

University of Louisville

ThinkIR: The University of Louisville's Institutional Repository

Electronic Theses and Dissertations

8-2011

Data center resilience assessment : storage, networking and security.

Yehia H. Khalil Mohamed
University of Louisville

Follow this and additional works at: <https://ir.library.louisville.edu/etd>

Recommended Citation

Mohamed, Yehia H. Khalil, "Data center resilience assessment : storage, networking and security." (2011). *Electronic Theses and Dissertations*. Paper 996.
<https://doi.org/10.18297/etd/996>

This Doctoral Dissertation is brought to you for free and open access by ThinkIR: The University of Louisville's Institutional Repository. It has been accepted for inclusion in Electronic Theses and Dissertations by an authorized administrator of ThinkIR: The University of Louisville's Institutional Repository. This title appears here courtesy of the author, who has retained all other copyrights. For more information, please contact thinkir@louisville.edu.

**DATA CENTER RESILIENCE ASSESSMENT:
STORAGE, NETWORKING AND SECURITY**

By

Yehia H. Khalil Mohamed
B.Sc., Alexandria University, 1994
M.Sc., Arab Academy for Science and Technology, 2001

A Dissertation
Submitted to the Faculty of the
J.B. Speed School of Engineering of the University of Louisville
In partial Fulfillment of the Requirements
For the Degree of
Doctor of Philosophy

Department of Computer Science and Computer Engineering
J.B. Speed School of Engineering
University of Louisville
Louisville, KY

August 2011

**DATA CENTER RESILIENCE ASSESSMENT:
STORAGE, NETWORKING AND SECURITY**

By

Yehia H. Khalil Mohamed
B.Sc., Alexandria University, 1994
M.Sc., Arab Academy for Science and Technology, 2001

A Dissertation Approved on
08/08/2011

By the following Dissertation Committee members

Adel S. Elmaghraby, Dissertation Director

Mehmed Kantardzic

Anup Kumar

Michael Losavio

Bradley Ellison

ACKNOWLEDGEMENTS

This dissertation would not have been possible without the guidance and the help of several individuals who in one way or another contributed and extended their valuable assistance in the preparation and completion of this study.

Foremost, I would like to express my gratitude to my advisor Adel S. Elmaghraby for the continuous support of my Ph.D. study and research, for his patience, and motivation.

Besides my advisor, I would like to thank the rest of my thesis committee: Mehmed Kantardzic, Anup Kumar, Michael Losavio, and Bradley Ellison for their encouragement, insightful comments, and hard questions.

I would like to extend my warmest thanks to the Computer Engineering and Computer Science department staff for their great help and support.

I owe my loving thanks for my wife Eman Ahmed, my daughters Maryam and Malak and my son Khaled. Without their encouragement and understanding it would have been impossible for me to finish this work. My special gratitude is due to my mother, my sisters, and my brothers for their loving support.

This work was partially funded by a grant from the U.S. Department of Treasury through a subcontract from the University of Kentucky. The opinions and conclusion in this dissertation are the sole responsibility of the authors.

ABSTRACT

DATA CENTER RESILIENCE ASSESSMENT: STORAGE, NETWORKING AND SECURITY

Yehia H. Khalil Mohamed

8/8/2011

Data centers (DC) are the core of the national cyber infrastructure. With the incredible growth of critical data volumes in financial institutions, government organizations, and global companies, data centers are becoming larger and more distributed posing more challenges for operational continuity in the presence of experienced cyber attackers and occasional natural disasters.

The main objective of this research work is to present a new methodology for data center resilience assessment, this methodology consists of:

- Define Data center resilience requirements.
- Devise a high level metric for data center resilience.
- Design and develop a tool to validate and the metric.

Since computer networks are an important component in the data center architecture, this research work was extended to investigate computer network resilience enhancement opportunities within the area of routing protocols, redundancy, and server load to minimize the network down time and increase the time period of resisting attacks.

Data center resilience assessment is a complex process as it involves several aspects such as: policies for emergencies, recovery plans, variation in data center operational roles, hosted/processed data types and data center architectures. However, in this dissertation, storage, networking and security are emphasized.

The need for resilience assessment emerged due to the gap in existing reliability, availability, and serviceability (RAS) measures. Resilience as an evaluation metric leads to better proactive perspective in system design and management.

The proposed Data center resilience assessment portal (DC-RAP) is designed to easily integrate various operational scenarios. DC-RAP features a user friendly interface to assess the resilience in terms of performance analysis and speed recovery by collecting the following information: time to detect attacks, time to resist, time to fail and recovery time.

Several set of experiments were performed, results obtained from investigating the impact of routing protocols, server load balancing algorithms on network resilience, showed that using particular routing protocol or server load balancing algorithm can enhance network resilience level in terms of minimizing the downtime and ensure speed recovery.

Also experimental results for investigating the use social network analysis (SNA) for identifying important router in computer network showed that the SNA was successful in identifying important routers. This important router list can be used to redundant those routers to ensure high level of resilience.

Finally, experimental results for testing and validating the data center resilience assessment methodology using the DC-RAP showed the ability of the methodology

quantify data center resilience in terms of providing steady performance, minimal recovery time and maximum resistance-attacks time.

The main contributions of this work can be summarized as follows:

- A methodology for evaluation data center resilience has been developed.
- Implemented a Data Center Resilience Assessment Portal (D\$-RAP) for resilience evaluations.
- Investigated the usage of Social Network Analysis to improve the computer network resilience.

TABLE OF CONTENTS

| | |
|------------------------------------------------------------------------|------------|
| ACKNOWLEDGEMENTS | III |
| ABSTRACT | IV |
| LIST OF TABLES | IX |
| LIST OF FIGURES | X |
| 1. INTRODUCTION | 1 |
| 1.1. RESEARCH MOTIVATION | 1 |
| 1.2. BACKGROUND | 2 |
| 1.2.1. <i>Data Centers</i> | 3 |
| 1.2.2. <i>Resilience</i> | 5 |
| 1.2.3. <i>Data Center Resilience</i> | 5 |
| 1.3. DISSERTATION OUTLINE | 6 |
| 2. DATA CENTERS OVERVIEW | 8 |
| 2.1. WHAT IS DATA CENTER? | 8 |
| 2.2. DATA CENTER ARCHITECTURE | 9 |
| 2.2.1. <i>Layered Approach</i> | 10 |
| 2.2.2. <i>Multi-Tier Approach</i> | 11 |
| 2.2.3. <i>Virtual Data Center architecture</i> | 13 |
| 2.3. DATA CENTER RATIONAL COMPONENTS | 16 |
| 2.3.1. <i>Data Storage Alternatives and Technologies</i> | 16 |
| 2.3.2. <i>Data Center Networking and Communication Protocols</i> | 18 |
| 2.3.3. <i>Data Mirroring Techniques and Methodologies</i> | 19 |
| 2.3.3.1. <i>Data Mirroring Challenges</i> | 22 |
| 2.3.4. <i>Network Connectivity Alternatives</i> | 25 |
| 2.3.4.1. <i>Load Balancing Algorithms</i> | 25 |
| 2.3.4.2. <i>Routing Protocols</i> | 28 |
| 2.3.5. <i>Security Threats and Vulnerabilities</i> | 29 |
| 2.4. DATA CENTER ROLES | 36 |
| 3. INFORMATION SYSTEMS EVALUATION & RELATED WORK | 38 |
| 3.1. EVALUATIONS PROCESS | 38 |
| 3.2. DATA CENTER PERFORMANCE ANALYSIS | 39 |
| 3.2.1. <i>Performance Challenges</i> | 40 |
| 3.3. RELIABILITY, AVAILABILITY, AND SERVICEABILITY (RAS) | 41 |
| 3.3.1. <i>Reliability</i> | 41 |
| 3.3.2. <i>Availability</i> | 44 |
| 3.3.3. <i>Serviceability</i> | 45 |
| 3.4. RESILIENCE CONCEPT | 46 |
| 3.5. METRICS COMPARISON | 47 |
| 3.6. RELATED WORK | 49 |

| | | |
|-----------|----------------------------------------------------------------------|------------|
| 3.6.1. | <i>Adaptive Response for Distributed Denial-of-Service Attacks</i> | 49 |
| 3.6.2. | <i>Cloud Sustainability</i> | 51 |
| 3.6.3. | <i>Approaches for Mitigation of Storage Security Risks</i> | 54 |
| 4. | NETWORK RESILIENCE ENHANCEMENT OPPORTUNITIES | 56 |
| 4.1. | ROUTING PROTOCOLS | 57 |
| 4.1.1. | <i>Routing Protocols Evaluations Metrics</i> | 58 |
| 4.1.2. | <i>Routing Protocols and Resilience</i> | 58 |
| 4.2. | LOAD BALANCING ALGORITHM | 59 |
| 4.2.1. | <i>Server Load Balancing Architecture & Algorithms</i> | 60 |
| 4.2.2. | <i>Our Server Load Balancing Evaluation Methodology</i> | 62 |
| 4.3. | USING SOCIAL NETWORK ANALYSIS FOR NETWORK RESILIENCE IMPROVEMENT | 64 |
| 4.3.1. | <i>Social Network Analysis Overview</i> | 65 |
| 4.3.2. | <i>Social Network Measurements</i> | 66 |
| 4.3.3. | <i>Benefits of Using SNA</i> | 67 |
| 5. | DATA CENTER RESILIENCE ASSESSMENT | 69 |
| 5.1. | PROBLEM STATEMENT | 69 |
| 5.2. | RESILIENCE EVALUATION APPROACHES | 70 |
| 5.2.1. | <i>Multi-Objective Optimization (MOO)</i> | 71 |
| 5.2.2. | <i>Applying MOO to Data Center resilience</i> | 72 |
| 5.2.3. | <i>Operational Analytics (OA)</i> | 75 |
| 5.2.4. | <i>Applying Operational Analytics (OA) to Data Center resilience</i> | 75 |
| 6. | DATA CENTER RESILIENCE ASSESSMENT PORTAL | 78 |
| 6.1. | TEST-BED OVERVIEW | 78 |
| 6.1.1. | <i>E-Cavern Project test-bed</i> | 78 |
| 6.1.2. | <i>University of Louisville Test-bed</i> | 80 |
| 6.2. | DATA CENTRE RESILIENCE ASSESSMENT PORTAL (DC-RAP) | 82 |
| 6.2.1. | <i>DC-RAP User's Interface</i> | 83 |
| 6.2.2. | <i>Experimentation Scenarios</i> | 85 |
| 6.2.3. | <i>DC- RAP Utilization</i> | 86 |
| 7. | EXPERIMENTAL RESULTS AND DISCUSSION | 87 |
| 7.1. | COMPUTER NETWORK RESILIENCE | 87 |
| 7.1.1. | <i>Network protocols</i> | 87 |
| 7.1.2. | <i>Server Load Balancing</i> | 89 |
| 7.1.3. | <i>Social Network Analysis & Network Resilience Improvement</i> | 91 |
| 7.2. | DATA CENTER RESILIENCE ASSESSMENT EXPERIMENTS | 97 |
| 8. | CONCLUSIONS AND FUTURE RESEARCH DIRECTIONS | 102 |
| 8.1. | FUTURE WORK | 103 |
| | REFERENCES | 106 |
| | CURRICULUM VITAE | 111 |

LIST OF TABLES

| | |
|------------------------------------------------------------------------|----|
| Table 1: SAN vs. SAN Summary..... | 17 |
| Table 2: Data Mirroring/Replications Models Summary..... | 22 |
| Table 3: Data Consistency Models Summary | 24 |
| Table 4: Vulnerability, Threats, and Attacks Categories Summary..... | 30 |
| Table 5: Remote Data Center Configuration Summery | 37 |
| Table 6: Summary for Data Center System Concerns | 48 |
| Table 7: Change in Network Routing Parameters for Local Protocols..... | 88 |
| Table 8: Change in Network Routing Parameters..... | 89 |
| Table 9: SLB Algorithm Performance Summary..... | 91 |
| Table 10: Distribution of Nodal Degree..... | 95 |
| Table 11: Distribution of Betweenness Centrality | 95 |
| Table 12: Distribution of Closeness Centrality | 96 |
| Table 13: Response Time Summary | 97 |

LIST OF FIGURES

| | |
|--------------------------------------------------------------------------------------------------------------|-----|
| Figure 1: Google data center map [source: www.royal.pingdom.com] | 3 |
| Figure 2: Typical Data Center Architecture | 4 |
| Figure 3: Three Layer Data Center Architecture | 11 |
| Figure 4: Multi-tier Approach Data Center Architecture | 12 |
| Figure 5: Data Center Rational Components | 16 |
| Figure 6: Storage Area Networks Elements | 17 |
| Figure 7: Synchronous Data Mirroring Process | 20 |
| Figure 8: Asynchronous Data Mirroring Process | 20 |
| Figure 9: Data Center Network Roles Summary | 25 |
| Figure 10: Server Load Balancing Models | 27 |
| Figure 11: Routing Paths with Various Cost Example | 28 |
| Figure 12: Developing Attacks Process | 30 |
| Figure 13: Security Layers Summary | 35 |
| Figure 14: Data Center Role Summary | 36 |
| Figure 15: System Evaluation Process | 39 |
| Figure 17: Reliability BathTUB Curve | 43 |
| Figure 18: Service Incident Lifecycle | 45 |
| Figure 19: Resilience illustration | 46 |
| Figure 20: Data Center Resilience Concerns | 49 |
| Figure 21: Traffic Redirection Attack Protection System Flow Chart | 51 |
| Figure 22: Balancing Cost and Security | 55 |
| Figure 23: SLB Scenarios | 63 |
| Figure 24: Sample of parameters affects resilience | 74 |
| Figure 25: SAN and NAS implementations | 74 |
| Figure 26: Resilience Measures Illustration | 76 |
| Figure 27: Data Center Operation Summary | 77 |
| Figure 28: Simulated view of E-Cavern Project test-bed | 80 |
| Figure 29: Test-Bed Basic Overview | 80 |
| Figure 30: DC-RAP User's Interface | 84 |
| Figure 31: Baseline Scenario | 90 |
| Figure 32: University of Louisville Gigabyte Backbone | 92 |
| Figure 33: Uniform Network Sociomatrix | 93 |
| Figure 34: Weighted Network Sociomatrix | 94 |
| Figure 35: Zoomed Section for the Routers Failure Time | 96 |
| Figure 36: Kernel Density Estimation for various network bandwidths | 98 |
| Figure 37: DC-RAP logger snapshot (Case 1) | 99 |
| Figure 38: DC-RAP logger snapshot (Case 2) | 100 |

| | |
|--------------------------------------------------------------------------|-----|
| Figure 39: Resilience Comparison for Different Server Configuration..... | 100 |
| Figure 40: Data Mirroring and Security..... | 104 |

1. INTRODUCTION

1.1. Research Motivation

Information systems have become significant part of our daily lives, and our dependency upon their infrastructure is increasing. Unprotected computers are vulnerable to viruses, attacks and other malicious activities. In addition, the new business models, industry requirements and the growing volume of critical data pressed the need for innovative computing environments such as cloud computing. Data Center (DC) is one of the core rudiments of cyberinfrastructure, which occupied the interest of system administrators, designers, researchers, and hackers. Operational continuity of data centers faces challenges from experienced cyber attackers and occasional natural disasters.

To create a data center that is both resistant to attack and resilient when under attack, new research is required that will help us to understand and fine tune the parameters affecting the reliability and availability of existing data centers, and enable new algorithms and architectures for next generation data center systems that are highly replicated, geographically distributed, secure, resilient to denial-of-service attacks, and robust to failures of their components.

Current DC infrastructure includes many features for increased Reliability, Availability, and Serviceability (RAS) attributes; however, terrorists' attacks and natural disasters threats underscore the need for a resilient data center. Data center resilience can be enhanced by improving the ability and the speed of the system to evolve and adapt to

unexpected situations as they occur. The traditional system evaluation metrics do not provide the essential information for resilience assessment. The main objectives of this dissertation is to present a new methodology for data center resilience assessment, define data center resilience requirements, devise a high level resilience metric, and develop a tool for testing and validation.

1.2. Background

Data centers (DC) are the core of any information technology infrastructure; for the last three decades computing and networking development dragged data center progression. The rapid development of computing architectures (mainframes/terminals, server/client and internet computing) lead to locally connected data center; followed by huge networking development (protocols, bandwidth and communications) which brought in the networked data center (Bloor 2005).

On the other hand, different business profiles shaped data center roles and requirements to achieve business goals and desires such as: data availability, data integration, and highest performance level.

To demonstrate how vital a data center can be, let us look at Google data center map for example. As shown in figure 1, Google has nineteen data center locations in the US, twelve in Europe, one in Russia, one in South America, and three in Asia, in total they are thirty-six locations (Miller 2008). According to Google's earnings reports, they spent \$1.9 billion on data centers in 2006, and \$2.4 billion in 2007. AS we can see it is a huge investment that requires a lot of management and rise many concerns.

Moreover, critical application data centers such as financial institutions, governmental and defense organization are targeted by different type of attacks and environmental disturbances such as: terrorists, industrial spy, and natural disasters.

The current evaluation metrics such as: availability, reliability, etc. answer many of the systems administrators' and designers concerns, but some concerns still remain for example: Is it a resilient data center? How to measure resilience level?

The rest of this chapter introduces a quick data center overview, resilience, and the dissertation organization.



Figure 1: Google data center map [source: www.royal.pingdom.com]

1.2.1. Data Centers

A data center (DC) is the facility used for housing a large number of computers, the servers themselves, data storages devices, and communications equipment to perform: data- management, storing, sharing, processing, and exchange. A data center usually provides different kind of data manipulation technologies and capabilities such as: data clustering, data availability, data warehousing, and disaster recovery. Data centers are required to support critical business applications by providing the highest level of data

availability, integrity, and data consistency economically feasible. Another aspect of data center performance is real time data backup and recovery process, Real-time backup allows data center managers to duplicate their files, directories or volumes without interrupting the work which makes real time backup a better solution for business that cannot effort to have their data systems interrupted or shutdown. Traditionally data center managers rely on different techniques to keep the data centers continually working and avoid any unexpected downtime using redundant hardware, local and remote backup sites (Maurizio Portolani 2003). Figure 2 shows a typical data center.

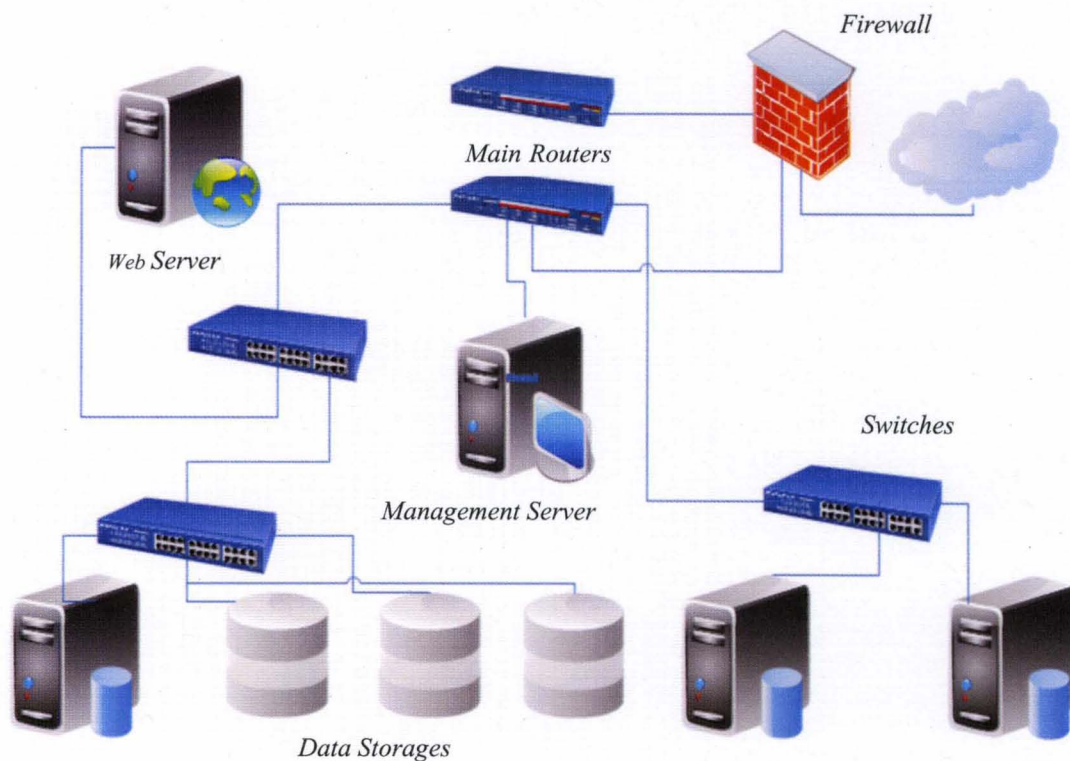


Figure 2: Typical Data Center Architecture

1.2.2. Resilience

Resilience has been defined in one of two ways, it can be defined as the *ability of the system to recover rapidly from any change affecting the system routine*, or as *quality or state of being flexible* (Hoffman and Nilchiani 2008). The main aspect of any of those definitions is to show how the performance of a system will be affected by variation of the running environment (Holling 1996). However, it is used quite differently in different fields for example computer network resilience is the ability of the network to provide and maintain acceptable level in terms of response or delay levels of services under different fault or an abnormal condition caused by cyber threats or any other threats (Mohammad, Hutchison and Sterbenz 2006). In business, resilience is the ability of a company to sustain the impact of a service interruption, and resume its operations to continue to provide service.

Since resilience -definition by Hoffman and Nilchiani 2008- evaluation consider the system ability to continue providing services while been hacked or attacked. The evaluation process will identify set elements or parameters which can be used to build a resilient and better systems. For system resilience evaluation process; systems parameters will be investigated such as system networks, data storage, and security gears (Cronholm and Goldkuhl 2003).

