



## IP SLA TCP 接続動作の設定

この章では、Cisco スイッチと IPv4 を使用するデバイスとの間の、TCP 接続動作の実行に要する応答時間を測定できるように、IP サービス レベル契約 (SLA) の TCP 接続動作を構成する方法について説明します。TCP 接続の精度は、宛先の 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。この章では、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ー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ーの応答時間の測定やサーバーの可用性の接続テストに役立ちます。

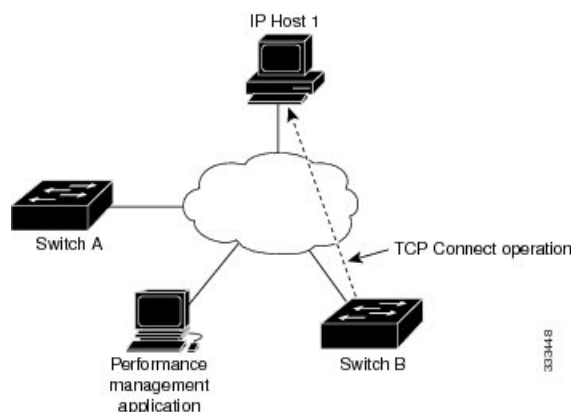
この章には、以下の項があります。

- [TCP 接続動作に関する情報 \(1 ページ\)](#)
- [IP SLA TCP 接続動作の設定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 TCP 接続動作の設定およびスケジューリング \(6 ページ\)](#)
- [TCP 接続動作の構成例 \(13 ページ\)](#)

## TCP 接続動作に関する情報

IP SLA TCP 接続動作は、Cisco スイッチと IP を使用するデバイスとの間の 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、スイッチ 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。



接続応答時間は、スイッチ 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への TCP 接続を確立します。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 サーバーには 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ー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。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。IPACL 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 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

この項では、接続先デバイスで IP SLA Responder を設定する方法について説明します。

### 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ク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 tcp-connect ipaddress ip-address port port**

例 :

```
switch(config)# ip sla responder tcp-connect ipaddress 172.29.139.132 port 5000
```

5. **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	<b>enable</b> 例 : <pre>switch&gt; enable</pre>	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 : <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 のレスポンス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 tcp-connect ipaddress ip-address port port</b>                例 :  <pre>switch(config)# ip sla responder tcp-connect ipaddress 172.29.139.132 port 5000</pre> </li> </ul>	- <ul style="list-style-type: none"> <li>• (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 IP SLA Responder 機能を一時的に有効にします。</li> <li>• (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。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 : <pre>switch(config)# exit</pre>	(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

ここでは、送信元デバイスでの TCP 接続動作を構成し、スケジューリングする方法について説明します。

送信元デバイスの TCP 接続動作を構成し、スケジューリングするには、次のいずれか 1 つのタスクだけを実行します。

- 送信元デバイスでの基本 TCP 接続動作の構成とスケジューリング
- 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 接続動作の構成とスケジューリング

## 送信元デバイスでの基本の TCP 接続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 TCP 接続動作を設定およびスケジューリングする方法について説明します。



(注) IP SLA レスポンダが宛先 IP アドレスとポートで永続的に有効になっている場合は、**control** を使用します。 **disable tcp-connect** を使ったキーワード制御メッセージを無効にするコマンド。



- 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。

### 手順の概要

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

6. **frequency** *seconds*
7. **exit**
8. **ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh:mm[:ss]* [*monthday* | *daymonth*] | **pending** | **now** | **after** *hh:mm:ss*}] [**ageout** *seconds*] [**recurring**]
9. **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	<b>enable</b> 例： <pre>switch&gt; enable</pre>	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： <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 sender</b> 例： <pre>switch(config)# feature sla sender</pre>	IP SLA 動作機能を有効にします。
ステップ 4	<b>ip sla operation-number</b> 例： <pre>switch(config)# ip sla 10</pre>	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	<b>tcp-connect</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>source-port</b> <i>port-number</i> ] [ <b>control</b> { <b>enable</b>   <b>disable</b> }] 例： <pre>switch(config-ip-sla)# tcp-connect 172.29.139.132 5000</pre>	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、 <b>control disable</b> キーワードの組み合わせを使用します。
ステップ 6	<b>frequency</b> <i>seconds</i> 例： <pre>switch(config-ip-sla-tcp)# frequency 60</pre>	(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	<b>exit</b> 例： <pre>switch(config-ip-sla-tcp)# exit</pre>	IP SLA TCP 構成モードを終了し、グローバル構成モードに戻ります。

	コマンドまたはアクション	目的
ステップ 8	<p><b>ip sla schedule</b> <i>operation-number</i> [<b>life</b> {<b>forever</b>   <i>seconds</i>}] [<b>start-time</b> {<i>hh:mm[:ss]</i> [<i>monthday</i>   <i>daymonth</i>]}   <b>pending</b>   <b>now</b>   <b>after</b> <i>hh:mm:ss</i>] [<b>ageout</b> <i>seconds</i>] [<b>recurring</b>]</p> <p>例 :</p> <pre>switch(config)# ip sla schedule 10 start-time now life forever</pre>	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	<p><b>exit</b></p> <p>例 :</p> <pre>switch(config)# exit</pre>	(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。

### 例

次に、即時に開始されて無期限に実行される TCP 接続の IP SLA 動作タイプを構成する例を示します。

```
feature sla sender
ip sla 9
  tcp-connect 172.29.139.132 5000
  frequency 10
!
ip sla schedule 9 life forever start-time now
```

