Network Analysis of SZABIST

Syed Zohaib Ali and Dr. Husnain Mansoor Ali
husnain.mansoor@szabist.edu.pk
SZABIST
Karachi, Pakistan

Abstract: *SZABIST is increasingly becoming dependant on computer-supported information processing. This increasing dependency on computers for operational support poses the risks that a lengthy loss of these capabilities could seriously affect the overall performance of the Institute. In this independent study, the network of SZABIST is analyzed and assessed. In the network analysis, threat analysis and assessment, risk analysis and assessment and vulnerability analysis and assessment are done and finally, to mitigate the risks, the mitigation strategies are discussed. Strategies are proposed that keep the SZABIST network alive or keep all systems functioning in case of any threat or disaster.*

1. INTRODUCTION

Computer networks are becoming general items in office and in business environments [2]. Computer networks provide distributed systems and applications in both wide area and local area networks. There are two major issues that exist in computer networks and require deep analysis: the communication formation and the network management formation [1].

The central part of network analysis and its security is risk assessment and risk analysis [3]. The analysis helps us to understand the network behavior but for this we require both analytical and mock-up ways of analysis [4]. The design of appropriate inter-connected computer network for inter-connectivity and inter-process communication is one of the key issues with respect to network performance [5] and with the use of efficient and effective analysis we can resolve these issues readily.

In this independent study, the network of SZABIST is analyzed and assessed. To remove the flaws at SZABIST's network, strategies are proposed that keep the SZABIST network alive or keep all systems inter-connected in case of any threat or disaster. A plan is given in this study, which details the availability of alternative inter-connectivity solutions from different sources in case of disaster, threats and cyber attacks.

2. OPERATIONS

SZABIST, Karachi has two campuses 90 and 100 Clifton which are connected together via disparate devices and links. SZABIST has their own software house, which is called ZAB Solutions and there is another department of SZABIST which is called ZAB Net. The ZAB Solutions manages and maintains all applications which are used at SZABIST like: Finance, Academics, Examinations, ZAB Desk and Admissions. The ZAB Net manages and maintains the inter-connectivity of both campuses.

3. RISK MANAGEMENT

Risk Management is crucial and vital piece of any project, because different projects have always different types of Risks [6]. Risk management concludes and classifies how all risks can be handled in an activity. Risk management is an important aspect with respect to performance for any institute. We distinguish various types of Risks [7] to determine the association between risk management helpfulness and enterprise progress.

3.1 Risk Categorization

The proposed solution and architecture of SZABIST's network is designed to reduce the risk to an acceptable level by ensuring the restoration of critical processing and systems. For this, we first need to categorize different risks according to their importance.

3.2 Risk Assessment

The risk evaluation starts with the help of assessment of all possible threats [6]. In this phase, we assess the threats which could stop the connectivity between the campuses of SZABIST. The threats which we assessed after analysis and discussions with concerned officials of SZABIST are given below:

3.2.1 Natural and Environmental Threats

Natural and environmental threats or disasters can happen in any place. A regions geographical location establishes whether there is more of a probability of a cyclone or a flood [7].

3.2.2 Fire

Fires are caused by a wide range of events, some of which are intentional, some accidental, and some environmental. Intentional fires come under the banner of arson.

Now according to our study, if it occurs at SZABIST, either intentionally or accidentally at computer labs, server rooms or in cabling area/place, network connectivity of whole campus goes down.

3.2.3 Earthquake

Earthquake is very un-predictable threat and disaster, and when it happens above a thresh-hold value, almost 90% percent physical infrastructure collapse. Now God for bade, if such an event occurs in Karachi and SZABIST building collapses, all equipments and networks will be damaged and people from outside SZABIST or from within country or outside country cannot access the services of SZABIST like: Zabdesk, website, ftp and so on.

3.2.4 Human Threats

Human threats come up to in all dimensions and nature. We are forced to differentiate between planned and unplanned operations. The Human threats according to our study are defined below:

3.2.5 Theft

Theft is a planned operation done by staff, former staff, and visitors. According to our study, if there is any theft carried out, burglar can steal network equipments (Switches, Routers and Cables) and servers/computers.

3.2.6 Terrorism

There are different types of terrorism and in certain situations it cannot be stopped. If anyone blasts a bomb or deliberately cuts all fiber optic cables, all inter-connectivity of SZABIST, Karachi will be lost.

3.2.7 Fire (Arson)

Human-caused fires can happen indoors or outdoors. Fires are the most common disaster, so in spite of whatever planning we do, a fire can occur. If there is arson in cabling area, in server room and in labs, there will not any connectivity between both campuses. Now in these conditions students and staff will face service disruption.

