ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (474-476), Month: April - June 2015, Available at: www.researchpublish.com

Protecting Radio Access Network through Automation

Sober Lourembam

Visvesvaraya Technological University,Belagavi., Bmsce, Bengaluru, India.

Abstract: **The Radio Access Network (RAN) in a UMTS/ W-CDMA network might experience downtime of long durations which occur as a result of failure, malfunction, physical damage or maintenance shutdown of its components. During the down time ,which may last from several hours to days, calls and other services will not be supported in the User Equipments (UE) or mobile phones located among the various cells controlled by the RAN. In order to reduce this downtime to few minutes, before the network is restored, the Radio Network Controller(s) (RNC) need to be backed up-so that when a particular RNC malfunctions, the backup takes over all its functionalities and returns the control once the original RNC is up. The protection of a RAN against undesirably long downtime is essentially the protection of its RNCs because RNCs are unarguably the most important components of a UTRAN which controls several Nodes Bs or the Base Transceiver Stations (BTS) which in turn control the "cells". Several RNCs could be configured with a backup RNC which is located far away physically and remains idle and could be activated only when the original RNC(s) are down. In this paper, the automation framework for activating the backup RNC has been described so as to achieve Protection Of the Network**

Keywords: **W-CDMA, UMTS, UTRAN, RAN, MGW, SGSN, RNC, NODE B, BTS, CRON JOB, IUB, IUCS, IUPS.**

I. INTRODUCTION

The role of a Radio Network Controller in a Radio Access Network (UTRAN in a UMTS/W-CDMA network) remains paramount as it is responsible for allocation of traffic channels towards the Node Bs, MGW and SGSN, management of radio channel configurations- On call initiation, the RNC decides on the resources allocated to the call on the basis of the bandwidth option available and services supported, operation and maintenance functionalities by way of hardware configuration, alarm system and centralized recovery functions. More importantly, the RNC controls the Node Bs connected to it and manages some of the important mobility management functions. Additionally, data encryption/ decryption is performed in this unit to protect the user data from eavesdropping. The modern day RNCs are essentially a collection of various cards connected together by a switching fabric. These cards which are powered by multi-core processors have specific functions and they are arranged to form a box, mounted on a rack and connected to the core network and Node Bs through routers and gateways. An Operations and Maintenance system is required to control the RNC from the outside world and provides a platform for different operation and maintenance applications. It also offers different post-processing and value adding functionalities like post-processing of fault and performance management data and SW upgrade support. On account of the above discussion, Radio Network Controllers need to be protected against physical damage which might occur due to earthquakes, floods, thunderstorms or other natural calamities or manmade disasters like fire. At the same time, RNCs might be required to be shutdown during maintenance or new build installation which occurs frequently. In such circumstances, the backup RNC need to take over so that the Radio Access Network downtime is reduced to few minutes. The Control is transferred to the Original RNC once, it is repaired or once it becomes up and working.

II. THE PROTECTED RNCS FRAMEWORK

A number of Radio Network Controllers within the same or in different Radio Access Networks (RAN) are configured with a backup RNC which is having the same load and having the same software build. The backup RNC does not belong to any RAN when it is in idle mode. A Telnet/SSH channel need to be established from the RNCs to the backup RNC. The objects for the RNCs need to be created in the backup RNC while a backup RNC object need to be created in each of the RNCs. The objects are just identifiers which refer to a particular RNC or a backup RNC. All the configuration data of the original RNC which includes the information on the IuB to the Node Bs and the IP addresses and IuPS and IuCS connection information to the core network must be transferred to the backup RNC for every object. Once, the backup RNC gets these data, it should configure its ports and IP address for the specific RNC that it wishes to take over. In this fashion, the backup RNC is now connected to the Node B's and the Core network of the original RNC. Thus, this backup RNC can now become a part of the RAN in which the original RNC served before the take over. Once the backup RNC becomes active, it will be running a different build than it was when no RNC object was activated.

