International Journal of
Advances in Scientific Research and Engineering (ijasre)

E-ISSN : 2454-8006

DOI: 10.31695/IJASRE.2019.33602

Volume 5, Issue 11
November - 2019

Fault -Tolerance Techniques for an Enterprise Network

MOMOH Monica O[1], MUHAMMAD Sanusi[2], ATUMOSHI Adamu Y[3]

Research Scholar[1], Senior Lecturer[2], Lecturer[3]

[1-3]Department of Computer Science,

University of Abuja,

Nigeria

ABSTRACT

An Enterprise network is a combination of different types of networks consisting of Ethernet, wireless, Voice over IP and several others. It is a fact that as the size of the organization increases so also the networks, as well as the number of computational requirements on its network, should be increased and optimized. Hence, effective management of these resources in a high-traffic environment in a reliable manner is challenging and requires a stable network flow. Fault-tolerance in an enterprise network for large organizations poses a big challenge for the network designers. In this Research work, two techniques are proposed to provide a fault tolerance system. The use of redundancy in the network infrastructure and the use of adaptive technology are proposed. Conducted simulations and research revealed that network robusity will be improved by employing these techniques. The redundancy technique is the provision of hot and cold functional capabilities that would allow system continuity and functionality in the case of component failure or capacity limitation. Redundant components that automatically take over operation when an equivalent functional component fails or seized. Riverbed Opnet Modeler Simulation tool is used to simulate the performance of the technique. As part of an increasing system, robusity and continuity in failure situations and faults, adaptive components such as H.264 codec and beyond (H.265) be employed for better performance.

Key Words: *Fault Tolerance, Redundancy, Enterprise Network, Error, Fault, Failure, Adaptive strategy, Data packet.*

---

1. INTRODUCTION

Enterprise Networks are private computer networks that are owned by a single organization in order to connect their various offices in order to share computer resources. Enterprise Networks comprise of uniform type of network [1]. Often it is a combination of different type of networks like Ethernet, wireless, Voice over IP, etc. Enterprise Networks tend to be designed secure and robust. Hence the need for adaptive and fault tolerant system. A high performance requirement necessitated for a fault detection and isolation system.

Enterprise networks require several configuration issues such as: number of independent departments or offices, categorization of nodes for creating VLANs, IPv4 or IPv6, subnetting – number of users per subnet, managing spanning tree protocol, available global IP addresses, block size of every subnet, which routing protocol to use and quality of service requirement.

Redundancy is a good way of providing backup routes. This helps to protect the network from link failures. Redundancy can be of two types namely switch redundancy (Layer 2 redundancy) and router redundancy (Layer 3 Redundancy). Also, Fast convergence implies the time taken by a router to find a new path to a node in case the old one is down. This can be achieved by using Dynamic routing protocols. We have to make sure to minimize the convergence time. Rapid Spanning Tree protocol is used to achieve high availability. Access Control Lists are used for load balancing operations in case of failure. Link Aggregation or Ether-channel is used to equip a network with high capacity for data transfer.

Designing any system to tolerate faults first requires the selection of a fault model, a set of possible failure scenarios along with an understanding of the frequency, duration, and impact of each scenario. A simple fault model merely lists the set of faults to be considered; inclusion in the set is decided based on a combination of expected frequency, impact on the system, and feasibility or

cost of providing protection. Most reliable network designs address the failure of any single component, and some designs tolerate multiple failures. In contrast, few attempts to handle the adversarial conditions that might occur in a terrorist attack and cataclysmic events are almost never addressed at any scale larger than a city.

2. FAULT TOLERANCE AND EXITING APPROACHES

2.1. Fault Identification and Management in Network

Today, enterprise networks connect large numbers of servers that provide functionality to large numbers of users using a very large number of software applications. Widely distributed systems are common in enterprises that are geographically dispersed. The network provides all connectivity between various computer platforms and clients. In systems of such complexity, even with careful planning, monitoring and assessment, it is difficult to predict the service demands on the network. Failures can arise from insufficient capacity, excessive delays during peak demands as well as a catastrophic failure arising from the loss of a vital component or resource.

