A Case Study on Comprehensive Renovation for a Corporate Network

Zuhair Ali[1], Maryam Shareef[2,] Shehryar Raza[3] Indrani Palanisamy[4]
Department of Computing,
Middle East College,
Sultanate of Oman.

***Abstract*-This exploratory case study gives an exposure to analyze and implement a way out to save appropriate amount of time and a cost effective solution for a corporate network. The initial phase of the study was carried out to identify the existing network system of a corporate network and finding a feasible way by removing all unnecessary clutter from the existing network infrastructure. During the study we identified that all the services are provided from separate physical servers and so there is a need for implementing virtualization concept for the servers which will be required to make better use of the hardware. This will be achieved by implementing virtualization of the services into one stable physical machine. These services include Active directory, DNS, DHCP, update, web, and file server spread across multiple virtual machines. Firewall and intrusion prevention system was recommended to protect the network from internal and external threats. Cisco VoIP will be implemented for telephony and conference call purposes. In order to handle live communication, Microsoft Exchange and Lync servers will be implemented for email and chat services. This case study covers all underline areas where issues exist and effective solution was provided to solve them and also to secure the network and modernize the network from its current outdated implementation. The significance of this exploratory study and the recommended solution for the comprehensive renovation of an organizations existing corporate network infrastructure makes us to better understand the day to day work environment complications and recommending a feasible solution based on the current technology to overcome such difficulties will help to create an influence for better development for comprehensive renovation for a corporate network.**

Keywords: Active directory, Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), Voice over IP (VoIP), Virtualization.

I. INTRODUCTION

The scope of this project is enhancing the new branch to function and communicate with the main branch. Reduce by removing all unnecessary clutter from the network. Currently all the services are provided from separate physical servers and so virtualization of the servers will be required to make better use of the hardware. This will be achieved by virtualization the services onto one physical machine. These services include active directory, DNS, DHCP, update, web, and file server spread across multiple virtual machines.

Firewall and intrusion prevention system will be implemented to protect the network from internal and external threats. Cisco VOIP will be implemented for telephony and conference calls purposes. Microsoft Exchange and Lync servers will be implemented for emails and chat services. Future implementation of DMZ will be established for security concerns.

II. PROBLEM DEFINITION

This project is about enhancing the main branch network as well as setting up the new branch office network. The new branch network infrastructure will need to be overhauled and connection between the two branches needs to be established. Emphasis on security, redundancy, and availability will be the focal point of this project. Removing unnecessary hardware, removal of clutter, virtualization, and organization will be implemented. Communication will be a big part of the company so implementation of Lync server and VOIP technology will be made.

III. REVIEW OF LITERATURE

A literature review is the process of researching case studies conducted by professionals and analyzing, summarizing and reviewing the case study. The case studies presented in this project are about the primary objectives of this project.

VLAN’s are network policies configured to group host under one common administrator without any physical intervention. The VLANs allow static links to communicate with physical network ports (Tariq, 2009). VLANs provide security, broadcast control and physical layer transparency all while being cost effective (Alexa 2013). The benefits of VLANs are they provide management flexibility and security policies, ability to apply group policies on large number of users, and isolate hosts into multi broadcast domains. Each port on a switch can be located on a different VLAN regardless of their physical location and enable users to receive ip addresses from one subnet even when they are not on the same switch or network (Garimella, 2007).

(Steinder, 2008) Server virtualization is the method of using virtual machines to create multiple servers or services onto as few physical servers as possible; ideally one physical server. The benefits are a reduction of clutter, increasing space, power consumption, and decrease in operational cost. Optimal use of hardware as well as the decrease in the number of physical machines tends to require less maintenance and replacement. VMs tend to unlock unused hardware capacity (Daniels J, 2009). VMware, MS HyperV, and VirtualBox are some of the best virtual machine software available on the market today (Eisen 2011).

Demilitarized Zone or DMZ is a physical or logical outer network of an organization which tends to contain the external services available to the internet. Usually the external network is placed inside the DMZ and the internal network is always hidden. The DMZ can be located remotely or on site. If there is an attack on the network at any given time only the DMZ will be affected and not the whole network (Sharma, R. K., & Mogha, R. 2002). For DMZ to be secure, the devices must communicate publically with the internet and be placed in the DMZ. The DMZ also requires support from the firewall and anti-spoofing technologies. The DMZ needs to be the perimeter network in the network topology (Mick, 2001).

IV. METHODOLOGY

(Sim Sim) Cisco hierarchical model is a network designed by cisco which separates corporate networks into three different layers. These layers are the core layer, distribution layer and the access layer. The benefits of using this network design are: high performance, efficient management, scalability, behavior prediction, and policy creation.

