Journal of Software Engineering

ISSN 1819-4311

Academic Journals Inc.

www.academicjournals.com

Journal of Software Engineering 8 (2): 89-99, 2014
ISSN 1819-4311 / DOI: 10.3923/jse.2014.89.99

Research and Implementation High Availability of ForCES Control Element

[1]Wang Chao, [1]Wang Wei-Ming, [1]Wu Xiao-Chun, [1]Zhou Jing-Jing, [2]Lan Ju-Long and [3]Chen Chen

[1]College of Information and Electronic Engineering, Zhejiang Gongshang University, Hangzhou, China
[2]National Digital Switching System Engineering and Technological Research Center, Zhengzhou, China
[3]National University of Defense Technology, Changsha, China

Corresponding Author: Wang Chao, College of Information and Electronic Engineering, Zhejiang Gongshang University, Hangzhou, China

ABSTRACT

The open programmable network element architecture which based on Forwarding Element (FE) and Control Element (CE) Separation (ForCES) is an important trend of the next generation network element. How to realize the high availability and flexibility of the next generation network has presently become the important research work. This study studied on the high-availability requirement of CE in detail, including some rules and methods of ensuring backup data and brought forward the detection mechanism based on the heartbeat which is benefit for finding out the CE fault. In brief, the contributions are to (a) Analyze and improve the task of taking over methods between the CEs, (b) Realize this high-availability overall software architecture on the basis of analysis and studies of above techniques and (c) Test the high-availability of ForCES CE and the effectiveness of methods is finally validated by simulations.

Key words: ForCES, ForCES CE, high-availability, failure detection

INTRODUCTION

In the network information age, the computer communications system are faced on the most critical problem that how to establish and maintain the stability of system and the persistent of operation. As to the network equipment, it is mainly make use of computer systems to provide timely and reliable information and data processing but hardware and software will inevitably malfunction in the long running time, these failures may bring great damage to the network device and even lead to paralysis of all the networks. Therefore, the High Availability (HA) of the system is particularly important (Dong *et al*., 2011).

With the rapidly expanding of application range of the computer networks, the new generation network equipment should not only have sufficient flexibility and openness but also have some standardization characteristics. This development is conducive to healthy competition and reducing costs. Forwarding and control element separation (ForCES) precisely meet the above requirements of the next-generation network equipment at present which has been widely studied and applied. The research is mainly carried out under the guidance of the IETF. IETF set up a special working group named Forwarding and Control Element Separation (ForCES). ForCES network element as a new generation of network equipment, represents the development requirements of network equipment. Therefore, its high-availability is an important problem that must be considered. There

have been many studies on its high-availability. But they are all from the point of the data plane to analyze the HA of the network, this article will analyze the HA of the system from the internal router device that is, from control layer to research the system high availability.

In a high-availability theory, it generally uses the RAS to define the system's robustness and perfection. It includes: Reliability, Availability and Serviceability. Reliability is usually based on the average time between failures of the system running that is, Mean Time To Failure (MTTF). Availability concerned about how long it will take to recover and re-provision of services after system failure occurs. Maintainability concerned about the complexity of the system or its components maintenance, it is usually based on the average repair time, namely the Mean Time To Repair (MTTR). Availability is determined jointly by the reliability and maintainability. Therefore, to improve the availability of the system can be in two ways: The First, to improve the reliability, namely to increase the system's MTTF. The second, to improve the maintainability, namely to reduce the MTTR of the system. These two aspects of the technology should be used in the design of high-availability systems both (Soro *et al.*, 2010).

Hardware system through the way of maximizes the availability of the system components and minimizes fault repair time to ensure high availability. For example, component redundancy, hot standby and so on. High availability of the software system is essential either, it can be considered from the following aspects: fault-tolerant technology, data backup etc. In general, design a high-availability system need to consider the questions as: the establishment of backup data, the method of takeover between active and standby equipment and the method of failure detection and so on.

