Detect the Increase in StarOS Error Port Datalink and NPU Counters

Contents

Introduction

This document describes the script which detects the increase in error Datalink or NPU counters per port.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- StarOs

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Problem

Error counters at the port level can be a great source of information in order to troubleshoot various issues with a StarOS node.

The most valuable information, in this case, is the variation of those counters during a certain period of time.

Static values that are available in the output of a single "**show"** command aren't providing sufficient information to make meaningful conclusions.

A typical approach is to collect several outputs of **show** commands and then make the difference manually.

This can be a difficult task, especially when it is not known what port exactly is impacted.

This script simplifies this process by providing the variation of error counters over a certain period of time per port.

Examples of issues that can be detected:

- MTU mismatches
- VLAN misconfiguration
- DataLink level errors

How does the Script Work?

In the SSD file, there are two outputs of **show port npu counters** and **show port datalink counters** taken at several minutes interval.

This permits to see the port level counters at a certain moment in time and also see their dynamics.

This script is checking the error counters from the command outputs and generates an alert when an increase in the counter is observed.

Usually, this indicates a problem at the physical or network level. Proceed with the steps to troubleshoot depending on the situation.

NPU Counters

These NPU counters are being observed:

Counter	Description	Notes
HW error	The number of packets discarded due to first-in, first-out (FIFO) overrun or underrun.	
Port non-operational	The number of packets discarded due to port not operational.	
SRC MAC is multicast	The number of packets discarded due to source MAC address is multicast.	
Unknown VLAN tag	The number of packets discarded due to an unrecognized virtual local area network (VLAN) tag.	Check the VLAN configuration on the ne hop switch
Bad IPv4 header	The number of packets discarded due to invalid IPv4 header	
IPv4 MRU exceeded	The number of packets discarded due to packet length is too long.	
TCP tiny fragment	The number of packets discarded due to TCP tiny fragment	

TTL expired	The number of packets discarded because their time-to-live parameter was exceeded.	
Too short: IP	The number of packets discarded due to IP packet too short	
Too short: ICMP	The number of packets discarded due to ICMP packet too short for lookup key	
Too short: IGMP	The number of packets discarded due to IGMP packet too short for lookup key	
Too short: TCP	The number of packets discarded due to TCP packet too short for lookup key	
Too short: UDP	The number of packets discarded due to UDP packet too short for lookup key	
Too short: IPIP	The number of packets discarded due to UDP packet too short for lookup key	Apparently a typo in documentation. Probably it is IPIP packet to short for lookup key.
Too short: GRE	The number of packets discarded due to GRE header size < 8 bytes	
Too short: GRE key	The number of packets discarded due to GRE header says key present but header size < 13 bytes	
Don't frag discards	Packets requiring fragmentation that are discarded by the NPU because the IP header don't fragment bit is set.	
IPv4VlanMap dropped	Total number of IPv4 VLAN map packets that were dropped.	
MPLS Flow not found	Total number of packets dropped when an MPLS flow was not found.	

Datalink Counters

These datalink counters are analyzed:

Counter	Description	Notes
RX Bytes	The number of received bytes.	
TX Bytes BAD	The number of bytes that were transmitted with errors.	
RX OVF	The number of overflows received.	
TX DEFER	The number of frames deferred upon the first transmit attempt due to a busy line.	
TX COL	The number of regular collision events occurring during transmission.	
RX SHORT CRC	The number of frames, less than 64 bytes in length, received with cyclical redundancy check (CRC) error.	
TX SCOL	The number of frames transmitted without any error following a single collision.	
RX NO SFD	The number of frames received without start frame delimiter (SFD) detection but with carrier assertion.	
TX MCOL	The number of frames transmitted without any error following multiple collision.	
TX	The number of frames that have experienced 16 consecutive	

