



## IP SLA UDP エコー動作の設定

この章では、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、Cisco スイッチと IPv4 を使用するデバイスとの間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、接続先の Cisco スイッチで 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。

この章は、次の項で構成されています。

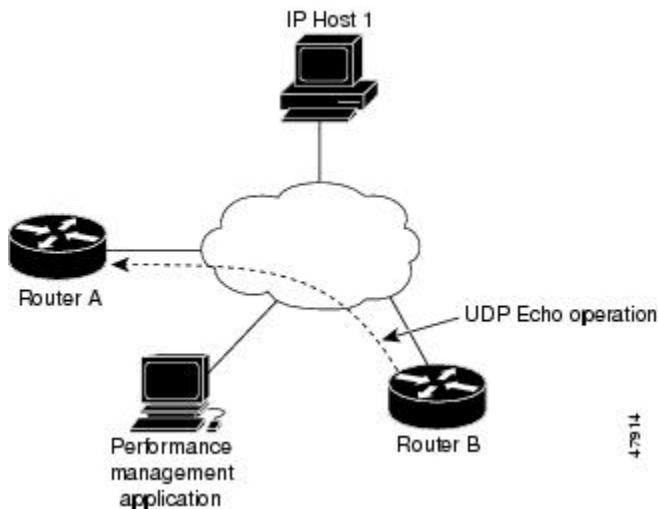
- [UDP エコー動作 \(1 ページ\)](#)
- [UDP エコー動作に関する注意事項と制約事項 \(2 ページ\)](#)
- [宛先デバイスでの IP SLA Responder の設定 \(4 ページ\)](#)
- [送信元デバイスでの基本 UDP エコー動作の設定 \(6 ページ\)](#)
- [送信元デバイスでのオプション パラメータを使用した UDP エコー動作の設定 \(7 ページ\)](#)
- [IP SLA 動作のスケジューリング \(10 ページ\)](#)
- [UDP エコー動作の構成例 \(13 ページ\)](#)

## UDP エコー動作

UDP エコー動作は、Cisco スイッチと 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、スイッチ A が IP SLA Responder として設定され、スイッチ B が送信元 IP SLA デバイスとして設定されています。

## ■ UDP エコー動作に関する注意事項と制約事項



スイッチ B から宛先スイッチ（スイッチ A）に UDP エコー要求メッセージを送信し、スイッチ 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、スイッチ A (宛先の Cisco スイッチ) でレスポンダを使用することによって向上します。宛先スイッチが Cisco スイッチの場合、IP SLA Responder 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、Cisco および Cisco 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連した問題のトラブルシューティングを行う際に、UDP エコー動作の結果が役立つことがあります。

## UDP エコー動作に関する注意事項と制約事項

- 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。

## 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-12-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-12-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 ポート範囲の一一致

IP SLA は、ローカルのネットワー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。

## 宛先デバイスでの IP SLA Responder の設定

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 1: 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)
```

## 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. feature sla responder

4. 次のいずれかを実行します。

- ip sla responder

例 :

```
switch(config)# ip sla responder
```

- ip sla responder udp-echo ipaddress *ip-address* port *port*

例 :

```
switch(config)# ip sla responder udp-echo ipaddress 172.29.139.132 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	<b>enable</b> 例 : <pre>switch&gt; enable</pre>	特権 EXEC モードをイネーブルにします 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	<b>configure terminal</b> 例 : <pre>switch# 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	<b>feature sla responder</b> 例 : <pre>switch(config)# feature sla responder</pre>	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。 <ul style="list-style-type: none"> <li>• <b>ip sla responder</b> 例 : <pre>switch(config)# ip sla responder</pre></li> <li>• <b>ip sla responder udp-echo ipaddress <i>ip-address</i> port <i>port</i></b> 例 : <pre>switch(config)# ip sla responder udp-echo ipaddress 172.29.139.132 port 5000</pre></li> </ul>	- <ul style="list-style-type: none"> <li>• 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 IP SLA Responder 機能を一時的に有効にします。</li> <li>• 送信元でプロトコル制御が無効である場合のみ必須です。このコマンドは、指定の IP アドレスおよびポートで IP SLA Responder 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。</li> </ul>
ステップ5	<b>exit</b> 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。

