Resolución de problemas de caídas de entrada en IOS XR

Contenido

Introducción

Este documento describe cómo resolver problemas de caídas de entrada en la interfaz en los routers XR.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este artículo trata sobre los routers de la serie ASR 9000, los routers de la serie CRS y los routers de la serie GSR 12000.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Las caídas de entrada en IOS XR tienen un significado completamente diferente que las caídas de entrada en IOS. Puede confundirle cuando migra IOS a IOS XR y comienza a ver sus contadores de caídas de entrada en el comando show interface.

En IOS, una caída de entrada se debió a la cola de entrada de la interfaz que se llena. Esto significa que demasiados paquetes fueron impulsados a la CPU para la conmutación de procesos y no fue capaz de manejarlos lo suficientemente rápido. La cola de entrada se acumula hasta que se llena y hay algunas caídas.

En IOS XR, no hay una definición estricta de una caída de entrada. Básicamente, depende de los desarrolladores de un componente decidir si desean incrementar el contador de caídas de entrada cuando deciden descartar un paquete. La clave aquí es que en algún punto del código, el router decide descartar el paquete, lo que significa que es probable que el router no deba reenviar ese paquete y que el router decida conscientemente descartarlo. Por lo tanto, esto no está relacionado con la congestión como en IOS. Sin embargo, es más bien un paquete que fue recibido por el router y que se suponía que no debía reenviarse, por lo que el router decidió descartarlo y es muy probable que no sea una razón para alarmarse. Aunque, no puede decir si es algo de qué preocuparse o no hasta que haya entendido completamente el tipo de paquetes que están incrementando el contador de caídas de entrada y eso no es tan simple, por desgracia.

Examples:

- Un router XR está conectado a un switch que envía algunos paquetes UDLD y unidades de datos de protocolo de puente (BPDU). El router XR no tiene spanning-tree ni UDLD configurados en sus interfaces de capa 3, por lo que simplemente descarta estas tramas e incrementa el contador de caídas de entrada en show interface. En este caso, no hay nada de qué preocuparse, ya que es justo lo que hay que hacer para descartar estos fotogramas, ya que las funciones no están configuradas.

- Un ASR 9000 tiene una entrada de Cisco Express Forwarding (CEF) programada incorrectamente debido a un error de funcionamiento, de modo que no apunta a una adyacencia válida. En este caso, el procesador de red de la tarjeta de línea (LC) ASR 9000 se da cuenta de que el router pierde una información de carga e incrementa un contador de caídas del procesador de red (NP) que se carga en el contador de caídas de entrada de la interfaz.

Cuando se informan las caídas de entrada, el problema es averiguar si son caídas legítimas como en el ejemplo 1 o la consecuencia de un problema como en el ejemplo 2.

Problema: Incremento en el descarte de entrada

Este documento enumera las razones de las caídas de entrada que se incrementan y cómo verificar si es esa razón:

Caídas del controlador

Runts, Frame Check Sequence (FCS), aborts, desbordamientos FIFO (First Input First Output), caídas de paquetes gigantes sobre SDH/SONET (POS).

```
RP/0/RP0/CPU0:equinox#show controllers poS 0/2/0/0 framer statistics
POS Driver Internal Cooked Stats Values for port 0
================================================
```

```
Rx Statistics                   Tx Statistics
-------------                   -------------
Total Bytes:    71346296        Total Bytes:    67718333
Good Bytes:     71346296        Good Bytes:     67718333
Good Packets:   105385          Good Packets:   67281
Aborts:         0               Aborts:         0
FCS Errors:     0               Min-len errors: 0
Runts:          0               Max-len errors: 0
FIFO Overflows: 0               FIFO Underruns: 0
Giants:         0
Drops:          0

RP/0/RP0/CPU0:equinox#
```

Para una interfaz ethernet (gige, tengige...), verifique algo como:

show controllers gigabitEthernet 0/0/0/18 stats

Vea si hay un contador en las estadísticas del controlador que aumenta a la misma velocidad que el contador de caídas de entrada en show interface. Algunos de estos contadores de errores también deben estar en show interface.