1.2.3. Data Center Resilience

The growth of critical data sets volumes, technology's vulnerabilities, natural disaster and terrorist attacks are the main worries for any data center managers. How will the system perform during the malicious activity? Would it be able to resist a disruptive

event? and, if so, for how long? For resilience level evaluation process, the main parameters mentioned above are included in addition to some others such as:

- Replication technology: using Synchronous versus Asynchronous Technology; the selection based on the distance of that remote data center from the main site. Based on the available platforms Synchronous replications are limited to 300 KM and other parameters such as latency. (Lei Gao 2003).
- Application Characterization: each application requires certain setting for the replication such as the block size, drain time and others based on the used platform. In some cases it is a good idea to monitor the system performance while installing the center (McGill 2006).
- Communication: Use of private, public, semi-public networks in addition to the distance affect the selection of appropriate security techniques which may add overhead and affect the overall performance (Seokwoo Song 2007).

1.3.Dissertation Outline

The main objectives of this research are to develop a methodology for data center's resilience evaluation. An additional objective is to explore opportunities for improving computer networks resilience. The following chapters represent the accomplished activities to achieve these research objectives. The second chapter introduces an overview of data center design, architecture, and technologies. Chapter three discusses the current information systems metrics: reliability, availability, and serviceability (RAS). And study the relation between RAS and data center resilience metric. Chapter four illustrates the research work done to investigate network resilience enhancement in terms of minimizing the network down time. Chapter five demonstrates data center resilience

assessment methods: multi-objective optimization and operational analytics. Chapter six introduces the assessment portal. Results and discussion can be found in chapter seven. Chapter eight presents conclusions and future research direction.

2. DATA CENTERS OVERVIEW

2.1. What is Data Center?

Critical infrastructure, global businesses applications, and rapid growth of data volumes highlight the demand for a high-quality information infrastructure system. Data centers are the core of any information systems, a well design data center is required to meet many challenges such as: evolving of new technology, accommodating different data types, providing the highest level of availability and data consistency to support the various needs of the hosted applications whose requirements are, in turn, driven by business needs.

Data centers designing and planning are a complex processes that deals with different aspects; some related to the functional requirements such as: (Snevely 2003)

- Secure location for computers, storages, and networking devices.
- Maintaining reliable power source and other alternative to secure power needs.
- Healthy environment to run these devices safely.

While some other aspects related to the data center architectural properties such as: (Maurizio Portolani 2003)

- Flexibility: is the ability of a DC to support new applications, services, and hardware substitution without major technology compatibility problems.

- Availability: there is no room for risk with critical applications so many data centers must be available *all the time* to process clients' request.
- Scalability: data center services quality should not be affected by variations in the data volume or categories.
- Security: DC security wrap up several factors: physical, operational, communication network, data storage, and application security which create conflicts in some cases, for example: operating systems security may overlook application security needs or not tuned enough.
- Manageability: keeping DC design simple make it easier for administration, troubleshooting and management, in addition to maintain good documentation.

In other words, data center as a multi objective system requires a very skilled management team.

2.2. Data Center Architecture

In general a data center is a set of devices and tools including but not limited to routers, servers, data storage devices, and monitoring devices/tools. The ultimate goal for any smart architecture is to provide a secure, efficient, and reliable operation environment that can allow E-business and others applications to provide good service and protect the critical applications and data. This section demonstrates the basic foundation of the data center design which can be based on a layered approach or a multi-tier approach.

2.2.1. Layered Approach

This approach has been evaluated and enhanced over the last few years to improve data center performance, availability, reliability, and flexibility (Cisco 2007).

Figure 3 shows a three layer model basic design, the three layers are:

- 1) Core Layer: this layer provides high speed switching for all the packets going in, out and within the data center; it runs on a layer three routers and use certain protocols.
- 2) Aggregation layer: this layer implement double side networking layer functions layer two and layer three as follows:
 - (i) Layer two functions:
 1. Spanning Tree Protocol (STP).
 2. Services: such as multicast and ACLs for services such as QoS, security, rate limiting, broadcast suppression.
 - (ii) Layer three functions as follows:
 1. Forwarding packet between servers and rest of the network.
 2. Maintaining the routing process dynamically.
 3. Maintain gateways, firewall, and server load balancing.

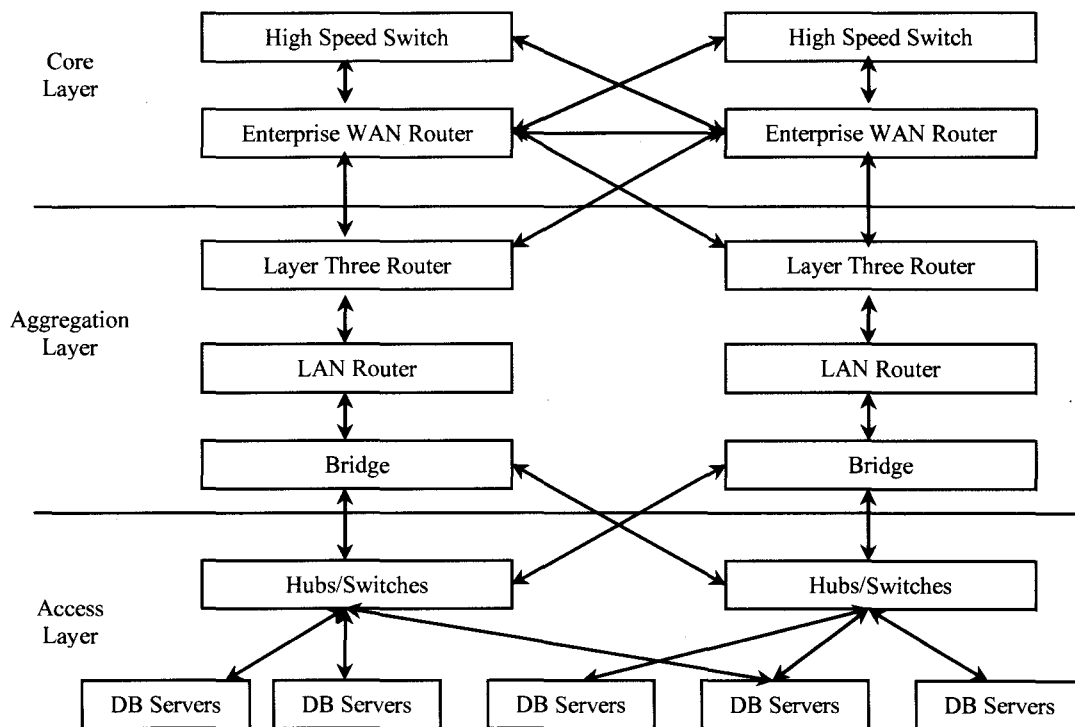


Figure 3: Three Layer Data Center Architecture

- 3) Access layer: this layer consists of modular switches, layer two and layer three switches to support different topologies requirement, blade server and cluster servers. It maintains the various server services requirement such as broadcasting or administration requirement.

2.2.2. Multi-Tier Approach

In this approach data center architecture are built from a front and a back end network as shown in figure 4. Front end performs access control function, security and packet switching (forward) function, while the back-end can be defined as a type of storage area network (SNA) it maintain the actual server layout, data storage, server clustering, and data replication tools (Sarka, et al. 2003).

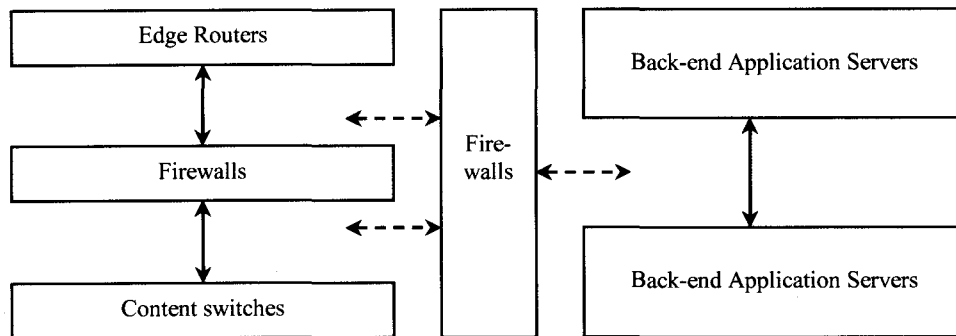


Figure 4: Multi-tier Approach Data Center Architecture

A. Front-end Components

- Edge routers: an edge router provides the fundamental access between two networks and in this case between the data center network and WAN or Web.
- Firewalls: protect the data center by preventing the unauthorized access or connection from outside the data center and provide address translation function to support intrusion detection systems.
- Virtual private networks: used to authorize external IP address to access to data center through authenticated and encrypted connection. Some data storage software such as IBM global mirroring limits it to 2 connections.
- Content switches: provide many functions such as:
 - Monitor server performance.
 - Load balancing between servers or cluster of servers.
 - Monitor data center connectivity.

B. Back-end Components

A back end provides direct high-speed data exchange between servers and storage devices: (Sarka, et al. 2003)

- Server to storage: it is a well-known model of communication with storage devices. The advantage is that the same storage device may be accessed serially or concurrently by multiple servers.
- Server to server: it may be used for application communications or for the clustered server communications.
- Storage to storage: this is used in case data need to be moved from a storage device to another or in case for data backup.

The previous sections illustrated the physical structure of data center, logically data center had four main components: Data storage devices, Communications, Data mirroring and replication and security as shown in figure 5. The following section will exhibit each component.

2.2.3. Virtual Data Center architecture

Building green, efficient, and flexible data centers is the dream of any data center architect. Several techniques such as: consolidation, standardization, and virtualization. Virtualization can be implemented for storage, servers and networking.

With virtualization, there's efficiency in the hardware requirements because of improved utilization. Less hardware or cheaper hardware can be used to do the same job. Based on the current cost analysis, virtualization gives 5 times the performance for a third of the cost in comparison to server farm that cost. However, several challenges are there such as: feasibility of specific application deployment in virtual environment. The amount of data and any replication algorithms involved may also limit feasibility.

Modern storage virtualization technologies provide advanced features such as non-disruptive migration of data and thin provisioning. The first form of storage virtualization was developed within server environment. Since networked storages approaches such as SAN or NAS represents a bottleneck for applications communications, Network-based storage virtualization incorporated the intelligence of managing the storage resources in the network layer, either in-band or out-of-band. In the other hand storage controller virtualization enhanced the physical storage resource for large scale RAID. (Wolf and Halter 2005)

Network Virtualization allows multiple applications to run side-by-side over the same physical infrastructure. The key element of virtual network is its ability to follow business policies and maintain the desired level of security, availability, and quality of services. Virtual networks optimize the usage and control of physical networks that are shared for several applications. Network virtualization has several advantages for example:

- Minimize downtime and ensure operational Continuity.
- Provide higher level of data and resources protection.
- Assurance high performance level and Quality of Service.
- Accelerate the inauguration of new services.

Network virtualization is very good solution for enterprise requirements, as within the same organizations, different groups, and departments have dissimilar requirements that need to be provided. In particular, wireless networks, user mobility, and the cross group collaboration with resource sharing are the main challenges for Network virtualization (Moreno, Moreno and Reddy 2006).

Server virtualization technologies are the main aspect of creating dynamic datacenters. It is a powerful solution for responding dynamically to business necessities and goals. Although VMware leaded the server virtualization market for long time, there are now more options and technologies available for consumers.

It is very important to select the right technology matching application requirements and cost analysis. Server virtualization can be implemented for several scenarios such as follows: (Ruest and Ruest 2009)

- Physical Server consolidation
- Environment standardization
- Help desk
- Training
- Software development
- System testing
- Physical data center consolidation
- Improved asset utilization (efficiency, both environmentally and financially)

It is very important to keep in mind that to have an efficient virtualization solution an effective virtualization management tools are required. Virtualization provides unique advantages for data centers:

- Less power consumption.
- Fewer servers but more critical.
- Applications are dynamically reallocated easily.
- The data center footprint will be smaller.

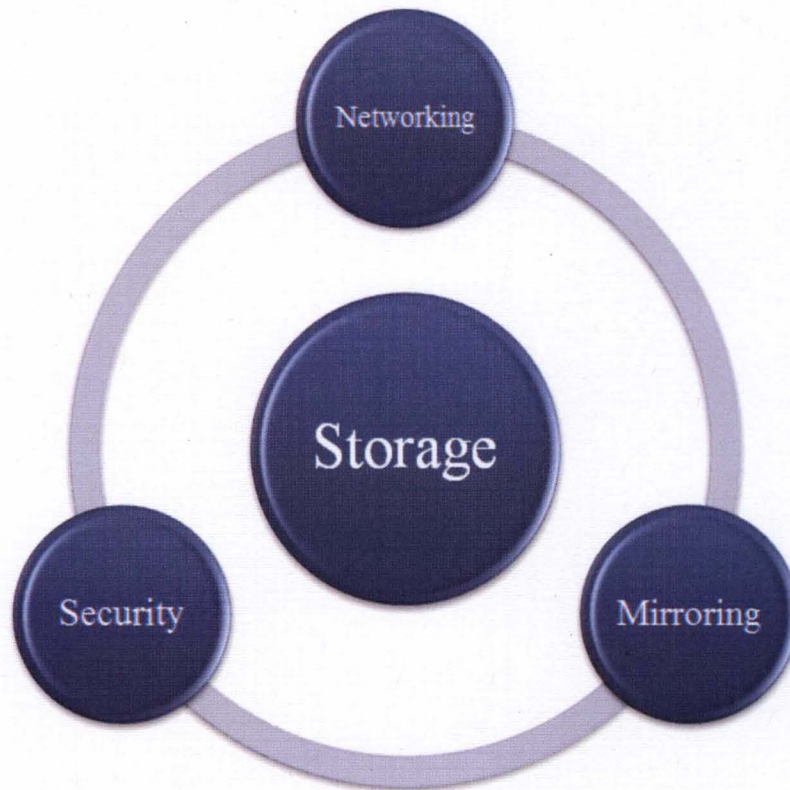


Figure 5: Data Center Rational Components

2.3.Data Center Rational Components

2.3.1. Data Storage Alternatives and Technologies

Data storage is integral part of data centers architecture, over the years several storage solutions have been develop to satisfy applications requirements and demands. There is a diversity of storage alternatives offered, yet the most common ones are: Direct-Attached Storage (DAS), Network-Attached Storage (NAS) and Storage Area Networks (SAN). Selection of appropriate data storage solution is complex process because the various needs and plans of each business applications. In large scale data center SAN and NAS are dominating the market, table 1 presents preliminary guidelines for storage solution selection process and comparison between SAN and NAS (Villars 2004).

Table 1: SAN vs. SAN Summary

| Criteria | <i>SAN</i> | <i>NAS</i> |
|----------------------------------|------------------|-----------------------------------|
| Cost | Expensive | Inexpensive |
| Setup | Complicated | Straightforward |
| Management | Easy | Complicated for large environment |
| Environment size | Better for large | Better for small |
| Disk system compatibility | Any | Device orientated |
| Impact on network | None | Can swamp down network |

However, the future of SAN is brighter as the SAN setup cost is getting cheaper and decreasing in management complexity. Figure 6 shows SAN basic elements.

1. *Disks*: can be connected as point to point without an interconnection device or be a part of server-storage model. SANs are independent from storage device types; thus disks, tapes, RAIDs, and file servers can be used.
2. *Servers*: fundamental elements of SAN, which can be mix of platforms and Operating systems.
3. *Communications*: SAN communications implemented by Fibre channel or InfiniBand®, where data loss rate is zero, and exhibiting high throughput rate.



Figure 6: Storage Area Networks Elements

2.3.2. Data Center Networking and Communication Protocols

TCP/IP is the dominating communications protocol over the internet but because of the sensitive nature of data centers; managers and DC designers used another set of communication protocols for data center interconnection. Interconnection scheme are one of the aspects which define the number of storage devices that can be connected, data transfer speed, and system vulnerabilities. Current technologies offer a list of storage access protocols such as: (Long 2006)

- FCIP: Entire Fibre Channel Frame Over IP
- FCP: Fibre Channel Protocol
- iFCP: Internet Fibre Channel Protocol
- iSCSI: Internet Small Computer System Interface
- iSNS: Internet Storage Name Service
- SAS: Serial Attached SCSI
- NDMP: Network Data Management Protocol
- Fibre Channel over Ethernet

The most commonly used access protocols are Fibre Channel Protocol (FCP) and Small Computer System Interface (SCSI); The Fibre Channel Standards supports high-speed communication mechanism between servers, supercomputers, and data storage devices. FCP supports considerably higher number of attached disks, longer distance between nodes and sustains necessitate for very fast transfers of large data volumes than competing protocols. On the other hand SCSI Protocols is an ANSI standard which supports different I/O interconnects. The parallel interface is the most used between any SCSI device and their hosts. SCSI interfaces support faster data transmission rates than

standard serial and parallel ports. The architecture of the SCSI is based on the client/server model, which is mostly implemented in an environment where devices are very close to each other and connected with SCSI buses. There are many variations of SCSI: SCSI-1, SCSI-2, SCSI-3 and Serial Attached SCSI (SAS) (Gary Field 2000).

2.3.3. Data Mirroring Techniques and Methodologies

Data mirroring, Data replication and data backup techniques are used to provide a high level of data availability, consistency, and recovery (Yun 2003). Ensuring data recovery is a part of building a resilient system, so it is vital to differentiate between the usages, and limitation of each method. By definition *Data Backup* is the process of copying data (files/databases) onto other data storage units to be retrieved when needed in case of device failure. It is considered a regular process of system management and usually done overnight (Dorian Cougias 2003).

Data replication involves making additional copies whether for load balancing, or for backup/business continuity. Data reapplication can be done within/off the facility. For speedy recovery and critical data application Data Mirroring is mandatory; where *Data Mirroring* is copying data from one location to a storage device/ different location in real time. It always a good idea to have the mirroring site within safe distance from the main site. Based on the distance and data criticalness data mirroring can be implemented as synchronous or asynchronous.

In the case synchronous mirroring each transaction is sent to the mirror site and the clients don't get response until the main site gets acknowledged from the mirror site

as shown in figure 7. Yet this approach affects the system performance and increases services response time. (Gary Field 2000).

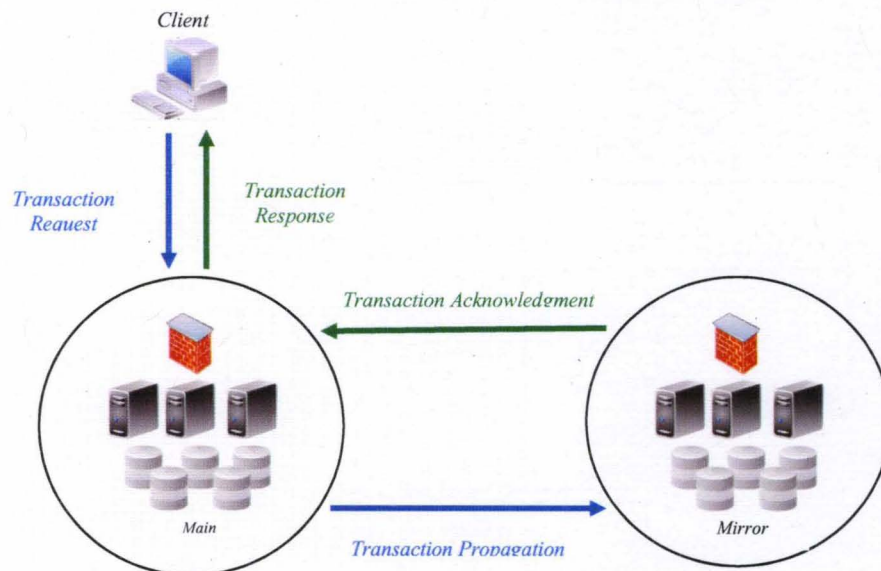


Figure 7: Synchronous Data Mirroring Process

Also data mirroring can be implemented as asynchronous where the main site receive clients' request, processes it, responds to client and then send updates to the mirror site as shown on figure 8.

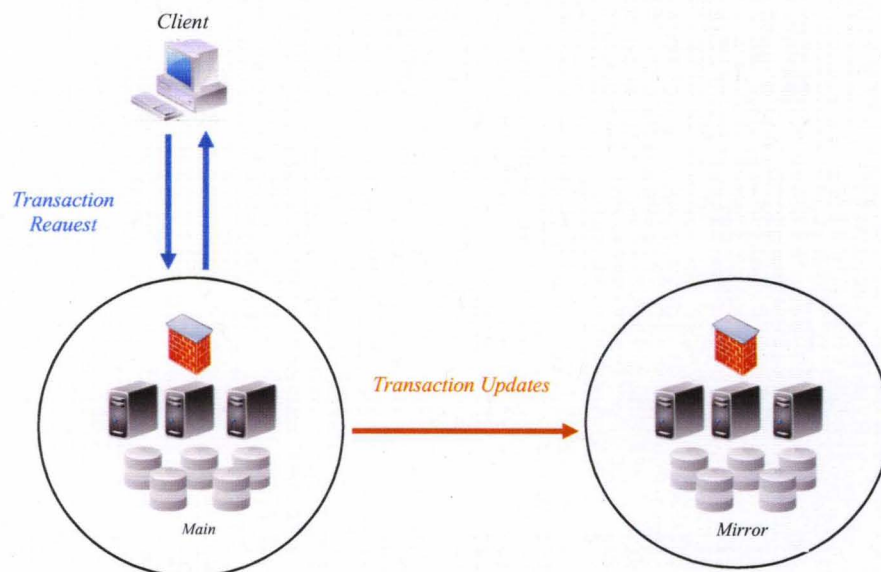


Figure 8: Asynchronous Data Mirroring Process

In this case, mirror site will be few transactions behind; but the system performance will not be affected (Bernstein, Hadzilacos and Goodman 1987).

Data mirroring and replication models can be classified in different categories, based on how the models work. There are three common approaches as table 2 illustrates (Jin 2004).

