Cisco IP SLA 動作に対する予防的しきい値モニタリングの設定

このマニュアルでは、しきい値と反応トリガーを使用した Cisco IOS IP Service Level Agreement（SLA; サービス レベル契約）の予防的モニタリング機能について説明します。

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。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「IP SLA 予防的しきい値モニタリングに関する機能情報」（P.10）を参照してください。

プラットフォームおよびソフトウェア イメージのサポート情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

目次

予防的しきい値モニタリングに関する情報

（注） IP SLA 動作の一般的な情報については、『*Cisco IOS IP SLAs Overview*』を参照してください。

IP SLA の反応の設定

IP SLA の反応は、モニタリング対象の値が指定のレベルを超えるか、下回った場合、または、タイムアウトや接続損失などのモニタリング対象のイベントが発生した場合にトリガーされるように設定します。IP SLA によって測定された反応の設定が高すぎたり、低すぎたりすると、IP SLA では、ネットワーク管理アプリケーションへの通知を生成したり、より多くのデータを収集する別の IP SLA 動作をトリガーしたりすることがあります。

IP SLA しきい値モニタリングおよび通知

IP SLA は、ほとんどの IP SLA 動作に関する平均ジッタ、単方向の遅延、双方向の Round-Trip Time（RTT; ラウンドトリップ時間）、および接続などのパフォーマンス パラメータについての予防的しきい値モニタリングおよび通知をサポートします。予防的モニタリング機能には、単方向ジッタ、単方向パケット損失、および単方向 VoIP 音声品質スコアを含む重要な VoIP 関連パラメータに対する反応しきい値を設定するためのオプションも用意されています。

IP SLA の通知は、トリガー応答として設定します。パケット損失、ジッタ、および Mean Operation Score（MOS; 平均動作スコア）統計情報は、IP SLA ジッタ動作に固有です。通知は、いずれかの方向（送信元から宛先、または宛先から送信元）の違反に対して、またはパケット損失とジッタの範囲外の RTT 値に対して生成できます。RTT 値が指定したしきい値を上回るか下回ると、トラップなどのイベントがトリガーされます。

応答条件が発生した場合、IP SLA ではシステム ロギング（syslog）メッセージを生成できます。システム ロギング メッセージは、CISCO-RTTMON-MIB を使用して Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）トラップ（通知）として送信できます。IP SLA の SNMP トラップは、CISCO-RTTMON-MIB および CISCO-SYSLOG-MIB でサポートされます。

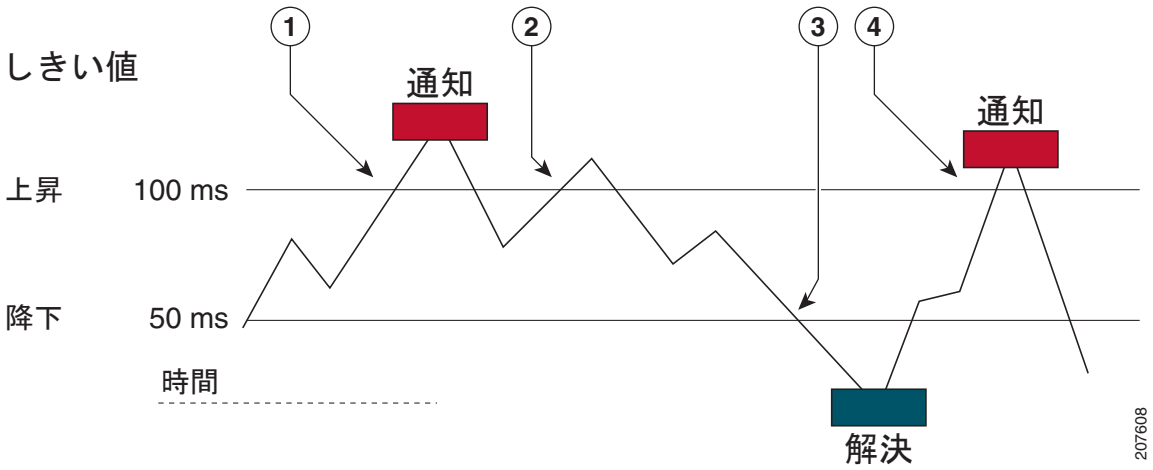
（注） CISCO-SYSLOG-MIB の重大度レベルは、SyslogSeverity INTEGER {emergency(1), alert(2), critical(3), error(4), warning(5), notice(6), info(7), debug(8)} のように定義されます。