XCOL	collisions or more.	
TX LCOL	The number of transmission abortion due to a collision occurring after transmission of packets that are 64 byes in length.	
TX PAUSE	The number of correct transmitted flow-control frames.	
RX LONG CRC	The number of frames, larger than the maximum frame size, received with CRC error.	
TX ERR	The number of frames transmitted with an error due to transmit FIFO underflow or TXERR signal assertion	
RX PAUSE	The number of correct received flow-control frames.	
RX FALS CRS	The number of false carrier events detected.	
RX SYM ERR	The number of received frames during which physical (PHY) symbol errors were detected.	
RX BAD frames	The number of received frames with errors.	
RX Runt frames	The number of received frames of less that expected size.	
RX Oversize frames	The number of received oversize frames.	Probably an error in documentation. Should be the same as "RX OverSize frames"
RX OverSize frames	The number of oversized frames received.	
RX NORM CRC	The number of frames, with lengths between 64 bytes and the maximum frame size, received with an integral number of bytes and a cyclical redundancy check (CRC) error.	
RX NORM ALI	The number of frames, with lengths between 64 bytes and the maximum frame size, received with a non-integral number of bytes and a cyclical redundancy check (CRC) error.	
RX GPCS ERR	The number of received frames during which physical (PHY) symbol errors were detected.	

There is a series of datalink counters seen only for STM interfaces:

Counter	**Description**	**Notes**
rx frames FECN set		Frame Relay related
rx frames BECN set		Frame Relay related
rx CRC errors		
rx alignment errors		
rx length violations		
rx FBP empty		
rx host queue full		
rx illegal header		
rx abort		
rx parity errors		
rx unsupported DLCI		Frame Relay related
rx SOP/EOP errors		
rx total error bytes		

tx frames FECN set	Frame Relay related
tx frames BECN set	Frame Relay related
tx underrun	
tx aborted frames	

Example Output

Increase in some of the error or drop counters from**show port npu counters**or**show port datalink counters**outputs are observed in the provided SSD.
The script highlights all the counters being checked, but only the ones with increase must be analyzed, that is the ones that contain the '**Following increase observed for port'**statement
Note that such increases aren't necessarily pointing to an issue with the node. Usually, it is a problem with a cable, SFP, misconfiguration or network level problem.
Check the definition of the affected counter(s) and proceed forward with the steps to troubleshoot based on this.

```
########################## NPU COUNTERS #######################################

 No errors increase found during monitoring period

######################### DATALINK COUNTERS ###################################

 Errors observed in the output of 'show port datalink counters' between  Monday October 01
12:29:49 CDT 2018 and Monday October 01 13:03:24 CDT 2018 on the ports 6/10,6/16,5/15

 - Following increase in errors is seen on port 6/10:

      RX OverSize frames:Frames: 404



 - Following increase in errors is seen on port 6/16:

      RX OverSize frames:Frames: 402


 - Following increase in errors is seen on port 5/15:

RX OverSize frames:Frames: 3
```

How to Understand the Output?

If no variation was seen in any of the counters of our interest on any ports, the script returns nothing.

If there is a variation with at least one counter of our interest, on, at least, one port - the script would not generate an alert.

The alerts are grouped per type (NPU or Datalink) and then per port.

First, there would be a statement summarizing all findings and the monitoring period.

```
 Errors observed in the output of 'show port datalink counters' between  Monday October 01
12:29:49 CDT 2018 and Monday October 01 13:03:24 CDT 2018 on the ports 6/10,6/16,5/15
```

Above it is between Monday**, October 01 12:29:49 CDT 2018** and Monday**, October 01 13:03:24 CDT 2018**, i.e. it is around half an hour.

The timestamps are taken from the outputs of **show port datalink counters** or, respectively, **show port** npu **counters**

Afterwards, there is a summary of problematic counters identified per port.

```
- Following increase in errors is seen on port 6/16:

    RX OverSize frames:Frames: 402
```

In the example mentioned, there were 402 oversized frames received on the 6/16 port during the monitoring period (around half an hour).