(Todd Lammle, 2004) The core layer is the central layer or backbone of the network design. All layers connect and rely onto the core layer. It is responsible for fast and reliable transportation of data within the network. The purpose of the core layer is to provide reliable fast speed connection to the other layers of the network (Dinicolo 2004).

Operational Feasibility is the study to find out whether the technology, hardware, and software operate and communicate with each other and whether the scope and objectives are operationally feasible.

The project in terms of its logical design is operationally feasible because MPLS can be configured on a Cisco 2811 router. That connection is available in Omantel and Omantel does provide the service. All of the hardware mentioned above do communicate well with each other because the network devices are from the same vendor; Cisco.

The DMZ is just sub-compartmentalization of the network. Microsoft exchange and Lync server work well with the other services being implemented. The hardware server is powerful enough to support the system and should operate well. There are enough data points provided to easily operate the entire user end points. VoIP is probably the only issue because it is not allow without permission by Omantel and Ministry of Information but with the permission VoIP will operate as excepted.

V. PROJECT PLAN

Communication Plan: The communication plan is a plan used to visualize and organize the communication in each phase of the project. The plan focuses on the key persons to communicate with, the means of the communication, and the frequency of the communication to insure the project objective are met. It is an important aspect of the project plan because it gives direction to the team and others involved in the project.

Acceptance plan: An Acceptance plan helps to demonstrate that all criteria are met by Zawaya Oman's Standards and that the project is a success. It allows the stakeholders to verify that the system works well and that the objectives are met.

Resource plan: The resource plan will help identify the different equipment and manpower required within the project. The details below will provide more information as to what resources are required in each phase and why.

Risk management plan: Risk Management plan is an important plan to have because it identifies the risks that can occur and affect the project. Planning ahead and creating a mitigation plan ahead of time will insure the project completes successfully without any issues.

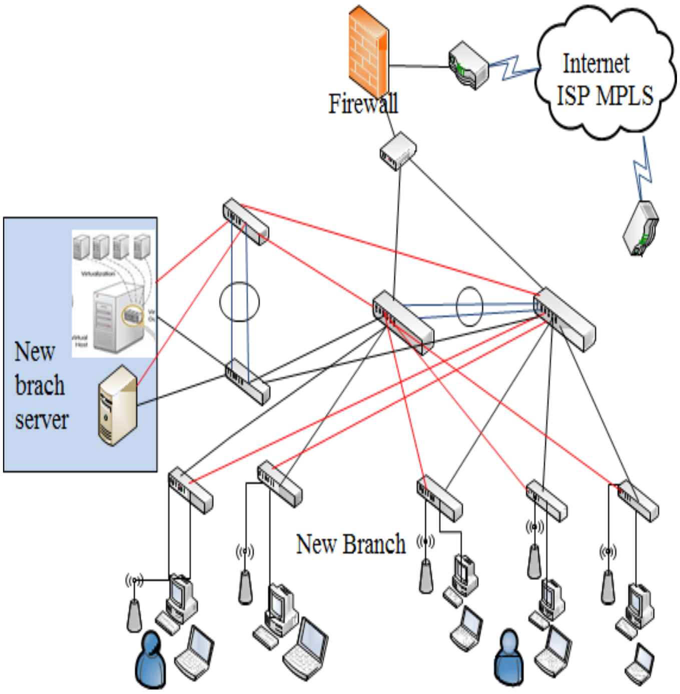

Fig-1: Logical Design

Block Design Networking: The design of the network contains principles of cisco hieratical model and the block design model. The fundamental rule of block design is to design the network as blocks or segments and allow for future extensions or "blocks" to be easily implemented into the network without causing design or hardware changes. It also provides for easier understanding of the network and a simplistic approach to logical designs without losing complexity. The network is segmented into three blocks here; The WAN, Collapse core, and Server Blocks.

Collapse Core: The collapse core is primarily used to reduce network cost with the added benefit of having the three tier cisco heretical model. A collapse core is basically fusing the distribution and core roles together. This minimizes the amount of switches needed and makes the core switches inside the collapse core work in unison with the distribution switches. In this design, four layer 3 switches are being used with the two outer switches playing the distribution role and the two inner switches playing both core/distribution roles.

The collapse cores are connected with each other using fiber optic cables using the ether-channel link method. The Ether-channel method is the use of multiple cables together to act as one link to maximize bandwidth and throughput. Redundant cables are connected to the distribution layer, access layer, and blocks to provide redundant paths in case of failure. These redundant cables are using the trunk method of implementation to allow for inter-vlan communication as well as avoid network loops. On the core switches, no packet filtering will be enabled to allow for fast packet delivery and low latency.

Distribution Layer: The Distribution layer will connect all layer 2 switches and work along with the collapsed core to provide connectivity to the access switches. Packet filtering, network policies, and access lists will be placed here to provide network security. If a distribution switch fails, the collapse core will take on the responsibility of the failed layer 3 switch. Trunk links are used to connect the access layer and collapsed core to it.

