*] 例： （IPv4 アドレス） `Switch(config-ip-sla)# udp-jitter 172.29.139.134 5000` 例： （IPv6 アドレス）	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。 • **control disable** コマンドを使用し、キーワードの組み合わせは、送信元スイッチとターゲット スイッチの両方で IP SLA 制御プロトコルを無効にする場合のみ、使用してください。

	コマンドまたはアクション	目的
	`switch(config-ip-sla)# udp-jitter 2001:DB8::134 5000`	
ステップ 6	**history distributions-of-statistics-kept** *size* 例： `Switch(config-ip-sla-jitter)# history distributions-of-statistics-kept 5`	（オプション）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： `Switch(config-ip-sla-jitter)# history enhanced interval 900 buckets 100`	（オプション）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	**frequency** *seconds* 例： `Switch(config-ip-sla-jitter)# frequency 30`	（オプション）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： `Switch(config-ip-sla-jitter)# history hours-of-statistics-kept 4`	（オプション）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	**owner** *owner-id* 例： `Switch(config-ip-sla-jitter)# owner admin`	（オプション）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 11	**request-data-size** *bytes* 例： `Switch(config-ip-sla-jitter)# request-data-size 64`	（オプション）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 12	**history statistics-distribution-interval** *milliseconds* 例： `Switch(config-ip-sla-jitter)# history statistics-distribution-interval 10`	（オプション）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：	（オプション）IP SLA 動作のユーザー指定 ID を作成します。

	コマンドまたはアクション	目的
	`Switch(config-ip-sla-jitter)# tag TelnetPollServer1`	
ステップ 14	**threshold** *milliseconds* 例： `Switch(config-ip-sla-jitter)# threshold 10000`	（オプション）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： `Switch(config-ip-sla-jitter)# timeout 10000`	（オプション）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	**tos** *number* 例： `Switch(config-ip-sla-jitter)# tos 160`	（オプション）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 17	**verify-data** 例： `Switch(config-ip-sla-jitter)# verify-data`	（オプション）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 18	**vrf** *vrf-name* 例： `Switch(config-ip-sla-jitter)# vrf vpn-A`	（オプション）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 19	**exit** 例： `Switch(config-ip-sla-jitter)# exit`	UDP ジッタ 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 20	**ip sla schedule** *operation-number* [**life** {**forever**| *seconds*}] [**start-time** {*hh*:*mm*[:*ss*] [*monthday* | *daymonth*] | **pending** | **now** | **after***hh*:*mm*:*ss*}] [**ageout***seconds*] [**recurring**] 例： `Switch(config)# ip sla schedule 5 start-time now life forever`	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。
ステップ 21	**exit** 例： `Switch(config)# exit`	（オプション）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 22	**show ip sla configuration** [*operation-number*] 例： `Switch# show ip sla configuration 10`	（オプション）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

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、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。 を実行する前に、ユーザ名がフィギュレーション ファイルに指定されていることを確認してください。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。

UDP ジッター動作の構成例

以下に、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構成されている、2 つの動作を示します。どちらの動作も無期限に実行されます。

```
feature sla sender
ip sla 1
 udp-jitter 20.0.10.3 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 20.0.10.3 65052 num-packets 20 interval 10
 request-data-size 20
 tos 64
 frequency 30
ip sla schedule 2 start-time after 00:05:05
```

ターゲット（宛先）デバイスの設定は、次のとおりです。

```
feature sla responder
ip sla responder
```

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