According to RFC3654 (Khosravi and Anderson, 2003) and RFC3746 (Yang *et al.*, 2004), the Network Element (NE) meet ForCES standard can be described in Fig. 1.

A NE consists of one or more CEs, as many as hundreds of FEs. Communication between CE and FE adhere to ForCES Protocol. For the purpose of backup, the study makes use of multiple control elements. CE is primarily responsible for the establishment, configuration and update of forwarding tables. FE is responsible for the handling and operation of each packet.

According to the description of ForCES framework and its protocol, the study designs and implements the ForCES software architecture; it can be described in Fig. 2.

The service component manager in this model is responsible for providing service for the various components of third-party developers and it provides a unified interface functions and the operation of coordination components. Control operation processor is responsible for the management of

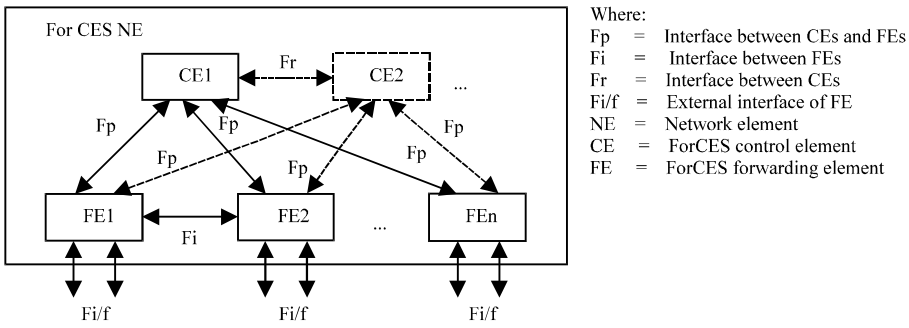

Fig. 1: ForCES network element structure model that meet ForCES standard

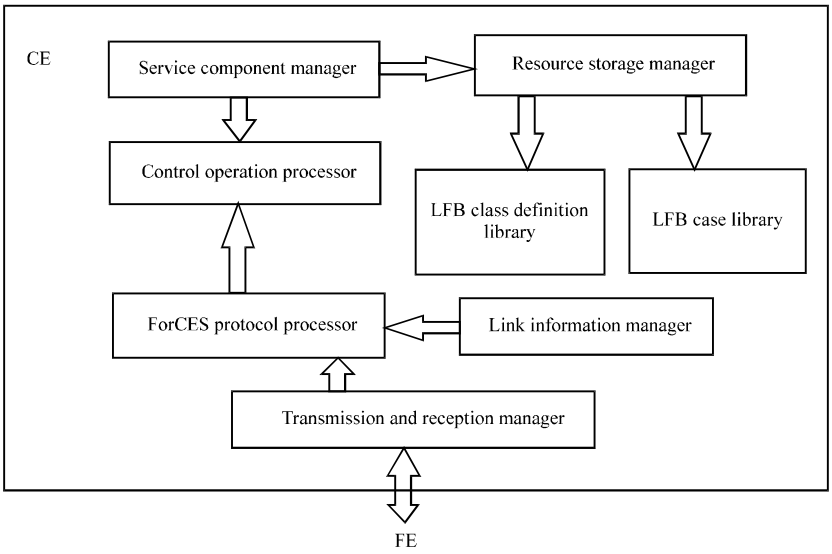

Fig. 2: ForCES software architecture model in ForCES control element

control operations which includes the verification of data format, the cache of instance data and the operating path. LFB class definition library saved the class definition information to provide the type of information for the data format validation. LFB instance library cached the instance data obtained from FE.

This study first introduced the background and the importance of high availability of Forces CE from the aspect of next-generation networks. The second chapter described the related key technologies and carried on the detailed introduction from the aspects of requirements, data backup, failure detection and tasks of takeover mechanism and so on. The third chapter designed and implemented the high availability of CE based on upper mechanism. The fourth chapter tested the high-availability system of ForCES CE and the effectiveness of methods by the simulator. Finally, this study comes to a conclusion.

