

IMPLEMENTATION OF ALARMS ON HOME DEVICE MANAGER

Sampriti Sarkar¹, R. S. Prasanna Kumar²

¹MTech, Department of Computer Science, PESCE, Mandya, India

²Assistant Professor, Department of Computer Science, PESCE, Mandya, India

Abstract

Alarms are generally being used these days for everything starting from morning wake-up alarms to sleep timers in television. Alarms have become the day to day life practice for many things. Here, alarms are an additional functionality added for an IT solution called as "Home Device Manager", which actually monitors the TR-069 devices and manages the devices remotely. Alarms are being implemented on Home Device Manager as an added functionality so that any service provider using this solution can easily monitor whether the device which malfunctioned is because of any of the most commonly occurring disabilities on the device.

Keywords: Alarms, Home Device Manager, IT Solution For Service Providers

I. INTRODUCTION

Home Device Manager (HDM): HDM remotely manages customer premises equipment (CPE) which includes residential gateways, modems, IP set top boxes. It provides all the CPE from multiple vendors who support Broadband Forum's TR-069 management support. HDM helps the service providers to verify if the device is working all right or any issues like gateway is switched on but doesn't respond to the connection requests.

II. ALARMS

Usually checking few of the most common device cases which lead to malfunctioning of the devices, 6 types of alarms are introduced. These alarms can help the customer care to notice whether any of those most commonly occurring cases have happened on the devices. Alarms getting raised on the device will help the customer care to find out if the device which is being complained about is not working because of some specific criteria's not being specified.

A. Types

The different types of alarms are:

- Frequent Inform event
- Device action failure
- Connection Request failure
- Value change alarm
- Generic alarm
- Missing gateway

III. ALARMS EXPLANATION

A. Frequent Inform event alarm

Beginning with Frequent informs event alarms, these alarms are based on the events being performed in between the

CPEs and the ACS. Sometimes if the device sends too many events for ex: inform event within the threshold time limit it creates congestion on HDM server. Thus an alarm will get raised on the device management console.

As shown in the following image, let's take an example of Frequent inform event alarm. We set the threshold of 3 inform in a day by the CPE to ACS, so as the fig. 1 shows

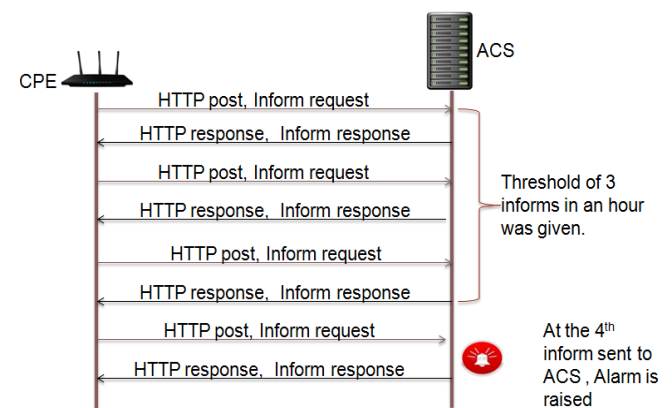


Fig.1. Frequent Inform event Alarm

here the device first initiates a connection to the ACS server and sends a periodic inform with the details about the device, so that the ACS server knows the details about the device which is trying to contact the server. Eventually if the device is not functioning as expected, thus it sends more than the required informs to be sent in a day and this may cause the HDM server to cause congestion. Thus, when the malfunctioned device sends the 4th inform to the ACS server, in the HDM device management console the alarm gets raised, thus informing the telecom provider about the device.

B. Device Action Failure alarm

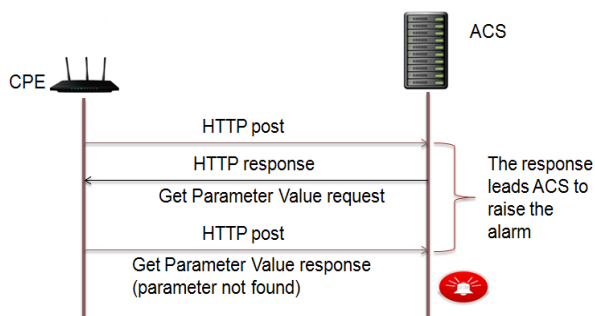


Fig.2. Device Action Alarm

Next coming to Device Action Failure alarm, this gets raised on HDM server only when any action fails on the device. This alarm is used to see whenever any action is queued on the devices and gets failed on the device then it raises the alarm.