Dirección de control de acceso medio (DMAC) de destino desconocida o VLAN dot1q

Paquetes con una dirección MAC de destino que no es la de la interfaz o con una red de área local virtual (VLAN) que no coincide con una subinterfaz. Estos pueden ocurrir cuando hay alguna inundación en un dominio L2 de direcciones MAC de unidifusión desconocidas, de modo que el router XR conectado a ese dominio L2 recibe tramas con una dirección MAC de destino que no es uno de sus controladores. También es posible cuando un router IOS envía señales de mantenimiento ethernet en su interfaz gige, de modo que estas señales de mantenimiento incrementan las caídas de entrada en el router XR ya que no tienen la dirección mac de destino del router XR. O cuando la interfaz está conectada a otro dispositivo que tiene más vlan/subinterfaces dot1q configuradas como en el router XR de modo que el router XR reciba tramas con una etiqueta dot1q desconocida.

En un módulo de interfaz de capa física (PLIM) fijo de CRS, puede encontrar estas caídas en:

```
RP/0/RP0/CPU0:pixies-uk#sh contr plim asic statistics interface tenGigE 0/1/0/3 location
0/1/CPU0
Wed Aug 22 16:07:47.854 CEST
                              Node: 0/1/CPU0


TenGigE0/1/0/3 Drop
--------------------------------------------------------------------------------
RxFiFO Drop       : 0                   PAR Tail Drop     : 0
PAR Err Drop      : 0                   Invalid MAC Drop  : 86
TxFIFO Drop       : 0                   Invalid VLAN Drop : 11
```

O en el estado del controlador tengige o gige:

```
RP/0/RP0/CPU0:pixies-uk#sh contr ten 0/1/0/3 stats
Wed Aug 22 16:22:42.059 CEST
Statistics for interface TenGigE0/1/0/3 (cached values):

Ingress:


    Input drop overrun          = 0
    Input drop abort            = 0
    Input drop invalid VLAN     = 11
    Input drop invalid DMAC     = 0
    Input drop invalid encap    = 0
    Input drop other            = 86
```

Nota: El error CSCub74803 existe, **Input drop other se incrementa** en lugar de **Input drop invalid DMAC** al menos en el PLIM fijo tengige de 8 puertos de CRS.

Para los adaptadores de puerto compartido (SPA) (CRS, XR 12000), el SPA l2-tcam descartará los paquetes con MAC no válido para que pueda encontrar estas caídas en **show controllers TenGigE a/b/c/d all**:

```
    Input drop other            = 107

   l2-tcam Invalid DA Drops: 107
```

En un ASR 9000, los contadores **Input drop invalid DMAC** y **Input drop other** en las estadísticas del controlador no se incrementan. Por lo tanto, la manera de reconocer estas caídas en el ASR 9000 es encontrar el NP que maneja la interfaz con las caídas de entrada:

```
RP/0/RSP0/CPU0:obama#sh int gig 0/0/0/30 | i "input drops"
Wed Aug 22 16:55:52.374 CEST
     1155 packets input, 156256 bytes, 1000 total input drops
RP/0/RSP0/CPU0:obama#sh contr np ports all location 0/0/CPU0
Wed Aug 22 16:56:01.385 CEST

                Node: 0/0/CPU0:
----------------------------------------------------------------

NP Bridge Fia                       Ports
-- ------ --- -----------------------------------------------------
0  0      0   GigabitEthernet0/0/0/30 - GigabitEthernet0/0/0/39
1  0      0   GigabitEthernet0/0/0/20 - GigabitEthernet0/0/0/29
2  1      0   GigabitEthernet0/0/0/10 - GigabitEthernet0/0/0/19
3  1      0   GigabitEthernet0/0/0/0 - GigabitEthernet0/0/0/9
RP/0/RSP0/CPU0:obama#
```