RELATED KEY TECHNIQUES

Requirements of high-availability of forces CE: ForCES architecture needs to support redundant and failure mechanisms. The specific requirements are summarized as follows:

- Be able to detect when lost connection between CE and FE, then restore their connection effectively and maintain state synchronization
- When FE and CE lost their connection, what kind of reaction should be adopt
- At any one time, only one CE to control FE, namely only one primary CE and others are redundant CE

Methodology: In order to meet the uninterrupted requirements of the CE, the study designed a hot standby program to achieve the high availability. Specific implementation process and related technologies will be described in the following sections.

CE analysis and determination of the data backup: The backup data principles of high-availability system are generally as follow: If a file may be used in a subsequent process, it

should be backed up; If the data in a file take long time to regenerate, this file should be backed up; If a file's loss will bring troubles, then the file should be backed up.

CE is responsible for the control of FE. The management is mainly reflected by various LFB in FEs. These operations include: configuration of capacity and attributes, query and event subscription. It is collectively referred to as the ForCES resources. If the redundant CE wants to take over the work of the primary CE, it should backup the information of LFB class library, the sample library and the resources information in the ForCES such as operation path which saved as the tuple {path data}.

Methodology: The redundant CE backup the ForCES resources of the primary CE can't immediately take over the primary CE when it fails, because it does not know which link is the correct. Therefore, the link information of the FE that connected to the CE should be backed up either. But not all the link information needs to be backed up. For example, the ForCES resources, the status messages and the link information of FEs, heartbeat strategy and statistics messages are all the data that need to be backed up.

Method of resource backup in ForCES: Based on the above analysis, the scope of backup data used in ForCES is different from the other system. For this feature, this subject will store different data in different databases to improve the speed of data storage and query. Many existing backup technologies have been quite maturity, it can improve the stability of the system but also can shorten the development cycle and reduce development costs. Berkeley DB database is an embedded database, its main features are as follows: Embedded, lightweight, flexible and scalable. Apply it on the data backup of ForCES CE is appropriate. Its logic structure diagram can be described in Fig. 3.

Methodology: In this model, the application of the CE directly transfer the Berkeley DB data access subsystem and transaction management subsystem, these two subsystems which in turn transfer the underlying memory management subsystem, the lock subsystem and logging subsystem.

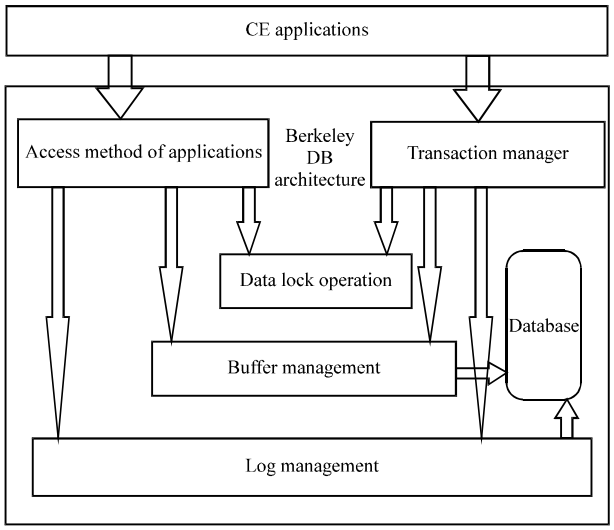

Fig. 3: Berkeley DB's logic structure diagram

Research of failure detection: The ForCES protocol specifies the heartbeat mechanism between the CE and the FE and gives different strategies for the corresponding heartbeat mechanisms in order to achieve failure detection. However, CE wants to achieve high availability not only achieves failure detection between the primary CE and the redundant CE but also need to consider the redundant CE how to build chains as the primary CE fails and consider the scalability of high availability. Currently there are already a variety of mature high availability heartbeat solutions which VRRP protocol (Nadas, 2010) and Heartbeat protocol are used widely.