- *Snapshot replication*: is the simplest one where all data (replica) will be copied from the Publisher database to the Subscriber's/Subscribers' database(s) on a periodic basis. Snapshot replication is best used as a method for replicating data that change infrequently and when the size of replicated data is not very large.
- *Transactional replication*: each committed transaction is replicated to the subscriber as it occurs. Replication process setting can be set so that it will accumulate transactions and send them at timed intervals, or transmit all changes as they occur. This type of replication is used in environments having a lower degree of latency and higher bandwidth connections. Transactional replication requires a continuous and reliable connection, because the Transaction Log will grow quickly if the server is unable to connect for replication and might become unmanageable.
- *Merge Replication*: it is an agent based model where merge agent will first copy changes from the publisher and apply them to the subscriber, and then take changes from the subscriber and apply them to the publisher. Once the changes have been applied both ways, the Merge agent will look at and resolve any conflicts.

Table 2: Data Mirroring/Replications Models Summary

| How replication works | How replication preformed | What data structure are replicated |
|---------------------------|--------------------------------------|------------------------------------|
| Transactional replication | Active | Accumulated Transactions |
| Snapshot replication | Passive | Database tables |
| Merge replication | Active/Passive, no active connection | Database with conflicts resolution |

Which data structures need to be replicated is another approach used to classify the data mirroring models: Database, File system are the basic element to mirroring/replication models as follow:

- *Database replication*: many database management systems use this approach, where the create logs of updates, which then ripple through to the slaves. The slaves acknowledge to the master node that the updates were processed. The success of this approach depends on very good communications solutions.
- *File system replication*: implemented by distributing updates of a virtual block device to several physical hard disks. This way, any file system supported by the operating system can be replicated without modification, because the file system code works on a level above the block device layer. Alternatively, updates to a block device can be replicated (that is, distributed) over a computer network.

2.3.3.1. Data Mirroring Challenges

Data mirroring is a complex process involves different issue such: multiple write processes concurrently, updating of all replicas, data consistency, system scalability, data characteristics, and application requirements. The most important challenge is how to

maintain the desired level “Data Consistency” vs. system performance and availability (Ganymed 2004).

Data Consistency: A consistency model is a contract between processes and the data store - if the processes behave in a certain expected way, the data store will work correctly. The term data store refers to shared file systems, memory space, database, etc. All consistency models work to return the results of the last write for a read operation, the key issue between different data consistency models is how the last write be determined. The only way to really make replication work is to relax the constraints for synchronization, the basic two types of consistency models based on consistency drive are: (Liu 1990)

- Data-centric model:

A data-store can be read from or written to by any process in a distributed system; any replica can support fast reads; any write process to a local replica needs to be propagated to all remote replicas.

- Client-centric model:

In this model the focus is more on maintaining a consistent view of data for current data store clients. The main assumption in this case that the number of concurrent writes is very few, which is the case of Domain Name server (DNS).

There are different types of Client-centric models such as:

- Monotonic-read consistency: if a process reads x, any future reads on x by the process will returns the same or a more recent value.
- Monotonic-write consistency: A write by a process on x is completed before any new write operations by the same process.

- Read your write: write by a process on x will be seen by a future read operation on x by the same process.
- Writes follow reads: write by a process on x after a read on x takes places.

Another approach classifying the data consistency models is to classify them based on the level of restriction on the synchronize process. Table 3 provides a short description for each model. The basic idea is that there is two processes: read and write, and in shared environments we will have different read/write hits so we need read process and change the data based on the correct write process.

Table 3: Data Consistency Models Summary

| Types of Consistency Model | Description |
|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| Models using synchronization | |
| Strict | Absolute time ordering of all shared accesses matters. |
| Linearizability | All processes must see all shared accesses in the same order. Accesses are furthermore ordered according to a (non-unique) global timestamp |
| Sequential | All processes see all shared accesses in the same order. Accesses are not ordered in time |
| Causal | All processes see causally-related shared accesses in the same order. |
| FIFO | All processes see writes from each other in the order they were used. Writes from different processes may not always be seen in that order |
| Models not using synchronization | |
| Weak | Shared data can be counted on to be consistent only after a synchronization is done |
| Release | Shared data are made consistent when a critical region is exited |
| Entry | Shared data pertaining to a critical region are made consistent when a critical region is entered. |

At this point, it is useful to clarify the difference between two closely related concepts: **Coherence and Consistency**: Fundamentally, these relate to synchronization. Coherence mechanisms ensure that modifications made by a processor propagate to all copies of the data. While Consistency mechanisms maintain in what order modification are propagated to other copies (Michael Resch 2010).

2.3.4. Network Connectivity Alternatives

Network connectivity represents a significant portion of data center architecture, either for Interconnection, Data Storage, Mirroring, and Public Access as shown in figure 9. Also computer networks sub-elements (topologies, links, connecting devices, routing protocols and load balancing) are very critical aspects on computer network performance and resilience level.

| Interconnection | Data Storage | Mirroring Alternatives | Public Access |
|----------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none">•Servers•Switches•Internal Protocols•Routers•Links | <ul style="list-style-type: none">•Fibre Swtiches•Fibre Protocols•Optical Links | <ul style="list-style-type: none">•Fibre Connections•VPN•Leased lines | <ul style="list-style-type: none">•FireWall, PIX•Load Balancing•External Protocols |

Figure 9: Data Center Network Roles Summary

2.3.4.1. Load Balancing Algorithms

In a Data Center (DC) environment, it is fundamental to have more than one server to process users' requests. System administrators used Server Load Balancing algorithms (SLB) to distribute and balance the system's workload over the available servers, primarily SLB algorithms have been used to optimize DC resources utilization, improve performance, and ensure high availability and reliability. DC's resilience level is affected by each component of DC's architecture; since SLB algorithm is fundamental component of DC, it will have significant effect on DC resilience level. SLB primarily classified as follow:

- *HTTP redirect*: It can be used with others approaches to make better selection of redirected site, also provide high level of backup activity, Also consider it only work for HTTP, clients has to go to the main site first and then redirected which increases the latency (Heinz Stockinger 2002).
- *Domain Name System (DNS)*: commonly used because it is application protocol independent and provides proximity but it has some limitations: DNS client implementation dependent and don't support propriety network protocol which is needed for banking applications (Swaminathan Sivasubramanian 2004).
- *Route health injection (RHI)*: This is implemented using layer 3 router. The advantage of using RHI: application protocol independent, don't need DNS proxy and support hard coded for the important data center IP address but it is limited to the network topology complexity and the service provider network configuration (Zeeshan Naseh 2006).

An optimum SLB algorithm will distribute system's workload over the available servers with minimum variation between servers' workloads. SLBs are require to provides certain function such as: (Bourke, Server load balancing 2001)

- Divide the incoming traffic into independent services request.
- Apply dispatching policy.
- Keep track of each server: load, response, and availability (IP/Ports).
- Perform NAT network address translation.
- Real server health monitor.

Generally, SLB algorithms are implemented by devoted software or hardware device with various architecture scenarios. SLB architectures can be classified into two categories:

- NAT-based SLB network architecture.
- Flat-based architectures.

Some references refer to them as DNS-Based system & Dispatcher-Based system. The main difference between the two categories is that the SLB unit performs a NAT from one network to another. In a DNS-Based system, basically it use a functions of DNS to associated different IPs with the same host name, the SLB device sits between the clients and the server, in some case it apply NAT to mask the server IP addresses. For the Dispatcher-Based system, the dispatcher receives job requests and then sends it to the right server based on SLB's policy. As shown on figure 10.

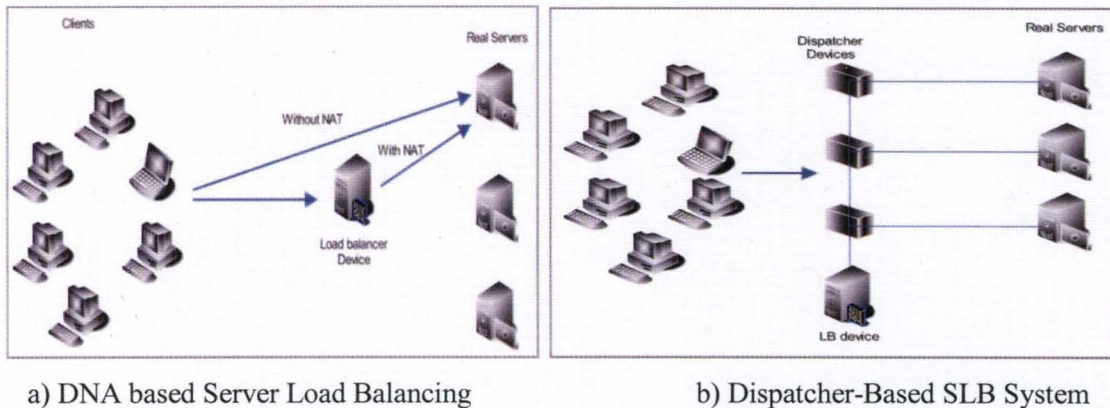


Figure 10: Server Load Balancing Models

2.3.4.2. Routing Protocols

Packet routing is a very critical process which affects computer network performance and the quality of service (QoS). Simply packet routing is forwarding packets from one point to another; there are several routing protocols which specify how routers communicate with each other which will result as routing tables (Macfarlane, Network Routing Basics: Understanding IP Routing in Cisco Systems 2006). As shown in figure 11, there are several paths between point A and Point B, an optimum routing protocol will route traffic from A to B with minimum cost.

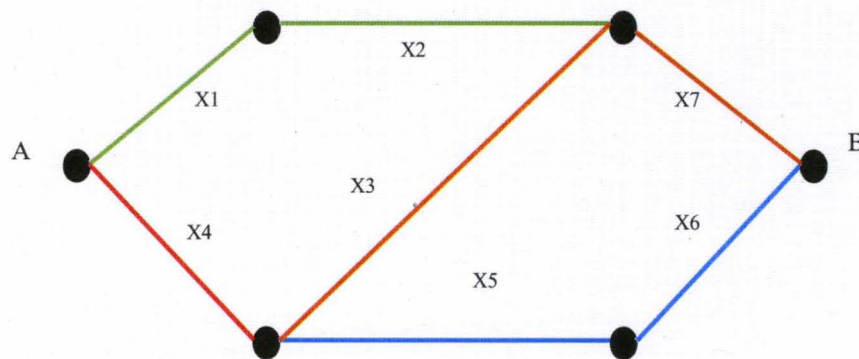


Figure 11: Routing Paths with Various Cost Example

Routing protocols can be classified as follow (Deepankar Medhi 2007):

1- Static versus Dynamic

Routing algorithms can be classified into static and dynamic algorithms. Although a static routing algorithm is not an appropriate term but it has been used referring to the use of a static routing table.

2- Single-path versus Multi-path

Some advanced algorithms will maintain multiple paths to the same destination while other algorithms will provide one path.

3- *Link state versus Distance vector*

It classifies routing algorithms based on whether the routing table or its shared portion is shared with all routers or only with neighboring routers.

Dynamic routing protocols also can be categorized into: *Interior vs. Exterior* routing protocols. Interior routing protocols are used within an autonomous system, while exterior protocols can be used among autonomous systems.

2.3.5. Security Threats and Vulnerabilities

The fact that data center is the core of any legacy system and it host large critical data volumes make it target for all type of attacks physical or cyber. Surveillance cam, high-tech doors, and other technologies improved data center physical security level. In the other hand data center cyber security is a challenging process.

The terms of *Vulnerability, Threats, and Attacks* must be found in any security concerns. System *vulnerabilities* refer to system liability to be attacked, while *Threats* are the events its occurrence damage data center resources. *Attacks* are the actual use of *Vulnerability* to put *Threats* in actions. System hacking is a continuous process where hackers continue to discover system vulnerability to develop attacks as figure 12 illustrates. Restraining data center vulnerability, threats and attacks to an exact list is not feasible, yet they can be categorized as table 4 shows.

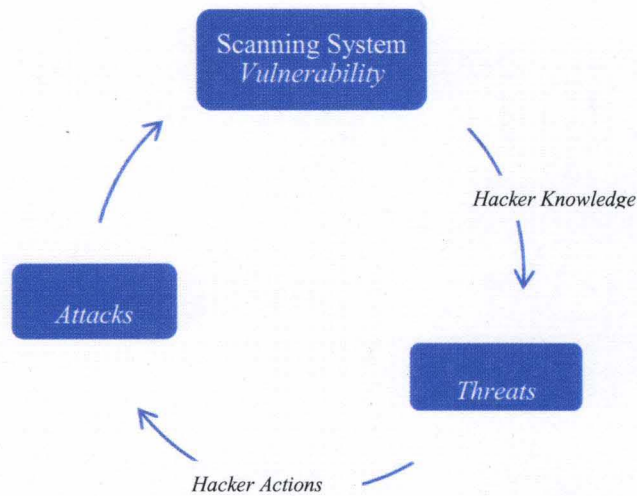


Figure 12: Developing Attacks Process

Table 4: Vulnerability, Threats, and Attacks Categories Summary

| Vulnerabilities | Threats | Attacks |
|------------------------|----------------|------------------------------|
| Designing | Intrusion | Denial of Service DoS& DDoS |
| Technologies | Spam | Un-authorized Access |
| Applications | Worm | Information Tampering |
| Database | Virus | Cross Site Scripting |
| Networks | Malware | IP Spoofing |
| Monitoring tools | Spyware | Insider malicious Activities |

Data center security embrace the main elements of data center, in this section the focus will be on: Fibre channel network, Storage devices, Severs, Network management and access (Harold F. Tipton 2004).

- *Fiber Channel network:*

Fiber channel specification does not provide a robust security model standard, focus on what the vendor provides and implement as many of its security mechanisms as possible. Most switch vendors provide their own method for security and each method is specific to that vendor. It is important to make certain that switches are as

secure as possible. Ensure that the default passwords on each switch are changed in compliance with the corporate security policy and that user- level access is maintained in accordance with the policy, too. In some cases, user and password information is not required to access a switch's internal configuration via FTP and TFTP. The most secure method is to use port zoning approaches which enforce the security thought the hardware level.

- *Storage devices:*

Storage security target data Confidentiality, Integrity and Destruction or Access loss of data. Logical unit number (LUN) security is the lowest level of physical security currently implemented. LUN level security is the ability for the storage device to physically limit host access only to servers connected to a physical storage port. This prevents servers from accessing storage resources not allocated to them, which could potentially corrupt valuable data. The practice of using *LUN-level security* helps to make sure that the proper hosts WWNs are accessing the proper storage units. LUN masking, as it is often called, also helps ensure that rogue server access is not permitted for a specific set of LUNs. LUN-level security in conjunction with port zoning will help provide the correct access level for each host. The tape backup infrastructure is susceptible to security problems. If Fibre Channel bridges are used to convert SCSI tape drives to Fibre Channel, it is critical to ensure that user and password information is in compliance with the corporate security model.

- *Server access:*

The servers in the DC environment are often the biggest targets for attackers, especially in some applications where external Web servers may have access to

resources in the DC. Often attackers targeted application server to gain unauthorized access into the DC resources. When hackers gain control of server, they have a wide range of options to steal, damage, or deny access to data. Storage virtualization servers also suffer from the same security threats as application servers, so it is of equal importance to protect these assets from unauthorized access. Ensure that server network ports are reconfigured from the defaults and opened only if needed. Possible option is to use IPSec wherever possible for administrative accesses, Persistent bindings or LUN mapping at the server level can also provide an additional level of security.

- *Management network access:*

It provides the ability to monitor and manage the devices in the DC. In most cases, this network is outside the path of the storage network and provides the framework for management applications. In a Fibre Channel network, there are two primary ways to manage switches and other devices. The most common method is out-of-band management, which typically uses IP to communicate with the SAN devices. The second method is in-band management, which requires a Fibre Channel connection into the environment.

The Storage Network Industry Association (SNIA) has identified the following business drivers associated with data security: (Eric A Hibbard. 2005)

- Theft Prevention – Threats of insider larceny, industrial espionage, and organized crime exploitation are on the rise. Perpetrators are often faced with few defenses, motivated by potentially high rewards, and confronted with light penalties if

caught. Data security may provide enough of a deterrent that it prevents the crime altogether or makes it less rewarding

- **Prevention of Unauthorized Disclosure** – Increasingly, data protection and privacy regulations are holding firms accountable for safeguarding their data. The unauthorized (whether intentional or accidental) disclosure of regulated data (customer records, trade secrets, business information) has resulted in serious embarrassment, significant inconveniences and harsh penalties to organizations that do not exercise appropriate due diligence and care. This trend is expected to continue with increasingly severe penalties and an expanding scope of the types of data that are explicitly regulated.
- **Prevention of Data Tampering** – Whether for purposes of theft, blackmail, or malicious destruction (e.g. viruses and worms), unauthorized modifications to data can cause substantial financial losses. An equally insidious possibility occurs in the form of a successful attack with inconclusive evidence of tampering (data may or may not have been modified) that erodes confidence in the integrity of the data.
- **Prevention of Accidental Corruption/Destruction** – The combination of increased complexity within IT, flat or declining budgets, expanding workloads, limited expertise, and inadequate training have increased the likelihood of human error. Something as simple as adding a switch to a live storage network could result in a complete network outage or corruption of data in-flight if the appropriate precautions have not been taken.

- Mistakes within the storage layer can have catastrophic impacts because this is where permanent data resides.
- Accountability Corporate officers are being held to higher accountability.
- Authenticity – As more and more digital records are created, modified, processed, archived, and ultimately destroyed there is a need to demonstrate the authenticity of this data at each stage of its lifetime. To establish the authenticity of data, additional information such as chain of custody, change logs, and conversion records must be maintained.
- Verifiable Transactions – While identification, authentication, and authorization are usually considered to be technologies primarily directed at controlling who can do what to which data, they can also play a role in verifying responsibility for particular transactions that change data values. To fulfill this role, technologies and procedures must be strengthened to meet the standards required for acceptance as evidence in legal proceedings.
- Service Continuity – For many organizations, the availability of business or mission critical data along with the IT resources that use them is of paramount importance. Thus, substantial resources have been dedicated to ensuring continuity of business operations (deal with limited disruption events like system failures, hacker attacks, denial of service attacks, and operator errors) and disaster recovery (deal with "smoking crater" events). These solutions are in addition to high availability designs, redundant configurations, regular backups, and snapshots. Storage technology already figures heavily into these solutions and is expected to play an even more dominant role in the future.

- **Regulatory and Legal Compliance** – Compliance is the ability to demonstrate that a data storage system in a specific industry fulfills criteria established by law or regulation with respect to the operations and outcomes of the storage system. Retention of electronic records has been mandated in both statutory and regulatory law during the last decade. The preservation of legal, medical, and enterprise data in digital form, previously a concern in sound administration of the business, has become a legal necessity that confronts the networked storage industry with both challenges and rich opportunities. How effective a particular security technology, product, or solution succeeds in helping an organization address these business drivers will determine its acceptance. The converse is also true: solutions without links to these business drivers are likely to be rejected.

As the hackers are working hard to revoke data center security, data center designers, vendors, and security teams working hard to ensure data center safety and security. Their efforts evolved many technologies such as: firewalls, Intrusion detection and preventions tools, DoS & DDoS detection and mitigation, access lists, access restriction. Data center defense system works on three layers: 1) Networks, 2) Applications, 3) Databases, figure 13 demonstrate the current available security mechanisms.

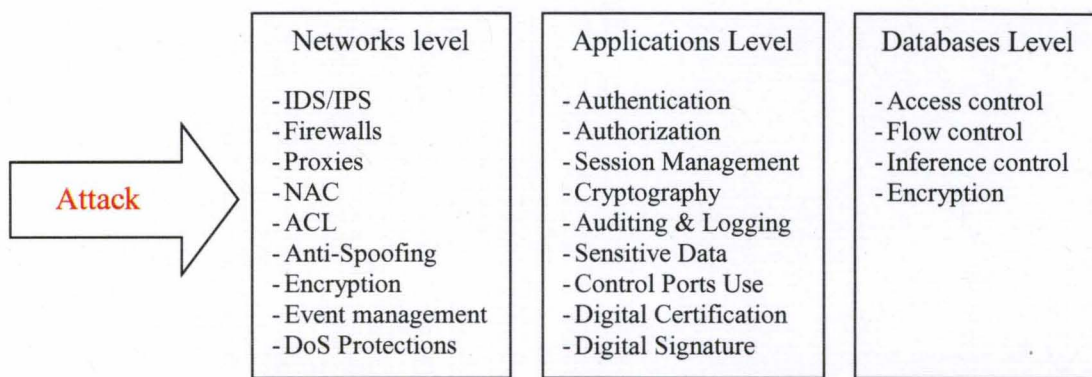


Figure 13: Security Layers Summary

Where: **IDS**: *Intrusion Detection Systems*, **IPS**: *Intrusion Prevention Systems*, **NAC**: *Network Admission Control*, **ACL**: *Access Common List*.

For a resilient data center, security technologies and methodologies expected to grantee system functionally, information assurance, events management and correlations while security policies must ensure speedy detection process and ability to utilize system resources to mitigate attacks effects.

2.4. Data Center Roles

Data Centers play different roles within information system environments, Data center roles are defined based on each application needs and goals. **Active**, **Stand-by**, and **Disaster Recovery** are the main roles as shown in figure 14. (Khalil, Kumar and Elmaghraby, 2007).

