# Applying Reliability Solutions to a Cooperative Network

Qutaiba Ali, Salah Alabady, and Yehya Qasim
Computer Engineering Department, University of Mosul, Iraq

**Abstract:** *Reliability is one of the most important concepts in computer networks field. Any network must be supplied with different techniques and methods to guarantee its continuity and functionality under the most sever circumstances. This paper highlights the steps taken at the University of Mosul to enhance the reliability of its computer network. Firstly, the current topology of the network is examined and its resources are investigated. Our methodology suggests supplying the network with different techniques to enhance its robustness, such as, Link redundancy (using Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP) or Etherchannel Technology with different network topologies), Server Redundancy, Redundant switch components , Dual power input and standby Wireless LAN in case of sever cabling failure. The affectivity of the suggested solutions and their impact of the network behavior were tested using an experimental network.*

**Keywords:** *Network reliability, redundancy, recovery time, spanning tree protocol, rapid spanning tree protocol, etherchannel*

*Received December 16, 2008; Accepted February 22 2009*

## 1. Introduction

Survivability, also known as terminal reliability, refers to keeping at least one path between specified network nodes so that some or all of traffic between nodes is routed through. Survivability in high capacity cooperative networks is crucial as failure of network component such as nodes or links between nodes can potentially bring down parts of the network, as happened in some real-world cases. Adding redundant network components increases the survivability of a network with an associated increase in cost [1-3].

In this paper, different reliability solutions were presented and intended to be applied to Mosul university network. Mosul university network was established in 2004. The purpose of the network is to connect the different locations of the university by a high speed (1 Gigabit Ethernet) links. The network introduces several services to its client (2200 user in 2008), such as internet sharing, Email accounts, web hosting and internal chatting. The future may witness its application to be extended to cover more sophisticated fields such as database sharing and interactive multimedia applications. The topology of the basic installation of the network is shown in Figure (1). The Description of the different network devices and its current configuration are listed in Table (1).

The network consists of (41 Cisco 3750 & 2950) switches connected (via 1 Gbps Ethernet) to the Cisco 6051E core switch. These switches represent different university departments. Each switch is connected down to many layer 2 switches and different department's hosts. The connection to the internet is achieved through the Private Internet eXchange (PIX515E) device (which act as a firewall) and the Cisco2800 Network Address Translation (NAT) router.

The internet service of the network could also be accessed through several IEEE802.11b WLAN connections It is obviously clear that network availability concepts have not been considered during the installation of the network. In numerous occasions, the failure of an optical cable prevents wide sector of network clients from accessing it to make use of its services. Thus, it is important to insert different reliability methods in a transparent fashion without affecting the performance of the network.

Table 1. Current Configuration of Network Devices

| DEVICE NAME | QTY. | DESCRIPTION | CURRENT CONFIG. |
|---|---|---|---|
| Cisco Router 2800 | 1 | ●2 Fast Ethernet ports, 2 serial ports<br>●IOS=12.3<br>●Support=Rip1,Rip2,EIGRP,IGRP,OSPF,IS-BGP,VPN,VLAN,VTP | ●Dynamic Routing= IGRP<br>●Extended access list,Static NAT<br>●No Encrypted Password |
| Cisco Switch 2950 | 30 | ●Layer 2 switch<br>●24 Fast Ethernet ports<br>● IOS=12.3<br>● VLAN, VTP | ●1VLAN/Switch<br>●No Encrypted Password |
| Cisco firewall(PIX) 515E | 1 | ●3 Fast Ethernet ports,2 serial ports, IOS=7.21 | ●Access-list<br>●Static NAT<br>●Default configuration |
| Cisco Core switch 6051E | 1 | ●Layer 3 switch<br>●3 modules (fiber optic, Gigabit Ethernet, Fast Ethernet,48 port)<br>●IOS=12.4 | ●(50)Port Based VLANS<br>●Extended access-list<br>●Encrypted Password |
| Cisco switch 3750 layer2 switch | 11 | ●24 Fast Ethernet ports<br>●2 Gigabit Ethernet Ports<br>●IOS=12.4 | ●1VLAN/Switch<br>●No Encrypted Password |
| Antivirus Server | 1 | ●DELL POWER EDGE 6600 SERVER | ●Password required |
| Access point | 1 | ● AP 1200 | ●64 bit WEP<br>●MAC Address Filtering |