## 送信元デバイスでの基本 UDP エコー動作の設定

コマンドまたはアクション	目的
switch(config)# exit	

# 送信元デバイスでの基本 UDP エコー動作の設定

ここでは、送信元での基本 UDP エコー動作を構成する方法について説明します。



(注) トランプを生成する目的、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。

### 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} sourceport port-number] [control {enable | disable}]**
5. (任意) **frequency seconds**
6. (任意) **end**

### 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	<b>enable</b> 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	<b>configure terminal</b> 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	<b>ip sla operation-number</b> 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 モードに移行します。

	コマンドまたはアクション	目的
	switch(config)# ip sla 10	
ステップ 4	<b>udp-echo {destination-ip-address   destination-hostname} destination-port [source-ip {ip-address   hostname} sourceport port-number] [control {enable   disable}]</b> 例： switch(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。
ステップ 5	(任意) <b>frequency seconds</b>  例： switch(config-ip-sla-udp)# frequency 30	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	(任意) <b>end</b>  例： switch(config-ip-sla-udp)# 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 UDP エコー動作の設定

ここでは、送信元デバイスでオプションパラメータを使用して UDP エコー動作を構成する方法について説明します。



(注) トランプを生成する目的、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。

### 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。「接続先デバイスでの IP SLA Responder の構成」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} sourceport port-number] [control {enable | disable}]**
5. (任意) **history buckets-kept size**

## ■ 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

6. (任意) **data-pattern** *hex-pattern*
7. (任意) **history distributions-of-statistics-kept** *size*
8. (任意) **history enhanced** [*interval seconds*] [**buckets** *number-of-buckets*]
9. (任意) **history filter** {none | all | overThreshold | failures}
10. (任意) **frequency** *seconds*
11. (任意) **history hours-of-statistics-kept** *hours*
12. (任意) **history lives-kept** *lives*
13. (任意) **owner** *owner-id*
14. (任意) **request-data-size** *bytes*
15. (任意) **history statistics-distribution-interval** *milliseconds*
16. (任意) **tag** *text*
17. (任意) **threshold** *milliseconds*
18. (任意) **timeout** *milliseconds*
19. (任意) **tos** *number*
20. (任意) **verify-data**
21. **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	<b>enable</b> 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	<b>configure terminal</b> 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	<b>ip sla operation-number</b> 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 4	<b>udp-echo</b> { <i>destination-ip-address</i>   <i>destination-hostname</i> } <i>destination-port</i> [ <b>source-ip</b> { <i>ip-address</i>   <i>hostname</i> }] <b>sourceport</b> <i>port-number</i> ] [ <b>control</b> { <b>enable</b>   <b>disable</b> }] 例： switch(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。
ステップ 5	(任意) <b>history buckets-kept</b> <i>size</i>  例：	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。

	コマンドまたはアクション	目的
	switch(config-ip-sla-udp) # history buckets-kept 25	
ステップ 6	(任意) <b>data-pattern</b> <i>hex-pattern</i> 例： switch(config-ip-sla-udp) # data-pattern	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	(任意) <b>history distributions-of-statistics-kept</b> <i>size</i> 例： switch(config-ip-sla-udp) # history distributionsof- statistics-kept 5	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	(任意) <b>history enhanced</b> [ <i>interval seconds</i> ] [ <b>buckets number-of-buckets</b> ] 例： switch(config-ip-sla-udp) # history enhanced interval 900 buckets 100	IP SLA 動作に対する拡張履歴収集を有効にします。
ステップ 9	(任意) <b>history filter</b> { <b>none</b>   <b>all</b>   <b>overThreshold</b>   <b>failures</b> } 例： switch(config-ip-sla-udp) # history filter failures	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	(任意) <b>frequency</b> <i>seconds</i> 例： switch(config-ip-sla-udp) # frequency 30	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	(任意) <b>history hours-of-statistics-kept</b> <i>hours</i> 例： switch(config-ip-sla-udp) # history hours-ofstatistics- kept 4	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	(任意) <b>history lives-kept</b> <i>lives</i> 例： switch(config-ip-sla-udp) # history lives-kept 5	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	(任意) <b>owner</b> <i>owner-id</i> 例： switch(config-ip-sla-udp) # owner admin	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	(任意) <b>request-data-size</b> <i>bytes</i> 例： switch(config-ip-sla-udp) # request-data-size 64	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。