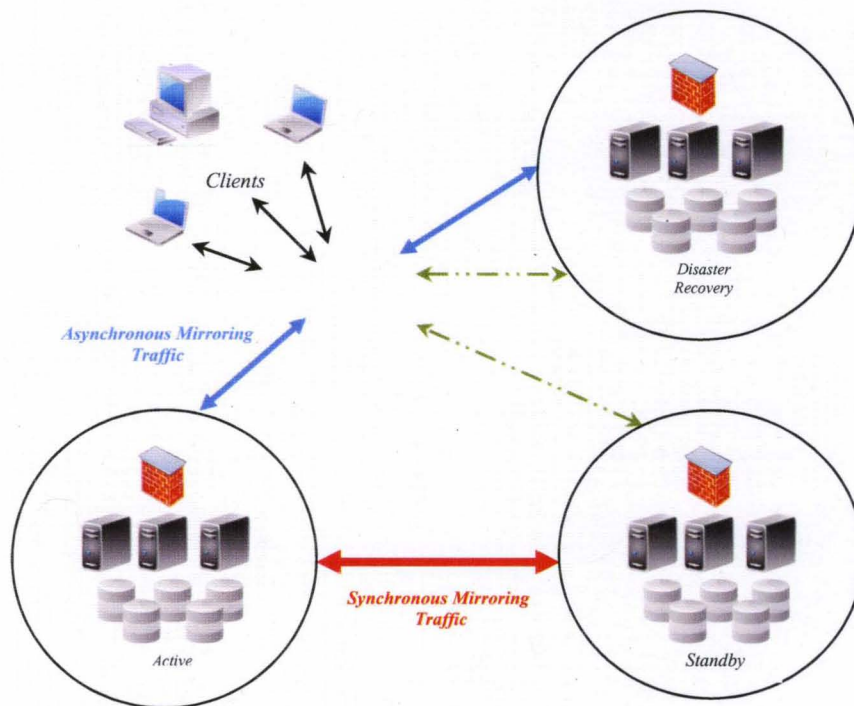


Figure 14: Data Center Role Summary

- *Active Site*: is the main data center which process all clients requested and maintain local data backups.
- *Standby Site*: this data center is ready to process client requests at any point of time if any request was redirected to it,- mainly for load balancing issues- , it is connected to the active site through fibre optics to performer synchronous data replication and it is located within a small distance from the active site.
- *Disaster Recovery Site*: it is located geographically far away from the active site for security reasons, not ready to process user clients while the active site is up, and connected to the active site to perform asynchronous data replication.

Business application requirements and threats determine data center system layout, the following table summarizes data center roles and functionally. In some scenarios a system can consist of active & Standby or active & recovery sites.

Table 5: Remote Data Center Configuration Summery

| | Active – Active scenario | Active – Standby scenario |
|----------------------|------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| Purpose | - Handle traffic requests | - Backup for the active system |
| Configuration | - Replication is bidirectional - Users can access both sites - Application Characterization | - Replication is unidirectional - Users access active site only - Application Characterization |
| Tools | - Data Mirroring & replication - Load balancing tools - Network monitoring tools - Security tools | - Data Mirroring & replication - Desks unlock tools - Security tools |
| Comment | - Active all the time - Adequate use of resources | - Idle most of the time - An inadequate use of resources |

3. INFORMATION SYSTEMS EVALUATION & RELATED WORK

3.1. Evaluations Process

The evaluation process of computer systems seeks a response for some concerns about the system including performance or availability. The initial step is to analyze the users or designers concerns to comprehend the problem, and state the target and restrictions as accurately as possible (Gunter Bockle 1996). Any evaluation problem has four basic components:

- a) The system architecture (Hardware and/or software): Identify the system and its sub-systems components, structure, and parameters that affect the evaluation.
- b) Workloads that the system has to cope with it represent the jobs and services handled by that serving system.
- c) Metrics to evaluate the system: It is the system properties (criteria), which help the user or the designer to make decision.
- d) Evaluation method: Different approaches can be used for evaluation such as analytical models, simulation, real measurements, or any combination.

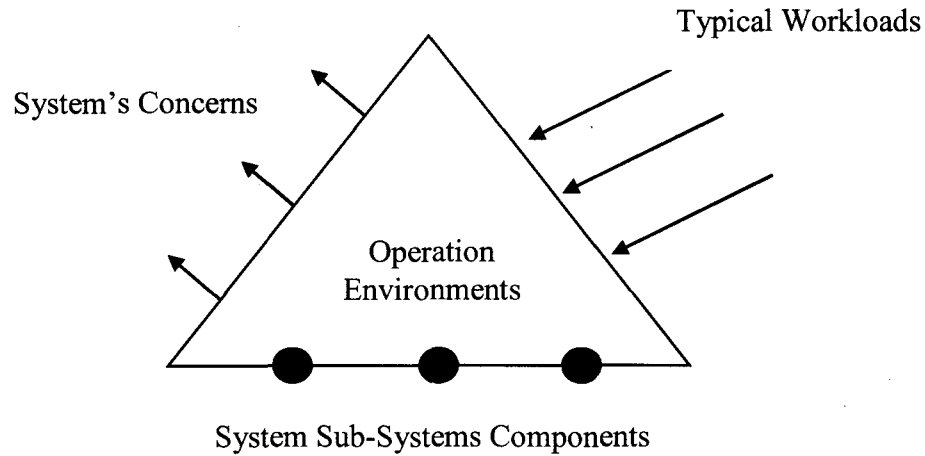


Figure 15: System Evaluation Process

Where systems concerns, in this case, are resilience requirements, system sub-systems are data storages, computer networks, security storage and data mirroring.

For any evaluation process it is very important to have well controlled/ isolated environment to designate the impact of different factors on the overall evaluation results, which raise the need for a realistic test-bed that is able to provide accurate measurements and responses for the mandatory parameters needed for the evaluation process.

3.2.Data Center Performance Analysis

From a logical perspective, a DC environment consists of different components and resources, as well as their relationships, dependencies and other associations. Relationships, dependencies, and associations between DC components are not necessarily limited to their physical connectivity for example; a DC relationship may be established between a client and a group of storage devices that are not physically collocated. Logical relationships play a key role in the management of DC environments. Some of the basic relationships for a typical DC are: (Wilson 1998)

- Storage subsystems and interconnect entities.
- Between storage subsystems.
- Server systems and storage subsystems (including adapters).
- Server systems and end-user components.
- Storage and end-user components.
- Between server systems.
- Physical facility elements

3.2.1. Performance Challenges

Some of the major issues facing Data center DC include physical complexity, proprietary architectures, high availability, scalability, and over-provisioning. The following factors are involved in defining the desired performance level and the data center's ability to meet those levels:

- Application complexity: applications get more complex over time, with commensurately higher computing requirements.
- More users and transactions: The number of people and enterprises connected to applications are rapidly increasing.
- External networking means unprecedented volatility in load, with daily and weekly fluctuations of five or 10 to one now commonplace. The brute-force approach of over-provisioning for the highest predicted load as an inelegant solution to the problem.
- Increasingly layered and disaggregated architecture: The standards underlying networked applications tend toward a complex, layered architecture that manifests itself as a disaggregated, distributed environment. Originally intended to

minimize software and system intricacies, separating components onto different execution environments has increased datacenter complexity and exposed fundamental server limitations.

- OS limitations: Despite continued progress in OS technology, experience has led users to isolate applications on separate servers for increased reliability and manageability.

3.3. Reliability, Availability, and Serviceability (RAS)

Reliability, Availability, and Serviceability (RAS) features are mandatory for any critical information systems. The magnitude of each feature is related to system objective and requirements; RSA requirements are increasing as the system goals are demanding and data criticalness. The following sections will illustrate an overview for Reliability, Availability, and Serviceability.

The term was first used by IBM to define specifications for their mainframes and originally applied only to hardware. (RAS) is a set of related attributes that must be considered when designing, manufacturing, purchasing, or using a computer product or component.

RAS features were evolved through several strategies such as: Homogenize infrastructure and Operations, Ensuring quality of delivered service, Layers of redundancy and data-checking mechanisms.

3.3.1. Reliability

Reliability is defined by the IEEE as *“the ability of a system or component to perform its required functions under stated conditions for a specified period of time”*.

System reliability is a key challenge in system design. Avoiding downtime and the cost of actual downtime make up more than 40% of the total cost of ownership for modern systems. *Reliability*, in the simplest form, is described by the exponential distribution (Lusser's equation), which describes random failures:

$$R = e^{-(n \cdot t)} = e^{-(t/Q)} = e^{-N}$$

Where, t = target,

n = failure rate,

Q = mean time between failures,

N = number of failures during the targeted time

The fundamental element for building more reliable systems is to first better understand what makes system unreliable, i.e. what do failures in today's large-scale production systems look like. Much research, in industry as well as academia, is based on hypothetical and often simplistic assumptions, e.g. "the time between failures is exponentially distributed" and "failures are independent". The reason is that there is virtually no data on failures in real large-scale systems publicly available that could be used to derive more realistic models (Bauer 2010).

System Reliability consists of:

- Hardware Reliability.
- Software Reliability.
- Reliability of interaction between hardware and software.
- Reliability of interaction between the system and the operator.

The reliability “bathtub curve” models particular form of the hazard function. For example, the following figure, there are three main areas; each one represents certain stages as follow (Georgia-Ann Klutke 2003):

- The early life period: elements fail at a high but decreasing rate.
- Useful life period: elements have a relatively constant failure rate caused by randomly occurring defects.
- The Wear out period: failure rate increases due to critical elements wearing out.

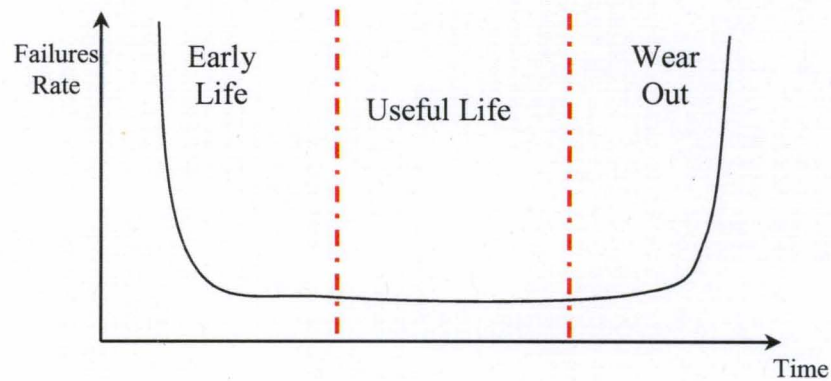


Figure 16: Reliability BathTUB Curve

The bathtub curve is often modeled by a piecewise set of three hazard functions:

$$h(t) = \begin{cases} c_0 - c_1 t + \lambda, & 0 \leq t \leq c_0/c_1 \\ \lambda, & c_0/c_1 < t \leq t_0 \\ c_2(t - t_0) + \lambda, & t_0 < t \end{cases}$$

Where, λ is the failure rate

3.3.2. Availability

Availability is defined as *“the degree to which a system of component is operational and accessible when required for use”*.

$$\text{Availability} = \text{Uptime} / (\text{Uptime} + \text{Downtime})$$

The main goal is to minimize downtime, since as downtime reaches zero availability get the 100%. However, not all downtime consists of unexpected events, since it also includes planned maintenance (Dougall 1999).

Availability Measurements can go through many layers as follow:

- 1- Network Infrastructures
- 2- Application layer
- 3- System Software
- 4- Operating Systems
- 5- Hardware & Storages
- 6- Foundational facilities

Monte Carlo principles and Markov techniques may be used to represent the complete system as a series of identified states because they break down the problem into:

- 1- States and Transitions,
- 2- The time taken
- 3- Probability of moving between states.

The typical parameters used are (Bauer 2010):

- MTBF - the mean time between failure in hours
- MTTR - the mean time to repair a specific failure
- FIT - Faults in time, measured as failures in one billion

- LFTR - Chance of a Latent Fault

3.3.3. Serviceability

Serviceability is a broad definition describing how easily serviced or repaired a system is. Serviceability is also known as supportability. It depends on several issues such as the easy access for the broken elements, easy to find replaceable components and the capacity to provide easy updates.

Product data contains the date the product was manufactured, when it was vended, when it was repaired and how, etc. Similar events consist of the same or similar types of alerts and other information coming from products and into the back end data center. Finally

Serviceability interfaces enable remotely querying product data, updating firmware, reconfiguring and other serviceability action which could be performed remotely. Unified serviceability dramatically reduces service delivery cost because of unification of tools, educating operators, increased automation, etc. The following figure shows the Service Incident Lifecycle. (Chris Connelly 2009)

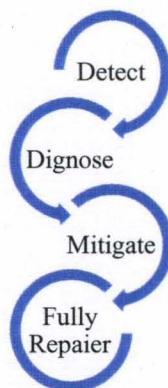


Figure 17: Service Incident Lifecycle

RAS goals can be categorized into three main points: Minimize planned downtime, Minimize unplanned downtime, and Rapid recovery after a service degradation (Griffith, Virmani and Kaiser 2007). Yet, there is no sufficient information about the system behavior before/during and after the malicious activities (attacks, natural disaster). The next section will introduce resilience concept.

3.4. Resilience Concept

The term Resilience has used mainly within the psychology domain to characterize the positive capacity of people to cope with stress and adversity (Holling 1973). However, the common interpretations can be summarized as: The ability to recover from or adjust easily to misfortune or change. The following figure (Fig. 18) illustrates the main differences between a resilient system and non-resilient system.

Two thesaurus definitions for resilience are available as follows: (Resilience)

- 1- “The capability of a strained body to recover its size and shape after deformation caused especially by compressive stress”.
- 2- “An ability to recover from or adjust easily to misfortune or change”.



a



b

Source: a) <http://maasstreesservice.com> b) www.sxc.hu

Figure 18: Resilience illustration

As shown, Figure (18.a) represents a huge healthy tree but it could not resist the stormy winds. While the palm tree (18.b) bent to avoid breakage and after the storm it typically returns to its original shape.

Basically, it is very important to ensure that the nations' information system infrastructures are resilient like the palm tree where its performance, efficiency or QoS can be degraded but able to recover immediately once the illegitimate activities termination.


The adapted Resilience Definition for use in this research is *“The ability of information systems to tailor any unexpected changes in the operation environment without significant changes in the information system **“efficiency/performance”** and achieve speedy recovery from attacks/disturbance”*.

3.5.Metrics Comparison

Resilience metric differs from the other existing metrics because it measures another feature of the system, which is “The resilience level”. Based on resilience definition, the speed of recovery and quality of service during the up-normal operational conditions should be investigated to ensure system resiliency. The speeds of recovery and service quality are impacted by systems elements and architecture. For example, the speed of recovery affected by recovery process system (automated vs. manual). We surveyed different data center architectures and proposed a list of parameters can impact the resilience level. For example: mean recovery time, mean attack detecting time and mean failure time for a given system are considered.

Table 6: Summary for Data Center System Concerns

| Metric /Architecture | Performance | | | | Availability | | | | Fault Tolerance | | | | Robustness | | | | Resilience | | | |
|---------------------------------------------|-------------|---|---|---|--------------|---|---|---|-----------------|---|---|---|------------|---|---|---|------------|---|---|---|
| | DS | N | S | R | DS | N | S | R | DS | N | S | R | DS | N | S | R | DS | N | S | R |
| Sub-criteria | | | | | | | | | | | | | | | | | | | | |
| Response T. | • | • | | | | | | | • | | | | • | • | | | • | • | | |
| Delay | • | • | | | | | | | • | | | | | • | | | • | • | | |
| Throughput | • | • | | | | | | | | | | | • | • | | | | • | | |
| Dropped P. Ratio | | • | | | | • | | | | | | | • | • | | | | • | | |
| L. utilization | | • | | | | | | | | | | | | | | | | • | | |
| Retransmission rate | | • | | | | • | | | | | | | | • | | | | • | | |
| Service rate | • | | | | • | | | | • | | | | • | | | | | • | | |
| Disk I/O rate | • | | | | | | | | • | | | | | | | | • | | | |
| CPU Utilization | • | | | | • | | | | • | | | | • | | | | • | | | |
| Latency | | | | • | | | | | | | | • | | | | • | | | | • |
| No. of positive Alerts/ total no. of alerts | | | • | | | | | | | | | | | | • | | | | | |
| Detection T. | | | | | | | | | | | | | | | | | | | • | |
| Recovery time | | | | | | | | | | | | | | | | | • | • | | |
| Time to fail | | | | | | | | | | | | | | | | | • | • | | |
| Time down/ operation time for device | | | | | • | • | | | | | | | | • | | | • | • | | |
| Mirroring pause time | | | | | | | | | | | | | | | | | | | | • |
| Mirroring time | | | | • | | | | | | | | | | | | • | | | | • |

Table Key: DS: Data Storage, N: Computer Network, S: Security System, R: Replication Approach
: Not covered by any of the existing metrics

One of the important questions which need to be answered was “Do we really need to have a new metric for resilience?” By studying the existing metrics and survey the elements of each metrics, we realize lack of measures for the following parameters as shown by Table 6 and Figure 19 (Khalil, Elmaghraby and Kumar, Evaluation of resilience for Data Center systems 2008).

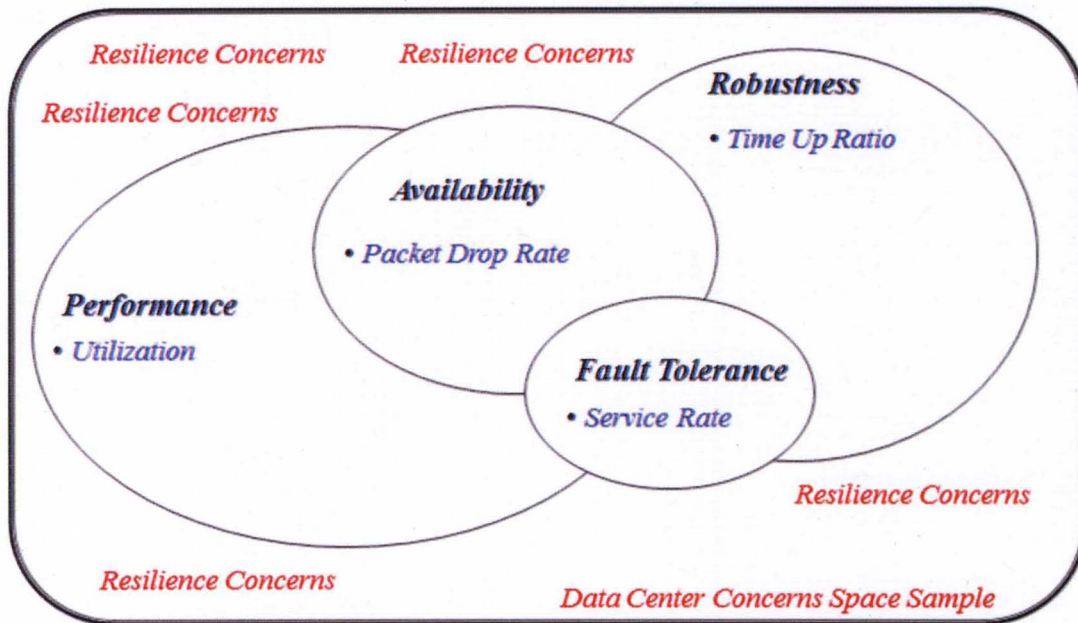


Figure 19: Data Center Resilience Concerns

3.6.Related Work

Although that the concept of developing a resilient information systems still growing, there is a lot of research work have been to done contributing to resilience development. For example, developing methods for mitigation of attacks impacts on QoS of computer network or data storages will contribute to the one of the systems resilience. In the other hand, it is important for this research to highlight the relations between resilience and merging concepts such as cloud sustainability.

3.6.1. Adaptive Response for Distributed Denial-of-Service Attacks

This dissertation presents a Distributed denial-of service Adaptive Response (DARE) system, capable of executing appropriate detection and mitigation responses automatically and adaptively according to the attacks. It supports easy integration of distributed modules for both signature-based and anomaly-based detection. Additionally, the innovative design of DARE's individual components takes into consideration the

strengths and weaknesses of existing defense mechanisms, and the characteristics and possible future mutations of DDoS attacks. The distributed components work together interactively to adapt detection and response according to the attack types. Experiments on DARE show that the attack detection and mitigation were successfully completed within seconds, with about 60% to 86% of the attack traffic being dropped, while availability for legitimate and new legitimate requests was maintained. DARE is able to detect and trigger appropriate responses in accordance to the attacks being launched with high accuracy, effectiveness and efficiency. (Thing, Sloman and Dulay 2009)

Yet, as for the DARE limitations, the attack detections rely heavily on the network monitoring data captured and collected. It is not practical to reroute all transit traffic, so only flow-based traffic statistics and the content of selected packets are exported. As a consequence, the attack detection possibilities are restricted by the nature of the available monitoring data, which causes a limitation in DARE such that all the detection modules have to be designed by taking into consideration such restrictions. The following figure show the Traffic Redirection Attack Protection System (TRAPS) used for experiments.

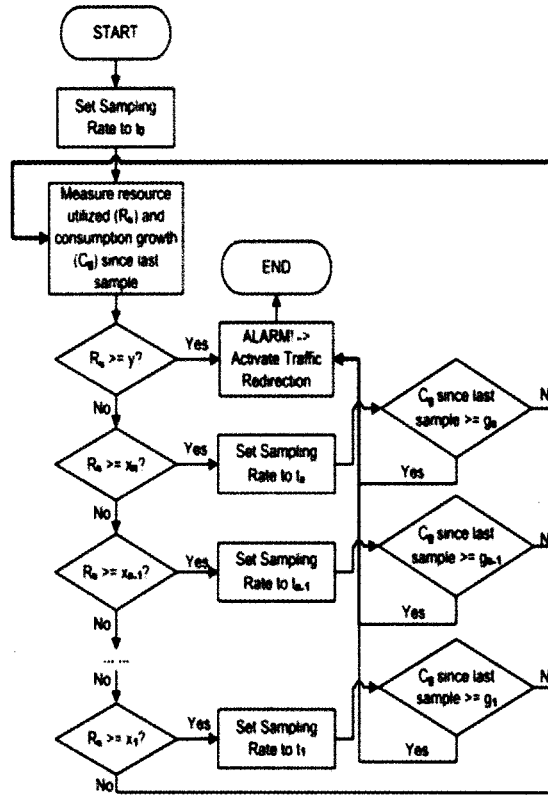


Figure 20: Traffic Redirection Attack Protection System Flow Chart
Proposed by Thing, Sloman and Dulay 2009

3.6.2. Cloud Sustainability

Cloud Computing is an emerging paradigm providing on-demand IT services. From the providers point of view managing the ultra large scale computing platform within a successful business model is a challenging process. On the consumer side, clients are looking for secure, reliable, and economical services. The increased awareness of the environmental impacts of data center and Cloud Computing highlighted the need for using sustainability as a performance indicator for Cloud Computing.