### 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。

## 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 接続動作の構成とスケジューリング

ここでは、オプション パラメータを使用して、送信元デバイスでの TCP 接続動作を設定し、スケジュールする方法について説明します。





(注) IP SLA Responder が宛先 IP アドレスとポートで永続的に有効になっている場合は、**control disable** キーワードを **tcp-connect** コマンドで使用して、制御メッセージを無効にします。



- 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。イネーブルになると、各動作の応答が破損していない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に使用します。

## 手順の概要

1. **enable**
2. **configure terminal**
3. **feature sla sender**
4. **ip sla operation-number**
5. **tcp-connect** *{destination-ip-address | destination-hostname} destination-port [source-ip {ip-address | hostname} source-port port-number] [control {enable | disable}]*
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. **history statistics-distribution-interval** *milliseconds*
15. **tag** *text*
16. **threshold** *milliseconds*
17. **timeout** *milliseconds*
18. **tos** *number*
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

	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>feature sla sender</b> 例： switch(config)# feature sla sender	IP SLA 動作機能を有効にします。
ステップ 4	<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 5	<b>tcp-connect</b> {destination-ip-address   destination-hostname} destination-port [source-ip {ip-address   hostname} source-port port-number] [control {enable   disable}] 例： switch(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、 <b>control disable</b> キーワードの組み合わせを使用します。
ステップ 6	<b>history buckets-kept size</b> 例： switch(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 7	<b>history distributions-of-statistics-kept size</b> 例： switch(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 8	<b>history enhanced</b> [interval seconds] [buckets number-of-buckets] 例：	(任意) IPSLA 動作に対する拡張履歴収集をイネーブルにします。

	コマンドまたはアクション	目的
	<code>switch(config-ip-sla-tcp)# history enhanced interval 900 buckets 100</code>	
ステップ 9	<b>history filter</b> {none   all   overThreshold   failures} 例： <code>switch(config-ip-sla-tcp)# history filter failures</code>	(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	<b>frequency</b> <i>seconds</i> 例： <code>switch(config-ip-sla-tcp)# frequency 60</code>	(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	<b>history hours-of-statistics-kept</b> <i>hours</i> 例： <code>switch(config-ip-sla-tcp)# history hours-of-statistics-kept 4</code>	(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	<b>history lives-kept</b> <i>lives</i> 例： <code>switch(config-ip-sla-tcp)# history lives-kept 5</code>	(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	<b>owner</b> <i>owner-id</i> 例： <code>switch(config-ip-sla-tcp)# owner admin</code>	(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	<b>history statistics-distribution-interval</b> <i>milliseconds</i> 例： <code>switch(config-ip-sla-tcp)# history statistics-distribution-interval 10</code>	(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 15	<b>tag</b> <i>text</i> 例： <code>switch(config-ip-sla-tcp)# tag TelnetPollServer1</code>	(任意) IP SLA 動作のユーザー指定 ID を作成します。
ステップ 16	<b>threshold</b> <i>milliseconds</i> 例： <code>switch(config-ip-sla-tcp)# threshold 10000</code>	(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。

	コマンドまたはアクション	目的
ステップ 17	<b>timeout</b> <i>milliseconds</i> 例：  switch(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 18	<b>tos</b> <i>number</i> 例：  switch(config-ip-sla-jitter)# tos 160 例：	(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 19	<b>exit</b> 例：  switch(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	<b>ip sla schedule</b> <i>operation-number</i> [ <b>life</b> { <b>forever</b>   <i>seconds</i> }] [ <b>start-time</b> { <i>hh:mm:ss</i> } [ <i>monthday</i>   <i>daymonth</i> ]   <b>pending</b>   <b>now</b>   <b>after</b> <i>hh:mm:ss</i> ] [ <b>ageout</b> <i>seconds</i> ] [ <b>recurring</b> ] 例：  switch(config)# ip sla schedule 10 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	<b>exit</b> 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 22	<b>show ip sla configuration</b> [ <i>operation-number</i> ] 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。

### 例

次に、TCP 接続動作番号 10 の IP SLA パラメータをすべて (デフォルトを含む) 設定する例を示します。

```
switch# show ip sla configuration 10
IP SLAs Infrastructure Engine-III
Entry number: 10
Owner: admin
Tag: TelnetPollServer1
Operation timeout (milliseconds): 10000
Type of operation to perform: tcp-connect
```

```

Target address/Source address: 101.101.101.1/0.0.0.0
Target port/Source port: 5000/0
Type Of Service parameter: 0xa0
Vrf Name: default
Control Packets: enabled
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): Forever
  Entry Ageout (seconds): never
  Recurring (Starting Everyday): FALSE
  Status of entry (SNMP RowStatus): Active
Threshold (milliseconds): 10000
Distribution Statistics:
  Number of statistic hours kept: 4
  Number of statistic distribution buckets kept: 5
  Statistic distribution interval (milliseconds): 10
Enhanced History:
  Aggregation Interval:900 Buckets: 100
History Statistics:
  Number of history Lives kept: 0
  Number of history Buckets kept: 25
  History Filter Type: Failures

```

### 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。

## TCP 接続動作の構成例

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、スイッチ 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 (スイッチ B) で制御プロトコルが無効になっています。IP SLA は制御プロトコルを使用して、ターゲット ポートを一時的に有効にするように IP SLA レスポンダに通知します。このアクションにより、レスポндаは TCP 接続動作に応答できません。この例では、ターゲットがスイッチではなく、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。

### スイッチ A の設定

```

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

```

## スイッチ B の設定

```
configure terminal
feature sla sender
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 21）を使用し、IP SLA レスポンダを使用せずに TCP 接続動作を構成する例を示します。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。

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

## 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。