排除ASA介面溢位計數器錯誤故障

目錄

簡介

本檔案介紹「overrun」錯誤計數器以及如何調查網路上的效能問題或封包遺失問題。管理員可能會注意到自適應安全裝置(ASA)上的**show interface**命令輸出中報告的錯誤。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

問題

ASA介面錯誤計數器「overrun」跟蹤網路介面上接收到資料包的次數，但介面FIFO隊列中沒有儲存資料包的可用空間。因此，封包遭捨棄。可以使用**show interface**指令看到此計數器的值。

顯示問題的輸出示例：

```
ASA# show interface GigabitEthernet0/1
```

```
Interface GigabitEthernet0/1 "inside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec
Full-Duplex(Full-duplex), 1000 Mbps(1000 Mbps)
Input flow control is unsupported, output flow control is off
MAC address 0026.0b31.0c59, MTU 1500
IP address 10.0.0.113, subnet mask 255.255.0.0
580757 packets input, 86470156 bytes, 0 no buffer
Received 3713 broadcasts, 0 runts, 0 giants
2881 input errors, 0 CRC, 0 frame, 2881 overrun, 0 ignored, 0 abort
0 pause input, 0 resume input
0 L2 decode drops
905828 packets output, 1131702216 bytes, 0 underruns
0 pause output, 0 resume output
0 output errors, 0 collisions, 0 interface resets
0 late collisions, 0 deferred
0 input reset drops, 0 output reset drops, 0 tx hangs
input queue (blocks free curr/low): hardware (255/230)
output queue (blocks free curr/low): hardware (255/202)
```

在上方範例中，自ASA開機或輸入命令**clear interface**以手動清除計數器後，在介面上觀察到2881溢位。

介面溢位的原因

介面溢位錯誤通常是由以下因素組合導致的：

- 軟體級別 — ASA軟體從介面FIFO隊列中提取資料包的速度不夠快。這會導致FIFO隊列被填滿，新資料包被丟棄。
- 硬體級別 — 資料包進入介面的速率太快，這會導致FIFO隊列在ASA軟體將資料包拉出之前被填滿。通常，資料包的突發會導致FIFO隊列在短時間內填充最大容量。

排除介面超限原因的步驟

排除和解決此問題的步驟如下：

1. 確定ASA是否出現CPU佔用以及它們是否導致問題。緩解任何長時間或頻繁的CPU佔用問題。
2. 瞭解介面流量速率並確定是否由於流量配置檔案而超額訂用ASA。
3. 確定間歇性流量突發是否導致問題。如果是，請在ASA介面和相鄰交換機埠上實施流量控制。

潛在原因和解決方案

ASA上的CPU定期忙於處理傳入資料包（CPU佔用資源）

ASA平台處理軟體中的所有資料包，並使用處理所有系統功能（如系統日誌、自適應安全裝置管理器連線和應用程式檢查）的主CPU核心來處理傳入資料包。如果軟體進程佔用CPU的時間超過其應有時間，則ASA將此記錄為CPU佔用事件，因為進程「佔用」了CPU。CPU hog閾值以毫秒為單位進行設定，並且對於每種硬體裝置型號不同。閾值基於給定硬體平台的CPU功率和裝置可以處理的潛在流量率，填充介面FIFO隊列需要多長時間。

CPU佔用有時會導致單核ASA（例如5505、5510、5520、5540和5550）上的介面溢位錯誤。持續時間為100毫秒或更長時間的長時間生豬尤其會導致相對較低流量級別和非突發流量速率發生超支。此問題對多核系統的影響不大，因為如果其中一個CPU核心被進程佔用，其它核心可以從Rx環中取出資料包。

持續時間超過裝置閾值的hog會導致生成id為711004的系統日誌，如下所示：

```
201320614:40:42:%ASA-4-711004:60= sshPC = 90b0155= Feb 06 2013 14:40:42:%ASA-4-711004:60= sshPC
= 90b0155= 0x090b0155 0x090bf3b6 0x090b3b84 0x090b3f6e 0x090b4459 0x090b44d6 0x08c46fcc
0x09860ca0 x080fad6d0 80efa5a 0x080f0a1c 0x0806922c
```

系統也會記錄CPU佔用事件。**show proc cpu-hog**命令的輸出顯示以下欄位：

- Process — 佔用CPU的進程的名稱。
- PROC_PC_TOTAL — 此進程佔用CPU的總次數。
- MAXHOG — 該進程觀察的最長CPU佔用時間（毫秒）。
- LASTHOG — 上次暫掛保持CPU的時間量（毫秒）。
- LASTHOG At — 上次發生CPU佔用時間。
- PC — 發生CPU佔用時進程的程式計數器值。(思科技術協助中心(TAC)的相關資訊)
- Call stack — 發生CPU佔用時進程的呼叫堆疊。（Cisco TAC的資訊）