Cisco IOS ソフトウェアのシステム ロギング プロセスに対しては、異なる重大度レベル値が定義されます。Cisco IOS ソフトウェアのシステム ロギング プロセスに対する重大度レベルは、{emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), informational (6), debugging (7)} のように定義されます。

Cisco IOS システム ロギング プロセス内の IP SLA のしきい値違反は、レベル 6（infomational）として記録されますが、CISCO-SYSLOG-MIB からはレベル 7（info）トラップとして送信されます。

通知は、しきい値違反が発生するたびに発行されるわけではありません。図 1 に、モニタリング対象の要素が上限しきい値を超えた場合に生じるトリガー応答の順序を示します。最初に上昇しきい値を超えたときに、イベントが送信され、通知が発行されます。後続のしきい値超過通知は、モニタリング対象の値が上昇しきい値を再び超える前に下限しきい値を下回った場合に限り発行されます。

図 1　　IP SLA のしきい値超過に関するトリガー応答条件と通知



1	最初に上昇しきい値を超えたときに、イベントが送信され、しきい値超過通知が発行されます。
2	上昇しきい値の超過違反が連続して発生しても、追加の通知は発行されません。
3	モニタリング対象の値が下限しきい値を下回っています。
4	上昇しきい値を超えたときに別のしきい値超過通知が発行されているのは、モニタリング対象の値が最初に下限しきい値を下回った後だけです。

（注） また、モニタリング対象の要素が下限しきい値を最初に下回った時点で（3）、下限しきい値超過通知が発行されます。前述のように、下限しきい値超過違反に対する後続の通知が発行されるのは、上昇しきい値を超えた後で、モニタリング対象の値が下限しきい値を再び下回った場合に限られます。

ジッタ動作に対する RTT 反応

ジッタ動作に対する RTT 反応は、動作の最後にのみトリガーされます。これには、平均リターントリップ時間（RTTAvg）値とマッチングされる、リターントリップ時間の最新値（LatestRTT）が使用されます。

ジッタ動作に対する RTT の SNMP トラップは、動作全体の平均リターントリップ時間（RTTAvg）値に基づいており、動作中に送信される個々のパケットの RTT 値は含まれません。たとえば、平均がしきい値を下回っている場合、実際には最大で半数のパケットがしきい値を上回っている可能性がありますが、あくまでも動作全体に対する値であるため、このような詳細は通知には含まれません。

RTTAvg しきい値違反に対しては、syslog メッセージだけがサポートされています。syslog メッセージは、CISCO-RTTMON-MIB から送信されます。

予防的しきい値モニタリングの設定方法

- 「予防的しきい値モニタリングの設定」（P.4）

予防的しきい値モニタリングの設定

この作業は、トラップを生成したり、別の動作を開始したりするためのしきい値および反応トリガーを設定する場合に実行します。

前提条件

- 違反条件を満たした場合に開始される IP SLA 動作を設定する必要があります。

制約事項

- ジッタ動作に対する RTT 反応は、動作の最後にのみトリガーされます。これには、リターントリップ時間の最新値（LatestRTT）が使用されます。
- ジッタ動作に対する RTT の SNMP トラップは、動作全体に対するリターントリップ時間の平均値（RTTAvg）のみに基づいており、動作中に送信された個々のパケットのリターントリップ時間値は含まれません。RTTAvg しきい値違反に対しては、syslog メッセージだけがサポートされています。
- ジッタ動作中の RTT 違反には、syslog メッセージだけがサポートされます。
- ジッタ以外の動作中の RTT 違反には、SNMP トラップだけがサポートされます。
- timeout、connectionLoss、または verifyError を除く RTT 以外の違反については syslog メッセージだけがサポートされます。
- SNMP トラップと syslog メッセージの両方がサポートされているのは、timeout、connectionLoss、または verifyError 違反のみです。

