SNMP Input Queue Full

Contents

SNMP input queue full

ICSeverity

5 - Notice

Impact

SNMP packets dropped

Description

This error indicates that Simple Network Management Protocol (SNMP) packets were dropped due to input queue full error. Often this syslog is an outcome of extensive SNMP polling activity. This syslog is expected when the device in question is processing extensive number of SNMP packets. Because SNMP is handled by the CPU, it is possible that "SNMP Engine" process is consuming large number of CPU cycles. SNMP is a low priority protocol, and whenever there is a choice between a higher priority task and a protocol like SNMP, device can discard SNMP packets first. If the syslog has occurred once/ a few times and is not showing up often, it can be safely ignored. In some situations, there can be a software defect which cancause unexpected/suboptimal operation of the SNMP process. Please review the list of known defects and consider upgrading the software of the cisco device in question to the recommended/latest version to ensure that most known software fixes are present in the software in use.

SyslogMessage

```
SNMP-3-INPUT_QFULL_ERR
```

MessageSample

```
Jun 28 00:53:02.442 EDT <> %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full THIS IS A SA
```

ProductFamily

- Cisco Catalyst 2960-X Series Switches
- Cisco Catalyst 4500 Series Switches
- Cisco Catalyst 3750-X Series Switches
- Cisco ASR 1000 Series Aggregation Services Routers
- Cisco Catalyst 6800 Series Switches
- Cisco Catalyst 6500 Series Switches
- Cisco Catalyst 3850 Series Switches
- Cisco Catalyst 3650 Series Switches
- Cisco 4000 Series Integrated Services Routers
- Cisco Catalyst 9200 Series Switches
- Cisco Catalyst 9300 Series Switches
- Cisco Catalyst 9400 Series Switches
- Cisco Catalyst 9500 Series Switches
- Cisco Catalyst 9600 Series Switches
- Cisco 5700 Series Wireless LAN Controllers
- Cisco Catalyst 9800 Series Wireless Controllers

Regex

N/A

Recommendation

There is a possibility this error could be the result of a software defect, or the result of a genuine limitation of the device. Software defect triggered sometimes result in a separate SNMP Response Delayed syslog which calls out a specific MIB that the system determined was taking an excessive amount of time to process. If a large number of these high-delay MIBs are polled, the input queue can fill up while the system attempts to process them. Once the queue is exhausted, this syslog can appear. Regardless of software defect or platform processing limitations, generally speaking this error is often not service impacting to traffic, and can result in SNMP servers showing incomplete data for the device showing the syslog. If you are suspecting a platform or processing limitation of the device, proceed through these steps to confirm the device operation.

1) Check the output of 'show process cpu sort' to verify if SNMP Engine is one of the top processes utilizing CPU. If the syslog occurred in past and is not actively occurring, there cannot be an ongoing CPU consumption by this process. Device# show process cpu sort CPU utilization for five seconds: 99%/0%; one minute: 22%; five minutes: 18% PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process 189 1535478456 697105815 2202 88.15% 13.40% 8.74% 0 SNMP ENGINE << Short CPU spikes lasting only a few seconds from SNMP are often expected and not a cause for concern. However if the CPU remains elevated for several minutes at a high rate of utilization, this likely indicates an aggressive level of polling which can be overwhelming the devices ability to process in time. If this is observed you need to reduce the rate at which this device is polled from the SNMP server(s).

2) Use the command 'show snmp' to see if packets were dropped in past or are actively in the input queue. Run this command several times and examine the output to see if SNMP packets are actively being dropped. Device#show snmp 0 Input queue packet drops (Maximum queue size 1000) Packets currently in SNMP process input queue: 0 This can help indicate how aggressively SNMP packets are being queued while waiting to be processed, and can indicate your SNMP servers are polling MIBs which require an extended

amount of time to process normally (which can or cannot result in elevated CPU). If you see during polling intervals the queue is constantly at a large non-zero value, look into steps 3 and 4 to determine if you can find the specific MIBs or if increasing the queue size can be beneficial. Otherwise, SNMP server side changes can be required to change what is polled, and/or how frequently this device is polled. 3) Some platforms support 'show snmp stats oid' command to show which OID is being polled the most. If this CLI is available, examine the output to find out the OIDs being polled most frequently and consider removing them from the list of OIDs being polled or configure the device to exclude that MIB from the view to prevent processing of it. 4) If drops are increasing at a small rate, consider increasing SNMP queue size. This can enable the device to accommodate more SNMP packets but errors can resurface if the queue becomes full again. Device(config)# snmp-server queue-length.

Commands

```
#show version

#show module

#show logging

#show cpu proc sort

#show run | s snmp

#show snmp

#show snmp stats oid
```