Quantifying the impact of sustainability of large systems such as Cloud Computing or data center involves three factors: economic, ecological, and social. Several challenges face researchers to quantify sustainability such as: developing

accurate model, measuring & assigning value to ecological & economic impacts, and incorporating sustainability practice into industry.

Sustainability interfaces with economic, ecological, and social, “Our Common Future” report by the Brundtland Commission (1987), defined sustainable development as, “Meeting the needs of the present generation without compromising the ability of future generations to meet their own needs.” (Bruntland 1987)

Different sustainability development models can be used to address different sustainability preference such as: (Scott Cato 2009)

- 3-Legged stool model where each economic, ecological and social have equal significance.
- 3-Overlapping-circles model where economic, ecological, and social have unequal significance.
- 3-Nested-dependencies model reflects economic, ecological, and social co-dependent feature.

Data center is core element of cloud architecture, disturbed data center was always a method to develop an efficient and resilient data centers (Vaidyanathan, et al. 2007). Site selection process for disaster recovery site or stand by site highlight the relation between data center resilience and cloud computing in terms of: economics of the selected site, the impact of building the site on area environment and how to utilize environment to reduce costs.

For Cloud Computing, Sustainability evaluation model can be constructed as follows:

$$\text{Sustainability} \sim f(\text{Economic, Ecological, Social})$$

Where: Economic $\sim f(\text{Servers, Storage, Networking, Facility, Support, Efficiency,})$

Ecological $\sim f(\text{Carbon Emission, Water Use, Resource Consumption,})$

Social $\sim f(\text{Economic Development, Sociopolitical Stability,})$

Using the Jericho Forum's Cloud Cube Model (CCM), the cloud computing business models can be classified into eight types: (Jericho Forum 2010)

- 1- Service Provider and Service Orientation;
- 2- Support and Services Contracts;
- 3- In-House Private Clouds;
- 4- All-In-One Enterprise Cloud;
- 5- One-Stop Resources and Services;
- 6- Government Funding;
- 7- Venture Capitals;
- 8- Entertainment and Social Networking.

A newly proposed Hexagon Model that includes six key elements for sustainability based on Sun Tzu's Art of War and literature review, and the sixth factor is rated based on case studies and peer reviews. Capacities occupied in the Hexagon can represent assets and weaknesses of a cloud business. Apart from the qualitative approach, the quantitative approach they use is the Capital Asset Pricing Model and Modern Portfolio Theory, both of which aim at computing organizational sustainability and predict how well an organization can perform. The OMII-UK data is used to demonstrate sustainability and study the impact on cloud businesses, and is presented by statistical

computation, 3-D visualization and the Hexagon Model. The adopting appropriate for cloud computing business model will help organizations investing in this technology to stand firm at all times (Chang, Wills and De Roure 2010) .

3.6.3. Approaches for Mitigation of Storage Security Risks

Data storage is an important element of data center where data are stored. Data storage faces several risks and threats such as attacks and natural disasters. Developing mitigation plans to face the impact of those risks is required. To achieve this goal - mitigation the impact risks- several functions need to be implemented as follows: assessing the risks associated with natural and man-made threats, formulating combinations of mitigation strategies for facilities exposed to those threats, and using economic tools to identify the most effective combination of strategies. (Arnold 2007) There are different approaches that can be used to mitigation of storage security risks such as:

- Authentication:
 - An administrator must log on to get the right to do any administrative actions are permitted. Complex password mechanisms are preferred such as hierarchal password.
 - Emerging technology: a device must not only be on the list of devices permitted in the storage network, but must also proving that it is in fact who it says rather than an impostor. This prevents a rogue system from, for example, pretending to be a switch and issuing unauthorized I/Os with

forged WWNs to bypass LUN-level security. Fibre Channel's FC-SP protocol works this way.

- Authorization
 - Verify that the specific administrator who issued a command is authorized to do so, before performing the requested action.
 - Disk arrays must verify that the specific system that issued a read or write command has permission to do so for that LUN.
- Audit
 - The storage subsystem as a whole must log all administrative actions and any events of significance. This is typically done individually in devices, but software to present a single view is required.
- Encryption (not wide use)
 - Protects both confidentiality and integrity of data.
 - Data on tape and other removable media can be encrypted.

The following figure demonstrate the balancing between security and cost

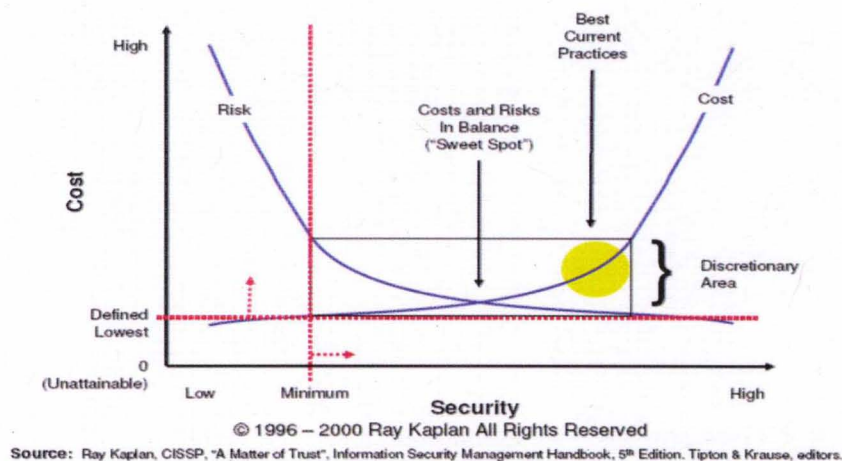


Figure 21: Balancing Cost and Security

4. NETWORK RESILIENCE ENHANCEMENT OPPORTUNITIES

Computer networks are one of the cores of the data centers endangered by malicious activities and natural disasters. These threats stress the need for a resilient computer networks to ensure business operational continuity and optimum performance. In general, fast recovery from a degraded system state is often termed as resilience (Trivedi, Kim and Ghosh 2009). A degraded system state can be caused by hacking the network or natural disaster, potential result for system hacking or natural disaster is the exchange of topology state information. System administrators used dynamic routing protocols to ensure QoS in case of topology changes (Ali, Mouftah and El-Sawi 1997).

Utilizing every single working sever within the data center is very important to provide high services level (Wenzheng and Hongyan 2010). In case of limited sever failure; the recovery can be done by redirecting the traffic to working server in a timely manner. This small recovery process can be done using sever load balancing algorithms (SLB).

As shown routing protocols and server load balancing play significant role in network reaction to certain failure caused by severs failure or unexpected network topology change. This chapter illustrates how routing protocols and several loads balancing can impact resilience.

In addition, recovery from degradation state requires using alternative paths or backup devices. System designer used severe approaches to implement network

redundancy (Jeng and Siegel 1988). In this chapter we proposed novel approach for select critical routers to be redundant to develop alternative routes.

4.1. Routing Protocols

Packet routing is a very critical process which affects computer network performance and the quality of service (QoS). Simply packet routing is the process of path selection to send traffic between two nodes. There are several routing protocols. A routing protocol specifies how routers communicate and collaborate to select suitable routing paths along the network. (Macfarlane 2006)

Routing protocols can be classified into static and dynamic algorithms. Although a static routing algorithm is not an appropriate term but it has been used referring to the use of a static routing table. (Medh and Ramasamy 2007)

The dynamic routing protocols are classified into several categories:

- Single-path versus Multi-path

Some advanced algorithms will maintain multiple paths to the same destination while other algorithms will provide one path.

- Link state versus Distance vector

It classifies routing algorithms based on whether the routing table or its shared portion is shared with all routers or only with neighboring routers.

In addition, dynamic routing protocols also can be categorized into: Interior vs. Exterior routing protocols. The interior routing protocols are used within an autonomous system, while the exterior protocols are used between autonomous systems. The next section will present a brief demonstration of routing protocols evaluations metrics.

4.1.1. Routing Protocols Evaluations Metrics

Graziani and Johnson in their book “Routing Protocols and Concepts, CCNA Exploration Companion Guide” demonstrated that the common used protocols are: (Graziani and Johnson 2007)

- Routing Information Protocol (RIP)
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Border Gateway Protocol (BGP)

Those routing protocols can be implemented with different variant, for example Border Gateway Protocol (BGP) has several versions: BGP4, EBGP, IBGP, and EGP. Recently, many researchers evaluated routing protocols performance or the impact of routing protocols on network QoS (quality of services) level. In general system administrators used the following metrics: (Medh and Ramasamy 2007)

- Ease of use
- Network topology limitation
- Vendor support
- IPv6 support
- Reliability/Robustness
- Load management

System administrators and researchers use all or combination of those parameters to select a routing protocols appropriate for their application.

4.1.2. Routing Protocols and Resilience

Several research works have been done to improve network resilience –speed recovery from degradation state- using routing protocol; Kvalbein et al presented a

recovery scheme called Multiple Routing Configurations (MRC). Their scheme uses a single mechanism to handle both link and node failures, regardless of the root cause of the failure. (Kvalbein, et al. 2006)

The same research group at Simula Research Laboratory developed a new routing protocol: Resilient Protocols and Internet Routing (REPAIR) which resolves some of the current protocols deficiency within the context of: (<http://simula.no/> 2007)

- Proactive local recovery
- Adaptive routing
- Scalability

Our efforts in network resilience section focus on finding a selection criterion for a resilient routing protocol using the following factors:

1. Performance/Efficiency degradation detection
2. Speedy recovery
3. Minimum overhead

4.2. Load Balancing Algorithm

System administrators used Server Load Balancing algorithms (SLB) to distribute and balance the system's workload over the available servers, primarily SLB have been used to optimize data center's resources utilization, improve performance, and ensure high availability and reliability. DC's resilience level is affected by each component of data center's architecture; since SLB algorithm is fundamental component of data center, it will have significant effect on data center resilience level.

An optimum SLB algorithm will distribute system's workload over the available servers with minimum variation between servers' workloads (Baruch Awerbuch, Mohammad T. Hajiaghayi, Robert Kleinberg and Tom Leighton 2005).

SLBs are providing certain function such as (for large scale systems): (Bourke 2005)

- Divide the incoming traffic into independent services request.
- Apply dispatching policy.
- Keep track of each server: load, response, and availability (IP/Ports).
- Perform NAT network address translation.
- Server health monitor.

Generally, SLB algorithms are implemented by devoted software or hardware device with various architecture scenarios. On the other hand to select an optimum SLB, different factors should be investigated such as: hardware, application type and the desirable goals such as performance, reliability, and system resilience.

4.2.1. Server Load Balancing Architecture & Algorithms

Data center's servers can be distributed locally within the same site or over geographically distributed sites. The focus of this research work on locally distributed servers. The main key aspects for distributed architectures classification are: existence of virtual server and the implementation of virtualization and its relation with the OSI network model. Based on those aspects the distributed architectures can be classified into (CARDELLINI, et al. 2002):

- Cluster-based web system: there is a single front-end device associated with virtual IP (VIP) address and the clients have access to the VIP.

- Virtual web cluster: the clients access only the VIP address but in this architecture, it is associated and shared to all the real servers.
- Distributed web system: the real IP addresses of the servers are exposed for the client's applications.

On the other hand, SLB architectures can be classified into two categories:

- NAT-based Architecture.
- Flat-based Architectures.

Some references refer to them as DNS-Based system & Dispatcher-Based system.

The main difference between the two categories is that the SLB unit performs a NAT from one network to another.

In a DNS-Based system, basically it use a functions of DNS to associated different IPs with the same host name, the SLB device sits between the clients and the server, in some case it apply NAT to mask the server IP addresses. For the Dispatcher-Based system, the dispatcher receives job requests and then sends it to the right server based on SLB's policy.

The main characteristic of any server load balancing algorithm is its ability to direct job requests to the proper server to provide optimum resources utilization. The basic server load balancing algorithms are: (Bryhni H., Klovning E. and Kure O. 2000)

- 1- Round-Robin: works by responding to client's requests by a list of IP addresses associated with the host name, the first IP address on the list is used number of times and then moved to the bottom of the list, then use the second IP address on the list.

- 2- Weighted Round-Robin: performs like Round-Robin, but able to maintain server with different capacity.
- 3- Least-Connection: server with minimum number of active connection gets the next request.
- 4- Weighted Least-Connection: performs like least-connection, with ability to manage servers with different processing rate.
- 5- Server Load: Based on predicted server load, direct the traffic to the server with minimum load.

Analytical modeling (Kohler 1979) and Simulations (J.W.Liu 1986) are the main approaches for evaluating and studying SLB algorithms, queuing network is the foundation for the analytical approaches. On the other hand, simulations are used for practical and reasonably accurate scenarios and options. Extensive SLB's performance evaluation has been done for various IT architecture using different methodologies.

Chhabra et. al. identified a group of general parameters for load balancing algorithms which can be used for comparison and classification purposes as follow: Nature, Overhead, Resource Utilization, Processor Thrashing, Predictability, Adaptability, Reliability, Response time and Stability (Chhabra Amit 2000).

4.2.2. Our Server Load Balancing Evaluation Methodology

Considering the following scenario; one of the servers got hacked by insider or physically damaged which resulted on sever breakdown. A resilient data center will absorb this change with minimum change on system performance/efficiency.

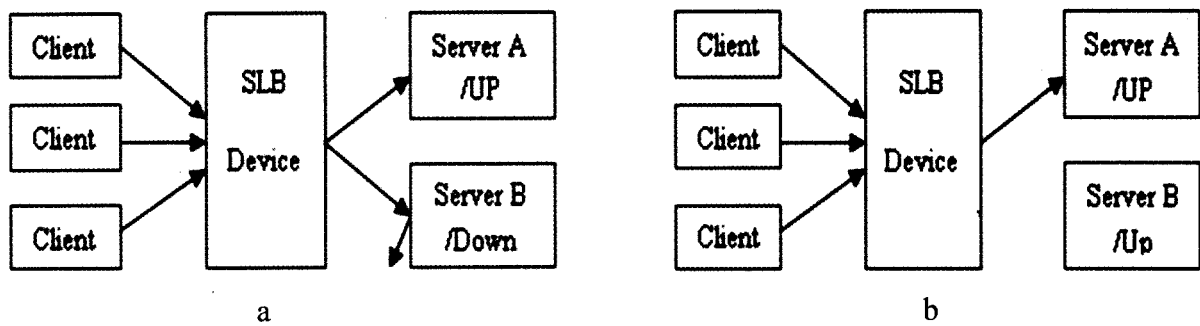


Figure 22: SLB Scenarios

As shown Figure 22 shows two cases:

- a. In this case the SLB device didn't update its available server list, so he still sending traffic to server B although it is down which cause higher rate of denied requests.
- b. SLB device didn't update the available server list, so server B doesn't receive any traffic to process although it is up.

As we can see in both cases the system didn't adjust probably to the operating environmental changes, which impacted in poor resilience level. The key element in this scenario is SLB algorithm; the SLB should be able to update its available server list in a very short time to better utilization and shorten the recovery time.

Different approaches for server health monitoring are available; some are simple such as SLB polling where SLB device check the server IP/ports to detect server status. Others are more complex by using scripts to check applications status, not only server status. However that activity will show up on the traffic between SLB device and servers which raise the need to study the traffic. In this research different parameters such as: send/received ACK count per connections, retransmission count, segment delay, response time and round trip segment deviation were investigated, yet theses parameters are affected by other factors other than SLB approach such as network protocol which will

create biased experiments. The traffic between load balancing device and the available servers, it can be categorize as:

1. Server health monitoring traffic
2. Clients' requests and responses

$$T_{\text{total}} = t_{\text{server monitoring}} + t_{\text{actual requests/responses}}$$

“ $t_{\text{server monitoring}}$ ” is a very tiny traffic which is ON all the time, our objective is to collect statistics about the “ $t_{\text{actual requests/responses}}$ ” when it initiated, resumed or blocked. Compare that with the server up/down statistics.

The results show that server health detecting time -the time SLB need to detect server statues-, time period to reach the steady state and CPU utilization can be utilized to designate which SLB will add to improve network resilience.

4.3. Using Social Network Analysis for Network Resilience Improvement

This section presents a novel approach to discover the critical network's nodes – to be redundant as alternatives in case of failure- based on social network analysis (SNA) which have been used for social studies and recently have been widely used in many domains. The main focus of social network analysis is to study the “relations” between network nodes. The term relations within computer network domain used to describe: traffic volumes, direct connections, active connections, number of connections (J. Scott 1992). In principle, critical network's nodes will be identified based on their magnitude for the network in terms of centrality: Degree, Betweenness, and Closeness.

4.3.1. Social Network Analysis Overview

Social network analysis is an emerging set of techniques and schemes for data analysis, many researchers, and scientists introduced several definitions based on their domain of interest. For example Hannemann proposed: “A social network is a set of actors that may have relationships with one another. Networks can have few or many actors (nodes), and one or more kinds of relations (edges) between pairs of actors.” (Wasserman and Faust 1994)

The major deviation for social network analysis over the other traditional approaches is its focus is to analyze information based on the relation between data entities. Social network can be represented as matrices or graphs; the plus of using graph is the ability to represent different types of relations between the nodes. One of the important concepts of social networks analysis is the hierarchical analysis, as the analysis can be proceed on different levels: Node, Dyadic, Triadic, Subset, and Network level. However, the focus of the majority of research work is narrowed to the node and network level. (J. Scott 1987)

At network level, network density can be obtained by dividing the number of relations by the number all possible relations; the result varies between 0 and 1, the higher ratio the denser network. Another level would be the node level where it is more concerned about how important is the node? How popular is the node? Is it a central node?

Within the context of social networks the term power/centrality refers to the impact of this node on others nodes, and what would be the consequence in case of removing this node. Social network analysis offers several measurements and this work focus on three

of them for centrality: Degree centrality, Closeness centrality and Betweenness centrality.
(Freeman, Borgatti and White 1991)

4.3.2. Social Network Measurements

This section presents the set of social network analysis measurement used to identify importance (or prestige) of various network nodes.

Degree Centrality: the degree centrality of a node A (DC_a) is number of connections/relations the node has. The node/actor with higher number of relations or ties maintains a higher traffic (in/out).

$$DC (N_i) = \sum_{j=1}^n a_{ij}$$

Where:

$DC (N_i)$: Degree Centrality of node N_i ,
 A : an adjacent matrix of relations network,
 n : number of nodes.

Centrality closeness: indicates how a node N_i close to the other nodes, depending on the application closeness would have different ways to be calculated. In computer networks scenario, our target will be physical distance.

$$CC(N_i) = 1 / \sum_{j=1}^n d(N_i, N_j)$$

Where:

$CC (N_i)$: Closeness of N_i ,
 $d(N_i, N_j)$: absolute distance between node N_i and node N_j ,
 n : number of nodes.

Centrality Betweenness: it measure characterizes of nodes as having a powerful positional i.e. a node is frequently shown in communication paths between any other nodes.

$$CB(N_i) = \sum_{j,k} \frac{P_{j,k}(N_i)}{P_{j,k}}$$

Where:

$CB(N_i)$: Betweenness of N_i ,

$P_{j,k}(N_i)$: shortest path between N_j , N_k and has N_i on it

$P_{j,k}$: shortest path between N_j , N_k

4.3.3. Benefits of Using SNA

Building a resilient computer network consolidates two main aspects:

- Device's redundancy: installing backup devices, such as power supplies, routers, switches, etc. that kicks in when the primary fails.
- Develop recovery methodologies and Policies: how to use the backup systems to ensure minimum quality of services (QoS) variation in case of emergency.

Generally, vendors will tell that we need to go with full redundancy, yet it will require large investments and also is complex for monitoring or management purposes. Therefore selecting the critical elements to be redundant is a vital process to ensure network service continuity, calculating the probability of system failure is one of the well-known approaches for redundancy as the more duplication the less failure probability (Connors 1984).

Calculating the probability of system failure approach has several drawbacks such as: assuming failure independency and non-realistic estimation of different probability

weights. The uses of social network analysis provide more realistic information about nodes importance and consider the correlation between devices failure.

Several routing and networking parameters can be affected when one of the routers fail down such as network latency, routing tables size, and packet drop rate. In this study we will focus on network latency as it can reflect the overall network performance. (Barker and Shenoy 2010)

The failure of a critical router or node impacts network latency negatively. In case, there is no backup router installed the latency will propagate faster and can lead to a system failure. Several experiments were implemented to validate the usage of social network analysis in selecting important routers.

5. DATA CENTER RESILIENCE ASSESSMENT

5.1. Problem Statement

To address resilience assessment problem, we adapted the FePIA methodology for deriving the degree of robustness. Shoukat and Sigel, 2004 have proposed a general four-step procedure for deriving robustness metric for any system. This procedure FePIA, where the abbreviation stands for identifying the performance features, the perturbation parameters, the impact of perturbation parameters on performance features, and the analysis to determine the robustness (Ali, et al. 2003).

Initially, we adapted FePIA proposed by Shoukat and Sigel, 2004 as follow to express data center resilience problem. (Khalil, Elmaghraby and Kumar 2008)

Let φ be the set of resilience features which are selected based on the resilience requirements. Φ will be set of performance features that should have limited deviation to ensure that the system is resilient

$$\varphi = \{ \varphi_1, \varphi_2, \varphi_3, \varphi_4, \dots, \varphi_n \},$$

Where, φ_i is resilience feature.

Each feature φ_i has minimum and maximum values: β_i^{\min} , β_i^{\max} . Those values can be determined based on manufacturer configuration such as processing rate or by measurement such as measuring typical bandwidth utilization.

$$\forall \varphi_i \in \varphi, \exists \{ \beta_i^{\min}, \beta_i^{\max} \mid \beta_i^{\min} \leq \varphi_i \leq \beta_i^{\max} \}$$

where,

β_i^{\min} : the min value for efficiency feature φ_i .

β_i^{\max} : the max value for efficiency feature φ_i .

Let Π be the set of perturbation parameters, whose values may be impact the QoS of the selected resilience feature selected belong to φ .

$$\Pi = \{ \pi_1, \pi_2, \pi_3, \dots, \pi_n \},$$

π_i : perturbation parameters.