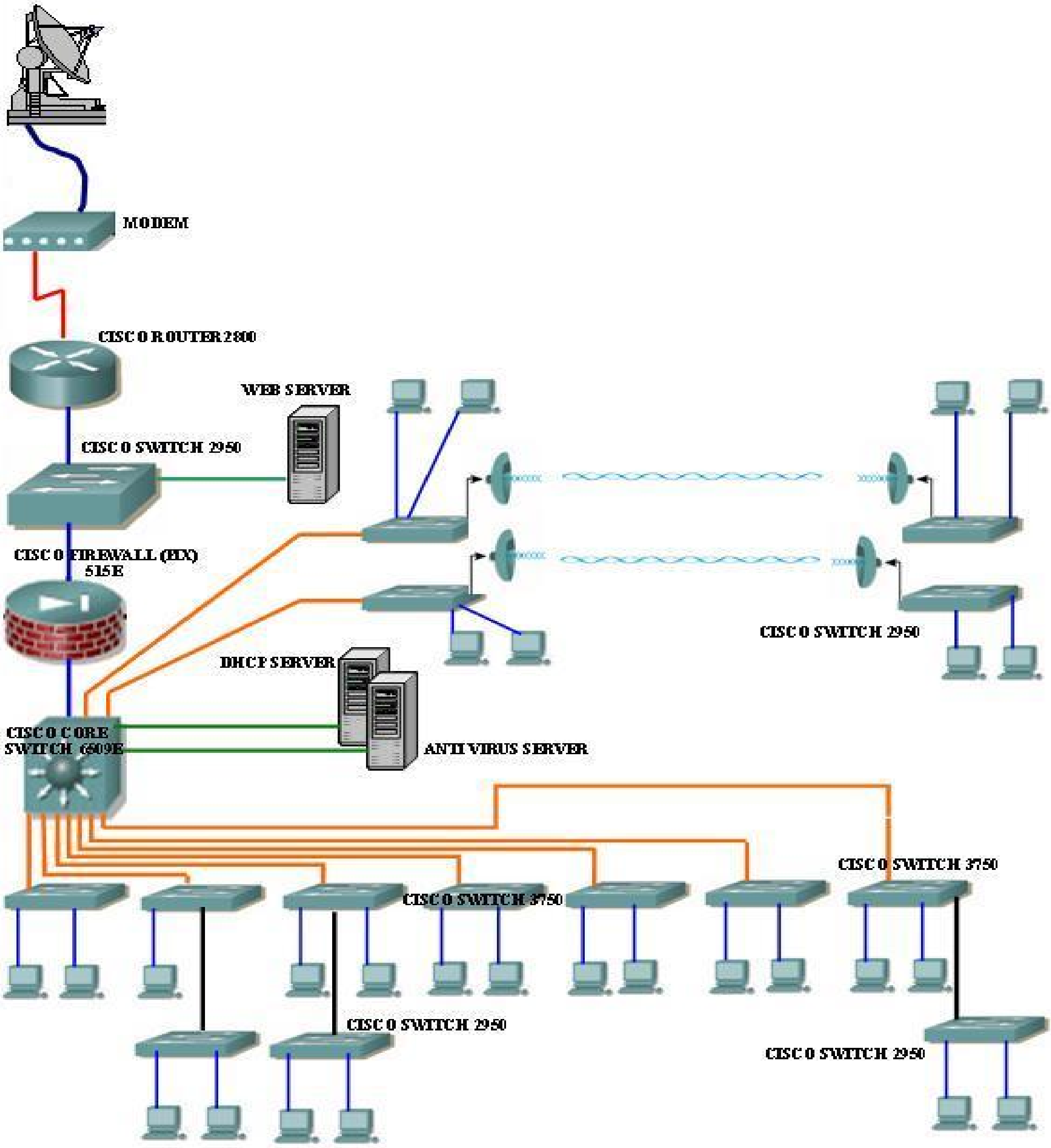

Figure 1. Topology of Mosul University Network

## 2. Related Work

Many papers have been published in the field of network reliability. Hui-Ling Liu and Shooman M.L. [4] describe simulation programs for packet switching networks with model congestion, routing and link failures. A computer network is modeled by a graph consisting of nodes (computers) and links (communication lines). Various routing rules (algorithms) are stored at the nodes to continue communication, via alternate paths, when congestion and/or link failures occur. Tongdan Jina and David W. Coitb [5] proposed an algorithm to approximate the terminal-pair network reliability based on minimal cut theory. Lynn et al. [6] discussed methods and approximation algorithm reliability analysis. Network reliability implies the search for algorithms that effectively calculate the reliability of any general network configuration provided that the reliabilities of components (or links) are known. Harms et al. [7] provided a comprehensive review of current combinatorial algorithms. Because the computation cost of exact methods increases exponentially as the network size increases, significant efforts were made to search reliability bounds. Tang J. et al. [8] used Bayesian approach used to derive the posterior reliability distribution based on prior information of components or the system. Mastran and Singpurwalla [9] estimated the moments of coherent system reliability estimates based on attribute test data from component level. Gary Hardy et al. [10] proposed an algorithm based on Binary Decision Diagram (BDD) for computing allterminal reliability defined as the probability that the nodes in the network can communicate to each other, taking into account the possible failures of network links. The effectiveness of this approach is demonstrated by performing experiments on several large networks represented by stochastic graphs. Jain, S.P. and Gopal, K [11] defined and evaluated Global reliability of a network using spanning trees of the network graph. An algorithm for generating spanning trees (termed, appended spanning trees) that are mutually disjoint is proposed. Each appended spanning tree represents a probability term in the final global reliability expression.