此示例顯示**show proc cpu-hog**命令輸出：

```
ASA#

show proc cpu-hog



Process:    ssh, PROC_PC_TOTAL: 1, MAXHOG: 119, LASTHOG: 119
LASTHOG At: 12:25:33 EST Jun 6 2012
PC:         0x08e7b225 (suspend)

Process:    ssh, NUMHOG: 1, MAXHOG: 119, LASTHOG: 119
LASTHOG At: 12:25:33 EST Jun 6 2012
PC:         0x08e7b225 (suspend)
Call stack: 0x08e7b225 0x08e8a106 0x08e7ebf4 0x08e7efde 0x08e7f4c9 0x08e7f546 0x08a7789c
            0x095a3f60 0x080e7e3d 0x080dcfa2 0x080ddf5c 0x0806897c

CPU hog threshold (msec): 10.240
Last cleared: 12:25:28 EST Jun 6 2012
ASA#
```

ASA SSH進程在2012年6月6日12:25:33保持CPU運行119毫秒。

如果介面上的溢位錯誤持續增加，請檢查**show proc cpu-hog**命令的輸出，以檢視CPU hog事件是否與介面溢位計數器的增加相關。如果您發現CPU佔用導致介面超支錯誤，最好使用Bug Toolkit搜尋錯誤，或向Cisco TAC提出問題。**show tech-support**命令的輸出還包括**show proc cpu-hog**命令輸出。

定期處理的流量配置檔案超額訂閱ASA

根據流量量變曲線，流經ASA的流量可能過多，無法處理，因此可能會發生超支。

流量量變曲線包括（其中包括）：

- 封包大小
- 封包間間隙（封包速率）
- 協定 — 某些資料包在ASA上進行應用檢測，比其他資料包需要更多的處理

以下ASA功能可用於識別ASA上的流量配置檔案：

- Netflow — 可以將ASA配置為將NetFlow版本9記錄匯出到NetFlow收集器。然後可以分析此資料以瞭解更多有關流量量變曲線的資訊。

- SNMP — 利用SNMP監控來跟蹤ASA介面流量速率、CPU、連線速率和轉換速率。然後可以分析該資訊，以便瞭解流量模式及其隨時間的變化。嘗試確定是否存在與超限增加相關的流量率峰值，以及導致該流量峰值的原因。TAC中曾出現過網路上的裝置行為不當（由於組態錯誤或病毒感染）並定期產生大量流量的情況。

間歇性資料包突發超額訂閱ASA介面FIFO隊列

到達NIC的資料包突發可能導致FIFO在CPU從其中取出資料包之前被填滿。通常，解決此問題不需要太多工作，但通過在網路中使用QoS來消除流量突發或對ASA和相鄰交換機埠進行流量控制可以緩解這一問題。