3.2.8 Cyber Crime

The fast growth of information technology and the addition of computer and communication technology have made major modifications to human information actions [8]. Cyber crime is a growing area of study as privacy, honesty and accessibility these all come under the umbrella of cyber crimes. In the case of cyber crime, there will be number of attacks like: system hack, DOS attacks, spoofing attacks and etc. And people will face slow internet speed, less processing power and low bandwidth on LAN.

3.3 Threat Assessment

The threat assessment is a very important phase to search and point out the threat in organization by using a method which may be either quantitative or qualitative [7]. In this study, the qualitative method is used to asses and analyzes the threats. In this report, the frequency, likelihood level and impact of threats are also defined and discussed.

3.4 Vulnerability Assessment

Vulnerability is defined as the weakness, susceptibility, or exposure to hazards or threats [7]. Vulnerabilities in the case of network connectivity in the various areas of the IT systems are:

3.4.1 People and Technology

It is pointed out here that network analysis activities require research into the impact of people and technology. When risks were being assessed and analyzed, these two areas came into play.

- **People**
  As defined above, we assessed the vulnerability level with respect to some specific threats posed by people which helped us to propose solutions.
- **Technology**
  Here, it is assessed that what will be the level of vulnerability on technology with respect to number of threats.

3.5 Impact Analysis

An impact analysis measures utility analysis, in which a squad gathers data through interviews and documentary resources, documents tasks, actions and operations. This phase provides and identifies the critical processes.

3.6 Critical Components

This study for SZABIST is conducted to reduce the risks to an acceptable level by ensuring the restoration of critical processes within the recovery times mentioned below.

Critical components of Inter-connectivity infrastructure have been identified through performing impact analysis. The time requirements (table [1]) table is developed on the business functions supported by the inert-connectivity components and their recovery time objectives (RTO) and working recovery time (WRT) (see time requirements table).

3.7 Time Requirements

There time requirements table tells the calculated MTD (Maximum Tolerable Down-time) with respect to components.

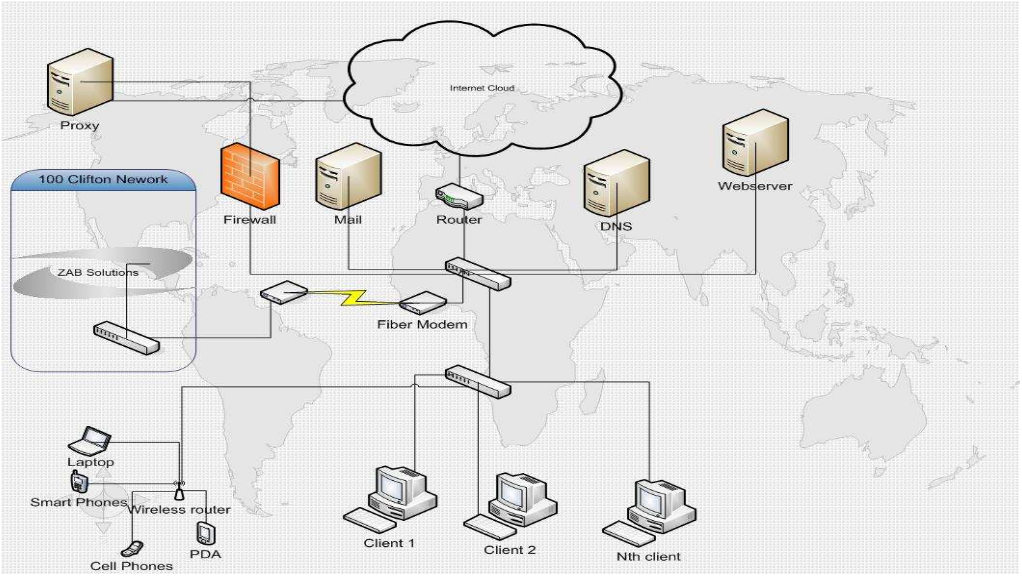
Table [1]: Time Requirements Table

	Component	RTO	WRT	MTD= RTO+WRT
Network	25 Switches (Cisco 2950 Series)	Immediate	1 hour	MTD=Approx 2 hours
	Router Cisco	Immediate	1 hour	MTD=Approx 2 hours
	CISCO PIX-501 Firewall	Immediate	1 .5hour	MTD= 2 hours
Applications /Servers	ZAB Desk	Immediate	4 hour	MTD= 5 hours
	SAS (SZABIST Admission System)	1 Day	2 hour	MTD= approx 1.5 days
	Examinations	4 Hours	3 hour	MTD= 7 hours
	Email Server	2 Hours	2 hour	MTD= 4 hours
	Antivirus Server	12 Hours	2 hour	MTD= 14 hours
	Internet /Gateway / Firewall Server (ISA 2000 Proxy Server Microsoft)	5 Hours	1 hour	MTD= 6 hours
	Web server	1 Day	2 hour	MTD=approx 1.5 days
Hardware	IBM X Series machines	Immediate	1 hour	MTD=Approx 2 hours
	Fiber Modem	6 Hours	2 hour	MTD= 8 hours