The Heartbeat protocol made by Linux-HA Working Group provides an external virtual IP address, so that the primary and the redundant devices have its own real IP address. Through the study of HA software, the high-availability system logic diagram based the Heartbeat software can be described in Fig. 4.

Methodology: In the Fig. 4 the HA Daemon monitors the state of CE, namely the Heartbeat that loaded in ForCES primary CE detects the viable state of the redundant CE through sending heartbeat messages and vice versa. It also provides the function of fault diagnosis.

Research of takeover mechanism: The task of takeover mechanism means that the redundant CE takes over all FEs that connected with the primary CE and establishes its own ForCES architecture network element. Based on IP refers to the IP address of CE is unchanged. The IP-based takeover mechanism means that the primary and redundant CE share a virtual IP address. It can be described in Fig. 5.

Methodology: In high-availability system of ForCES CE, the primary and redundant CE have its own real IP address (For example: The primary CE1 IP: 192.168.0.21, the redundant CE2 IP: 192.168.0.23) in the same time, CE1 has a virtual IP address (192.168.0.208). CE1 builds link with FEs through the virtual IP address. When CE1 fails, CE2 detects the failure and takeovers the virtual IP address (192.168.0.208). When CE1 rejoins high-availability system after repair, the virtual IP address (192.168.0.208) will not be assigned to CE1 again. The entire process is transparent to the FEs.

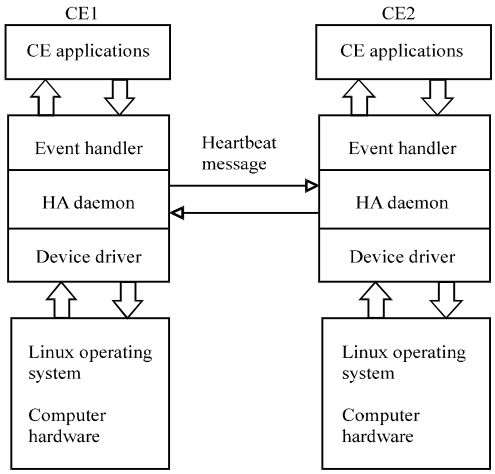

Fig. 4: System logic diagram based the heartbeat software

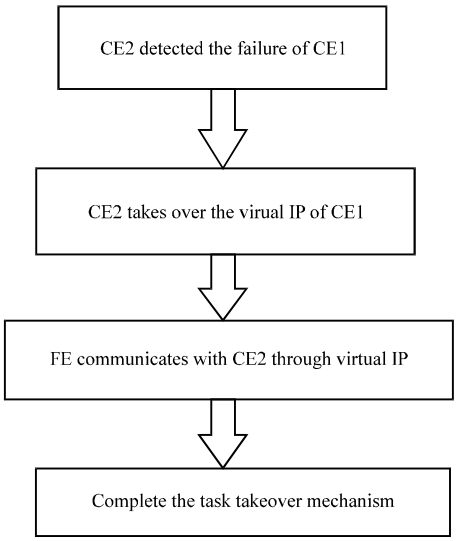

Fig. 5: IP-based takeover mechanism implementation process diagram

DESIGN AND IMPLEMENTATION OF HIGH-AVAILABILITY SYSTEM

This chapter is the design and implementation of the previous chapters to complete the high-availability in ForCES router.

From a functional perspective, the architecture of the module can be described in Fig. 6.

The high-availability system of the CE consists of configuration management module, data backup module and heartbeat detection module. Configuration management module is responsible for the election of the primary and redundant CE. Data backup module is responsible for the extraction and written of core data in ForCES middleware and data backup. Failure detection module is responsible for the detection of running state.