As the fig 2 shows, the CPE device sends a normal post where the ACS sends the HTTP response back along with the Get Parameters value request. When the action is executed on the device and found that the parameter is not found on the device, thus the action fails on the device and eventually the alarm gets raised on the device management console.

C. Connection Request Failure alarm

Coming to the 3rd type of alarm i.e. Connection request failure alarm which is raised once the device doesn't respond back to the ACS server with a connection request response. This alarm is also like the previous 2 alarms ACS initiated alarm.

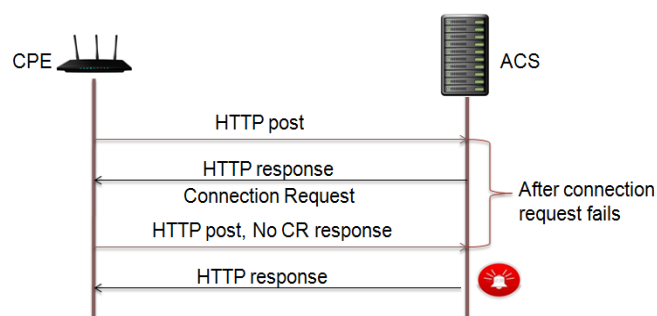


Fig.3. Connection Request Failure Alarm

As the fig shows, a connection request gets sent from the HDM server and within 5 seconds (hard coded) if the response from the CPE is not received then the alarm gets raised on the device management console.

D. Missing Gateway Alarm

The next type of alarm to be discussed is missing gateway alarm. This alarm is used to notify the ACS whenever a LAN device gets activated without any valid activated gateway device. This alarm informs the telecom provider that the gateway device which is associated to the LAN device is actually an invalid one or not activated in ACS yet.

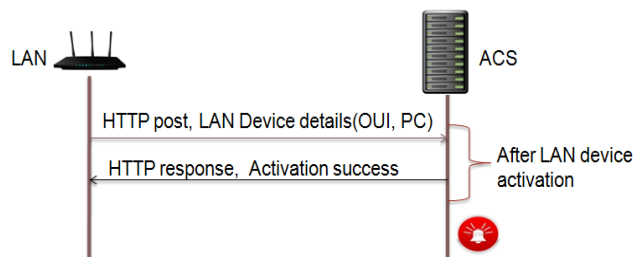


Fig.4. Missing Gateway Alarm

As the fig 4 shows, if a LAN device sends an activation request with incorrect details of the gateway device then its notified on the device management console by raising the alarm, even though the device gets activated since LAN device parameters are valid and unique. So this alarm helps in understanding whenever the LAN-gateway association is not proper.

E. Value Change Alarm

Value change is an alarm which gets raised whenever the value change event is sent to the ACS. This is the only alarm which is device initiated alarm activity. Whenever any parameter which is critical for the ACS gets changed on the device, the value change event is sent on the ACS thus informing the server about the change applied on the parameter.

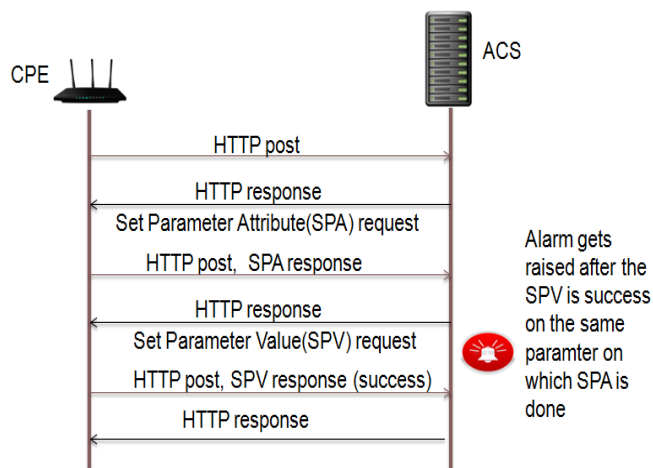


Fig.5. Value Change Alarm

As the fig 5 shows the ACS has done SPA on few parameters which are important to the device. Thus if in future any of these parameters values gets changed then the value change event is sent to the ACS informing about the change on the device, leading to raising an alarm on the device management page.