4. CURRENT ARCHITECTURE

There are many flaws in the current architecture which we found after assessment and analysis. We found some security issues, low–bandwidth issues, redundancy issues and so on. The detail about the current and proposed architecture is defined in **Mitigation Strategies and Proposed Architecture** section. For current architecture **see figure [1].**

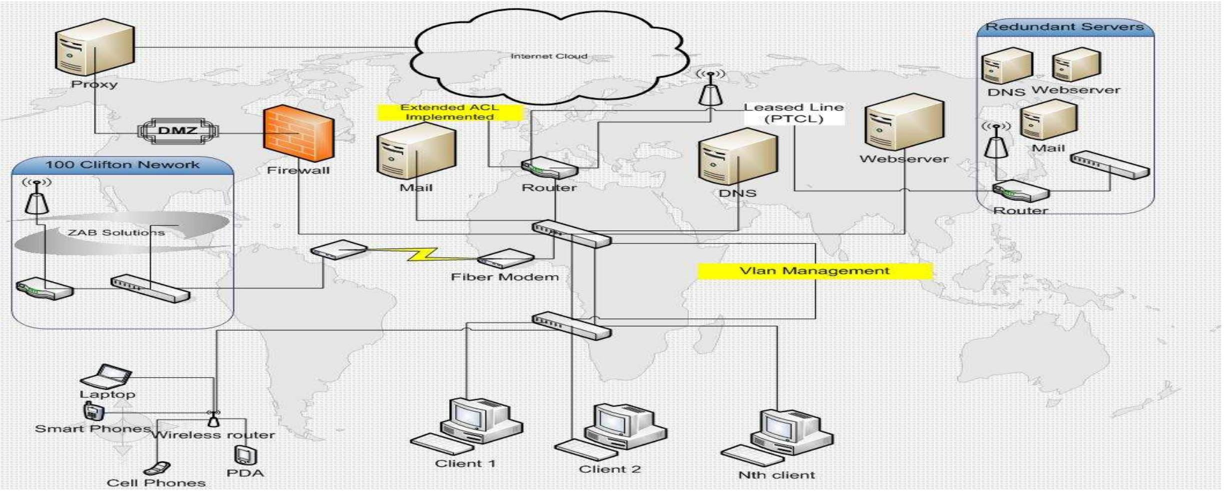
Figure [1]: CURRENT ARCHITECTURE FIGURE



5. MITIGATION STRATEGIES AND PROPOSED ARCHITECTURE

In the event of a major disruption in which the services are inaccessible or unusable, we propose the restoration strategy for SZABIST inter-connectivity. During the designing of proposed solution and architecture, we assessed the many risks, which can cause disruption after threat and disaster occurrence. They are defined below:

PROPOSED ARCHITECTURE FIGURE



- Redundant Link among switches
- DMZ
- Vlan
- Wireless Connection
- Redundant servers
- ACL (Access Control List)
- Server Operating System

6. REDUDANT LINK AMONG SWITCHES

(Current) Currently SZABIST has 25 switches, which are installed in both 90 and 100 campuses and all these switches are connected together. But in current situation there is no redundancy.
(Proposed) In this situation it is proposed that, there must be a redundant link among all switches. If current link goes down in case of any disaster or because of conges-

6.1 Dmz (Demilitarized Zone)

(Current) Currently in SZABIST there is just a Cisco firewall for security but there is no DMZ (demilitarized zone) layer.
(Proposed) A DMZ or demilitarized zone is an additional or logical network that is used by organizations to provide their services over the Internet. But in SZABIST there is no DMZ to maintain security measures and to control the security attacks and threats. We propose that there must be a DMZ for web servers, mail servers, FTP servers, and DNS servers so that no body from external network can get access to internal network except for the above services. Because SZABIST internal network contains confidential data and information like: Examination, Finance, academic and admissions.

6.2 VLANs (Virtual Local Area Networks)

(Current) Currently all 400-500 nodes present in SZABIST are on a single Vlan.
(Proposed) In the current situation, where all 400-500 nodes are on same Vlan, which is huge and can cause discontinuity of whole network and communication of SZABIST. This can happen as all nodes are on one large broadcast domain. The major advantage of VLANs is its flexibility to permit any logical LAN to be applied on any physical network [11]. Now it is one of universal truths that having many broadcast domains is good for our network. Now in the current situation we propose that there must be 5 to 7 Vlans at least as multiple Vlans reduce the broadcasts storms and congestion chances.