Let f_{ij} is mapping relation between π_i and $\{\varphi_i, \varphi_j, \dots\}$

$$\forall \pi_i \in \Pi \ \& \ \varphi_i \in \varphi \ \exists \{ f_{ij} \mid \pi_i = f_{ij}(\varphi_i, \varphi_j, \dots) \}$$

where, f_{ij} represents the relation between the perturbation parameters and resilience feature.

Finally determine the threshold for each π_i that will cause any of the resilience features of set φ to revoke the resilience requirement.

5.2. Resilience Evaluation Approaches

To evaluate data center resilience, several approaches were examined. In this section, two approaches will be illustrated: Multi-objectives optimization (MOO) and Operational Analytics (OA).

5.2.1. Multi-Objective Optimization (MOO)

The process of optimizing systematically and simultaneously a collection of objective functions are called multi-objective optimization (MOO) or vector optimization.

The main goal of multi-objective optimization is to model the rank or relative importance of system elements and objectives. The multi-objective optimization methods can be categorized depending on how decision-maker's preferences are achieved or implemented. (Marler and Arora 2003)

Approaches of MOO can be classified as follows:

- Priori articulation of preferences methods

This set of methods allow user to describe preferences, which may be articulated in terms of goals or the relative importance objectives. Most of these methods include parameters, which are coefficients, constraint limits, etc. that can be set to reflect preferences. For example, Weighted min-max method, Lexicographic method, and Exponential weighted criterion methods and others represent the Priori articulation set.

- Posteriori articulation of preferences methods

In many situations, it is very hard to express a clear and decided estimate of the preference function. Therefore, it can be more realistic to allow the decision maker to choose from the visible of solutions. Such methods incorporate a posteriori articulation of preferences, and they are called cafeteria or generate-first-choose-later approaches. Methods such as Normal boundary intersection

(NBI) method, Normal constraint (NC) method, Physical programming are used for Posteriori articulation approach.

- Methods with no articulation of preferences

For many cases, decision-maker may not be able to concretely define set of preferences, a simplified set of methods can be used which do not require any articulation of preferences such as Global criterion methods, Rao's method and others.

5.2.2. Applying MOO to Data Center resilience

We examined how to apply MOO on data center resilience, the first step was to scan all the parameters impacting the resilience level and define systems constraints. A Main-Recovery site operational scenario was examined. In this scenario, there are three main elements: main site, communications, and recovery site.

By applying the adapted FePIA procedure on the resilience problem, we get the following model:

- 1- Identify the resilience requirement: based on resilience definition, a resilient data center should provide a steady QoS during unstable conditions and recovery rapidly from the degradation state.

Thus $\varphi = \{\text{Steady QoS, Speed Recovery}\}$

- 2- Identify perturbation parameters; initially we identified all of the system and operation environment perturbation parameters and based on the set of features of φ , resilience related perturbation parameters were selected as follows:

Steady QoS can be represented by latency, delay, processing time, and response time (Jesshope and Egan 2006) (Patterson and Hennessy 2008). Since response time (RT) is the time between the end of a request on a computer system and the start of a response; RT cover the entire process and include network latency, application processing time. So the response time were selected as perturbation parameters.

Speed Recovery: is the process of system recovery over time, any recovery process has two main steps: errors detection and correction (Burke and Fisher 1982). Mapping those two stews over time, it is no guarantee that the correction steps will succeed to recover the system completely before or after its complete failure. So over the time line, system will have three periods as follows: Mean time to detect malicious activities, mean time to complete/partial failure, and time for complete recovery.

Thus $\Pi = \{\text{Response time, Mean time to detect malicious activities, mean time to complete/partial failure, and time for complete recovery}\}$

The following figure (Figure 24) shows the system and operational environmental potential parameters impacting resilience requirements.

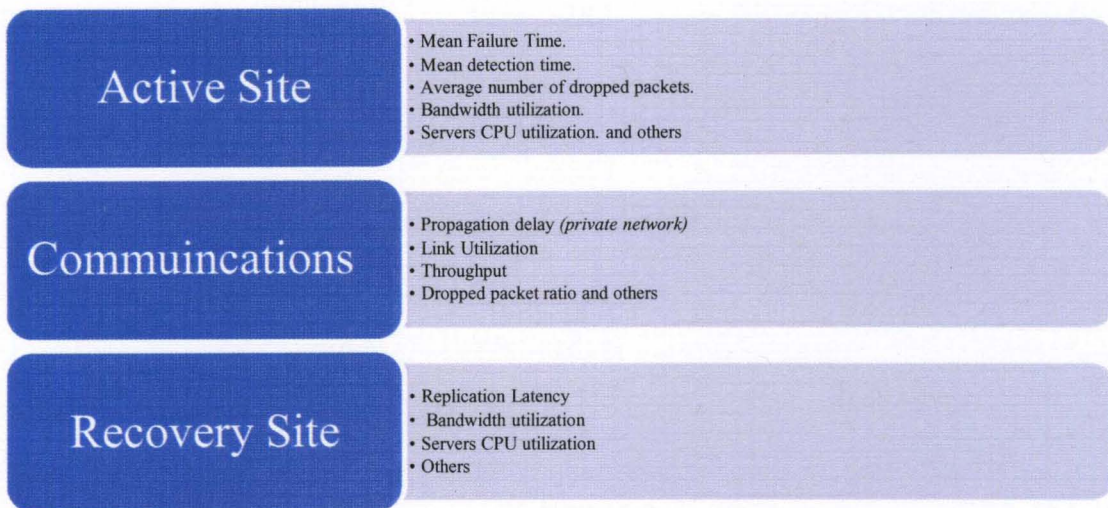


Figure 23: Sample of parameters affects resilience

Data center resilience evaluation process is complicated as it involves large number of parameters and in many cases some of those parameter values are not available or easy to find such as the compact factor for data mirroring approaches. In addition, several aspects and concerns such as diversity of implementations and operational roles. For instance, there are several approaches for employing data storage solutions such as: Network Area Storage (NAS) and Storage Area Networks (SAN) as shown on the following figure (Figure 25)

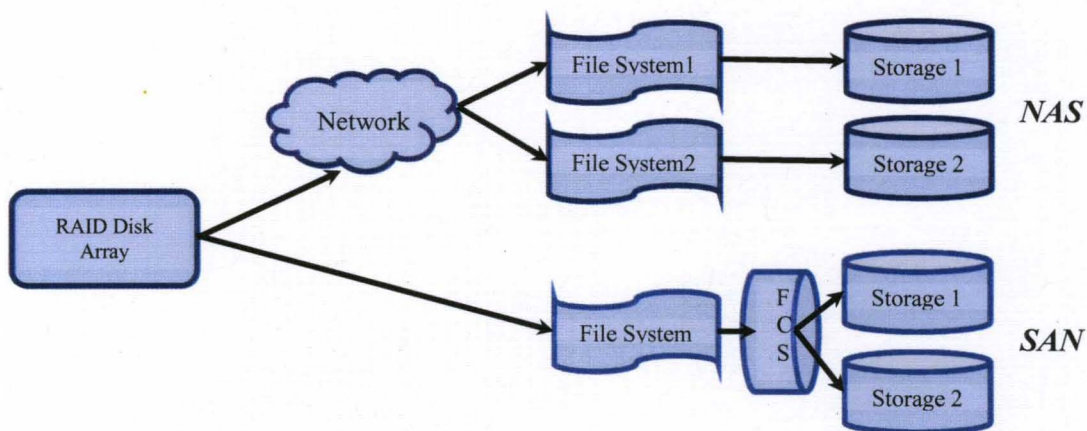


Figure 24: SAN and NAS implementations

In this case, the network element has different magnitude on the solution performance. Such incident highlight the need to develop evaluation approach which is not tied to the data center architecture, configuration or setting.

5.2.3. Operational Analytics (OA)

Operational analytics is a process that facilitates delivery of the in-depth and focused analysis of the performance of each key operational area of the business or systems. Business analytics has improved significantly over the last few years, providing users with better insights, particularly from operational data stored in transactional systems and log files. Operational analytics provide users a better way to utilize the extracted information and improve decision making process (Kohavi, Rothleder and Simoudis 2002).

Operational analytics have several practical challenges to accomplish accurate and realistic analysis (Souza, Manning and Gardiner 2001).

The key challenges are:

- Flexibility
- Pick the right metrics to analyze
- Build in decision analysis
- Others.

5.2.4. Applying Operational Analytics (OA) to Data Center resilience

Within Operational analytics, the first step is to designate which parameters values will be collected. Grounded on resilience definition, a resilient data center should be able to detect malicious activates in short time; resist malicious activates impact for

longer time, and provide speedy recovery. So the main target is to develop a tool able to measure time periods for each phase as shown on the following figure.

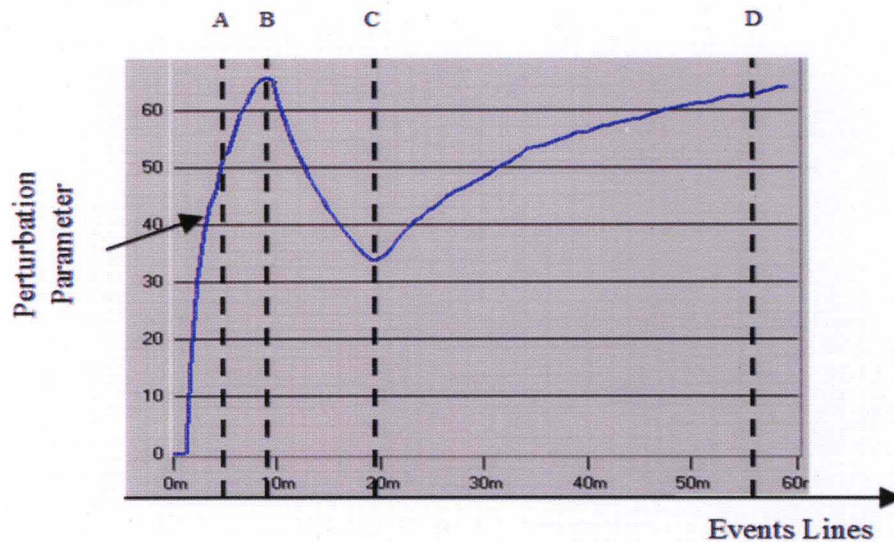


Figure 25: Resilience Measures Illustration

- At point (A): Illegitimate Event Occurred
- A → B: Time to detect Illegitimate Event Occurrence
 - ♦ System performance change
 - ♦ Counterattacking procedures activated
- B → C: Time to resist or to fail
 - ♦ Comprehensive System failure achieved
- C → D: Time to recover
 - ♦ Recovery procedures activated
 - ♦ Fully system recovery completed

Another important step is to select a measurement to reflect data center behavior during the analysis as shown on Figure 26. This measurement should reflect system behavior as an overall process and not dependent data center architect or operational roles. Several parameters were proposed such as: latency, processing time and response time (Jesshope and Egan 2006).

Response time measurement was selected as it can reflect system behavior regardless of the system architecture as shown in figure 26.

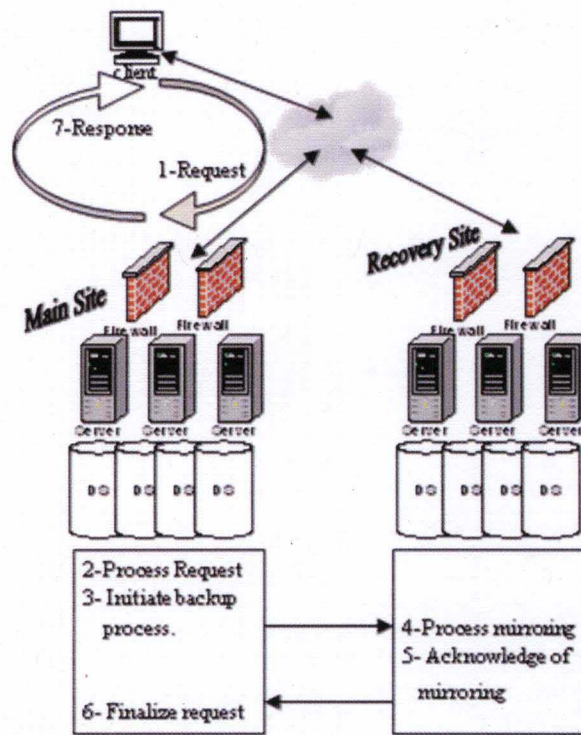


Figure 26: Data Center Operation Summary

As shown request is initiated, then if the main site is available it will respond but the response might be held until main site get mirroring ACK or NO based on which mirroring approach was used. So the response time will include the time for ACK or NO. In case that main site is not available then request will be redirected to active or recovery site, and again the response time will include the redirection time which will not be the same for both scenarios.

6. DATA CENTER RESILIENCE ASSESSMENT PORTAL

A resilience assessment portal to test and validate the proposed methodology was designed and implemented. For any evaluation process it is very important to have a controlled/ isolated environment to designate the impact of different factors on the overall evaluation process. The following section will describe the test-bed used for experiments.

6.1. Test-Bed Overview

In this study, two test-beds were used: E-Cavern Project test-bed and University of Louisville test-bed.

6.1.1. E-Cavern Project test-bed

The Kentucky Center for Resilient Information Systems (CRIS) staff has designed, implemented, and deployed a test-bed system specifically designed to address the issues facing the financial sector. The test-bed is housed at the University of Kentucky (which acts as the primary site) with the remote backup site being housed in the E-Cavern underground facility (CRIS 2006). It consists of the following:

- Client applications -- primarily workload generators that try to mimic the behavior of financial transaction systems. These are run on various types of machines and operating systems. The test-bed includes a pair of 8-CPU IBM X-series machines with fibre channel interfaces that are specifically reserved for the purposes of workload generation.

- Database Services – has run multiple Unix-hosed databases (including UDB, postgres, mysql) using an 8-processor IBM P-series machine as the server. The server machine directly mounts a mirrored disk (and IBM DS 8000) over a multi-interface fibre-channel network.
- Primary Data Storage System -- we use an IBM DS 8000 running in either metro or global mirror modes as our primary disk storage system. The system can be reconfigured to change the mirroring parameters, flash copying, etc.
- Secondary (Backup) Storage System -- we use an IBM DS 6800 as our remote mirror which is setup as either a global or metro mirror of the primary. It is physically located roughly 70 miles away from the primary, bounding the minimum latency.
- High-speed Wide Area Network Connection -- the primary and secondary are connected over a 1 GB/second leased line that is carried over the KPEN network.
- Emulab facility -- sits between the primary location and the secondary location and can be used to change the delay, loss rate, jitter, etc.

Additional Intel-based machines at both the primary and secondary site are used to test other types of software configuration (e.g., DRDB, FEC-based protocols, (D)DOS attacks, etc.) as shown on the following figure.

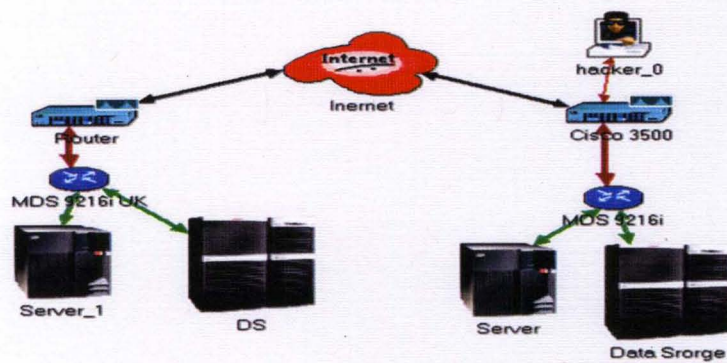


Figure 27: Simulated view of E-Cavern Project test-bed

6.1.2. University of Louisville Test-bed

This test-bed was developed to provide more flexible and controlled environment. This test-bed focus more in using open source tools, the incorporated data mirroring tools within SQL servers. As not most of the small and medium business size can afford standalone mirroring tools such as IBM global mirroring. The following figure shows main elements of the test-bed (Khalil and Elmaghraby 2008).

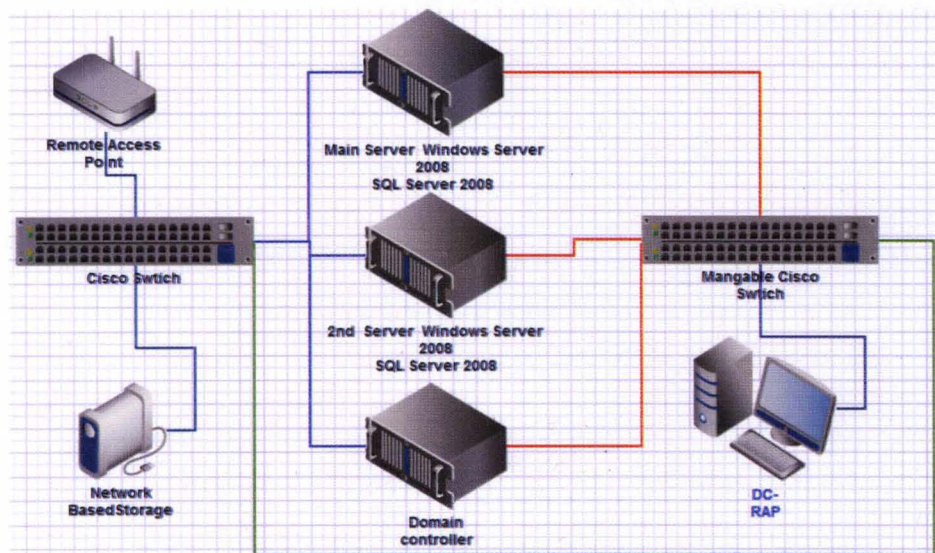


Figure 28: Test-Bed Basic Overview

- Hardware setup
 - Three high end servers configured as follow:
 - Principal server: hosts main database instance with connection can be configured to end-mirror server or remoter data storage device.
 - End-mirror server: hosts a copy of database instance, can be configured to be a synchronies or asynchronies setting.
 - Web application server: this server responsible for accepting web clients request and then responses to their request along with optional data contents. It is coded with two database connection to the principle server and End-mirror server.
 - Remote data storage: one terabyte storage area network connected to the network through the public network, for some scenarios it can be configured as endpoint mirror.
 - Communication networks: each server equipped with two NIC (network interface card), Gigabit bandwidth, each NIC is connected to physically separated networks (Public, Local).
 - Public network: for client's access and mirroring traffic.
 - Local network: for some scenarios: used for heart beat traffic.
- Software setup
 - AdventureWorks database was used to implement experiments; there are several versions of the AdventureWorks databases for SQL Server 2008: (Agarwal and Huddleston 2008)
 - AdventureWorks OLTP

- AdventureWorks DW
- AdventureWorks LT (Light)
- Network traffic shaper: to control of computer network traffic for:
(Traffic-Shaper-XP 2005)
 - Distance simulation between connected servers.
 - Simulate the impact of attacks.
- Network packet sniffer: installed on each server to collected data about traffic.
- Data Center Resilience Assessment Portal (DC-RAP): web based application to generate traffic and monitor.

6.2.Data Centre Resilience Assessment Portal (DC-RAP)

Based on the adapted FePIA methodology, the perturbation parameters were: response time, mean time to detect malicious activity, mean time to fail, and mean time to recover need to be collected. We designed and developed a tool to collect those parameter values to ensure resilience requirements. The proposed tool Data Center Resilience Assessment Portal (DC-RAP) works from the client site, so any variation on the data center site such as operational roles, or architectures will not interrupt the usage of DC-RAP. In addition, this tool can be used to compare between: different setting, hardware configurations, and recovery plans.

The core elements of DC-RAP can be introduced as follows:

- Traffic generator

It is designed to emulate accurate client/server activities; either to develop stress tests for servers using various data loads or develop consistent traffic to setup servers for other testing purposes.

- Response Time Monitor

It measures the time interval between sending the query by the traffic generator and receiving response from the targeted server.

- Controller

This component makes the decision of directing traffic to the desired server either manually as user preference or based on the timeout policy used. In this setting, the controller is set –automatic mode- to direct traffic to the alternative site in case of the complete failure of the main site.

- Logger

This object is used to log events such as start connection, redirect traffic and other events as needed by user.

6.2.1. DC-RAP User's Interface

Data Center Resilience Assessment Portal (DC-RAP) user interface provides an easy way to setup, configure testing scenarios and collect statistics. As shown on Figure 30, DC-RAP can be configured to implement various testing scenarios.

Several steps required to configure the tool:

- Automatic versus Manual modes: it is used to implement Active-Standby versus Active-Disaster Recovery mode. In case of Active-Standby scenario, clients will

be redirect automatically to the standby site in case of Active site failure. Yet for the Active-Disaster Recovery case, the Disaster Recovery site needs to be unlocked for public usage before client's redirection.

- Connections: two connections can be setup, in most cases data center managers will need to compare between two cases, so the tool was designed to test two connections. Yet another or more connection socket can be coded as needed.
- Query: this entity enables user to define the testing load using SQL query and how frequent it will happen.