Categories problems that are directly related to computer network into hardware and software. According to them, these can account for more than one-third of IT failures which are discussed, to better understand, in the context of the OSI model. Their work shows the distribution of errors among the layers of OSI model in Local Area Networks. Causes of failures within the lower layers of the model are often defective NIC cards, defective cables and connections, failures in interface cards in bridges routers and switches, beacon failure (Token Ring networks), checksum errors, and packet size errors. As Ethernet technologies have improved over time, there has been a decline in the failure rates within the lower layers of the OSI model but, there has been an increase in the failure rates in the Application Layer as software complexity continues to explode. Many of the errors and failures as described in the work are often localized (usually to one computer or user) and not catastrophic in nature. Localized failures are very different from that defined by the US Military and the Bell core models which allow for local failures to occur and not be considered a device failure. In understanding the contribution of localized failure to network reliability, it is important to consider the scale and size of failures that are caused by individual network components. For example, the failures of a NIC card will not likely results in a Single Point of Failure of the enterprise network. However, a Core Router failure without appropriate redundancy and switchovers can incapacitate an entire network.

Establish the relationships between fault, error and failure in their work. The article addresses the behavioral characteristics of faults, errors and failures in wireless sensor network. Viable usage of compact limited resource constrained micro sensors for advance deployment tends to face more challenges during the execution of various event handling and this action reflects to obtain deviated result from reaching the targeted goals. Achieving the targeted goals beyond the limitations necessitate special investigation of possible arising faults. Although many fault management approaches are addressed, none has focused on faulty issues at the wireless sensor network protocol stack level and also at sensor nodes' component side. Addressing and exploring various impacts of faults, errors and failures at different layers of wireless sensor network protocol stake and at the level of inter-functional units of sensor node components are concerned to be the main theme of this paper. Moreover, the overall investigation along with three phases (prevention, diagnosis, and recovery) of fault management furnishes generic life-cycle of fault tolerance management with potential basic relevant parameters. The point of interest of this work is the establishment of relationships between fault, error and failure

3. RESEARCH METHODOLOGY

3.1 Research Plan

We present here the research methodology, a generic framework and procedures adopted at the course of making the research. Here, the research specifies the research method or procedures as well as the justification for adopting the said method(s). Also, we develop research plan that entails how the research is carried out to achieve the stated objectives. The objectives of this thesis was the development and simulate fault tolerance in an enterprise network that can detect and recover from failures of network interface cards, network cables, switches, and routers in much less than one second from the time of failure. Since our focus is on large enterprise, the problem was divided into two parts: fault tolerance within a single local area network (LAN), and fault tolerance across many local area networks.

The first part involves the network interface cards, network cables, and switches within a LAN, while the second part involves the routers that connect LANs into larger internetworks. Both parts of the solution were simulated on OPNET network modeler. The analysis of the simulation data indicated that network failure was corrected within 300milliseconds of the failure.

3.2 Research Method

The framework for research methodology adopted in the work is presented in Figure 3.1 and the stages are explained below;

DOI: 10.31695/IJASRE.2019.33602

- ***Feasibility studies***: - Feasibility studies are the investigation carried out to know if the proposed project is realistic. Although, for this work we use the Pharmaceutical Council of Nigeria as a case study.
- ***Information Gathering***: - Here, information about the location and the capacity of the network are ascertained. Also, the main functioning devices are enlisted as well as the services expected from the proposed network.
- ***Adaptive infrastructure***- use of packet design to interpret large data for efficient decision making
- ***Network Design***: - This aspect deals with the explanation and illustration of how the network will function. Typically, this is more or less a paper work if the network is to be implemented in real live. Having said that, the focus here is to connect the devices together using standard communication procedures as it is though it is live.
- ***Network Simulation***: - The technique of representing the real world by a computer program. Here, we demonstrate how communication takes place among the networking devices using OPNET.
- ***Troubleshooting***: - This is the phase where packet is send from every host to every other host to check if there is any problem in the desired transmission scheme.

