S5130在配置未改变的情况下却有配置变更的日志提示信息且SNMP网管告警

SNMP 端口安全 **祁振峰** 2022-01-30 发表

组网及说明

不涉及组网

问题描述

现场根据mib库文件，使用第三方网管来管理设备。该网管的设定是只读取“修改配置（change）”和“保存配置（save）”对应的oid值，当网管侧读取到的 修改配置的oid时间值>保存配置的oid时间值，则认为是有在设备上更改配置，此时网管侧将会告警，提示对修改的配置的进行保存，当管理人员保存配置后，告警消失。

所以正常的情况下，保存过配置后，在未修改配置的情况下，网管侧读取到的save的oid时间是要大于change时间值。

但是现场遇到的情况是，在保存配置后，即使没有更改配置，在隔一段时间也会出现告警，且查看设备日志信息，有——snmp-COnfigSource=startup-COnfigDestination=running; Configuration changed.的日志记录，该日志的含义是：如果配置在过去的十分钟内发生了变化，设备将记录事件索引、引起配置变化的来源、源配置以及目的配置，尽管现场进行save操作，使得告警消失，在隔一段时间后，告警和上述日志信息会再次出现。

另外还有一台设备，其网管侧读取change的时间值远大于save，设备上多次执行save操作，网管侧读取的save的时间值会有相应的增加，但是依然小于change的时间值，因而网管侧的配置为保存告警一直存在。

未save：

第一次save：

第二次save：

过程分析

检查现场设备的诊断信息，发现现场有配置端口安全以及端口安全的老化时间——port-security timer autolearn aging 30，这个命令是用来配置安全MAC地址的老化时间，单位是分钟，通过观察日志信息的提示发现，该日志信息的提示也是30分钟一次：

%Dec 22 14:16:49:693 2021 KFCS-HQ-JR-H5130-6F-SW04 CFGMAN/5/CFGMAN_CFGCHANGED: -EventIndex=2-CommandSource=snmp-COnfigSource=startup-COnfigDestination=running; Configuration changed.

%Dec 22 14:46:49:694 2021 KFCS-HQ-JR-H5130-6F-SW04 CFGMAN/5/CFGMAN_CFGCHANGED: -EventIndex=3-CommandSource=snmp-COnfigSource=startup-COnfigDestination=running; Configuration changed.

%Dec 22 15:16:49:693 2021 KFCS-HQ-JR-H5130-6F-SW04 CFGMAN/5/CFGMAN_CFGCHANGED:

因此初步判断是由于该配置引起的，后续现场更改了老化时间后，发现该条日志信息的确和端口安全老化时间具有相关性，但是即使去掉该条老化时间的配置还是会不定时的会有日志提示信息出现，且网管侧也有相应的配置未保存的告警。

后经研发确认，日志提示信息是由端口安全配置引起的：

port-security intrusion-mode **disableport-temporarily**

port-security mac-address dynamic

port-security max-mac-count 1

port-security port-mode autolearn

------现有实现：配置了端口安全Mac地址后，这个Mac开始学习和老化的时候还是会有告警，安全Mac涉及到操作配置文件，如果是静态的重启会从配置中恢复，如果是动态的不会恢复，但是在学习的时候都会操作配置文件，这是设备当前的实现机制，这里的配置文件指的是运行配置库（相当于正在运行的配置）。

而现场的一台change的oid时间值远大于save的oid时间值的问题，现场增加了设备的vlan，此时网管侧读取到的change的oid时间值减小，且在进行save操作后，网管侧的change时间值小于save时间值，恢复正常。

经研发确认：现场反馈的save时间远小于change时间，是由于时间计数为32位，达到了取值上限发生翻转从0计数开始产生的现象。现场配置长时间未改变，保持最后一次修改的时间节点。后面计数翻转后，设备上进行save操作后，记录的savetime会从0开始重新计数，导致savetime远小于changetime。

解决方法

针对配置变更的日志提示信息，可以通过增加port-security mac-address aging-type inactivity命令使该Mac如果一直有流量就不会老化，减少告警产生。这个Mac开始学习和没有流量老化的时候还是会有告警，是设备当前实现机制导致的，是正常告警。

对于读取change的时间达到峰值没有计数翻转导致的change 的oid时间值一直大于save的oid时间值的问题，该问题会在设备长时间运行且近期没有配置修改的情况下出现，如现场操作配置上稍微修改下，即可让changetime也从当前翻转后的时间开始计算，save后可以恢复 savetime大于changetime。 计数翻转通常是设备运行时间五百天及以上会出现，后面有过配置修改即可恢复。