This paper focuses on suggesting a methodology for the transparent addition of various reliability solutions to a previously installed network. In the following sections, several methods and techniques were examined in order to select the best method to serve the purpose of building highly available and more robust network.

## 3. Links Redundancy

### 3.1. Introduction to Spanning Tree Protocol (STP) and Rapid STP (RSTP)

The IEEE 802.1D standard Spanning Tree Protocol (STP) has been available for use with managed switches and bridges for several years. This software provides a mechanism for resolving redundant physical connections in order to maintain operation of standard Ethernet LANs that does not allow more than one path for a packet to be in use at a given time. The Spanning Tree Protocol is included with the managed switch software provided by all major Ethernet managed switch product suppliers, and is widely available in the marketplace. Further, STP has proven in general use over many years to be interoperable, and commercial systems utilizing products from multiple vendors are routinely implemented. Standard STP supports redundant configurations of any type: meshes or rings or combinations [2].

Ethernet switches operate by forwarding traffic between their ports. The switch examines each Ethernet frame and records (learns) its MAC address and the port upon which it resides. When a frame arrives for a given MAC address, the switch decides on which outgoing port to send it. If a frame arrives and its destination MAC address is unknown, the switch will "flood" the frame out all of its ports [3].

If switches in the network are connected in a loop a ‘broadcast storm’ will result where a single broadcast frame will circulate endlessly. This condition consumes all available bandwidth on the loop making the network unusable [12].

The Spanning Tree Protocol (IEEE 802.1D) was designed to solve the fundamental problem of traffic loops. The key idea in STP is to prune (looping) links in order to reduce the network topology to that of a tree. The resulting tree "spans" (i.e. connects) all switches, but eliminates loops. The steps in order to best accomplish this process are [2]:

1. Allowing all switches to send messages to each other that convey their identity and link "cost".
2. Electing a single switch, among all the switches in the network to be a "root", or central switch.
3. Permitting all other switches to calculate the direction and cost of the shortest path back to the root using messages received from switches closer to the root. Each switch must have only one way to forward frames to the root.
4. If two switches servicing the same LAN exchange messages with each other, the one with the lowest cost to the root will service the LAN. The other switch will discard all frames received from that LAN, thus opening the link and blocking a traffic loop.

The STP protocol has proved to be the tried and tested method for providing path redundancy while eliminating loops. The STP protocol does suffer from a number of drawbacks that limit its applicability, namely [13]:

- STP has lengthy failover and recovery times. When a link fails in STP, a backup link to the root requires at least 30 second to recognize that it is the best (or only) path to the root and become usable (actions of different timers of the protocol).
- When a failed link returns to service, information about the "better" route will instantly cause a backup link to start blocking. But the portion of the network below the link that is returning to service will be isolated (for about 4 seconds) until that link becomes forwarding.
- Another problem with STP is that it requires that all links must pass through a lengthy period of address learning, even if the link is a point-to-point link to a device such as an ordinary PC.

As an Alternative, Rapid Spanning tree protocol (RSTP IEEE802.3W) was suggested to solve STP's problem with failover time by a number of means. Whereas STP switches store only the best path to the root switch, RSTP switches store all potential paths. When links fail, RSTP has pre-calculated routes to fall back upon. Additionally, unlike STP switches, an RSTP switch will respond to another switch that advertises an inferior or incorrect route to the root switch. This information allows the switch with incorrect information to be rapidly trained [14].

RSTP solves STP's problem with lengthy recovery time by introducing a procedure called proposing-agreeing. Proposing and agreeing works after a better path to the root is restored by "shuffling" the restored part of the network one hop at a time towards the network edge. This method also enables the network to come up quickly at inception. RSTP also introduces a method for quickly bringing up ports at the edge of the network, while still protecting them against loops. If the port is designated as an "edge" type of port, RSTP will continue to send configuration messages out the port (in order to detect loops) but will allow traffic to flow as soon as the port rises. In the event of a loop, some looped traffic may flow before RSTP quickly seals the network. PC's connected via edge ports can send traffic without the extensive delays imposed by RSTP [15].