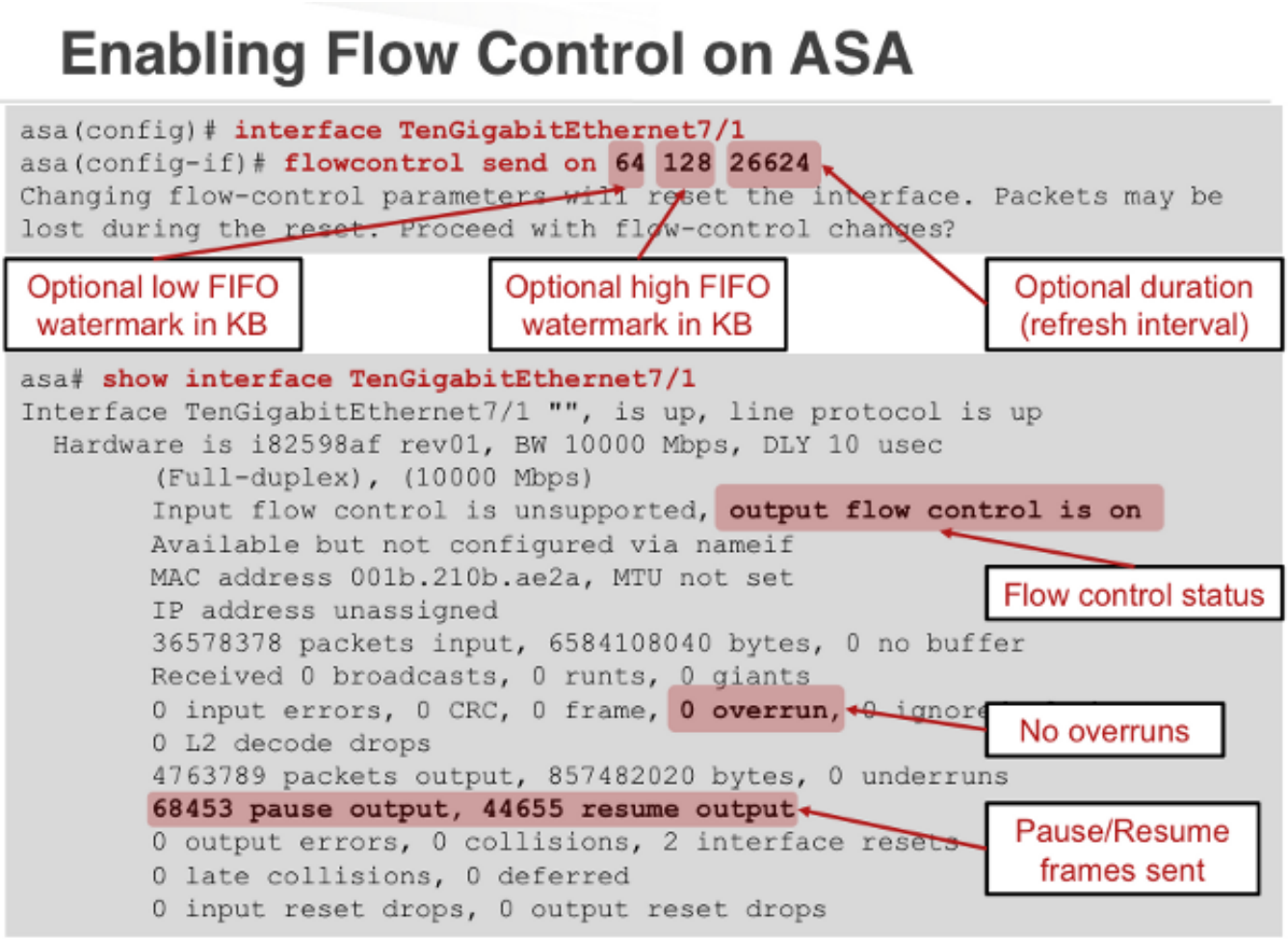
流量控制功能允許ASA的介面向相鄰裝置（例如，交換機埠）傳送消息，以指示其在短時間內停止傳送流量。當FIFO達到一定的高水位時，它就會這樣做。一旦FIFO釋放出一定量，ASA NIC將傳送恢復幀，交換埠將繼續傳送流量。此方法運行良好，因為相鄰交換機埠通常具有更多的緩衝區空間，並且在傳輸時可以比接收方向的ASA更好地緩衝資料包。

您可以嘗試在ASA上啟用捕獲，以檢測流量微猝發，但通常這樣做沒有幫助，因為資料包在ASA處理並新增到記憶體中的捕獲之前會被丟棄。外部監聽器可用於捕獲和識別流量突發，但有時外部監聽器也可能被突發量壓倒。

啟用流量控制以緩解介面超載

在8.2(2)版及更高版本中，流控制功能已新增到ASA（用於10GE介面），8.2(5)版及更高版本中（用於1GE介面）。事實證明，能夠在遇到超限的ASA介面上啟用流量控制是防止丟包發生的有效技術。

有關詳細資訊，請參閱Cisco ASA 5500系列命令參考8.2中的流量控制功能。



（來自Andrew Ossipov的Cisco Live Presentation BRKSEC-3021的圖表）

請注意，「輸出流控制開啟」意味著ASA將流控制暫停幀從ASA介面傳送到相鄰裝置（交換機）。「輸入流量控制不受支援」表示ASA不支援從相鄰裝置*接收*流量控制幀。

流量控制示例配置：

```
interface GigabitEthernet0/2

flowcontrol send on

 nameif DMZ interface
 security-level 50
 ip address 10.1.3.2 255.255.255.0
!
```

相關資訊

- [ASA 8.3及更高版本：監控和排除效能問題]
- [Cisco Live演示「最大化防火牆效能」] - 本演示概述了各種ASA平台的架構，並包含有關效能和調整的資訊。要訪問此演示，請登入到 Ciscolive!365 並搜尋演示編號BRKSEC-3021。
- [Cisco TAC安全播客第#7集「監控防火牆效能」] — 此播客本集討論監控防火牆效能和識別效能問題的技術和方法。
- [技術支援與文件 - Cisco Systems]