Por lo tanto, puede ver que la interfaz gig 0/0/0/30 es manejada por el NP 0 en 0/0/CPU0. Verifiquemos los contadores NP de NP0 en 0/0/CPU0:

```
RP/0/RSP0/CPU0:obama#sh contr np counters np0 location 0/0/CPU0
```

```
Wed Aug 22 16:56:19.883 CEST

                Node: 0/0/CPU0:
----------------------------------------------------------------

Show global stats counters for NP0, revision v3

Read 26 non-zero NP counters:
Offset  Counter                                         FrameValue   Rate (pps)
--------------------------------------------------------------------------------
  22  PARSE_ENET_RECEIVE_CNT                                 1465           0
  23  PARSE_FABRIC_RECEIVE_CNT                               2793           0
  24  PARSE_LOOPBACK_RECEIVE_CNT                             2800           0
  28  MODIFY_FABRIC_TRANSMIT_CNT                               80           0
  29  MODIFY_ENET_TRANSMIT_CNT                               1792           0
  32  RESOLVE_INGRESS_DROP_CNT                               1000           0
  35  MODIFY_EGRESS_DROP_CNT                                 1400           0
  36  MODIFY_MCAST_FLD_LOOPBACK_CNT                          1400           0
  38  PARSE_INGRESS_PUNT_CNT                                  465           0
  39  PARSE_EGRESS_PUNT_CNT                                   155           0
  45  MODIFY_RPF_FAIL_DROP_CNT                               1400           0
  53  PARSE_LC_INJECT_TO_FAB_CNT                               80           0
  54  PARSE_LC_INJECT_TO_PORT_CNT                             864           0
  57  PARSE_FAB_INJECT_UNKN_CNT                               155           0
  67  RESOLVE_INGRESS_L3_PUNT_CNT                             465           0
  69  RESOLVE_INGRESS_L2_PUNT_CNT                             464           0
  70  RESOLVE_EGRESS_L3_PUNT_CNT                             1400           0
  93  CDP                                                     464           0
  95  ARP                                                       1           0
 109  DIAGS                                                   154           0
 221  PUNT_STATISTICS                                        9142           1
 223  PUNT_DIAGS_RSP_ACT                                      155           0
 225  PUNT_DIAGS_RSP_STBY                                     155           0
 227  NETIO_RP_TO_LC_CPU_PUNT                                 155           0
 373  L3_NOT_MYMAC                                           1000           0
 565  INJECT_EGR_PARSE_PRRT_PIT                               928           0

RP/0/RSP0/CPU0:obama#
```

Por lo tanto, L3_NOT_MYMAC en el contador NP significa que el router recibió una trama en una interfaz de Capa 3 con una dirección MAC de destino que no es una de las interfaces. Y el router lo descarta como se esperaba y esto se informa como caídas de entrada en show interface.
En el ASR 9000 para paquetes recibidos con una VLAN dot1q no configurada en una subinterfaz del ASR 9000, el contador **Input drop unknown 802.1Q** no se incrementa en **show controllers gigabitEthernet 0/0/0/30 stats**. El procedimiento es el mismo que el anterior para el DMAC desconocido: identifique qué NP maneja las interfaces y luego verifique estos contadores de NP. Verá que el contador NP **UIDB_TCAM_MISS_AGG_DROP** aumenta en ese caso.