Specific state transition can be described in Fig. 7. Its specific implementation process as follows:

- Start and initialize the primary and redundant CE
- The primary CE undertakes the communication task with FEs, the redundant CE is responsible for monitoring the state and redundancy
- When the primary CE fails, the redundant CE takeovers the work of the primary CE, then the repaired primary CE will serve as the new redundant CE in high-availability system. This is a continuous cyclic process (Zhuge *et al*., 2012)

In a high-availability system, the CE configuration management module is responsible for the management of the CE state configuration, to ensure that the system has one and only primary CE. This state transition diagram consists of two parts: CE state configuration initialization and state update following with the query. Data backup management module mainly consists of two parts: Interface API management and Data backup management. The coursing of data backup is that the data in the primary CE stored by the redundant CE.

Failure detection between the primary and redundant CE is completed in Linux system by Heartbeat Software. First of all, install the Heartbeat software and set the necessary parameters of the system host. Secondly, configure the Heartbeat of the primary and redundant CE. Finally, compile the Heartbeat monitoring script.

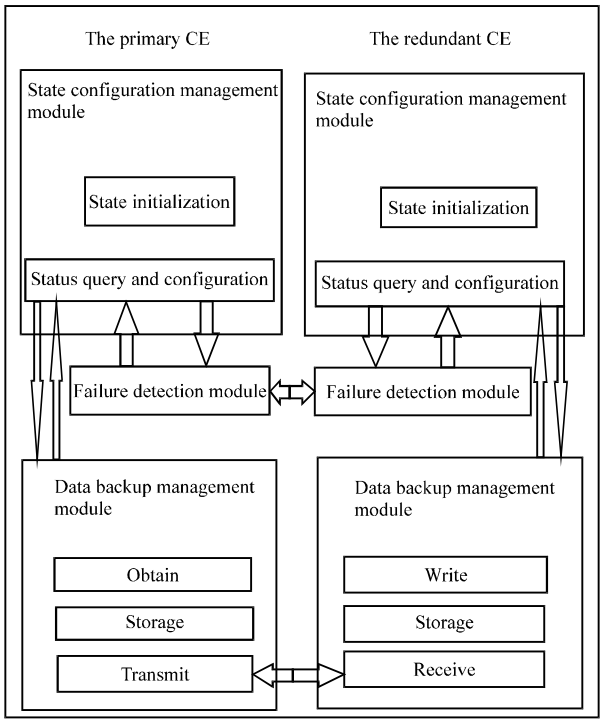

Fig. 6: Architecture of the high-availability system module in ForCES router

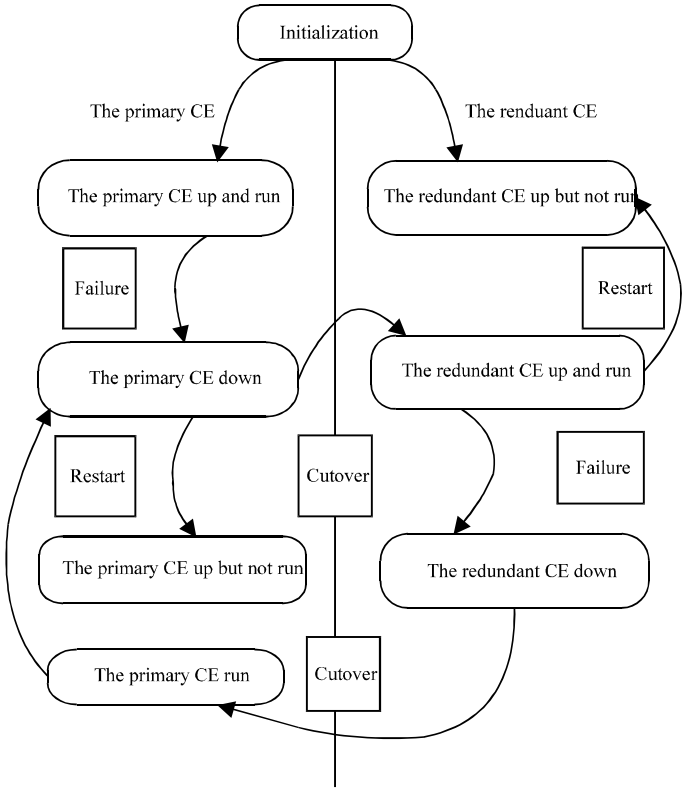

Fig. 7: State transition diagram in failure detection module

TEST AND ANALYSIS

According to the implementation of high-availability system and the previously published studies, the study designed the system functional test platform. It can be described as Fig. 8.