## 3.2. Etherchannel Technology

EtherChannel technology builds upon standards-based 802.3 full-duplex Fast Ethernet to provide network managers a reliable, high-speed solution for the campus network backbone. EtherChannel technology offers bandwidth scalability within the campus by providing full-duplex increments of 200 Mbps to 8 Gbps [16-17]. Fast EtherChannel and Gigabit EtherChannel port bundles allow grouping multiple Fast or Gigabit Ethernet ports into a single logical transmission path between a switch and a router, server, or another switch. Depending on the hardware, EtherChannel can be formed with up to four compatibly configured Fast or Gigabit Ethernet ports on the switch. All ports in an EtherChannel must have the same speed [16-17]. The switch (which supports EtherChannel) distributes frames across the ports in an EtherChannel according to the source and destination Media Access Control (MAC) addresses. The operation that determines which link in an EtherChannel is used is very simple. A connection across an EtherChannel is determined by the source - destination address pairs. The switch performs an X-OR operation on the last two bits of the source MAC address and the destination MAC address. This operation yields one of four possible results: (0 0), (0 1), (1 0), or (1 1). Each of these values points to a link in the EtherChannel bundle. Also, various load balancing techniques is used to guarantee fair distribution of traffic between the channels. When the load on a channel exceeds (1%) of its capacity, it is directed to other less load channels [16-17]. EtherChannel technology provides many benefits such as high bandwidth, load sharing and redundancy. This technology provides load balancing and management of each link by distributing traffic across the multiple links in the channel. Unicast, multicast, and broadcast traffic is distributed across the links in the channel. [8-9]. This technology provides redundancy in the event of link failure. If a link is cut in an EtherChannel, traffic is rerouted to one of the other links in less than a few milliseconds, and the convergence is transparent to the user [16-17].

## 3.3. Experimental Setup

In this section, different techniques are used to enhance the links availability of an experimental network. This network was built to represent a model analogue to that of Mosul university network, see Figure (2). The purpose on these experiments is to find the optimum method in terms of resistance to failures and recovery time.

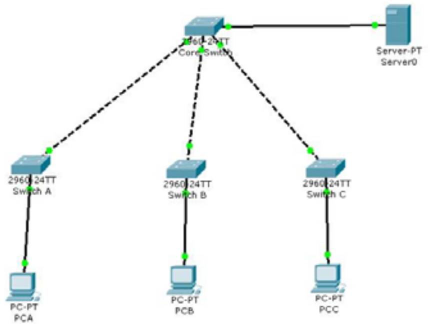

Figure 2. Basic experimental setup

### 3.3.1. Using Ring Topology

A ring topology offers built-in link redundancy and is often the most economical in terms of interconnection costs. The popular method of implementing rings is distributed switch. The distributed switch method, or simple ring (See Figure 3), is employed when network connected clients are geographically distributed. The clients at each location are aggregated onto switches, which are organized into a ring. The connections between switches in the ring may be made using dual redundant links to obviate the possibility of failure at a fiber, connector or port level. Latency in ring networks tends to be greater than in tree networks. The network is tested when using spanning tree protocol and it is found that it takes (30 Sec.) to recover the network against a failed link. The green dots (as shown in Figure (3)) indicates “active port”, while red dots stand for “Blocked port”. On the other hand, using RSTP decreases the recovery time to *one* second only. When the original link restores its activity, STP needs (4 Sec.) to accomplish this task, while RSTP takes (30 mSec.) only to retrieve the original situation.

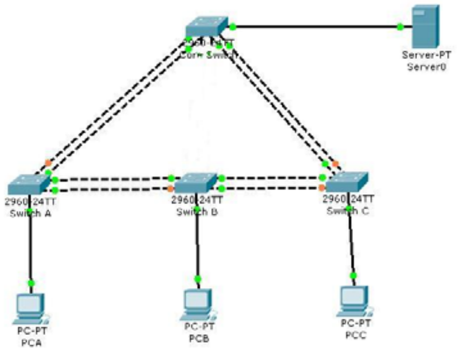

Figure 3. Dual link ring topology

### 3.3.2. Dual Link Star Topology

In this experiment, the reliability of star topology was enhanced using a second link in addition to the original link. The operation of both STP and RSTP causes activating one of the links while disabling the other, see Figure (4). Implementing STP on the network indicates that (30 sec.) is needed to recover the network and (4 Sec.) in the case of RSTP. The star topology provides less delay to the packets travels through the network and permits a central control fashion on the whole network.

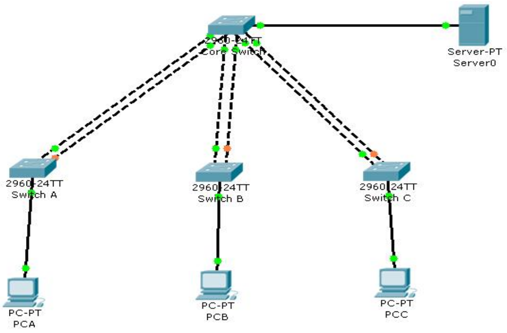

Figure 4. Dual link-star topology

### 3.3.3. Using Star-Ring Topology

In this experiment, more robust network is built by adding more redundant links to the network, see Figure (5). The recovery times in this situation is equivalent to the values mentioned earlier in the formal experiments. This topology suffers from higher costs due to the extensive wiring and installation difficulties.