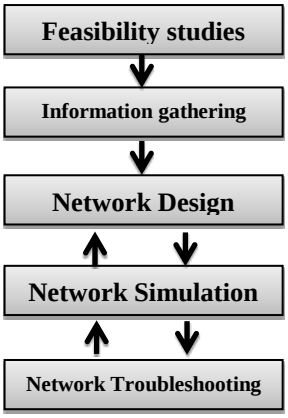

Figure 3.1: Research Methodology

3.3 Simulation Method

Unlike software development project, computer networking project is an expensive project that involves hardware equipment. The problem becomes more complex when we consider large networks like CAN that involves many LANs that need to be networked together. For this reason, we adopt simulation method for this research work. Simulation allows us to develop a model that represent the real networks, perform analysis, report results and make recommendations. We can then replicate this in real live and validate the real live network with the simulated version.

3.4 Tools Used For The Work

Riverbed Modeler Academic Edition provides a virtual environment for modeling, analyzing, and predicting the performance of IT infrastructures, including applications, servers, and networking technologies. Based on Riverbed's award-winning Modeler product, Academic Edition is designed to complement specific lab exercises that teach fundamental networking concepts. The commercial version of Modeler has broader capabilities designed to increase network R&D productivity; develop proprietary wireless protocols and technologies; and evaluate enhancements to standards-based protocols. Riverbed software is used by thousands of commercial and government organizations worldwide, and by over 500 universities. Also, Wireshark was used to capture packets for analysis

3.5 Fault Tolerant Detection Technique

The modeled enterprise network would be simulated using OPNET for different scenarios, this result would be compared to the result of the network while watching out for anomaly and embedded is a sensor or alarm which flags if the network is fault tolerant or not.

DOI: 10.31695/IJASRE.2019.33602

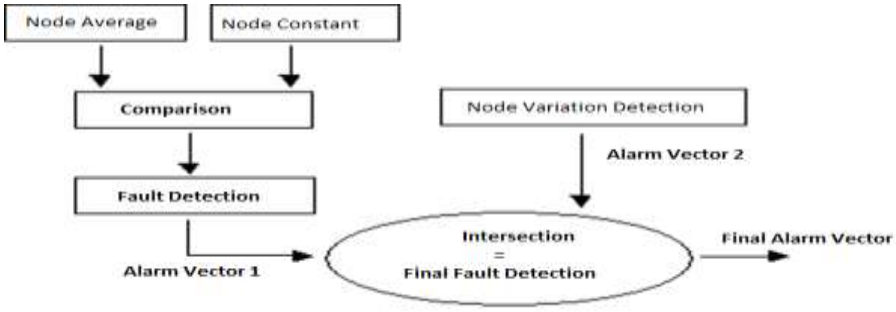

Figure 3.2: An existing fault tolerant detection technique

4. USE OF ADAPTIVE TECHNIQUES FOR FAULT TOLERANCE

Network tolerance and adaptation is a useful technique and method to implement in a system. The system will involve a choice of adaptive component that tolerate network failure and congestion. Various Simulations as in figure 4.1a and figure 4.1b informs that H.264 codec and beyond H.265 transmits with various levels of bit streams that carry various levels of capacity [13]