手順の概要

1. **enable**
2. **configure terminal**

3. **ip sla reaction-configuration** *operation-number* **react** *monitored-element* [**action-type** *option*] [**threshold-type** {**average** [*number-of-measurements*] | **consecutive** [*occurrences*] | **immediate** | **never** | **xofy** [*x-value y-value*]}] [**threshold-value** *upper-threshold lower-threshold*]
4. **ip sla reaction-trigger** *operation-number target-operation*
5. **ip sla logging traps**
6. **snmp-server enable traps rtr**
   または
   snmp-server enable traps syslog
7. **snmp-server host** {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]
8. **exit**
9. **show ip sla reaction configuration** [*operation-number*]
10. **show ip sla reaction trigger** [*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	**enable** 例： `Router> enable`	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	**configure terminal** 例： `Router# 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 reaction-configuration** *operation-number* **react** *monitored-element* [**action-type** *option*] [**threshold-type** {**average** [*number-of-measurements*] | **consecutive** [*occurrences*] | **immediate** | **never** | **xofy** [*x-value y-value*]}] [**threshold-value** *upper-threshold lower-threshold*] 例： `Router(config)# ip sla reaction-configuration 10 react jitterAvg threshold-type immediate threshold-value 5000 3000 action-type trapAndTrigger`	指定のしきい値の違反に基づいて行われる処理（SNMP トラップまたは IP SLA トリガー）を設定します。
ステップ 4	**ip sla reaction-trigger** *operation-number target-operation* 例： `Router(config)# ip sla reaction-trigger 10 2`	（任意）違反条件が満たされた場合に、別の IP SLA 動作を開始します。 • **ip sla reaction-configuration** コマンドを **trapAndTrigger** キーワードまたは **triggerOnly** キーワードを指定して設定した場合にのみ必須です。
ステップ 5	**ip sla logging traps** 例： `Router(config)# ip sla logging traps`	（任意）CISCO-RTTMON-MIB からの IP SLA syslog メッセージ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 6	**snmp-server enable traps rtr**
	または
	snmp-server enable traps syslog
	
	例：
	`Router(config)# snmp-server enable traps rtr`
	または
	`Router(config)# snmp-server enable traps syslog`
		（任意）システムによる CISCO-RTTMON-MIB トラップの生成をイネーブルにします。
		または
		システムによる CISCO-SYSLOG-MIB トラップの生成をイネーブルにします。

ステップ 7	**snmp-server host** {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*] **例：** `Router(config)# snmp-server host 10.1.1.1 public syslog`	（任意）リモート ホストにトラップを送信します。 • **snmp-server enable traps** コマンドを設定した場合に必須です。
ステップ 8	**exit** **例：** `Router(config)# exit`	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 9	**show ip sla reaction configuration** [*operation-number*] **例：** `Router# show ip sla reaction configuration 10`	（任意）予防的しきい値モニタリングの設定を表示します。
ステップ 10	**show ip sla reaction trigger** [*operation-number*] **例：** `Router# show ip sla reaction trigger 2`	（任意）トリガーされるターゲット動作の設定ステータスと動作状態を表示します。

予防的しきい値モニタリングの設定例

例：IP SLA 反応の設定

次の例では、MOS 値が 4.9（最高品質）を超えたとき、または 2.5（低品質）を下回ったときに SNMP ロギング トラップを送信するよう、IP SLA 動作 10 を設定しています。

```
Router(config)# ip sla reaction-configuration 10 react mos threshold-type immediate
threshold-value 490 250 action-type trapOnly
```

次に、**ip sla reaction-configuration** コマンドのデフォルト設定の例を示します。

```
Router# show ip sla reaction-configuration 1

Entry number: 1
Reaction Configuration not configured

Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip sla reaction-configuration 1
Router(config)# do show ip sla reaction-configuration 1

Entry number: 1
Reaction: rtt
Threshold Type: Never
Rising (milliseconds): 5000
Falling (milliseconds): 3000
Threshold Count: 5
Threshold Count2: 5
Action Type: None
```