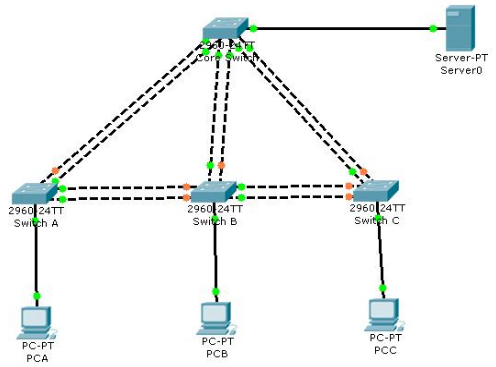

Figure 5. Dual star-ring topology

### 3.3.4. Using Etherchannel Technology

The arrangement shown in Figure (6) makes use of Etherchannel properties to enhance network reliability. In addition to the higher bandwidth provided by this technique, the failure of any link is recovered by less than (5 mSec.) in a transparent fashion to the packet transfer operation (only forwarding the packet to the second link). These brilliant result candidates Etherchannel to be the first choice in the proposed solutions.

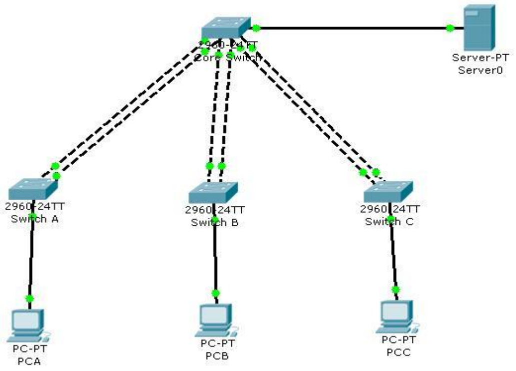

Figure 6. Etherchannel Technology

### 3.3.5. Using Etherchannel-Ring Topology

From the above experiments, the optimum solution could be obtained. The network topology shown in Figure (7) combines both star topology (supported by Etherchannel technology) with ring topology. This arrangement was configured to be subjected to RSTP operation, which disables the ports, denotes with the red dots.

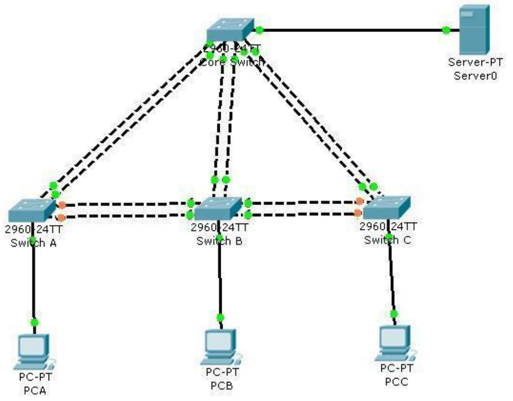

Figure 7. etherchannel-ring topology

This topology has three defense lines against links failure: Dual Etherchannel links and two redundant ring links. The fail over procedure could be accomplished in less time due to the benefits obtained from adopting Etherchannel technique.

## 3.4. Effect of Links Redundancy Solutions on Network Performance

In this section, the effect of different network recovery solutions on the network applications performance is investigated. Etherchannel-Ring topology is chosen, in which two nodes were ordered to exchange continuous Internet Control Message Protocol (ICMP) messages between them (i.e., PING command). The first case examines the effect of STP when one of network links fails. Figure (8) shows that the flow of data packets paused for (90 Sec.) until STP finish its path finding procedure.

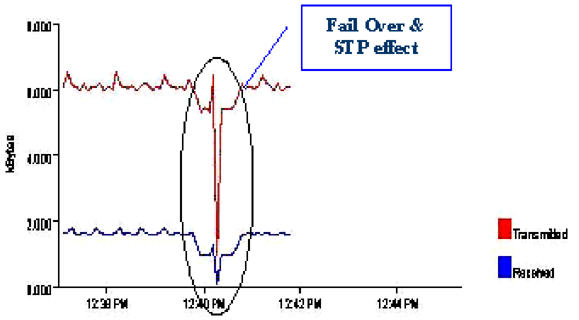

Figure 8. Fail over & STP effect on network performance

Repeating the above procedure in the case of using RSTP shows that (30 Sec.) is needed to retrieve the packet exchange procedure between the two nodes, see Figure(9).

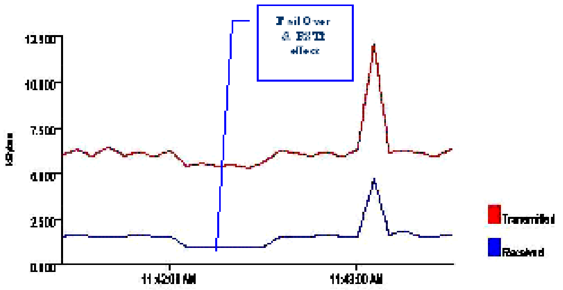

Figure 9. Fail over & RSTP Effect on Network Performance

The last issue to discuss in this section is the Etherchannel effect on the data transmission operation in the case of the failure of one of its links. Figure (10) shows that the failed link was replaced immediately by the second link in a transparent fashion to the packet transmission operation.