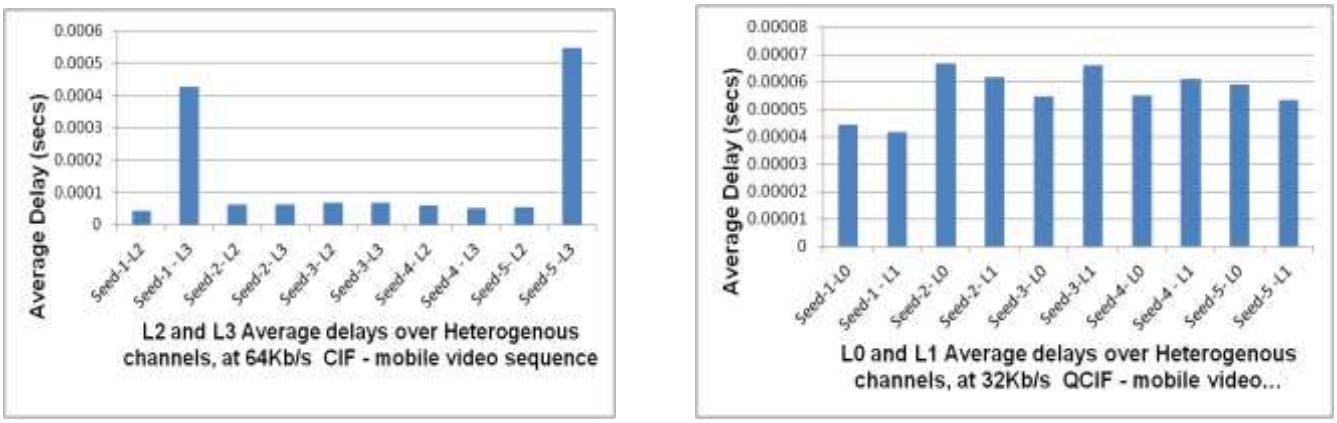

Figure 4.1(a.b): Real Time Performances for sub-layers in a t+s+q mobile bit-stream (L0, L1, L2 and L3)

4.1 Large Enterprise Network Model

Enterprise networks connect the departments of an organization, local users and remote users each other, and provide access to information processing and communication resources. They have generally large structures and many applications with strict security rules. Enterprise networks support hundreds of users, in much larger cases this number may become hundred thousands of users. As illustrated in Figure 4.2. Before an enterprise network is constructed, during the design phase of an enterprise network, creating enterprise network scenarios using a reliable simulation tool and designing the enterprise network in the virtual environment, simulating the use of network applications and network traffics, and verifying designs provide cost and time savings.

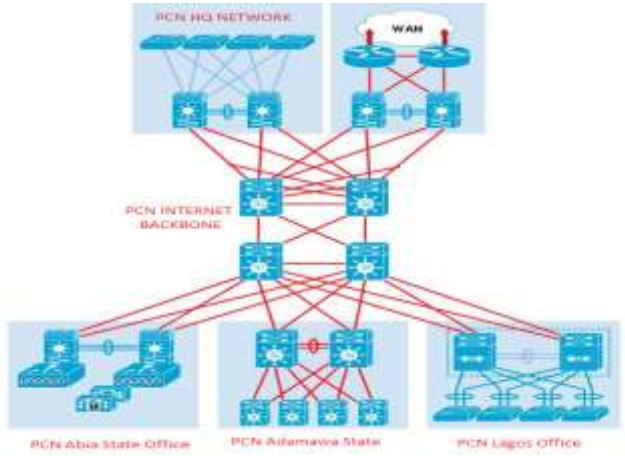

Figure 4.2: Large enterprise network model

DOI: 10.31695/IJASRE.2019.33602

4.2 Virtual Modeling and Configuration of an Enterprise Network with Opnet

The designed model is composed of two domains. The first domain is the internal enterprise local network where the enterprise network devices, servers and applications are located. The second domain is the remote connection which is used to access the enterprise network with an external link (like ADSL) over a VPN connection. An ADSL modem for remote access to the enterprise model, IP32 Cloud for Internet access from the enterprise model, Linux IP Tables Firewall, Linux OpenVPN VPNServer, Microsoft DNS Server, Windows 2008-IIS 7.0 Web Server, FTP Server, Linux DHCP Server and a Windows XP PC for Wireshark packet capturing tool were used in the real model. Several tests were performed over the VPN remote connection to access the enterprise network model. HTTP requests generated by JMeter were sent to the IIS 7.0 Web Server over the remote connection in 30 second periods. Test duration was 10 minute, and network packets were captured using the Wireshark packet capturing tool, and the performance information on the server was collected with the Windows Performance Monitor tool.

