排除ASA接口溢出计数器错误

目录

简介

本文档介绍“溢出”错误计数器以及如何调查网络上的性能问题或数据包丢失问题。管理员可能会注意到自适应安全设备(ASA)**的show interface**命令输出中报告的错误。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

问题

ASA接口错误计数器“溢出”跟踪网络接口上收到数据包的次数，但接口FIFO队列中没有可用空间来存储数据包。因此，数据包被丢弃。使用show interface命令可以看到此计**数器的**值。

显示问题的输出示例：

```
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)
```

在上例中，自ASA启动或输入命令clear interface以手动清除计数器以来，在接口上观察到2881个超限。

接口超限的原因

接口溢出错误通常由以下因素组合引起：

- 软件级别 — ASA软件从接口FIFO队列中提取数据包的速度不够快。这会导致FIFO队列填满并丢弃新数据包。
- 硬件级别 — 数据包进入接口的速率太快，这会导致FIFO队列在ASA软件能将数据包拉出之前填满。通常，数据包突发会导致FIFO队列在短时间内填满最大容量。

排除接口超限原因的步骤

故障排除和解决此问题的步骤如下：

1. 确定ASA是否遇到CPU主机，以及它们是否导致了问题。努力减轻任何长时间或频繁的CPU占用。
2. 了解接口流量速率并确定ASA是否因流量量变曲线而超订用。
3. 确定间歇性流量突发是否导致问题。如果是，请在ASA接口和相邻交换机端口上实施流量控制。

潜在原因和解决方案

ASA上的CPU定期太忙，无法处理传入数据包（CPU主机）

ASA平台处理软件中的所有数据包，并使用处理所有系统功能（如系统日志、自适应安全设备管理器连接和应用检测）的主CPU核心来处理传入的数据包。如果软件进程持有CPU的时间比它应持有的时间长，则ASA将其记录为CPU占用事件，因为进程“占用”了CPU。CPU占用阈值以毫秒为单位设置，并且对于每个硬件设备型号不同。阈值取决于在硬件平台的CPU功率和设备可处理的潜在流量速率下填充接口FIFO队列可能需要多长时间。

CPU主机有时会在单核ASA（例如5505、5510、5520、5540和5550）上导致接口溢出错误。长猪

持续100毫秒或更长时间，尤其可能导致在较低的流量水平和非突发流量速率下发生超支。该问题对多核系统的影响不如此大，因为如果某个CPU内核被进程抱住，其他内核可以从Rx环中提取数据包。

持续时间超过设备阈值的占用导致以ID 711004生成系统日志，如下所示：

```
201320614:40:42:%ASA-4-71100460= sshPC = 90b0155= Feb 06 2013 14:40:42:%ASA-4-71100460= sshPC =
90b0155= 0x090b0155 0x090bf3b6 0x090b3b84 0x090b3f6e 0x090b4459 0x090b44d6 0x08c46fcc 0x09860ca0
0x080fad6d 0x080efa5a 0x080f0a1c 0x0806922c
```

CPU占用事件也由系统记录。show proc cpu-hog**命令的输出**显示以下字段：

- 进程 — 承载CPU的进程的名称。
- PROC_PC_TOTAL — 此进程占用CPU的总次数。
- MAXHOG — 该进程观察到的最长CPU占用时间，以毫秒为单位。
- LASTHOG — 最后一个占用者保持CPU的时间（以毫秒为单位）。
- LASTHOG At - CPU占用上次发生的时间。
- PC — 发生CPU占用时进程的程序计数器值。(思科技术支持中心(TAC)的信息)
- 调用栈 — 发生CPU占用时进程的调用栈。（思科TAC的信息）

此示例显示**show proc cpu-hog命**令输出：

```
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#
```

2012年6月6日美国东部时间12:25:33日，ASA SSH进程将CPU保留119毫秒。

如果接口上的溢出错误持续增加，请检查**show proc cpu-hog**命令的输出，以查看CPU hog事件是否与接口溢出计数器的增加相关。如果发现CPU主机导致接口超限错误，则最好使用Bug Toolkit搜索Bug，或向Cisco TAC提出问题。show tech-support命**令的输出**还包括**show proc cpu-hog命令**的输出。

定期处理的流量量变曲线超订用ASA

根据流量量变曲线，流经ASA的流量可能过多，无法处理，并且可能会发生超限。

流量量变曲线包括（除其他方面外）：

- 数据包大小

- 数据包间隙（数据包速率）
- 协议 — 某些数据包在ASA上接受应用检查，需要比其他数据包处理更多

以下ASA功能可用于识别ASA上的流量量变曲线：

- Netflow - ASA可配置为将NetFlow版本9记录导出到NetFlow收集器。然后，可以分析这些数据，以了解有关流量量变曲线的更多信息。
- SNMP — 使用SNMP监控来跟踪ASA接口流量速率、CPU、连接速率和转换速率。然后，可以分析信息，以了解流量模式及其随时间的变化。尝试确定是否存在与超支增加相关的流量率高峰，以及该流量高峰的原因。在TAC中，网络上的设备出现故障（由于配置错误或病毒感染）并定期生成大量流量。

间歇性数据包突发超订用ASA接口FIFO队列

到达NIC的数据包突发可能导致FIFO在CPU从CPU中提取数据包之前被填充。要解决此问题，通常无法做太多工作，但可以通过在网络中使用QoS来平滑流量突发，或在ASA和相邻交换机端口上进行流量控制来缓解此问题。