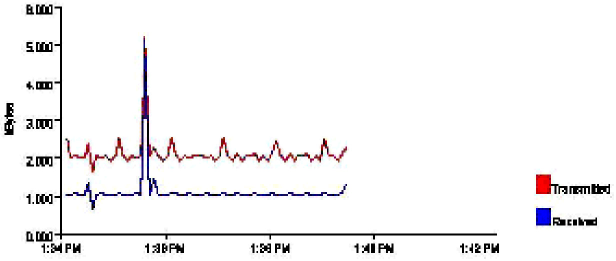

Figure 10. Etherchannel effect on network performance

Table (2) below, summarize the characteristics of the arrangements mentioned earlier.

When reflecting these solutions on Mosul university network, a compromise was achieved between the level of link redundancy and the required cost. The most important locations in the network (such as core switch, ISP and data sensitive locations) were supplied with Etherchannel-Ring topology, while Dual-Ring could be applied on the less important network sectors.

Table 2. Different redundancy solutions

| Topology | Redundancy | Relative Cost | Recovery Time | Afforded B.W |
|---|---|---|---|---|
| Star (No redundancy) | Low | Normal | Very High | Normal |
| Dual Star | Moderate | High | Moderate | Normal |
| Dual Ring | Moderate | Moderate | High | Normal |
| Dual Star-Ring | High | High | Moderate | Normal |
| Etherchannel | High | High | Low | High |
| Etherchannel-Ring | Very High | High | Low | High |

## 4. Recommendations towards the Establishment of a Reliable Network

In the previous sections, we have concentrate on different methods to supply the network with links redundancy. In this section, a discussion is made to consider the redundancy of other components of the network.

The design goal of a fault tolerant network should be to reduce the service interruption at service level, while keeping the total cost low. However one cannot provide an optimal solution to address both these needs. A sub optimal solution which can provide reasonable amount of reliability at reduced cost can be an achievable solution.

The major factor which helps in increasing the reliability is having no single point of failure in a system. Redundancy helps in avoiding a single point of failure in a system. Redundancy can be built into the system at various levels; typically it is at following levels. Each of the following helps in increasing the overall reliability of the network.

### 4.1. Redundant Servers

A server typically performs the functions of providing services in a network. Having a redundant server based architecture helps in achieving few milliseconds (specifically 7 msec. as measured in the Lab) fail over for the network. Needless to say this capability implies that any running applications can easily recover from server failover without any significant data loss. Having few millisecond failover time additionally helps in reducing system requirements (Because less data needs to be stored in the event of a server failure since the redundant server takes over in much less time). The benefits from redundant server architecture can be increased by having additional capabilities like online diagnostics (which help in predicting a server failure), design for synchronization of databases and state information (which help in newly active server know about the current on-going transactions and re-request the same for completion).In our system, the following servers must be redundant : DHCP server, E-mail server, Internet Service Providing(ISP) server, Data Storage server, security server, management server and antivirus server.

## 4.2. Redundant Switch Components

Having a redundant switch fabric implies that the system does not fail when an active switch fabric fails. In normal operation, when two switch fabrics in redundant mode are installed in a system, one is active and the other is in protection mode. The databases of both the switch fabrics are completely in sync indicating the same configuration for both of them. For a port, the incoming user data is routed to both the active and the redundant switch and however the outgoing data at each user port is selected to be from the active switch. In case of a failure of active switch, the other switch fabric board becomes active and user ports are instructed to select the outgoing data from the switch fabric which was working in protected mode earlier.

Also, a redundant power supplies in a switch can operate on load sharing principle, that is each power supply unit, though capable of supplying current requirement of entire system, still supplies typically one half of the current requirement, the other half being supplied by the other power supply unit. This helps in increasing the system reliability in two ways, firstly since each of the power supply operates at half of its rated capacity, its components are subjected to much less thermal stress (compared to scenario where it was operating at full rated load), secondly in the event one of the power supply completely fails, the other one takes over the function of supplying the full current requirement of the system and hence system operation is uninterrupted. The most important switches (must subjected to redundancy) in our network are: core switch, ISP Server switch, NAT router and switches lies in front of sensitive data locations.

## 4.3. Dual/Redundant Power Input

In this scheme, the system would have two redundant power input feeds, normal electricity and long live Uninterruptible Power Supply (UPS) unit. Having a dual power input would have the additional effect of keeping the system operational even if one of the power input feeds fail.

## 4.4. Standards Based Management Plane

Having a separate system management plane, which is different from the system control plane, helps in providing a dedicated management plane, which can isolate and report failures. It can help in capturing and reporting unusual events that can cause service disruptions. It supports user defined thresholds and allows the system manager to set early warning levels that allows him to react to a problem before it becomes catastrophic.