4.3 Performance Evaluation

The enterprise network is a multi-access network, meaning that a set of nodes sends and receives frames over a shared link. It implements the capability of transmitting and monitoring a connected star link at the same time. It has full duplex capability. For Successful performance evaluation, we will consider 6 scenarios, varying users and resources.

A Simulation set-up for Fast Ethernet in an Enterprise Network

The Fast Ethernet network model operating at a data rate of 100 Mbps in a star topology using OPNET Modeler with 10 users in remote subnets making 30 users can be made by using the parameters as shown in Table1.

Table 1: Parameters for Fast Ethernet Model

Start > New > File >PCN Network> scenario-1 > create empty scenario > campus > X,Y =10 miles > Model family – Ethernet	
Topology	Rapid Configuration
Configuration	Star
Centre Node Model	Ethernet_16_switch
Periphery Node Model	Ethernet_station
Link Model	100 Base T
Number	10
Centre X,Y	1.92856,1.62981
Radius	3.11235

Figure 4.3: Enterprise network of Pharmaceutical council of Nigeria with three remote sites

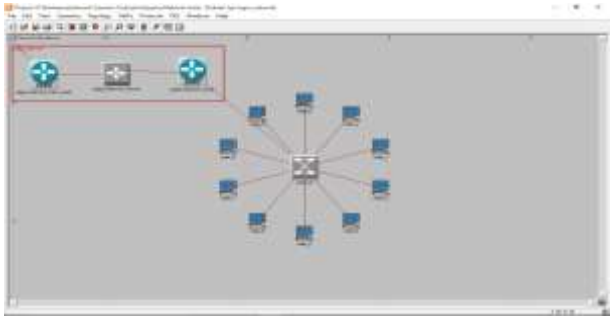

Figure 4.4: Lagos Office Network Infrastructure (Nigeria)

DOI: 10.31695/IJASRE.2019.33602

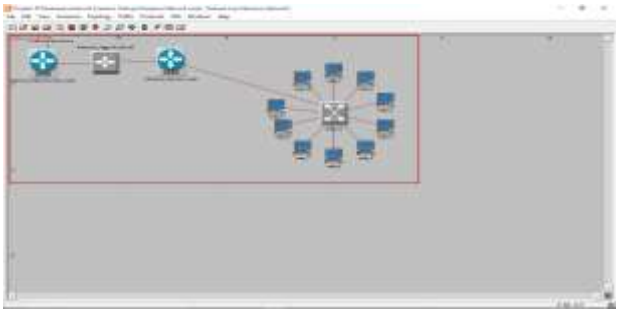

Figure 4.5: Adamawa Office Network Infrastructure (Nigeria)

Figure 4.6: Abuja HQ Network Infrastructures (Nigeria)

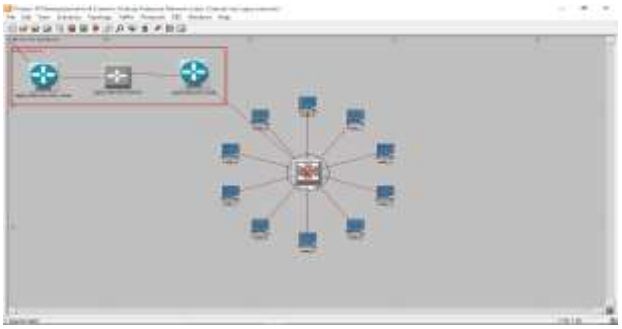

Figure 4.7: Lagos Office Network Infrastructure with a broken link from all system nodes