F. Generic Alarm

Last alarm is Generic Alarm. This alarm is used only by the OSS/BSS for the purpose to check any of the failure conditions. This can be performed only via NBI (Northbound Interface). All other alarms are done over the Southbound Interface.

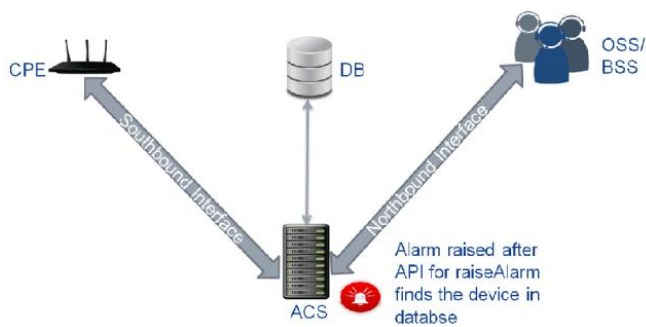


Fig.6. Generic Alarm

As the fig 6 shows, the CPE doesn't participate here whereas only the OSS/BSS tries contacting the server and fetches the required details from there through the database. OSS/BSS have APIs which help in testing the cases on the server and if the failure condition is success, then the alarm is raised on the CPE.

IV. CONCLUSION

Alarms are used for the sole purpose of notifying the service providers that the device being complained about is having which problem. Alarms are used in this product to help the service providers detect the most commonly faced business issues on the devices which are being monitored by the HDM. Thus it helps in faster detection of the problem if it is out of these 6 known issues. For future practices, even more alarms can be launched on HDM, which are most commonly occurring in the daily life.

It helps the service provider companies to detect the problems with the devices pretty faster (for the common 6 types), which helps in reduction of the call cost and the call timings being done by the customer to the companies complaining about the device.

ACKNOWLEDGMENT

It gives me immense pleasure to thank the Head of the Department Dr. M.C. Padma for giving me an opportunity to present this paper.

I extend my sincere gratitude to Mr. R.S. Prasanna Kumar, Assistant Professor, Department of CSE for their regular inputs and for constantly guiding me. I am obliged to the staff members of CSE department, PESCE for the valuable information provided by them as and when necessary.

REFERENCES

- [1] Home Network Configuration Management & Service Assurance, Stan Moyer and Simon Tsang, Copyright 2001, Telcordia Technologies, Inc.
- [2] Virtual Home Environment: Building & Testing an Efficient Prototype, Ioanna Roussaki, Maria Chanma, Stavros Xynogalas, Miltiades Anagnostou, National Technical University of Athens (NTUA), GREECE, 0-7803-7605-6/02 02002 IEEE
- [3] Intelligence Service Binding Architecture for Interoperability between Home Network Devices,

Seung-Ryun Lee, Dong-Kyu Lee, Dae-Ho Bae, Soon-Ju Kang, Member, IEEE, 0-7803-9459-3/06©2006 IEEE

- [4] NAT Issues in the Remote Management of Home Network Devices, Choongul Park, Kitae Jeong, and Sungil Kim, KT Technology Lab, 0890-8044/08 © 2008 IEEE
- [5] Design of Home Gateway based on Intelligent Network, Cuizhi Chang, 2008 IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application
- [6] System Architecture Challenges in the Home M2M Network, Michael Starsinic, 978-1-4244-5550-8/10 ©2010 IEEE
- [7] An Intelligent Home Networking System, Vukasin Nuhijevic, Sasa Vukosavljev, Boris Radin, Nikola Teslic, Mirko Vucelja, 978-1-4577-0234-1/11 ©2011 IEEE