

通過命令列介面(CLI)配置交換機上的遠端網路監控(RMON)事件控制設定

目標

遠端網路監控(RMON)是由Internet工程任務組(IETF)開發的，用於支援區域網(LAN)的監控和協定分析。它是一種標準監控規範，允許不同的網路監控器和控制檯系統相互交換網路監控資料。它使裝置中的簡單網路管理協定(SNMP)代理能夠主動監控指定時段內的流量統計資訊，並將陷阱傳送到SNMP管理器。本地SNMP代理將實際的即時計數器與預定義的閾值進行比較，並生成警報，而無需由中央SNMP管理平台進行輪詢。如果相對於網路基線設定了正確的閾值，則這是一種有效的主動管理機制。

附註：要瞭解如何通過交換機的基於Web的實用程式配置SNMP陷阱設定，請按一下[此處](#)。有關基於命令列介面(CLI)的說明，請按一下[此處](#)。

RMON允許您從網路監控探測器和控制檯中選擇滿足特定網路需求的功能。RMON專門定義了任何網路監控系統應該能夠提供的資訊。統計資訊、事件、歷史記錄、警報、主機、前N個主機、矩陣、過濾器、捕獲和令牌環是RMON中的十個組。

本文提供如何通過CLI在交換機上配置RMON事件設定的說明。

附註：要瞭解如何通過交換機的基於Web的實用程式配置RMON事件控制設定，請按一下[此處](#)。

適用裝置

- Sx300系列
- Sx350系列
- SG350X系列
- Sx500系列
- Sx550X系列

軟體版本

- 1.4.7.05 — Sx300、Sx500
- 2.2.8.4 — Sx350、SG350X、Sx550X

通過CLI配置交換機上的RMON事件

配置RMON事件

由於SNMP管理器不必頻繁輪詢裝置以獲取資訊，因此RMON減少了管理器和裝置之間的流量，並且由於裝置在發生事件時報告事件，RMON使管理器能夠獲得及時的狀態報告。

按照以下步驟配置交換機上的RMON事件設定。

步驟1. 登入到交換機控制檯。預設使用者名稱和密碼為cisco/cisco。如果您已配置新的使用者名稱或密碼，請改為輸入憑據。

```
User Name:cisco
Password:*****
```

附註：在本範例中，交換器是透過Telnet存取的。

步驟2.在交換機的特權EXEC模式下，輸入以下命令進入全域性配置上下文：

```
SG350X#configure
```

步驟3.輸入rmon event命令以通過輸入以下內容配置新事件：

```
SG350X#rmon event [index] [none | log | trap | log-trap]
[community text] [description text] [owner name]
```

- index — 指定事件索引。範圍是從1到65535。
- none — 指定裝置不為此事件生成任何通知。
- log — 指定裝置在日誌表中為此事件生成通知條目。
- trap — 指定此事件的裝置向一個或多個管理站傳送SNMP陷阱。
- log-trap — 指定在日誌表中生成一個條目，並且此事件的裝置會向一個或多個管理站傳送SNMP陷阱。
- community text — （可選）指定傳送SNMP陷阱時使用的SNMP社群或密碼。它應為八位元組字串，長度範圍為0到127個字元。
- 注意:這必須是配置SNMP主機時使用的團體。若要詳細瞭解如何透過交換器的CLI設定SNMP社群，請按一下[此處](#)。
- description text — （可選）指定描述此事件的註釋。長度範圍為0到127個字元。
- 所有者名稱 — （可選）指定配置此事件的人員的姓名。如果未指定，則所有者名稱預設為空字串。

```
SG350X#configure
SG350X(config)#rmon event 1 log-trap community Community1 owner cisco
SG350X(config)#
```

附註：在本例中，事件索引為1，通知型別為log-trap，社群名稱為Community1，所有者為cisco。

步驟4.（可選）要刪除事件，請輸入以下內容：

```
SG350X#no rmon event [index]
```

步驟5.輸入exit命令返回交換機的特權執行模式。

```
SG350X#exit
```

```
[SG350X#configure
[SG350X(config)#rmon event 1 log-trap community Community1 owner cisco
[SG350X(config)#exit
SG350X#
```

步驟6. (可選) 在交換機的特權EXEC模式下，輸入以下命令，將配置的設定儲存到啟動配置檔案中：

```
SG350X#copy running-config startup-config
```

```
[SG350X]copy running-config startup-config
Overwrite file [startup-config]... (Y/N)[N] ?
```

步驟7. (可選) 出現Overwrite file [startup-config]...提示後，在鍵盤上按Y選擇「Yes」，或按N選擇「No」。

```
[SG350X#copy running-config startup-config
Overwrite file [startup-config]... (Y/N)[N] ?Y
04-May-2017 07:21:46 %COPY-I-FILECPY: Files Copy - source URL running-config des
tination URL flash://system/configuration/startup-config
04-May-2017 07:21:48 %COPY-N-TRAP: The copy operation was completed successfully
SG350X#
```

現在，您應該已經通過CLI成功配置交換機上的RMON事件設定。

檢視RMON事件

「事件」頁顯示已發生的事件或操作的日誌。可以記錄兩種型別的事件：Log或Log and Trap。當事件繫結到警報且警報條件已發生時，將執行事件中的操作。有關如何在交換機的基於Web的實用程式上配置RMON警報的說明，請按一下[此處](#)。對於基於CLI的，請按一下[此處](#)。

步驟1. 在交換機的特權EXEC模式下，輸入以下命令以顯示交換機上配置的rmon事件設定：

```
SG350X#show rmon events
```

- 索引 — 標識此事件的唯一索引。
- 描述 — 描述此事件的註釋。
- 型別 — 裝置生成的有關此事件的通知的型別。它可以具有以下值：無，記錄，陷阱，記錄。對於日誌，在日誌表中為每個事件建立一個條目。在陷阱的情況下，SNMP陷阱被傳送到一個或多個管理站。
- Community — 如果要傳送SNMP陷阱，則其傳送時將使用此八位組字串指定的SNMP社群字串。
- 所有者 — 配置此事件的實體。
- 上次傳送時間 — 此條目上次生成事件的時間。如果此條目未生成任何事件，則此值為0。

```
SG350X# show rmon events
```

Index	Description	Type	Community	Owner	Last time sent
1	Default Description	log-trap	Community1	cisco	04-May-2017 06:55:17
10	Default Description	log-trap	Default Community	manager	
20	Default Description	log	Default Community	cisco	

步驟2.要顯示交換機上的RMON事件日誌，請輸入以下內容：

```
SG350X#show rmon log [event]
```

- event — (可選) 指定事件索引。範圍是從1到65535。
- 此表顯示以下欄位：
- 事件 — 事件的日誌條目編號。
- Description — 觸發警報的事件的描述。
- 時間 — 輸入日誌條目的時間。

附註：在此示例中，使用了RMON事件1。

```
[SG350X# show rmon log 1
```

```
Maximum table size: 300
```

Event	Description	Time
1	MIB Var.: 1.3.6.1.2.1.2.2.1.10.3 , Delta , Falling , Actual Val: 0 , Thresh.Set: 20 , Interval(sec): 30	04-May-2017 07:19:39
1	MIB Var.: 1.3.6.1.2.1.2.2.1.10.3 , Delta , Rising , Actual Val: 282 , Thresh.Set: 10 , Interval(sec): 30	04-May-2017 07:20:24

現在，您應該已經通過CLI檢視交換機上配置的RMON事件設定。