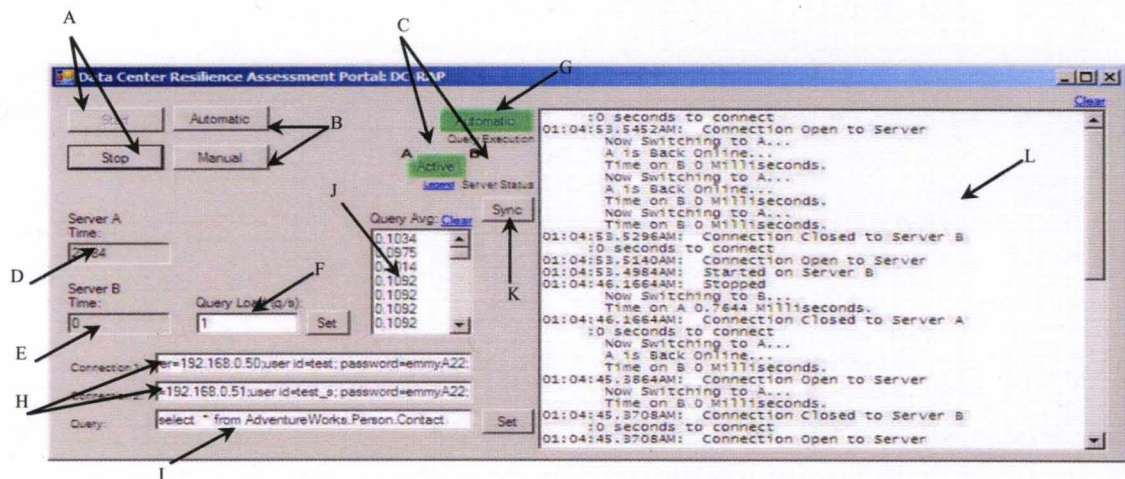


Figure 29: DC-RAP User's Interface

As shown on figure 30, the user interface elements are described as follows:

- A. Used to start and stop the portal.
- B. Automatic/Manual: use to switch operation modes to develop different scenarios.
- C. Indicate the status of each server: Active, Down, and Ready
- D. Total time first server was available for clients
- E. Total time second server was available for clients
- F. Used to set the number of query/sec
- G. Indicate operation mode: Manual or Automatic switching

- H. Used to setup connections: Server IPs, User Names, and Password
- I. Setup the query using SQL based on applications history
- J. Log of response time
- K. Used to add time stamp of external actions to the log files
- L. Log window

6.2.2. Experimentation Scenarios

For testing, experiments focused on three scenarios:

- Comparing various configurations:

In this scenario we can have two sites or two servers with different setting or configuration. Each system will be evaluated separately and then results will be compared in terms of which system can be more resilient. This scenario can be implemented by using the network traffic shaper or using various SQL servers' configurations, and then response time statistics will be collected and analyzed to designate cost-effectiveness solution.

- Resilience evaluation: Active-Standby:

Distributed data center has been used to ensure resiliency, however there are several variations to implement Distributed data center such as: Active Site – Active Standby where the standby site are open and available for users as needed. In this case the DC-RAP will be configured to an automatic operation mode, attack the active site with simple Denial of Service attack (DoS). Measure times and study response time log.

- Resilience evaluation: Active-Disaster recovery:

Another way to implement distributed data center is Active site- Disaster recovery site. In the case the disaster recovery site will not be immediately available for public use. In this case DC_RAP will operate on manual mode, and the decision of switching to the Disaster recovery site will be made based on the estimated time to make the site available for public.

6.2.3. DC- RAP Utilization

Data Center Resilience Assessment Portal (DC-RAP) can be utilized to perform several functions:

- Stress Test: by using several workloads in terms of different SQL queries and the number of queries to identify sever break points and sever capacity.
- QoS comparison: this tool also can be used to compare the change of QoS for different hardware setting or configuration as cost effectiveness analysis.
- Vulnerabilities Scanning: this tool can be utilized to scan system weakness as in identify malicious activity in timely manner or the effectiveness of attack mitigation approaches.

7. EXPERIMENTAL RESULTS AND DISCUSSION

This research focused on evaluating data center resilience and enhancing computer network resilience level. This chapter presents various experiments and results. The following section presents computer network resilience efforts.

7.1. Computer Network Resilience

7.1.1. Network protocols

In this set of experiments, several routing network protocols are compared to evaluate their resilience level. (Khalil and Elmaghraby 2010)

Testing environment can be summarized as follows:

OPNet: computer network simulation tool was used for testing and experiment.

(www.opnet.com 2005)

SAS Enterprise Miner : a data analysis tool was used for data analysis. (www.sas.com 2005).

Network Topology:

- Eight IP-based routers support Ethernet interfaces, serial line IP interfaces.
- Three subnets, each one has access router, switch, two servers and 5-10 workstation LAN.
- Router has been connected in a way to ensure multipath between tested points.

Traffic Load:

- Applications: Email & HTTP servers.

- Users: salesman, researcher, and engineer
- Traffic broadcasting workstations for background traffic.

Attacks:

Simple and disturbed denial-of-service attacks, Poisson model were used for attack traffic generation process.

Simulation scenarios:

The simulation time is divided into three intervals:

- First interval will be attack free (0 min – 9 min 59 sec.)
- Second interval one of the routing paths will failed (10 min – 19 min 59 sec.)
- Finally only one routing path will be available (20 min – End of simulation).

Data collection:

Experiments' focus will be network throughput rate, traffic received at destination point, routing overhead (routing table size) and convergence time.

Results

Initially, we examine the local network protocols as shown on the following table.

Table 7: Change in Network Routing Parameters for Local Protocols

| Protocol | Throughput change % | converging time (sec) | Table size change % |
|------------|---------------------|-----------------------|---------------------|
| RIP V1 | -6% | 14 | + 38% |
| RIP V2 | -5% | 15 | + 62% |
| EIGRP Pkt | -1% | 0.000771 | + 1.3% |
| EIGRP Des. | -0.7% | 0.000755 | + 1.2% |

EIGRP Pkt : EIGRP Packet based version (Pkt)

EIGRP Des.: EIGRP Destination based version (Des)

As shown by Table 7, each routing responded to the attacks differently. For example the converging time ranged between: 0.000755 to 14 sec, which illustrated a big difference between the protocols. This result confirmed how using a particular protocol can influence the overall network resilience in terms of speedy recovery.

In many cases, data centers or other computing platforms require the usage local network with combination of other protocols such as Border Gateway Protocol (BGP) (Nicholes and Mukherjee 2009).

Table 8: Change in Network Routing Parameters

| Protocol Name | Throughput change % | converging time (sec) | Table size change % |
|---------------|---------------------|-----------------------|---------------------|
| BGP/RIP | -1% | 74 | 0 |
| BGP/EIGRP | -3% | 0.01 | 23% |

As it is shown by Table 8, the combination has different behavior for protocols parameters. In this case the results don't show that, there is one combination better than the others. So network administrators will have to select the optimum based on the application requirements or goals. As in some applications, the throughput degradation is not as important as the change on routing table size (overhead cost).

7.1.2. Server Load Balancing

In this set of experiments (Khalil and Elmaghraby 2008) the following scenarios were examined:

- a. Baseline: no SLB algorithm were used
- b. Random
- c. Round Robin algorithm
- d. Number of Connections algorithm

In the Baseline scenario, to ensure realistic operation environment, several runs were used to adjusted the number of users, traffic generation parameters (arrival rate, pause time, etc.). Then acknowledge the system characteristics: the server CPU utilization and the total traffic received at the targeted server as shown in the following figure.

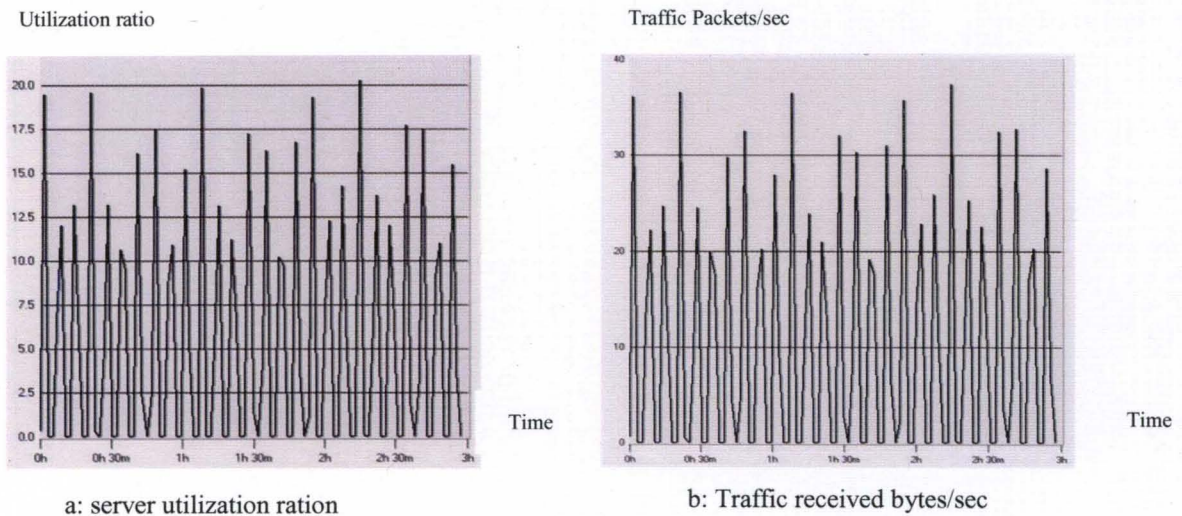


Figure 30: Baseline Scenario

In this experiment, the traffic sent (packets/sec) parameter recorded “As Is” over time interval not as average values. In order to identify the following values:

- SLB detecting time: time needed to update SLB’s server list
- Time interval SLB need to balance the traffic distribution with minimum variation (steady state)
- CPU utilization average

The following table summarizes those values as follows

Table 9: SLB Algorithm Performance Summary

| Parameters | Server load Algorithm | | | Round Robin Algorithm | | | # of connections Algorithm | | |
|----------------------|-----------------------|-------|-------|-----------------------|-----|------|----------------------------|------|------|
| SLB Detecting Time | 2 min 17 sec | | | 2 min 5 sec | | | 2 min 22sec | | |
| Time to Steady state | 22 min 5 sec | | | 25 min 5 sec | | | 4 min 9 sec | | |
| CPU Utilization | S1 | S2 | S3 | S1 | S2 | S3 | S1 | S2 | S3 |
| Ratio | 0.751 | 0.751 | 0.751 | 1.5 | 1.5 | 2.26 | 1.84 | 1.81 | 1.48 |

Data center (DC) managers and administrators expect from SLB to support higher availability and easy maintained server farm environment, in addition to improve DC resilience level. By projecting DC resilience objectives into SLB performance parameter, SLB should be able to adapt to operation environment conditions such as high level of traffic or unexpected server failure. An optimum SLB algorithm will:

- Adapt to variation on operation environment in short time (SLB detecting time)
- Under different workload and work condition will distribute traffic with minimum variations over the available servers.

As shown by Table 9, it was concluded that: Server Load algorithm provide the best way to optimum sever utilization, while Round Robin algorithm has higher capability to monitor server health. However, # of connections algorithm showed good ability to absorb the operation environment disturbance and recover rapidly. Thus system administrators should select the SLB approach which provide higher resilience for their applications.

7.1.3. Social Network Analysis & Network Resilience Improvement

The main purpose of these experiments it is to validate the ability of social network analysis methods at identifying critical routers within a network. (Khalil, Sheta and & Elmaghraby 2010).

Experiments configuration:

For illustration purpose, the simulation scenarios were based on a modified version of the University of Louisville computer routers infrastructure as shown in the following figure (Figure 31). The physical topology was imported to the OPNET simulation tool, also network traffic were collected between network routers and exported to the simulation tool.

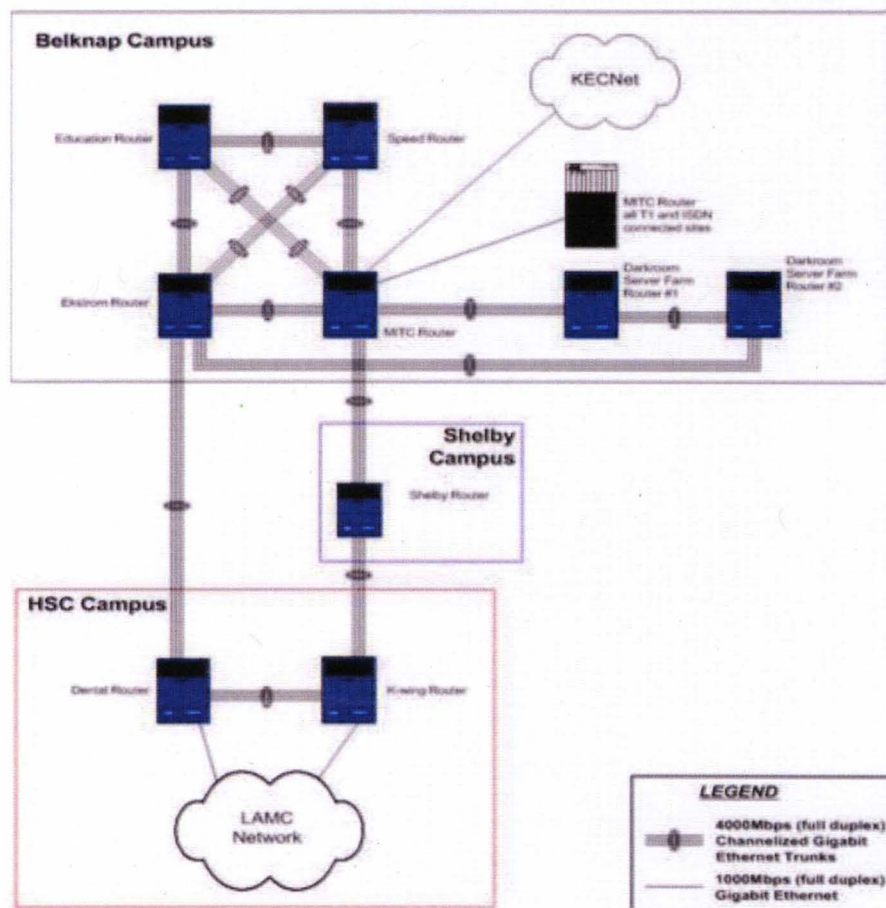


Figure 31: University of Louisville Gigabyte Backbone

(Source: Miller Information Technology Center, U. of Louisville)

Testing scenarios:

For testing purpose, malicious activities were simulated either by injecting the system with overloading traffic or implementing a node failure. A traffic broadcasting node was hooked up to the network to implement both scenarios, the traffic generation process follows the Exponential distribution with $\lambda = 0.025$ and 1.

For validation purpose, simulation will run with two routers fail/recovery scenario and network latency information will be collected. For social network analysis, The Applied Graph and Network Analysis (AGNA 2.1); an application in use in for communication networks analysis. (Benta 2005)

The following graph represents the sociomatrix; a matrix of size (8×8) represents the ties between network elements. For comparison and validation purposes, we build two sociomatrix as shown figures:

- Uniform sociomatrix: all the links have the same weight and symmetric matrix.
- Weighted sociomatrix: each link got its weight based on the throughput rate bits/sec in average created nonsymmetrical matrix

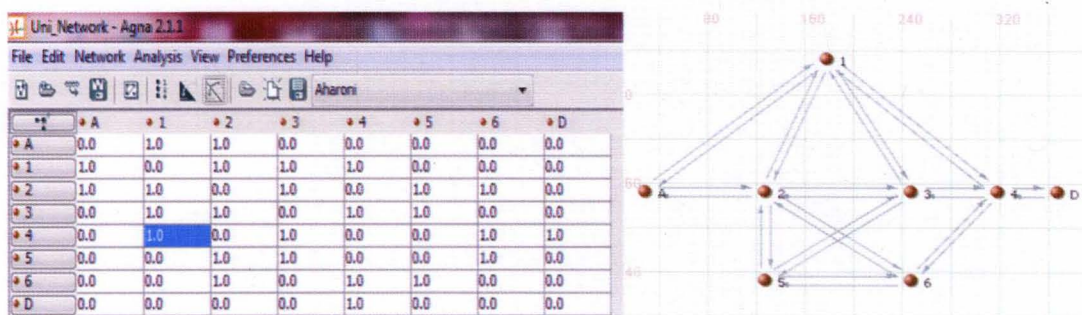


Figure 32: Uniform Network Sociomatrix

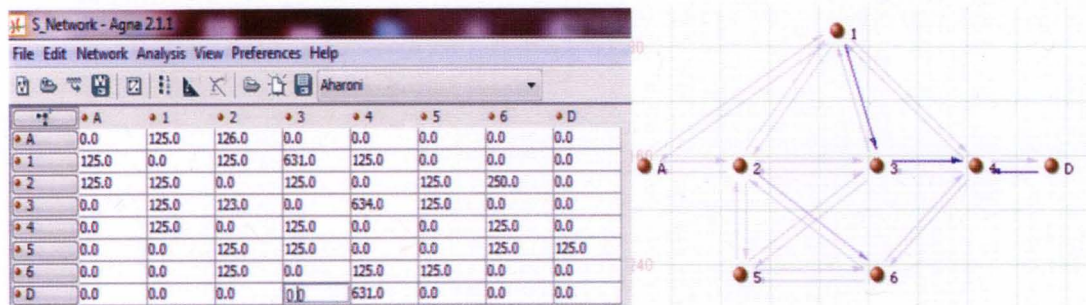


Figure 33: Weighted Network Sociomatrix

Virtualization of network ties represents easier way to understand network behavior, For example, by visual inspection, it is clear that some nodes process higher traffic than others also those routers A & D can be identified as source/destination points. The first step in Social network analysis is to calculate the network density, this information can be used to determine the possibility for adding more paths/connection between nodes with constrain to the hardware limits. The calculated Network Density= 0.4642857 and Weighted Network Density = 87.41071, which indicated that this network is not very dense, so administrators can add more routers or connections to accommodate more traffic and services.

The following step is to evaluate the Centrality based on the physical layout and concoctions; the following results show no difference between the uniform networks and the weighted network which match the logic of those metrics. The ANGA tool calculates the Centrality/Degree entitled Nodal Degree. The following table represents the nodal degree for each node and also compares it to other nodes.

Table 10: Distribution of Nodal Degree

| Node | Degree | Relative Degree* | Relative Degree** |
|------|--------|------------------|-------------------|
| A | 2.0 | 0.285714285 | 0.25 |
| 1 | 4.0 | 0.571428571 | 0.5 |
| 2 | 5.0 | 0.714285714 | 0.625 |
| 3 | 4.0 | 0.571428571 | 0.5 |
| 4 | 4.0 | 0.571428571 | 0.5 |
| 5 | 3.0 | 0.428571428 | 0.375 |
| 6 | 3.0 | 0.428571428 | 0.375 |
| D | 1.0 | 0.1428571428 | 0.125 |

* Relative to number of all other nodes (self-excluded)

** Relative to number of all nodes (self-included)

As the table shows, routers (in order): 2, 3, 4 and 1 have higher level of centrality/degree as those nodes have higher number of relations which provide more flexibility. The next step is to evaluate Centrality/ Betweenness on a node level; ANGA 2.1 generates the following table.

Table 11: Distribution of Betweenness Centrality

| Node | Betweenness |
|------|-------------|
| A | 0.0 |
| 1 | 6.3333335 |
| 2 | 7.6666665 |
| 3 | 4.3333335 |
| 4 | 13.666667 |
| 5 | 0.6666667 |
| 6 | 3.3333333 |
| D | 0.0 |

As shown routers A and D have the lowest Betweenness level, the network was designed as router A and D are source and destination points which confirm the obtained results. In addition, router 4 has the highest level and that confirmed as it the only router connected to destination point. Routers: 4,3,2,1 have higher level of betweenness.

Table 12: Distribution of Closeness Centrality

| Node | Closeness |
|----------|-------------|
| Router A | 0.07692308 |
| Router 1 | 0.1 |
| Router 2 | 0.1 |
| Router 3 | 0.1 |
| Router 4 | 0.1 |
| Router 5 | 0.083333336 |
| Router 6 | 0.09090909 |
| Router D | 0.0625 |

The last measurement of Centrality is of Centrality/Closeness; this index is the inverse of the sum of the geodesic distances from that node to all the other nodes as follow. It provides vital information for network planning and design concern. By excluding router A and router D as they are the source and destination, we can see that routers 4, 2, 1, and 3 are very close to other nodes.

SNA concluded that router B, router C and router 1 are the critical routers in the examined network. Network manager should install backup routers be used in case of failure of any of those routers to ensure speed recovery of degradation state.

To validate the obtained result, we examined the effect of their failure on the network performance in terms of latency and throughput rate to the destination nodes. We do this by successively disabling routers as shown in the following figure.

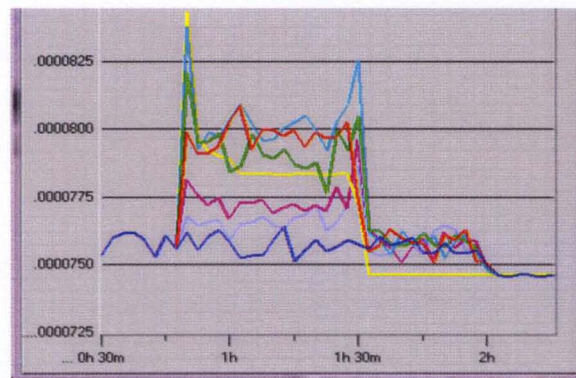


Figure 34: Zoomed Section for the Routers Failure Time

As shown each router failure impacted the latency differentially. SNA shows that routers 4, 3, 2 and 1 caused higher level of latency than the other routers in the network. In addition SNA can provide vital information for network design process such as: shortest path, etc.

7.2. Data Center Resilience Assessment Experiments

In this section, the focus will be on:

- a. Comparing various configurations
- b. Resilience evaluation: Active-Standby

To implement the first scenario, the traffic network shaper tool was used to set limits on the network bandwidth. And for each bandwidth, the legitimate load was increased periodically and response time statistics were collected. The following table shows summary for the response time values mean, standard deviation, and max values for response time.

Table 13: Response Time Summary

| Bandwidth | Mean | Std Dev | Max Value |
|------------------|-------------|----------------|------------------|
| 10GB | 0.1140689 | 0.0151440 | 0.1557000 |
| 1GB | 0.1191940 | 0.0390786 | 0.5032000 |
| 100MB | 0.1408359 | 0.0466711 | 0.5515000 |

The above results illustrated expected system behavior as smaller bandwidth can reduce the throughput level and increases latency which will add up to the response time. However, results don't illustrate how the data center will adjust to the loads variation.

Kernel Density Estimation (KDE) is a non-parametric way of estimating the probability density function of a random variable (Fan and Yao 2005).