Paquetes rechazados debido a un protocolo de nivel superior no reconocido

Esa es fácil de detectar ya que hay un contador para estas caídas una línea debajo de las **caídas de entrada** en **show interface**:

```
RP/0/RSP0/CPU0:obama#sh int gig 0/0/0/18
Wed Aug 22 17:14:35.232 CEST
```

```
GigabitEthernet0/0/0/18 is up, line protocol is up

  5 minute input rate 4000 bits/sec, 0 packets/sec
  5 minute output rate 5000 bits/sec, 0 packets/sec
     7375 packets input, 6565506 bytes, 1481 total input drops
     1481 drops for unrecognized upper-level protocol
```

Aquí puede ver que todas las caídas de entrada se debieron a un protocolo de nivel superior no reconocido.
Esto significa que los paquetes se recibieron con un protocolo Ethernet en el que el router no está interesado. Esto significa que una función se configura en el vecino (o en un host conectado al dominio de capa 2 conectado a esa interfaz) de modo que nos envíe tramas con un protocolo no configurado en el router XR.
Ejemplos: BPDU, sistema intermedio a sistema intermedio (ISIS), protocolo de red sin conexión (CLNP), IPv6, UDLD, protocolo de detección de Cisco (CDP), protocolo de enlace troncal de VLAN (VTP), protocolo de enlace troncal dinámico (DTP), protocolo de detección de capa de enlace (LLDP), etc..

Cuando estas funciones no se configuran en la interfaz XR, el cuadro XR las descarta según lo esperado. Para averiguar qué tipo de tramas están incrementando este contador, tendrá que comparar qué funciones están habilitadas en el router XR con las funciones habilitadas en el vecino (puede ser un router o un switch), o las funciones habilitadas en todos los dispositivos conectados a los dominios de capa 2 conectados a esa interfaz (mucho menos fácil). Si el router XR está conectado a un switch, puede probar un tramo en ese switch de los paquetes que envía al router XR en la interfaz con caídas de entrada. Consulte:
ASR9000/XR: se descarta por error de protocolo de nivel superior no reconocido

Caídas de NP en ASR 9000

Los contadores de caídas en el proceso de red (NP) de ASR 9000 se notifican como caídas de entrada cuando se aplican a un paquete recibido en una interfaz y descartado. Esto no sucede con las caídas de Packet Switch Engine (PSE) en CRS y XR 12000: no se cuentan como caídas de entrada.

Por lo tanto, si tiene caídas de entrada en un ASR 9000 y no coinciden con una de estas razones, debería hacer un comando **show controllers np ports all location 0/<x>/CPU0** para encontrar el NP que maneja la interfaz con caídas de entrada y luego verificar sus contadores NP con **show contr np counters np<y> location 0/<x>/CPU0**.

Puede canalizar la salida para mantener solamente contadores DROP con un comando como **sh contr np counters np<y> location 0/<x>/CPU0 | i DROP** pero esto puede ser peligroso ya que a veces un contador de caídas no tiene DROP en su nombre. Ha visto un buen ejemplo con L3_NOT_MYMAC. Así que quizás canalice para **DROP|DISCARD|NOT|EXCD**.

Puede borrar los contadores de la interfaz y los contadores de NP con **clear controller np counters np<y> location 0/<x>/CPU0** aproximadamente al mismo tiempo para averiguar qué contador de NP aumenta a la misma velocidad que la entrada cae.

Por ejemplo, se obtiene IPV4_PLU_DROP_PKT en los contadores NP, lo que significa que la entrada CEF/PLU indica que el paquete debe ser descartado. No tiene una ruta predeterminada y tiene inaccesibles inhabilitados, por lo que los paquetes que no coinciden con una ruta más específica en la que llegan al controlador CEF predeterminado, que es una entrada descartada.

Si encuentra un contador de caídas en el NP que puede explicar las caídas de entrada a medida que aumentan a la misma velocidad, pero el contador de caídas NP no es muy autoexplicativo, puede navegar por esta página para tratar de entender lo que el contador significa: [ASR9000/XR: solución de problemas de caídas de paquetes y comprensión de los contadores de caídas NP]

> **Nota**: La página de Xander en los foros de soporte contiene las razones de caída para la primera generación de tarjetas de línea (Trident) y hay nuevos nombres de contadores para las tarjetas de línea de nueva generación (Typhoon)... pero en función del nombre, debe ser capaz de encontrar un nombre de contador similar al de Trident.