例：IP SLA 反応の設定の確認

次の例では、出力内の Reaction: 値に示されているとおり、複数のモニタリング対象要素が IP SLA 動作（1）に対して設定されています。

```
Router# show ip sla reaction-configuration

Entry Number: 1
Reaction: RTT
Threshold type: Never
Rising (milliseconds): 5000
Falling (milliseconds): 3000
Threshold Count: 5
Threshold Count2: 5
Action Type: None

Reaction: jitterDSAvg
Threshold type: average
Rising (milliseconds): 5
Falling (milliseconds): 3
Threshold Count: 5
Threshold Count2: 5
Action Type: triggerOnly

Reaction: jitterDSAvg
Threshold type:  immediate
Rising (milliseconds): 5
Falling (milliseconds): 3
Threshold Count: 5
Threshold Count2: 5
Action Type: trapOnly

Reaction: PacketLossSD
Threshold type:  immediate
Rising (milliseconds): 5
Threshold Falling (milliseconds): 3
Threshold Count: 5
Threshold Count2: 5
Action Type: trapOnly
```

例：SNMP 通知のトリガー

次に、RTT または VoIP MOS のしきい値に違反した場合に、10.1.1.1 のリモート ホストに CISCO-SYSLOG-MIB トラップが送信されるように、予防的しきい値モニタリングを設定する例を示します。

```
! Configure the operation on source.
Router(config)# ip sla 1
Router(config-ip-sla)# udp-jitter 10.1.1.1 3000 codec g711alaw
Router(config-ip-sla-jitter)# exit
Router(config)# ip sla schedule 1 start now life forever
! Configure thresholds and reactions.
Router(config)# ip sla reaction-configuration 1 react rtt threshold-type immediate
threshold-value 3000 2000 action-type trapOnly
Router(config)# ip sla reaction-configuration 1 react MOS threshold-type consecutive 4
threshold-value 390 220 action-type trapOnly
Router(config)# ip sla logging traps
! The following command sends traps to the specified remote host.
Router(config)# snmp-server host 10.1.1.1 version 2c public syslog
! The following command is needed for the system to generate CISCO-SYSLOG-MIB traps.
Router(config)# snmp-server enable traps syslog
```

次に示すシステム ロギング メッセージの例は、IP SLA しきい値違反通知が Cisco IOS システム ロギング プロセスでレベル 6（informational）として生成されることを示しています。

```
3d18h:%RTT-6-SAATHRESHOLD:RTR(11):Threshold exceeded for MOS
```

次の例は、同じ違反に対する CISCO-SYSLOG-MIB からの SNMP 通知であり、レベル 7（info）の通知となっています。

```
3d18h:SNMP:V2 Trap, reqid 2, errstat 0, erridx 0
 sysUpTime.0 = 32613038
 snmpTrapOID.0 = ciscoSyslogMIB.2.0.1
 clogHistoryEntry.2.71 = RTT
 clogHistoryEntry.3.71 = 7
 clogHistoryEntry.4.71 = SAATHRESHOLD
 clogHistoryEntry.5.71 = RTR(11):Threshold exceeded for MOS
 clogHistoryEntry.6.71 = 32613037
```

その他の参考資料

関連資料

内容	参照先
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*』

規格

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。また、このマニュアルに記載された機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB リンク
• CISCO-RTTMON-MIB • CISCO-SYSLOG-MIB	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、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
このマニュアルに記載された機能によってサポートされている特定の RFC はありません。	—

シスコのテクニカル サポート

説明	リンク
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。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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

IP SLA 予防的しきい値モニタリングに関する機能情報

表 1 に、この章に記載されている機能および具体的な設定情報へのリンクを示します。

プラットフォームおよびソフトウェア イメージのサポート情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連のソフトウェア リリースの以降のリリースでもサポートされます。

表 1　IP SLA 予防的しきい値モニタリングに関する機能情報

機能名	リリース	機能情報
IP SLA 反応しきい値	12.2(31)SB2 12.2(33)SRB1 12.2(33) SXH 12.3(14)T 15.0(1)S Cisco IOS XE 3.1.0SG	Cisco IOS IP SLA 予防的しきい値モニタリング機能を使用すると、特定の測定対象ネットワーク条件に反応するように IP SLA の動作を設定できます。
IP SLA VoIP しきい値トラップ	12.2(31)SB2 12.2(33)SRB1 12.2(33) SXH 12.3(14)T 15.0(1)S	Cisco IOS IP SLA VoIP 予防的しきい値モニタリング機能を使用すると、特定の測定対象ネットワーク条件に反応するように IP SLA の動作を設定できます。