III. PERL FOR AUTOMATION

The Radio Network Controllers are essentially Linux machines with proprietary commands for various operations. The Protection Feature could be installed in both the RNCs and their backup. There will be an array of commands to check whether if all the cards are up, to check the mode of the backup RNC, to check the status of the IuB link, to transfer the control to backup RNC etc. For automation framework, perl is found to be fairly efficient and simple. Perl can connect to Linux machines using pscp.exe and plink.exe. Perl can send commands to a remote SSH machine through a putty backend using pscp.exe and plink.exe. In this way, commands could be sent to the RNC one at a time. For sending multiple commands, either a recursion could be used or the commands could be copied to the Linux machine and executed one after the other. This approach is much simpler than using the currently popular SSH::Net module where we have to install modules and involves complications in the installation itself. Using pscp.exe and plink.exe provides for a plug and play framework, where the automation could be triggered from any machine connected to the intranet where the RNCs and the backup are part of. Perl also provides for easy file operations which could be used for writing system logs or console output which are useful in analysing failures.

IV. THE AUTOMATION SCENARIO

The Automation Framework essentially should contain the .pl file which contains all the steps to be performed for the transfer of control to the backup RNC. The steps are to be ordered in a logical flow in a careful manner so that all the steps are performed correctly with proper error/exception handling. Secondly, a .pm file is needed which contains all the functions and global variables (Scalar/hashes/arrays). The functions and the global are to be imported into the .pl file. In fact, the whole .pm file is to be included as a package in the .pl file. Thirdly, we need a .ini file which is used to store configuration details of the machines like IP addresses, user name and password. Another .ini file is also required to store the various expected values on the execution of each command. This is useful, when due to some errors, the execution of the commands gives errors and we might want to start from the beginning so that the whole process is successful.

A "cron job" could be run in any of the local system, which pings the RNCs at regular interval of time. If there is no response from the remote RNC machine for a set duration of time, this could mean that the RNC or its interfaces are down. At this point of time, the .pl file could be automatically executed which will bring up the idle backup RNC into an active state for the particular RNC object. The backup RNC now runs on a different built, referred to as, the base build for the particular RNC object. In this fashion, the backup RNC establishes control over the various Node Bs previously controlled by the original RNC. This whole activation might take few minutes. As soon as we get response from the original RNC, the automation script does an exit after deactivating the RNC object. Thus, the control is now transferred to the original RNC.

V. CHALLENGES

The backup and the original RNCs need to have the same software build. Since a backup RNC can be configured with many RNCs, though it could take over one RNC at a time, the system capacity of the backup needs to be higher than the original RNCs.There is a need for a link from the backup to the original RNCs where configuration files and other information could be transferred at high speed over long distance. As the RNCs may go down anytime, there is a need for synchronization of configuration data at frequent intervals.

The Adaptation of the backup RNC from the original RNC configuration to its interfaces (IP addresses) and ports should be efficient and fast and connectivity test to the core network and the node Bs for the newly configured backup RNC is required and should be implemented for the protection process to be successful.Lastly,the RNCs should have a linux platform so that the perl based framework could be implemented.

VI. CONCLUSION

Radio Network Controllers form the backbone of Radio Access Networks in UMTS/W-CDMA networks. In today's market ,there is a huge competition high speed, compact, efficient and high capacity Radio Network Controllers which could handle huge number of Node Bs or BTS.To achieve efficiency, the software builds are updated and during maintenance and natural disasters, the RNCs are unable to serve the RAN which is expensive from a business perspective. To achieve higher availability, protection of the RNCs is required. As manual supervision takes time and manpower, automation provides the solution and leads to better utilization of the available resources. The automation should be designed in such a way that provides for plug and play.

REFERENCES

[1] WCDMA for UMTS Radio Access For Third Generation Mobile Systems Wiley Third Edition

[2] http://ieeexplore.ieee.org/-ENABLING NETWORK REDUNDANCY IN THE RADIO ACCESS NETWORK-Kristiaan Venken*, Ignacio G6mez Vinagre', Rolf Sigle', Jose Diaz Cervera.

[3] http://ieeexplore.ieee.org/-Serving Radio Network Controller Relocation for UMTS All-IP Network -Ai-Chun Pang, Yi-Bing Lin, Hsien-Ming Tsai, and Prathima Agrawal