Netio

Puede recopilar un **show netio idb <int>** y esto le da la caída de entrada de la interfaz y los contadores de caída del nodo de netio:

```
RP/0/RP0/CPU0:ipc-lsp690-r-ca-01#show netio idb gigabitEthernet 0/2/0/1

GigabitEthernet0/2/0/1 (handle: 0x01280040, nodeid:0x21) netio idb:
---------------------------------
name:                     GigabitEthernet0_2_0_1
interface handle:         0x01280040
interface global index:   3
physical media type:      30
dchain ptr:               <0x482e0700>
echain ptr:               <0x482e1024>
fchain ptr:               <0x482e13ec>
driver cookie:            <0x4829fc6c>
driver func:              <0x4829f040>
number of subinterfaces: 4096
subblock array size:      7
DSNCNF:                   0x00000000
interface stats info:
  IN  unknown proto pkts:  0
  IN  unknown proto bytes: 0
  IN  multicast pkts:      0
  OUT multicast pkts:      0
  IN  broadcast pkts:      0
  OUT broadcast pkts:      0
   IN  drop pkts:           0 <============ cleared when added to input drop counter !!!
  OUT drop pkts:           0
  IN  errors pkts:         0
  OUT errors pkts:         0

Chains
--------------------
Base decap chain:
    ether                <30>  <0xfd018cd8, 0x482c736c>  <       0,        0>

Protocol chains:
---------------
<Protocol number> (name)  Stats
 Type  Chain_node       <caps num>  <function, context> <drop pkts, drop bytes>
 <snip>
 <13> (mpls)   Stats IN: 204 pkts, 23256 bytes; OUT: 0 pkts, 0 bytes
   Encap:
```

```
 mpls                <25>  <0xfcc7ddbc, 0x00000000>  <       0,        0>
 ether               <30>  <0xfd0189b4, 0x482c736c>  <       0,        0>
 l2_adj_rewrite      <86>  <0xfcaa997c, 0x4831a2e8>  <       0,        0>
 pcn_output          <54>  <0xfd0561f0, 0x48319f04>  <       0,        0>
 q_fq                <43>  <0xfd05f4b8, 0x48320fec>  <       0,        0>
 txm_nopull          <60>  <0xfcadba38, 0x4824c0fc>  <       0,        0>
Decap:
 pcn_input           <55>  <0xfd0561f0, 0x4830ba8c>  <       0,        0>
 q_fq_input          <96>  <0xfd05f330, 0x48312c7c>  <       0,        0>
  mpls               <25>  <0xfcc7b2b8, 0x00000000>  <     152,    17328>
Fixup:
 l2_adj_rewrite      <86>  <0xfcaa945c, 0x00000000>  <       0,        0>
 pcn_output          <54>  <0xfd0561f0, 0x48319f04>  <       0,        0>
 q_fq                <43>  <0xfd05f4b8, 0x48320fec>  <       0,        0>
 txm_nopull          <60>  <0xfcadba38, 0x4824c0fc>  <       0,        0>
```

Las caídas en el nodo de conmutación de etiquetas multiprotocolo (MPLS) aquí podrían deberse a que el tiempo de vida (TTL) de MPLS venció (en caso de un loop o cuando el cliente realiza un traceroute) o se requirió fragmentación y se estableció el bit No fragmentar (DF), por ejemplo. Puede ejecutar **debug mpls packet drop** y **debug mpls error** con la ubicación de la interfaz para intentar averiguar qué tipo de paquete está incrementando este contador.

Paquetes de multidifusión insertados. Cuando vea netio **IN drop pkts** pero no netio node a continuación con algunas caídas que podrían explicar los **paquetes de caídas IN**, entonces esto podría ser mcast punted packets y puede habilitar **deb mfib netio drop** para averiguar qué tipo de paquetes

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).