## IP SLA 動作のスケジューリング

	コマンドまたはアクション	目的
ステップ 15	(任意) <b>history statistics-distribution-interval milliseconds</b>  例： <pre>switch(config-ip-sla-udp)# history statistics distribution- interval 10</pre>	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	(任意) <b>tag text</b>  例： <pre>switch(config-ip-sla-udp)# tag TelnetPollServer1</pre>	IP SLA 動作のユーザー指定 ID を作成します。
ステップ 17	(任意) <b>threshold milliseconds</b>  例： <pre>switch(config-ip-sla-udp)# threshold 10000</pre>	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	(任意) <b>timeout milliseconds</b>  例： <pre>switch(config-ip-sla-udp)# timeout 10000</pre>	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	(任意) <b>tos number</b>  例： <pre>switch(config-ip-sla-jitter)# tos 160</pre>	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	(任意) <b>verify-data</b>  例： <pre>switch(config-ip-sla-udp)# verify-data</pre>	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	<b>exit</b>  例： <pre>switch(config-ip-sla-udp)# exit</pre>	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。

## IP SLA 動作のスケジューリング

ここでは、IP SLA 動作をスケジュールする方法について説明します。

## 始める前に



(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。



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。インペーブルになると、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 trace** コマンドを使用し、および**debug ip sla error** コマンドは、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ためのコマンドです。

## 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 schedule operation-number [life forever { | seconds}] [starttime {hh : mm[: ss]} [month day | day month] | pending | now | after hh : mm : ss}] [ageout seconds] [recurring]**

例：

```
ip sla schedule operation-number [life {forever | seconds}] [starttime {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}] [starttime{ hh:mm[:ss] [month day | day month] | pending | now | after hh:mm:ss}]**

例：

```
switch(config)# ip sla group schedule 1 3,4,6-9
```

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

## 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	<b>enable</b>  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	<b>configure terminal</b>  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	次のいずれかを実行します。  • <b>ip sla schedule operation-number [life forever {   seconds}] [starttime {hh : mm[: ss]} [month day   day month]   pending   now   after hh : mm : ss}] [ageout seconds] [recurring]</b>  例：  ip sla schedule operation-number [life {forever   seconds}] [starttime {hh : mm[: ss]} [month day   day month]   pending   now   after hh : mm : ss}] [ageout seconds] [recurring]  • <b>ip sla group schedule group-operation-number operation-id-numbers schedule-period schedule-period-range [ageout seconds] [frequency group-operation-frequency] [life{forever   seconds}] [starttime { hh:mm[:ss] [month day   day month]   pending   now   after hh:mm:ss}]</b>  例：  switch(config)# ip sla group schedule 1 3,4,6-9	-  • 個々の IP SLA 動作の場合のみ： 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の場合のみ： 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。
ステップ 4	<b>exit</b>  例： switch(config)# exit	特権 EXEC モードに戻ります。
ステップ 5	<b>show ip sla group schedule</b>  例： switch# 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	<b>show ip sla configuration</b>  例：	(任意) IP SLA 設定の詳細を表示します。

コマンドまたはアクション	目的
switch# show ip sla configuration	

### 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 エコー動作の構成例

以下に、ただちに開始され、無期限に実行される UDP エコーの IP SLA 動作タイプを構成する例を示します。

```
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
```

## ■ UDP エコー動作の構成例

## 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。