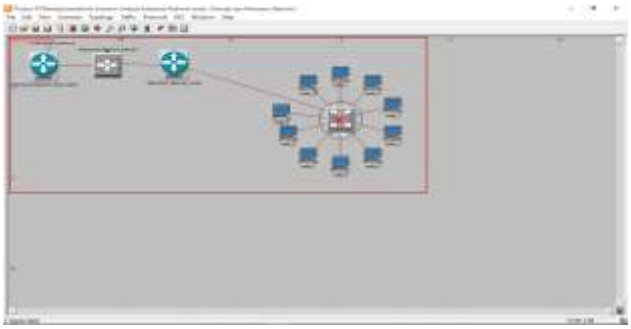

Figure 4.8: Adamawa Office Network Infrastructure with a broken link from all system nodes

Figure 4.9: Abuja HQ Network Infrastructure with a broken link to the firewall or without a firewall

Figure 4.10: Abuja HQ Network Infrastructure with a broken link to all system nodes

DOI: 10.31695/IJASRE.2019.33602

4.4 Introducing Fault Tolerance

The above network is not fault tolerant. We therefore, proposed fault tolerant using adaptive strategy based on introducing of redundancy. We intend to make the entire network adaptive by introducing alternatives such as switch, router and server redundancy. This will definitely eliminate a single point of failure, server unreachable and network failure. The plan is described in the next sections.

Redundancy

Redundancy is the key property of an enterprise network. Enterprise networks are designed in such a way that for every path there must be an alternate one. In case a node or a link goes down, the Enterprise networks are equipped with backup routes. Hence it is only a matter of seconds for back up routes to be discovered and the network to be back on track.

Router Redundancy

Router Redundancy is an important property of an Enterprise network. It is a method which is extensively used in enterprises. Basically, Hot Standby Router Protocol removes the need for the old design called "router on a stick". Once we have this protocol running the fear of a single point of failure is completely eliminated. A back up default gateway becomes available.

Alternatively, one can consider Virtual Router Redundancy Protocol (VR RP) and Common Address Redundancy Protocol (Open Source).

4.5 Network Evaluation for Fault Tolerance

The network designed above is non-fault tolerant; any fault in the link may obstruct the parts of the network. Figure 4.3 – 4.6 represents the flow of packets per second submitted and forwarded respectively to the transport layer by the FTP, Http, Email and Database Application. Figure 4.10-4.11represents the average packets per second forwarded to the FTP, Http, Email and Database. It can be inferred from the graph that the server traffic sent for FTP, Http, Email and Database is equal to the traffic received but at different time interval thus there was no packet loss.

Figure 4.11: Non-fault tolerant analysis based on traffic sent to servers.

Figure 4.12: Non-fault tolerant analysis based on traffic received from servers.

4.6 Performance Analysis

5. RESULT ANALYSIS FOR FAST ETHERNET

After creating the network models, run the Configure Discrete event simulation for 1hour. Then result of Scenario-1 of 30 Ethernet users for Global Statistics is as shown in Fig. 4.11-4.12. It is observed that the throughput range when 30 users are deployed is about 3,000 to 10,000 bits/sec. In this VLAN, ethernet16_switch is used which shows better performance when maximum 30 users are connected. So, increasing the number of users or failed resources will affect the performance and throughput of the network. Throughput increases and decreases relative to collision count and traffic at that time. During large traffic, the rate of collision count increases which further affects the throughput of the system. For scenario:1-6 as shown in Fig. 4.13 when the number of users is increased to 100 and also failed resources, the throughput in less as compared to previous scenario because more overhead and delay is encountered.

