IP SLA 動作の予防的しきい値モニタリングの設定

この章では、しきい値およびリアクション トリガーを使用した IP サービス レベル契約（SLA）の予防的モニタリング機能について説明します。

この章は、次の項で構成されています。

- IP SLA リアクション構成に関する情報 （1 ページ）
- IP SLA しきい値モニタリングおよび通知 （1 ページ）
- 予防的しきい値モニタリングの設定 （3 ページ）
- IP SLA 反応構成の設定例 （6 ページ）
- IP SLA リアクション構成の確認例 （6 ページ）
- SNMP 通知をトリガーするための構成例 （7 ページ）

IP SLA リアクション構成に関する情報

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 が測定するリアクション構成が高すぎたり、低すぎたりすると、IP SLA が、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、双方向のラウンドトリップ時間（RTT）、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は、単方向ジッター、単方向のパケット損失、および単方向 VoIP 音声品質スコアリングを含む重要な VoIP 関連パラメータの反応しきい値を設定するためのオプションを提供します。

IP SLA の通知は、トリガーされた応答として設定されます。パケット損失、ジッター、平均動作スコア（MOS）統計情報は、IP SLA ジッター動作に固有です。通知はいずれかの方向（送信元から宛先、および宛先から送信元）の違反、またはパケット損失およびジッターの範囲外 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 を使用して簡易ネットワーク管理プロトコル（SNMP）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。

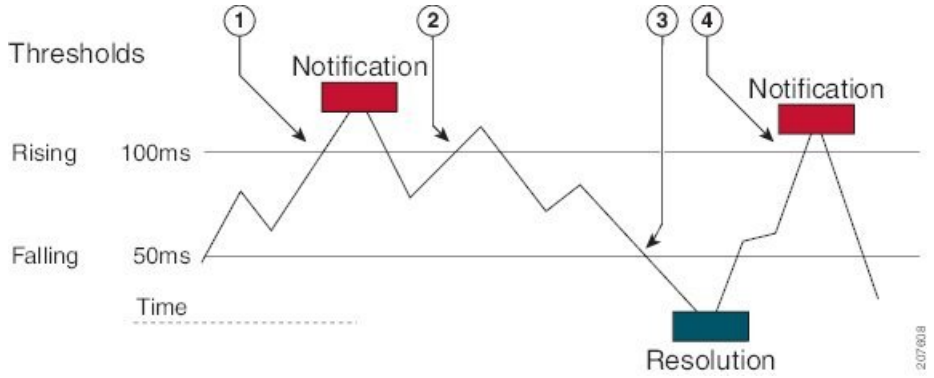
CISCO-SYSLOG-MIB のシビラティ（重大度）レベルは、SyslogSeverity INTEGER {emergency(1), alert(2), critical(3), error(4), warning(5), notice(6), info(7), debug(8)} です。

Cisco NX-OS ソフトウェアのシステム ロギング プロセスに対しては、異なるシビラティ（重大度）レベル値が定義されます。Cisco NX-OS ソフトウェアのシステム ロギング プロセスに対するシビラティ（重大度）レベルは、{emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), informational (6), debugging (7)} です。

IP SLA しきい値違反は、Cisco システム ロギング プロセス内ではレベル 6（informational）としてロギングされますが、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。次の図に、モニタリング対象要素が上限しきい値を超えたときに発生するトリガー リアクションの流れを示します。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* のトリガーされた反応条件およびしきい値超過通知



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。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。

ジッター動作に対する RTT 反応

ジッター動作に対する 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。

ジッター動作に対する 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

ここでは、トラップを生成したり、別の動作を開始するようにしきい値および反応トリガーを設定する方法について説明します。

始める前に

- 違反条件が満たされた場合に開始される IP SLA 動作を設定します。

（注）

- ジッター動作に対する 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。
- ジッター動作に対する 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。
- ジッター動作中の RTT 違反には、syslog メッセージだけがサポートされます。
- ジッター動作中以外の 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 以外の非 RTT 違反には、syslog メッセージのみ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-valuey-value*]}] [**threshold-value** *upper-thresholdlower-threshold*]
4. **ip sla reaction-trigger** *operation-number target-operation*
5. **ip sla logging traps**
6. **snmp-server enable traps ip sla**
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

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。

	コマンドまたはアクション	目的
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	**ip sla reaction-configuration** *operation-number* **react** *monitored-element* [**action-type** *option*] [**threshold-type** {**average** [*number-of-measurements*] | **consecutive** [*occurrences*] | **immediate** | **never** | **xofy** [*x-valuey-value*]}] [**threshold-value** *upper-thresholdlower-threshold*] 例： `switch(config)# ip sla reaction-configuration 10 react jitterAvg threshold-type immediate threshold-value 5000 3000 action-type trapAndTrigger`	指定したしきい値違反に基づいて実行されるアクション（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： `switch(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** の場合にのみ必要です。コマンドが、**trapAndTrigger** または **triggerOnly** キーワードのいずれかを含めて構成された場合にのみ必要です。
ステップ 5	**ip sla logging traps** 例： `switch(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。
ステップ 6	**snmp-server enable traps ip sla** 例： `switch(config)# snmp-server enable traps ip sla`	（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。
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： `switch(config)# snmp-server host 10.1.1.1 public`	（任意）リモートホストにトラップを送信します。 **snmp-server enable traps**の場合は必須です。 コマンドが構成されている場合にのみ必要です。
ステップ 8	**exit** 例： `switch(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： `switch# 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。

	コマンドまたはアクション	目的
ステップ 10	**show ip sla reaction trigger** [*operation-number*] 例： `switch# 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および動作状態を表示します。

IP SLA 反応構成の設定例

MOS 値が 4.9（最高品質）を超えた時点、または 2.5（低品質）を下回った時点で SNMP ロギング トラップを送信するように、IP SLA 動作 10 を設定する例を示します。

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

以下に、デフォルト設定を表示する例を示します。

```
switch# show ip sla reaction-configuration 1
Entry number: 1
Index: 1
Reaction: mos
Threshold Type: Immediate
Rising: 490
Falling: 250
Action Type: Trap only
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ip sla reaction-configuration 10 react mos threshold-type immediate
threshold-value 490 250 action-type trapOnly
switch(config)# 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
```

IP SLA リアクション構成の確認例

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) に対して構成されています。

```
switch# 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
```

SNMP 通知をトリガーするための構成例

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構成する例を示します。

```
! Configure the operation on source.
switch(config)# ip sla 1

switch(config-ip-sla)# udp-jitter 10.1.1.1 3000 codec g711alaw
switch(config-ip-sla-jitter)# exit

switch(config)# ip sla schedule 1 start now life forever

! Configure thresholds and reactions.
switch(config)# ip sla reaction-configuration 1 react rtt threshold-type immediate
threshold-value 3000 2000 action-type trapOnly

switch(config)# ip sla reaction-configuration 1 react MOS threshold-type consecutive 4
threshold-value 390 220 action-type trapOnly

switch(config)# ip sla logging traps

! The following command sends traps to the specified remote host.
switch(config)# snmp-server host 10.1.1.1 version 2c public

! The following command is needed for the system to generate CISCO-SYSLOG-MIB traps.
switch(config)# snmp-server enable traps
```

以下の例では、IP SLA しきい値違反通知が Cisco NX-OS 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が示されています。

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

以下の例では、同じ違反に対する CISCO-SYSLOG-MIB による SNMP 通知がレベル 7 （info）通知であることが示されています。

```
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
```

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。