## 4.5. Using Standby Wireless LAN

In the event of a sever wiring failure, Wireless networks could be used to keep the network services a live until fixing the wiring system. The design work in this case involves the wise selection of access points locations, the transmitting power, antennas gain (and type) and suitable management plane.

For Mosul university network, the typical locations of access points, together with their transmitting power and antenna type are shown in table(3) and Figure(11).

Table 3. Suggested WLAN Settings

| | |
|---|---|
| AP Type | Wireless LAN Outdoor AP/Bridge Model No. SP915G<br>Support IEEE 802.11b and 802.11g wireless standards<br>Support WDS (Wireless Distribution System) up to 6 Links<br>Support multiple operation modes for access point, gateway, bridge and repeater |
| Output power | 20 dBm |
| Antenna types | 1- Model No. SP920PA2-24 , 2.4GHz Directional Antenna 24 dBi high gain to extend coverage.<br>2- Model No. SP920MA-12, 2.4GHz Omni-Directional Antenna<br>Provide 12dBi gain to extend coverage |
| Data Rate | 54Mbps auto fallback |
| Security | 64(40)/128-bit WEP Encryption, WPA, 802.1x and Access Control List |
| Frequency band and Radio Modulation | 2.4 GHz , DSSS / OFDM |

# 5. Conclusion

This paper describes the necessary steps to build a highly reliable network. Although, Mosul university network is chosen to be the subject of the study, the suggested redundancy methods could be applied on any other network. The design goal of a fault tolerant network should be to reduce the service interruption at service level, while keeping the total cost low. The major factor which helps in increasing the reliability is having no single point of failure in a system. Redundancy helps in avoiding a single point of failure in a system. Redundancy should be added to the system at various levels, such as link redundancy, Server Redundancy, Redundant switch components, Dual power input and standby Wireless LAN.

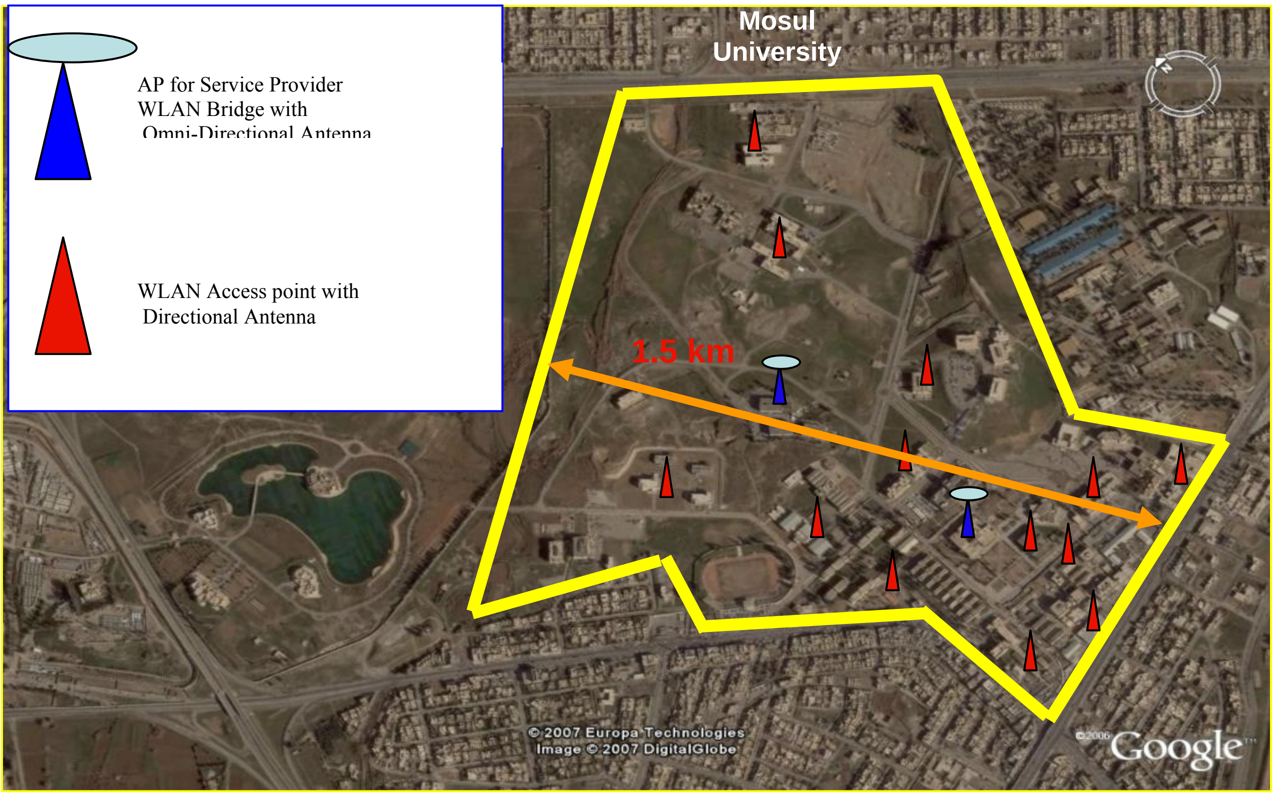

Figure 11. Map of the suggested WLAN system

## References

[1] Alex K., " Network Reliability and Resiliency in Next Generation Networks at Physical, Data link, and Network Layers ", *MSC Thesis* , Victoria University of Wellington, 2007.