Access Layer: This layer will used to provide end user with network access. The switches are all layer 2 switches with redundant paths leading to the collapse core and distribution switches. These paths are trunk links and provide multiple Vlan communication to pass through the link. Access points, end users, and printers will be connected to the access layer. The Vlan information of the designated switches

WAN Block: The wan block contains a few network components: The MPLS cisco router, the cisco ASA firewall, and the fiber-optic Omantel router. The firewall will contain all the network security policies and be the gateway to both the main branch and the internet. The MPLS router will provide connectivity to the main branch and the Omantel router will provide internet access.

Server Block: The server block contains the virtualized servers of DC, AD, Exchange, Lync, Update, web, DHCP, and Hyper-V roles on the physical machines. The block is connected to the collapse core to allow for fast packet switching and all communication inside and outside the block is handled by the firewall or distribution layer respectively.

VI. CONCLUSION

Based on the success of the implementation of this project, it will enhance network performance, security, availability, scalability, and communication compared to its existing company network. Fast past communication and network throughput will increase productivity within the employees. MPLS connection will enable secure connection between the main branch and the new branch of Zawaya Oman. Virtualized services will become easier to manage and always available. Security will also be enhanced with Firewall and network device protection. Vlans will enable Zawaya Oman to group users according to their security and access policies. VOIP technology along with Exchange and Lync servers will provide enhanced communication within the organization. Redundancy, fault tolerance, and load balancing through Cisco network devices will enable and to stay connected and run more efficiently.

This project has increased my understanding of how corporate network work, configured, designed and implemented.

REFERENCES

1) http://www.ehow.com/facts_6729147_definition-manpower.html
2) Hucaby, D. (2010). CCNP SWITCH 642-813 Official Certification Guide. cisco.
3) http://grammar.about.com/od/il/g/literaturereviewterm.htm
4) http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_1-2/switch_evolution.html
5) http://www.solarwinds.com/solutions/exchange-server-monitor.aspx
6) http://bug-free-zone.blogspot.com/2006/11/responsibilities-of-test-engineer.html
7) http://itknowledgeexchange.techtarget.com/network-technologies/introduction-to-port-security-and-the-reasons-to-implement/
8) PRTG Network Monitor 7 -User Manual. (2008). Paessler AG.
9) Dong, Y., Duan , J., & Tian , K. (2012). Virtualization Challenges: A View from Server Consolidation. 15-25.
10) http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps5528/product_data_sheet09186a00801f3d7d.pdf
11) http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps6406/product_data_sheet0900aecd80322c0c.pdf
12) http://en.wikipedia.org/wiki/EtherChannel
13) ALouneh, S., En-nouaary, A., & Agrawal, A. (2007, August). A Multiple LSPs Approach to Secure Data in MPLS Networks. Journal of Network, 2, 4.
14) Brunner, M., & Quittek, J. (n.d.). Retrieved Nov 15, 2012, from http://www.brubers.org/marcus/papers/im01_mpls_cameraready_final_with_conf.pdf
15) Divakar. (2009, Nov 23). Testing World. Retrieved May 19, 2013, from http://testingworld-tools.blogspot.com/2009/11/why-do-we-need-software-testing.html
16) Francesco, P., & Fiore, U. (2007, Sebtermer). Enhanced security strategies for MPLS signalling. 2, 5.
17) [http://www.thegeekpub.com/787/defining-the-role-of-an-it-manager/
18) Howlett, T. (2005). Open Source Security Tools Practical Applications for Security.
19) Jose, S. (n.d.). Retrieved Nov 15, 2012, from http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/mxinf_ds.pdf
20) Koziniec, T. W., & Dixon, M. W. (2002). Using OPNET to Enhance Student Learning in a Data
21) Daniels, J. (2009). Server Virtualization Architecture and Implementation. CrossRoads, 8-12.
22) Communications Course. Informing Science, 349-456.
23) Keith, M. (2001, Jun 22). Retrieved 3 14, 2013, from http://www.mail-archive.com/fw-1-mailinglist@beethoven.us.checkpoint.com/msg02113.html
24) http://www.investopedia.com/terms/f/feasibility-study.asp#axzz2GWNfeEkm
25) Garimella, P., Wei, Y., Sung, E., & Zhang, N. (2007). Characterizing VLAN usage in an Operational Network.
26) http://www.cisco.com/en/US/prod/collateral/routers/ps5854/ps5882/product_data_sheet0900aecd8016fa68_ps5854_Products_Data_Sheet.html
27) http://www.ask.com/wiki/DMZ_(computing)
28) https://www.asbtdc.org/DocumentMaster.aspx?doc=1039
29) A Case Study on Comprehensive Renovation for a Corporate Network, Part of project @ Middle East College, Department of Computing, Sultanate of OMAN.