DOI: 10.31695/IJASRE.2019.33602

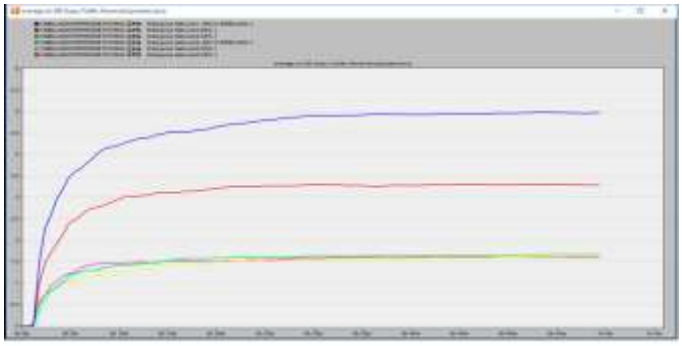

Figure 4.13a: Network scenarios for Db traffic received from servers

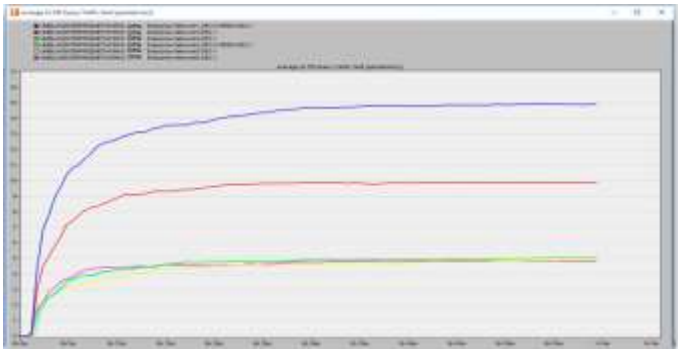

Figure 4.13b: Network scenarios for Db traffic sent from servers.

Comparing Throughput of Fast Ethernet with different resources in an Enterprise Network

While comparing throughput graph of Fast Ethernet in scenario:1-6 of 30 and 100 users and varying resources, the overlaid table and graph appears as shown in Fig. 4.14 and table 1.

Table 1: Parameters for Scenario simulations

Scenario	Resources	Congestion	Speed: packet/secs
PCN Enterprise Network router Scenario:1	6 routers, 3 switches, 3 firewall, 30 nodes, 4 servers, 3 subnets	0.23226	• 19.448 --> • 10.923 <--
PCN Enterprise Network Scenario:2	4 routers, 2 switches, 2 firewall, 20 nodes, 4 servers, 2 subnets	0.22888	• 19.161 --> • 10.754 <--
PCN Enterprise Network Scenario:3	2 routers, 1 switches, 1 firewall, 10 nodes,4 servers, 1 subnet	0.23111	• 19.348 --> • 10.869 <--
PCN Enterprise Network Scenario:4	6 routers, 3 switches, 3 firewall, 30 nodes, 4 servers, 0 subnets	0.22473	• 18.815 --> • 10.561 <--
PCN Enterprise Network Scenario:5	4 routers, 2 switches, 2 firewall, 20 nodes, 2 subnets	0.22005	• 18.423 --> • 10.345 <--
PCN Enterprise Network Scenario:6	No resource	-	-

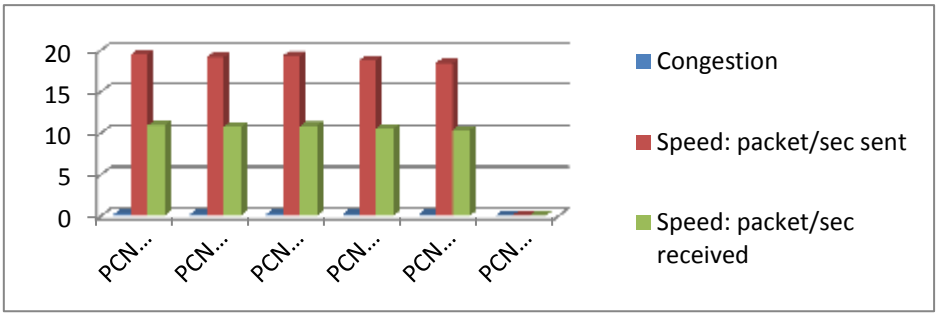

Figure 4.14: The graph of various scenarios and their congestions and speeds (packets/sec)

DOI: 10.31695/IJASRE.2019.33602

The simulated model for hybrid enterprise networks for large organizations is fault tolerant at scenario 1 using all the resources such as 6 routers, 3 switches, 3 firewall, 30 nodes, 4 servers, 3 subnets with a congestion of 0.23226 and packet speed of 19.448 for packet sent and 10.923 for packet received.