6.3 Wireless Connection

(Current) SZABIST has installed 4 fiber optics for inter connectivity of both 90 and 100 campuses.
(Proposed) In this current situation, if a disaster occurs or any terror attack happens and all 4 fiber optics are cut, then there will be no link available between both campuses. We propose that there must be another link like: SZABIST can take a leased line from PTCL or there can be a wireless link. In Pakistan many private companies provide very reasonable Wireless connectivity to connect one LAN to another LAN securely.

6.4 Redundant Servers

(Current) Currently in SZABIST, there is a department ZAB solution, which manages and maintains the all applications which are running in SZABIST. In ZAB solution they have one server for all these applications.
(Proposed) In current condition we propose that there must be at least two redundant servers so that if one goes down, other remains available. In this approach, the applications will not be stopped and there will be continuation of operations. Another proposed solution is that the redundant servers must be in another building or on another place.

6.5 ACL (Access Control List)

(Current) In SZABIST on router they have implemented ACL standard type for security reasons.
(Proposed) Here, to make network more secure, we propose that there must be ACL extended type implemented on router so that traffic of different requests and different types can be controlled.

6.6 Server Operating System

(Current) Currently, SZABIST operates all servers from MS- Windows Server- 2003.
(Proposed) We propose that the proxy server, mail server and web server must be made more secure and it must be ported to an Open Source systems like: Open Suse, Linux, Fedora etc, because these systems are more secure as compared to MS-Windows Servers.

7. CONCLUSION

In this independent study, the network of SZABIST is analyzed and assessed. In the network analysis, threat analysis and assessment, risk analysis and assessment and vulnerability analysis and assessment are done and finally, to mitigate the risks, the mitigation strategies are discussed.

To remove and reduce the flaws at SZABIST's network, strategies are proposed that keep the SZABIST network alive or keep all systems inter-connected in case of any threat or disaster. A comprehensive plan is given in this study. If all strategies and solution which are discussed in this study are applied, the network of SZABIST will become more secure and there will be less chances of failure.

8. REFERENCES:

1. "Computer network analysis"*Mathematics and Computers in Simulation*, Alberto Faro, Orazio Mirabella, Corrado Nigro Sciencedirect.com.
2. "Models and simulation for analysis of a computer network McAfee", L.C., Jr.; Circuits and Systems, Proceedings of the 36th Midwest Symposium.1993. IEEE Conferences.
3. "A risk assessment method of the wireless network security" Zhao Dongmei, Wang Changguang and Ma

Jianfeng Journal of Electronics (China), 2007, Volume 24, Number 3, Pages 428-432

4. "On the analysis and modelling of computer communication systems", Ivan Hanuliak. Kybernetes, (2002) Vol. 31 Iss: 5, pp.715 – 730
5. "Design and Reliability Analysis of a new Fault-tolerant Multistage Interconnection Network" Rinkle Aggarwal, Lakhwinder Kaur, Himanshu Aggarwal Department of Computer Science & Engineering,
6. "Enhancing RiskManagement with an efficient risk identification approach". Barati, S.; Mohammadi, S.; Management of Innovation and Technology, 2008. ICMIT 2008. 4th IEEE International Conference on Publication Year: 2008 , Page(s): 1181 - 1186
7. The impact of riskmanagement effectiveness on Power Utility performance" Jakasa, T.; Bedenik, N.O.; Iliopoulos, F.; Bratic, D.; - 5th International Conference on the European Electricity Market (IEEE) Publication Year: 2008 , Page(s): 1 - 6
8. "Cybercrime and challenges for crime investigation in the information era" Lee, H.C.; Intelligence and Security Informatics, 2008. ISI 2008. IEEE Publication Year: 2008 , Page(s): xxv - xxvi
9. "Throughput efficient solution for hybrid wireless network" Nadeem, F.; Leitgeb, E.; Awan, M.S.; Khan, M.S.; Kandus, G.; Satellite and Space Communications, 2008. IWSSC 2008. IEEE Publication Year: 2008 , Page(s): 316 - 320
10. "From Trees to DAGs: Improving the Performance of Bridged Ethernet Networks" Avin, C.; Giladi, R.; Lev-Tov, N.; Lotker, Z.; Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE Publication Year: 2009 , Page(s): 1 - 6
11. "Inference of network-wide VLAN usage in small enterprise networks" Sripanidkulchai, K.; Issariyapat, C.; Meesublak, K.; Publication Year: 2008 , Page(s): 1 - 4 IEEE.
12. "Case Study: Visualization Methodology For Analysing Network Data" Doris Wong Hooi Ten and Sureswaran RamadassNational Advanced IPv6 Centre (NAv6)Universiti Sains MalaysiaPenang, Malaysia. IEEE,2010
13. "Visualization of Network Components for Attack Analysis" Hoin Kim, Inyong Lee, Jaeik Cho, Jongsub Moon. IEEE,2009