Test platform includes: Three computers equipped with Red hat 9.0 and Ethernet Switch. The primary and redundant CE are dual NIC and have different IP addresses. One is used for communicating with FEs, the other is used for detecting each other's heartbeat.

Heartbeat detection test: The primary and redundant CE through heartbeat messages interaction to detect each other's state. The test procedure can be described as follows: Before the system initialization, the primary and redundant CE set the keep alive to 500 m sec, set the warn time to 1 sec and the dead time to 2 sec. In order to verify the correctness, the study disconnects the link status of the primary CE and then the redundant CE will not receive the heartbeat message from the primary CE. Setting the dead time, if the redundant CE can't receive the heartbeat message from the primary CE, it means that the primary CE is failed, then start the takeover mechanism. Figure 9 is the screenshot of the experimental result. It shows that the redundant CE can detect the breakdown of the primary CE, namely the Heartbeat detection test is successful.

High-availability testing: Firstly, the test imitated the fault artificially to lead the primary CE fails and then set the rebooting times to 200 in each round of testing. There are total of five rounds of testing. Secondly, the test set different failure numbers in each round of testing and then it can test the utilization rate of the system in different failure rate environment. Set the number of failures are as follows: 190, 170, 150, 100, 80 and 50. The test results as shown in Table 1.

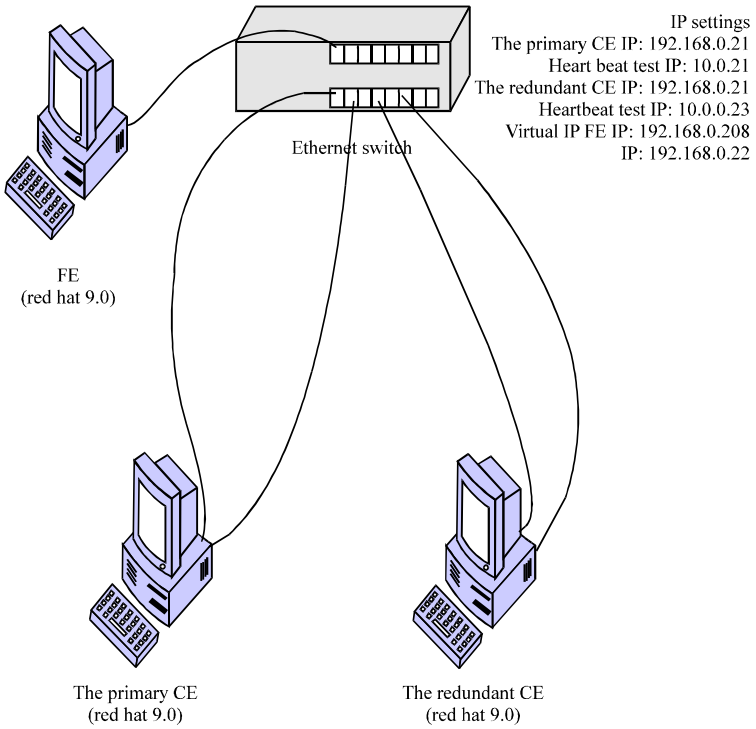

Fig. 8: System functional test platform module

Table 1: Test results of the utilization rate in different failure rate environment