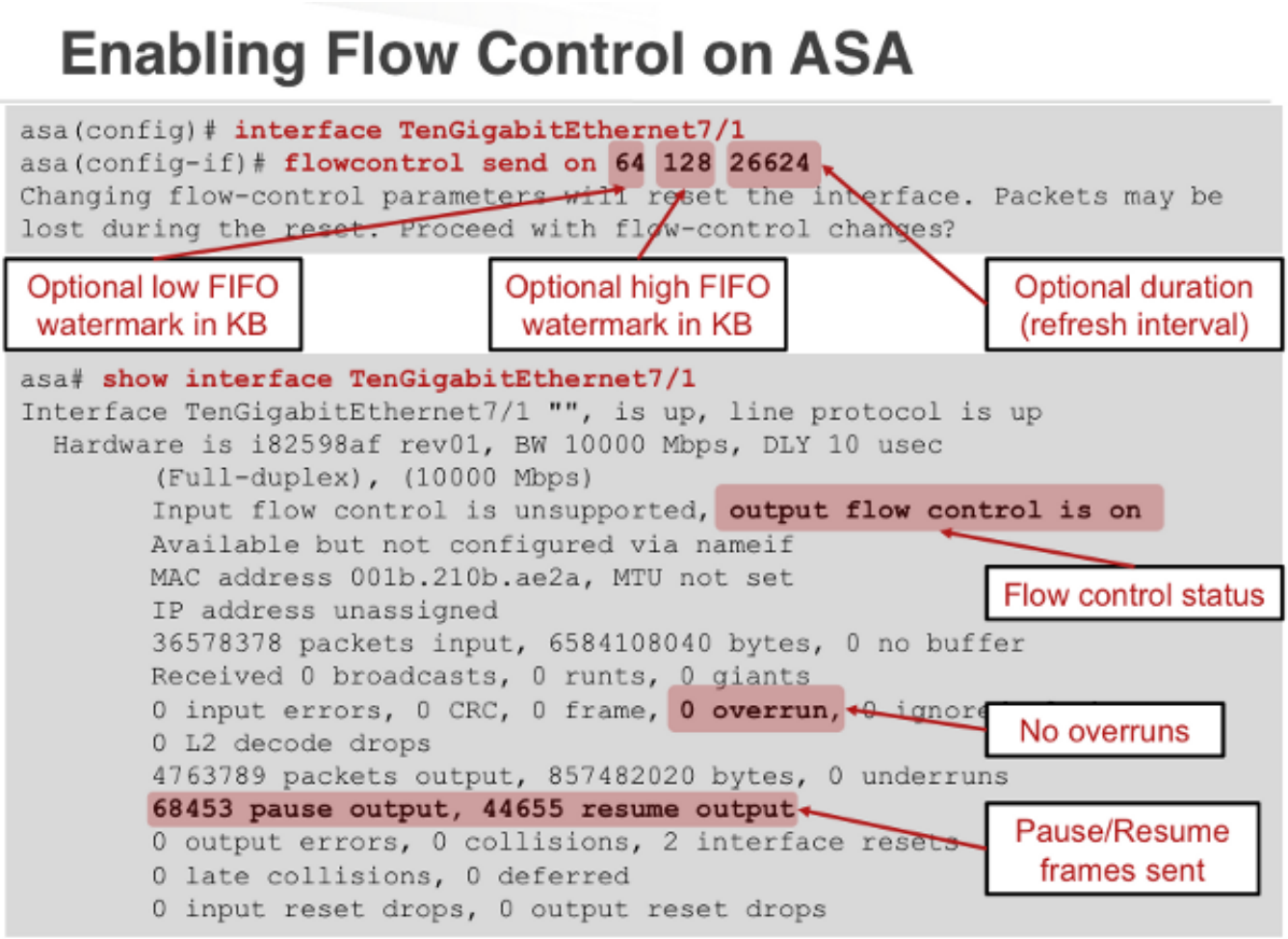
流量控制功能允许ASA接口向相邻设备（例如交换机端口）发送消息，以指示其在短时间内停止发送流量。当FIFO达到某一高水位时，它就执行此操作。FIFO释放一定数量后，ASA NIC会发送恢复帧，交换机端口继续发送流量。此方法运行良好，因为相邻交换机端口通常具有更多缓冲区空间，并且与ASA在接收方向相比，在传输时可以更好地缓冲数据包。

您可以尝试在ASA上启用捕获以检测流量微爆发，但通常这并不有用，因为数据包在ASA处理并添加到内存捕获之前会被丢弃。外部嗅探器可用于捕获和识别流量突发，但有时外部嗅探器也可能因突发而不堪重负。

启用流量控制以缓解接口超限

流量控制功能已在版本8.2(2)及更高版本（对于10GE接口）和版本8.2(5)及更高版本（对于1GE接口）中添加到ASA。事实证明，在ASA接口上启用流量控制（超限）是防止丢包的有效技术。

有关详细信息，请参阅《Cisco ASA 5500系列命令参考8.2》中的流控制功能。



（来自Andrew Ossipov的Cisco Live Presentation BRKSEC-3021的图表）

请注意，“输出流量控制已打开”表示ASA从ASA接口向相邻设备（交换机）发送流量控制暂停帧。“不支持输入流量控制”表示ASA不支持从相邻设备接收流量控制帧。

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
!
```

相关信息

- [ASA 8.3 及更高版本：监控并且排除性能问题故障]
- [Cisco Live演示“最大化防火墙性能”] - 本演示概述了各种ASA平台的体系结构，包括有关性能和调整的信息。要访问本演示，请登录 Ciscolive!365 并搜索演示号BRKSEC-3021。
- [思科TAC安全播客第#7集“监控防火墙性能”] — 本播客重点讨论监控防火墙性能和识别性能问题的技术和方法。
- [技术支持和文档 - Cisco Systems]