5. CONCLUSION

We modeled an enterprise network using OPNET modeling tool, the academy version. We modeled a non-fault tolerant network, we then simulate it to evaluate and make some research discovery served as the motivation for our research work.

In this research, two techniques are proposed to provide fault tolerant system by the employment of redundant component. This has been evaluated using different scenarios as presented in the paper.

By analyzing the presented graphs, it is verified that an enterprise network with different network topology and redundancy perform better. The simulated model for the enterprise networks for large organizations is fault tolerant at scenario 1 using all the resources such as 6 routers, 3 switches, 3 firewall, 30 nodes, 4 servers, 3 subnets with a congestion of 0.23226 and packet speed of 19.448 for packet sent and 10.923 for packet received and found to be fault tolerant to node and link failure.

The research has also identified that introducing network adaptive equipment and system can sustain and provide a robust fault tolerant system.

REFERENCES

1. Abduljalil Mohamed (2009). Fault Detection and Identification in Computer Networks: A Soft Computing Approach. A Ph.D. thesis presented to the University of Waterloo
2. Adam Meyerson, Kamesh Munagala, Serge Plotkin (2008) Cost-Distance: Two Metric Network Design. 41st IEEE Symposium on Foundations of Computer Science.
3. Behrouz A. Forouzan (2007). Data Communications and Networking - Fourth Edition. Publisher: Alan R. Apt, ISBN-13 978-0-07-296775-3 ISBN-to 0-07-296775-7
4. Bilel Ben Romdhanne, Navid Nikaein and Christian Bonnet (2010). Coordinator-Master-Worker Model for Efficient Large
5. Bradley Mitchell (2017). Introduction to LANs, WANs and Other Kinds of Area Networks.https://www.lifewire.com/lans-wans-and-other-area-networks-817376 Retrieved on 6/19/2017
6. Constantino Carlos Reyes Aldasoro (1994). An Algorithm for Calculating the Reduced Costs on a Graph. MSc. Thesis, Department of Electrical and Electronic Engineering Imperial College of Science Technology and Medicine University of London
7. ITU-T (2008). New global standard for fully networked home (http://www.itu.int/ITU-T/newslog/New+Global+Standard+For+Fully+Networked +Home.aspx), ITU-T, 2008-12-12, retrieved 10-03-2017
8. John Sullivan (2000). Network Fault Tolerance System. A Thesis for the Degree of Master of Science, Electrical and Computer Engineering, Worcester Polytechnic Institute
9. Karthick Raghunath K.M, Rengarajan N (2013). Investigation of Faults, Errors and Failures in Wireless Sensor Network: A Systematical Survey. International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970) Volume-3 Number-3 Issue-12 September-2013
10. Muriel Medard and Steven S. Lumetta (2002). Note on Network Reliability and Fault Tolerance. Massachusetts Institute of Technology & University of Illinois
11. Nitesh Kumar (2012). Fault Tolerant Enterprise Networks for Large Scale Organizations. National Institute of Technology, Rourkela Rourkela-769 008, Odisha, India
12. Personal Area Network (PAN) – Online resources Retrieved January 29, 2011 from http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci546288,00.htm.
13. S. Muhammed, & A.H Sadka 'Evaluation of H.264 AVC Coding Elements and New Improved Scalability/Adaptation'. . International Journal of Engineering Research Applications, Vol. 19, Issue 6, 2014.

DOI: 10.31695/IJASRE.2019.33602