No. of failures (times)	No. of achieve takeover (times)	Repair rate (%)	System failure rate (%)
190	172	90.523	9.0
170	159	93.523	5.5
150	141	94.000	4.5
100	93	93.000	3.5
80	75	93.750	2.5
50	48	96.000	1.0

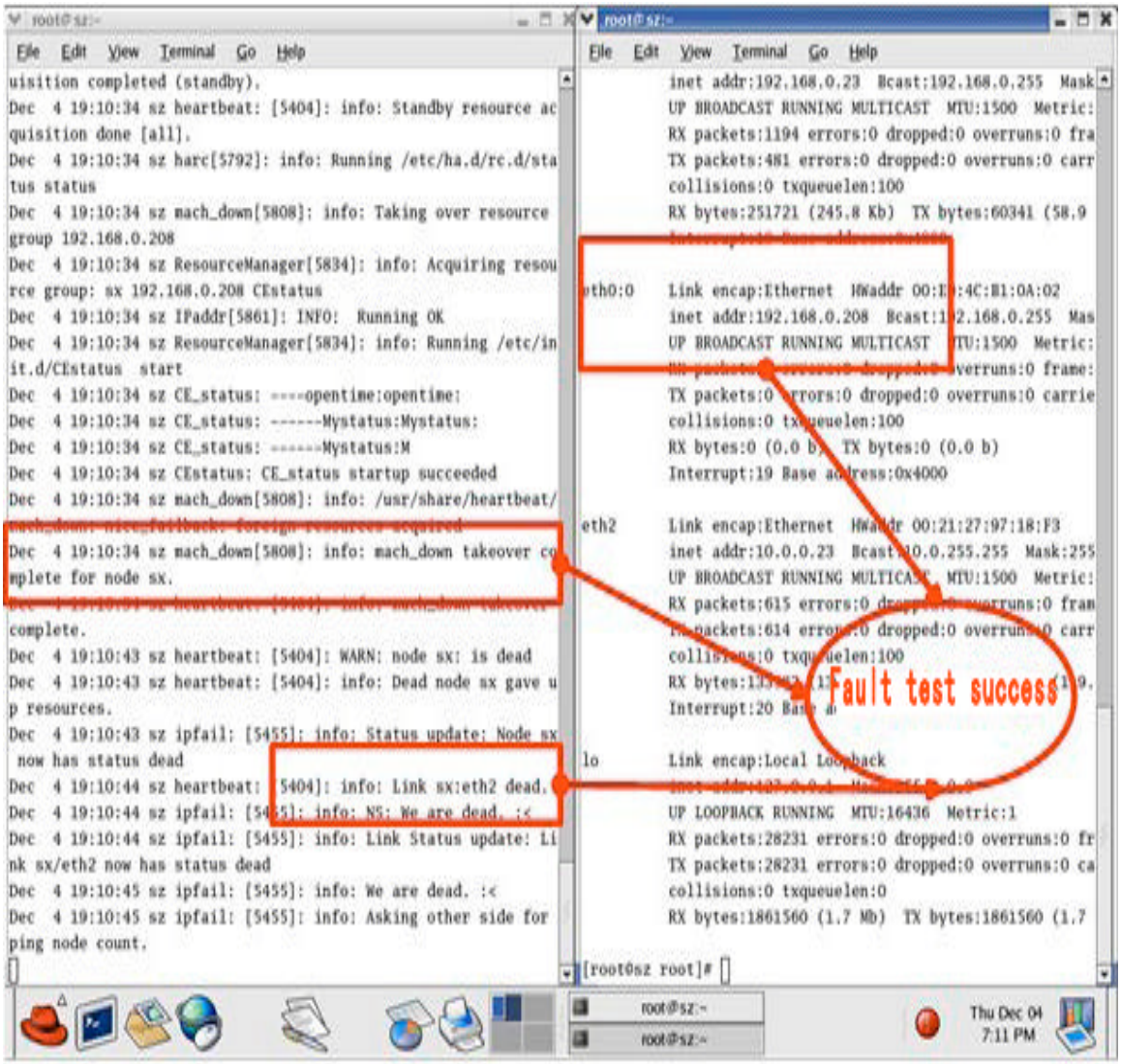

Fig. 9: Screenshot of heartbeat detection test results

The repair rate of the primary CE and the system failure rate can be described in Fig. 10. The diagram shows that: The repair rate of the primary CE is associated with its failure rate and remained stable at 90% above. The failure rate of the system is also subtle fluctuations but