[2] Forouzan B.,"*Data Communications and Networking*", 4'Th Edition, Mcgraw-Hill Publishing, 2006.

[3] Keiser G.,"*Local Area Networks*", Mcgraw-Hill Publishing, 1989.

[4] Hui-Ling Liu; Shooman, M.L. **"**Simulation of computer network reliability with congestion**",** *Reliability and Maintainability Symposium, Proceedings*, Annual Volume, Issue, 18-21, pp.208–213, 1999.

[5] Jina T., Coitb D., "Approximating network reliability estimates using linear and quadratic unreliability of minimal cuts" NJ 08854-8018, USA, 2003.

[6] Lynn N, Singpurwalla N, Smith A., "Bayesian assessment of network reliability. SIAM Rev; 40(2), pp. 202–227, 1998.

[7] Harms D, Kraetzl M, Colbourn C, Devitt J. "Network reliability: experiments with a symbolic algebra environment", Boca Raton, FL, CRC Press; 1995.

[8] Tang J, Tang K, and Moskowitzs H. "Exact Bayesian estimation of system reliability from component test data. Naval Res Logist, 44, pp127–46, 1997.

[9] Mastran D, Singpurwalla N. "A Bayesian estimation of the reliability of coherent structure", Oper Res, 26(4), pp 663–72, 1994.

[10] Hardy G., Lucet C., and Limnios N., "Computing all-terminal reliability of stochastic networks with Binary Decision Diagrams".

[11] Jain S. Gopal K., "An efficient algorithm for computing global reliability of a network", *IEEE Transactions on Reliability*, vol. 37, Issue 5, pp. 488 – 492, 1988.

[12] Tanenbaum A.,"*Computer Networks*", 4'Th Edition, Prentice-Hall Publishing, 2003.

[13] Stallings W. ,"*Data & Computer Communications,* "Sixth Edition, Prentice-Hall Publishing, 2003.

[14] Konak A. and Smith A., "A General Upper Bound for All-Terminal Network Reliability and Its Uses", *Proceedings of the Industrial Engineering Research Conference*, Banff, Canada, May, CD Rom format, 1998.

[15] Srivaree-ratana C., Konak A., and Smith A. "Estimation of all-terminal network reliability using an artificial neural network, "*Computers and Operations Research* 29 (7): 849–68, 2002.

[16] Cisco Systems,"*Internetworking technology handbook*", Indianapolis: Cisco Publication, (2001).

[17] Cisco Systems, "*packet-switching performance over the Fast EtherChannel bundle*" Cisco Publication, 2003.

**Qutaiba Ali** was born in Mosul, Iraq, on October ,1974. He received the B.S. and M.S. degrees from the Department of Electrical Engineering, University of Mosul, Iraq, in 1996 and 1999, respectively. He received his Ph.D. degree (with honor) from the Computer Engineering Department, University of Mosul, Iraq, in 2006. Since 2000, he has been with the Department of Computer Engineering, Mosul University, Mosul, Iraq, where he is currently a lecturer. His research interests include computer networks analysis and design, real time networks and systems, embedded network devices and network security and managements. Dr. Ali has attended and participates in many scientific activities and invited to be a member in many respectable organizations such as IEEE, IENG, ASTF and many others. Currently, he and has 20 published papers.

**Salah Alabady** was born in Mosul, Iraq, on October,1972, he received the B.Sc. degree in Electronic and Communications Engineering from the University of Mosul, Iraq in 1996, and in 2004 he received the M.Sc. degree in Computer Engineering from University of Mosul. From 2004 till now he is being a lecturer in Computer Engineering Department, Mosul University. His research interests include optical fiber communications, optical network architecture, network security and computer networks design. Alabady gets 10 certifications from Cisco Network Academy, and he is working as Instructor, Curriculum Leader, and Legal Main Contact in Mosul University Regional Academy for Cisco Network Academy program.

**Yahya Qassim** was born in Mosul, Iraq, on October ,1972, he received the B.Sc. degree in Electronic and Communications Engineering from the University of Mosul, Iraq in 1994, and in 2004 he received the M.Sc. degree in Computer Engineering from University of Mosul. From 2004 till now he is being a lecturer in Computer Engineering Department, Mosul University. His research interests include computer architecture & digital logic design using FPGA technique.