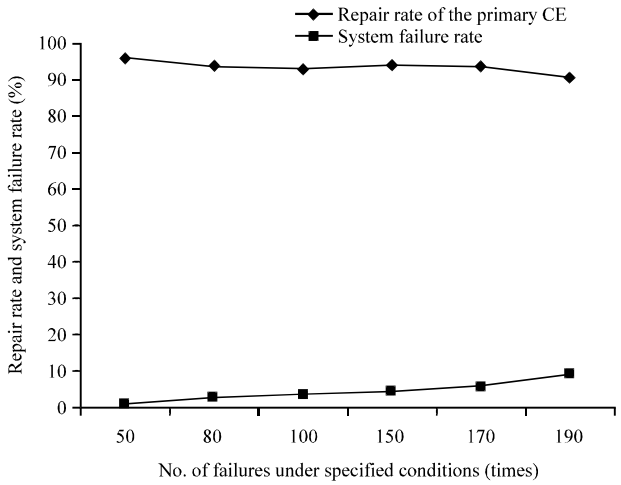

Fig. 10: Repair rate of the primary CE and the system failure rate diagram

remained largely unchanged at 10% or less. If not use the hot standby program, once the system fails, all the network equipment in the ForCES architecture will stop working, thus it can improve the utilization of the system.

CONCLUSION

The main object of this study is the high-availability of Control Element in ForCES. The open programmable network element architecture which based on ForCES is an important trend of the next generation network element. This study first introduced the ForCES framework, ForCES FE model and CE software architecture mode, then researched the requirements of high-availability of Forces CE and its related key techniques. Finally, it designed and implemented the high-availability system and proceed some related tests and analyses. It proved that the effectiveness of methods is finally validated.

ACKNOWLEDGMENTS

This study was supported in part by a grant from the National Basic Research Program of China (973 Program) under Grant No. 2012CB315902, the National Natural Science Foundation of China under Grant No. 61102074, 61170215 and Zhejiang Science and Technology Project under Grant No. 2012C33076. Zhejiang Provincial NSF China No. Y1111117, Q12F02013. Zhejiang Leading Team of Science and Technology Innovation (No. 2011R50010).

REFERENCES

Dong, L.G., L. Cai, L.F. Zhu and W.M. Wang, 2011. Research on high availability of ForCES control element. Inform. Technol. J., 10: 1683-1691.

Khosravi, H. and T. Anderson, 2003. Requirements for separation of IP control and forwarding. Network Working Group.

Nadas, S., 2010. Virtual Router Redundancy Protocol (VRRP) version 3 for IPv4 and IPv6. http://tools.ietf.org/pdf/rfc5798.pdf

Soro, I.W., M. Nourelfath and D. Ait-Kadi, 2010. Performance evaluation of multi-state degraded systems with minimal repairs and imperfect preventive maintenance. Reliability Eng. Syst. Safety, 95: 65-69.

Yang, L., R. Dantu, T. Anderson and R. Gopal, 2004. Forwarding and control element separation (ForCES) framework. RFC 3746. Network Working Group, The Internet Society, April, 2004. http://www.elook.org/computing/rfc/rfc3746.html.

Zhuge, B., G.W. Dai, L. Wan, H.H. Song, H. Wang and W.M. Wang, 2012. The design and research of cluster router based on ForCES protocol. J. Networks, 7: 1677-1686.