KDE can be used to study the variability in response time as consequences of load variation. Simply, when the KDE graph has many peaks, then the response time wasn't steady. Gaussian KDE - representation of a kernel-density estimate using Gaussian kernels - was calculated using SAS Business Analytics software, Enterprise Guide. (SAS 1999)

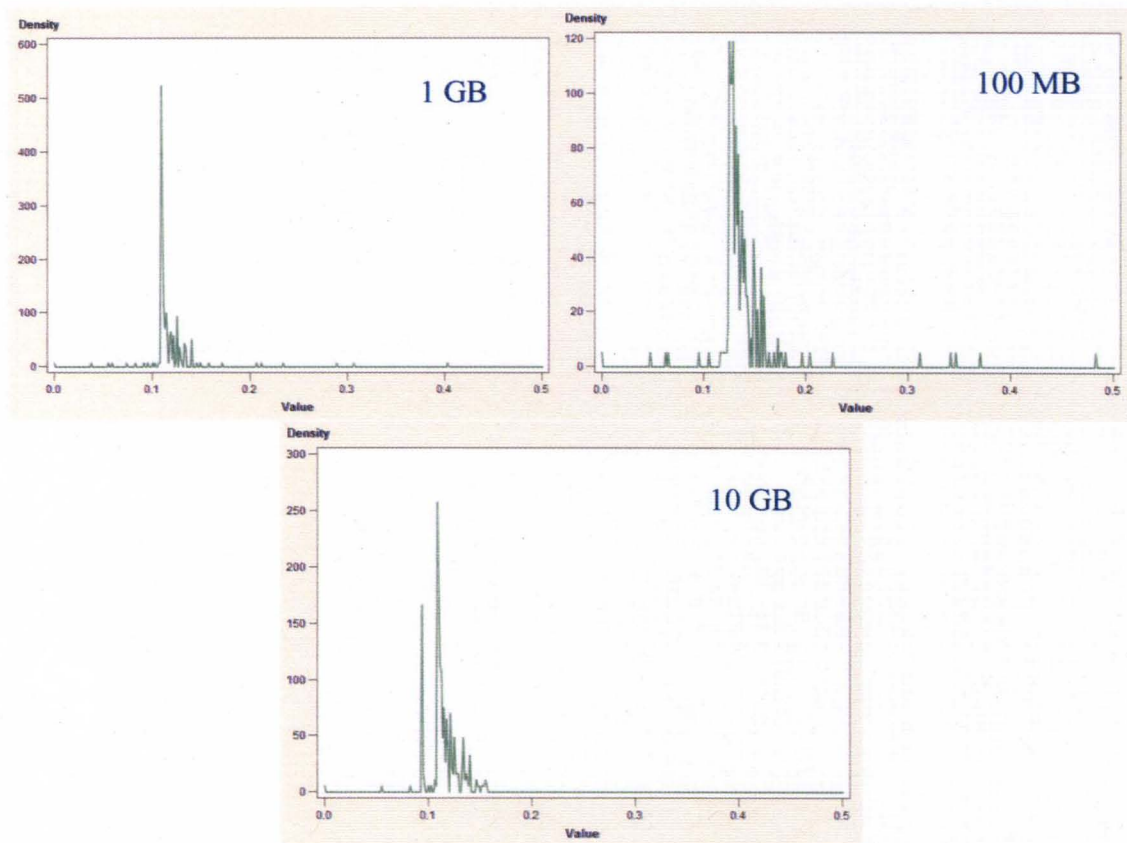


Figure 35: Kernel Density Estimation for various network bandwidths

The KDE's plot reflects the variability of particular parameter, in this case, it shown that that the KDE's plot for response time for the 100MB case has more peaks due to response time fluctuating versus load increased. Also it shows that the 10GB case shows

less peaks, i.e. more stability and higher resilience level towered the variation of operation loads.

Also, an important factor is to determine the maximum number of transactions per second that can be processed by servers. Transaction rate is affected by general system performance and resource constraints, such as I/O, cache size, and complexity of requests. And they should be studied with regards to the acceptable response time for this application.

To accomplish the second scenario, two experiments were executed. For the second experiment, the server memory was reduced by 50% to compare it with the initial configuration. Each run was repeated several times to minimize measuring errors and calculate average values. The following figure shows a logger snapshot that summarizes data center behavior.

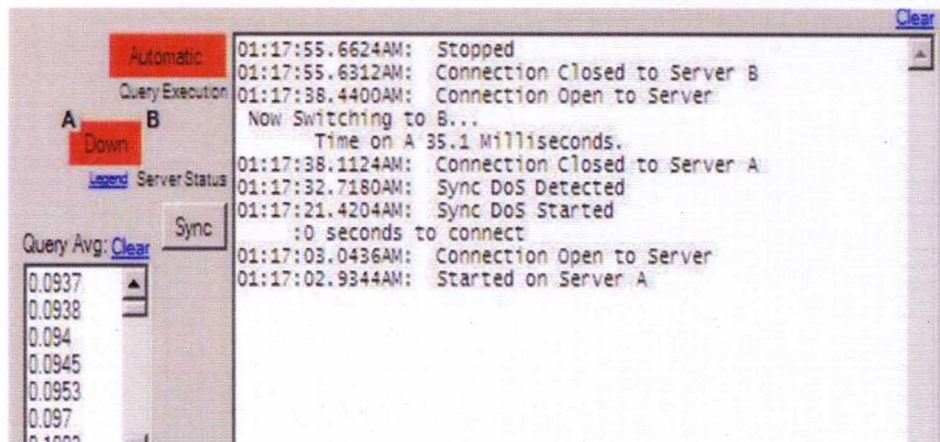


Figure 36: DC-RAP logger snapshot (Case 1)

As results show, DoS attack affected server performance within 12 MS, and it needed 0.0312 MS to initiate traffic redirection. Those values subject to change based on the used resources and applications yet it illustrates the ability of DC-RAP to measure

parameters needed for resilience evaluations. The following figure show logger snapshot for setting 2.

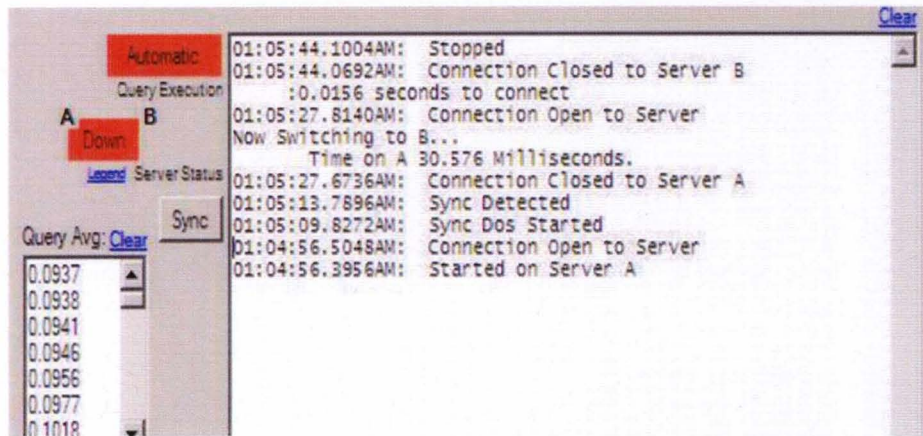


Figure 37: DC-RAP logger snapshot (Case 2)

For this case the influence of DoS on server performance ensued within 6 MS from initiating the attack. This experiment illustrated how resources can enhance the system ability to resist malicious activity impact and provide acceptable service level longer. The following figure presents the two system behavior using response time.

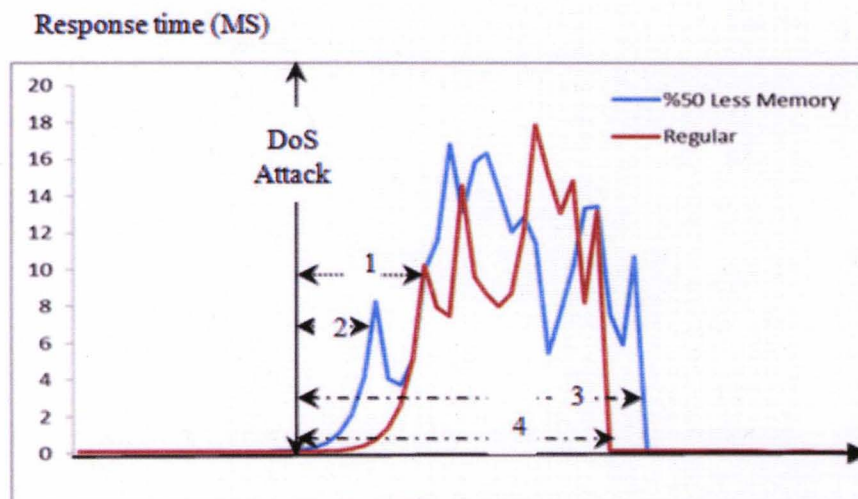


Figure 38: Resilience Comparison for Different Server Configuration

As shown on Figure 38, for both experiments the DoS attack started at the same time, as arrows 1 & 2 illustrates the “regular” setting was able more to resist the impact of the attack while for “50% less memory” setting the response time increased rapidly. Similarly, the “regular” setting recovered faster than “50% less memory” setting as shown by arrows 3 & 4.

As stated earlier, the Controller is an important element of the DC-RAP as it makes the decision of redirecting the traffic between site A and site B. The current version of DC-RAP support complete failure policy to direct the traffic to the alternative site B. Yet it can be easily adapted to support other switching policy such assigning threshold on response time, or using time-out setting related to communications, applications, or SQL servers.

Results illustrate the tool ability to quantify resilience elements. In addition, DC_RAP was used to evaluate server’s ability to process various traffic loads with regards to different network bandwidth or computing resources.

8. CONCLUSIONS AND FUTURE RESEARCH DIRECTIONS

This work achieved its goals by defining a new metric for resilience, proposing a new methodology to evaluate data center resilience levels, and demonstrating improvements to resilience through network re-design.

The proposed data center resilience assessment portal DC-RAP offers a configurable and easy to use tool to implement the proposed methodology independent of hardware or software configuration. Results illustrate the tool's ability to quantify resilience elements. In addition, DC_RAP was used to evaluate server's ability to process various traffic loads with regards to different network bandwidth or computing resources.

The experiments were done to achieve two goals: evaluate data center resilience as end-to-end process and improve computer networks resilience in terms of speed of recovery from degraded states.

Network Resilience assessment is a complex process as requires management of several aspects such as forming alternative solutions, designing and maintaining recovery plans and security approaches. Routing protocols play significant role on assembling computer networks response toward attacks in terms of reactions for nodes failure or recovery in timely manner. The results obtained from network resilience experiments, show that converges time, routing table size, and network throughput variation can be used to evaluate the network routing protocols behavior during the malaises activities.

Results show that server load balancing algorithms can play significant role in improving computer network resilience level by utilizing each working server to minimize recovery time. Although that different application and various architects will have different requirements and needs but the following factors can be used for determining the precise algorithm to enhance resilience level such as:

- SLB algorithm's efficiency on monitoring server's health.
- Algorithm's ability: adapt with the unexpected changes on operation environment.
- Optimize server's CPU resources.

On the other hand, identifying the important or critical network elements is required for redundancy as alternative devices for resiliency requirements. This research work presents a novel approach for identifying critical – for network service continuity- elements of computer networks. Consequently the network designers, planners and administrators can come to a decision regarding which elements should have recovery devices as a step toward enhancing the network resilience level. Social Network Analysis identifies the critical elements based on Centrality measurements for uniform and weighted networks; Sociomatrix provides flexible representation to accommodate various networks connection/edges strength and direction. The illustrated results showed that SNA successfully designated the critical routers.

8.1.Future Work

Cloud computing, ultra-large volumes of critical data and the new business model increased the importance of data centers to ensure service continuity. Several systems evaluation metrics are available; however, the current risks and the future threats

highlight the necessity for new metric such as resilience to evaluate data center ability to overcome unpredicted operational circumstances. It is highly recommended for investigating data mirroring aspects such as mirroring compression factor, mirroring algorithm and its relation with the data center architecture.

Moreover, an important aspect to be investigated is the scenario of backup or mirroring communication lines failure and the ability of the system to create mirroring checkpoints to be used for mirroring process resume in case of failure.

Also the following figure demonstrates the relation between security tools performance and mirroring approaches and setting.

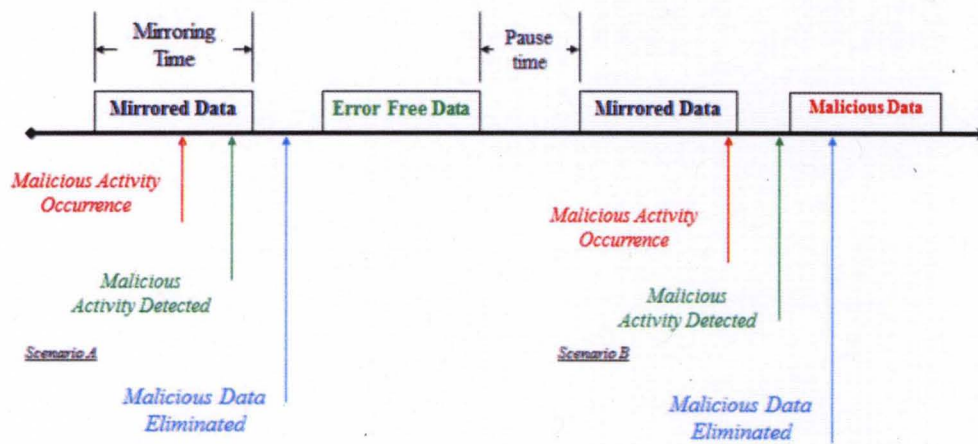


Figure 39: Data Mirroring and Security

In general, data mirroring algorithms will send data to the mirroring site and then will pause for certain time either fixed or variable based on the mirroring algorithms. This figure explains the relation between three time intervals:

1. Mirroring time
2. Mirroring pause time
3. Malicious activities detection time

As show, in scenario A, the system was able to detect malicious activities before starting the next mirroring session, so we are sure that the mirrored data are error free. Yet in scenario B, the system was not able to detect the malicious activities during the pause time. In cases such as scenario B there is a big probability that the mirrored data could be infected or damaged ad therefore future work is necessary.

REFERENCES

- Agarwal, Vidya Vrat, and James Huddleston. *Beginning VB 2008 Databases: From Novice to Professional*. Apress, 2008.
- Ali, I.A., H.T. Mouftah, and A.H. El-Sawi. "A dynamic routing protocol for broadband networks." *Second IEEE Symposium on Computers and Communications, 1997. Proceedings*. 1997. 495 - 500.
- Ali, S., A. A. Maciejewski, H. J. Siegel, and J.-K. Kim. "Definition of a robustness metric for resource allocation." *17th International Parallel and Distributed Processing Symposium IPDPS*. 2003.
- Arnold, Gordon. *Introduction to Storage Security*. Storage Networking Industry Association, 2007.
- Barker, Sean K., and Prashant Shenoy. "Empirical Evaluation of Latency-sensitive Application Performance in the Cloud." *ACM Multimedia Systems*. 2010.
- Baruch Awerbuch, Mohammad T. Hajiaghayi, Robert Kleinberg and Tom Leighton. "Online client-server load balancing without global information." *sixteenth annual ACM-SIAM symposium on discrete algorithms*. 2005. 197 – 206.
- Bauer, Eric. *Design for Reliability: Information and Computer-Based Systems*. John Wiley&Sons, Inc., 2010.
- Benta, Marius I. "STUDYING COMMUNICATION NETWORKS WITH AGNA 2.1." *Cognitie, Creier, Comportament / Cognition, Brain, Behavior*, 2005: 567-574.
- Bernstein, P. A., Vassos Hadzilacos, and N. Goodman. *Concurrency Control and Recovery in Database Systems*. Addison-Wesley, 1987.
- Bloor, Robin. *The Evolution of the Data Center*. Bloor Research, 2005.
- Bourke, Tony. *Server load balancing*. O'Reilly Media, Inc, 2001.
- . *Server Load Balancing*. O'Reilly, 2005.
- Bruntland, G. *Our common future: The World Commission on Environment and Development*. Oxford University Press, 1987.
- Bryhni H., Klovning E. and Kure O. "A Comparison of Load Balancing Techniques for Scalable Web Servers." *IEEE Network*, 2000: 58-63.
- Burke, Michael, and Gerald A. Jr. Fisher. "A practical method for syntactic error diagnosis and recovery." *Proceeding SIGPLAN '82 Proceedings of the 1982 SIGPLAN symposium on Compiler construction*. 1982.
- CARDELLINI, VALERIA, EMILIANO CASALICCHIO, MICHELE COLAJANNI, and PHILIP S. YU. "The State of the Art in Locally Distributed Web-Server Systems." *ACM Computing Surveys*, 2002: 263–311.
- Chang, V., G. Wills, and D. De Roure. "A Review of Cloud Business Models and Sustainability." *IEEE 3rd International Conference on Cloud Computing (CLOUD)*. 2010. 43-50.

- Chhabra Amit, Singh Gurvinder. "Qualitative Parametric Comparison of Load Balancing Algorithms in Distributed Computing Environment." *International Conference of Advanced Computing and Communications*. 2000. 58-60.
- Chris Connelly, Brian Cox, Tim Forell, Rui Liu, Dejan Milojicic, Alan Nemeth, Peter Piet, Suhas Shivanna, Wei-Hong Wang. "Reiki: Serviceability Architecture and Approach for Reduction and Management of Product Service Incidents." *IEEE International Conference on Web Services*. 2009. 775 - 782.
- Cisco. *Data Center Infrastructure Design Guide 2.1*. Cisco Systems, Inc., 2007.
- Connors, DC. "The variability of system failure probability." *Reliability Engineering journal by Elsevier Ltd.*, 1984: 117-125.
- CRIS. <http://protocols.netlab.uky.edu/treasury/>. 2006. (accessed 2011).
- Cronholm, Stefan, and Göran Goldkuhl. "Six Generic Types of Information Systems Evaluation." *The 10th European Conference on Information Technology Evaluation*. Madrid, 2003. 1-12.
- Deepankar Medhi, Karthikeyan Ramasamy. *Network routing: algorithms, protocols, and architectures*. Morgan Kaufmann Publishers, 2007.
- Dorian Cougias, E. L. Heiberger. *The Backup Book: Disaster Recovery from Desktop to Data Center*. Network Frontiers, LLC, 2003.
- Dougall, Richard Mc. *Availability - What It Means, Why It's Important, and How to Improve It*. Sun Microsystems, Inc, 1999.
- Eric A Hibbard., LeRoy budnik, Richared Austin. *Introduction to Storage Security*. Hitachi Data Systems, 2005.
- Fan, Jianqing, and Qiwei Yao. *Nonlinear Time Series: Nonparametric and Parametric Methods*. Springer, 2005.
- Freeman, L.C., S.P. Borgatti, and D.R. White. "Centrality in valued graphs: A measure of betweenness based on network flow." *Social Networks (Social Networks)*, 1991: 141-154.
- Ganymed, C. Plattner and G. Alonso. "Scalable replication for transactional web applications." *ACM/IFIP/USENIX International Middleware Conference*. 2004.
- Gary Field, and Peter Ridge. *SCSI 2/E: I/O for the New Millennium*. Publishers Group West, 2000.
- Georgia-Ann Klutke, Peter C. Kiessler, and M. A. Wortman. "A Critical Look at the Bathtub Curve." *IEEE TRANSACTIONS ON RELIABILITY*, 2003: 125-129.
- Graziani, Rick, and Allan Johnson. *Routing Protocols and Concepts, CCNA Exploration Companion Guide*. Cisco Press, 2007.
- Griffith, Rean, Ritika Virmani, and Gail E. Kaiser. "The Role of Reliability, Availability and Serviceability (RAS) Models in the Design and Evaluation of Self-Healing Systems." *Computer Science Technical Report Series*, 2007.
- Gunter Bockle, Hermann Hellwagne, Roland Lepold, Gerd Sandweg, Burghardt Schallenberger, Raimar Thudt, Stefan Wallstab, and Siemens AG. "Structured Evaluation of Computer Systems." *IEEE JNL*, 1996: 45-51.
- Harold F. Tipton, Micki Krause. *Information security management handbook*. CRC Press, 2004.
- Heinz Stockinger, Andrew Hanushevsky. "HTTP redirection for replica catalogue lookups in data grids." *ACM symposium on Applied computing*. New York, NY, 2002.

- Hoffman, J., and R. Nilchiani. *Assessing Resilience in the U.S. National Energy Infrastructure*. Center for Complex Adaptive Sociotechnological Systems, Stevens Institute of Technology, 2008.
- Holling, C.S. *Engineering resilience vs. ecological resilience*. Washington, D.C.: National Academy Press, 1996, 32-43.
- J.W.Liu, C.H.Hsu and. "Dynamic Load Balancing Algorithms in Homogeneous Distributed System." *6th International Conference on Distributed Computing Systems*. 1986. 216-223.
- Jeng, M., and H.J. Siegel. "Design and analysis of dynamic redundancy networks." *IEEE Transactions on Computers*., 1988: 1019 - 1029.
- Jericho Forum. *Cloud Cube Model: Selecting Cloud Formations for Secure Collaboration Version 1.0*. Jericho Forum Specification, 2010.
- Jesshope, C. R., and Colin Egan. "Advances in computer systems architecture." *11th Asia-Pacific conference, ACSAC*. 2006.
- Jin, A. Bestavros and S. "Popularity-Aware Greedy DualL-Size Web Proxyz Caching Algorithms." *20th International Conference on Distributed Computing Systems*. 2004.
- Khalil, Y.H., A. Elmaghraby, and A. Kumar. "Evaluation of resilience for Data Center systems." *IEEE Symposium on Computers and Communications, 2008. ISCC 2008*. 2008. 340 - 345.
- Khalil, Y.H., and A.S. Elmaghraby. "Computer Networks Resilience Challenges: Routing Protocols." *2010 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT)*. 2010. 28-33.
- Khalil, Yehia H., and A.S. Elmaghraby. "Evaluating Server Load Balancing Algorithms for Data Center's Resilience Enhancement." *21st International Conference on Parallel and Distributed Computing and Communication Systems*. 2008. 111-116.
- Khalil, Yehia H., and Adel S. Elmaghraby. "Data Center Resilience Evaluation Test-bed: Design and Implementation." *IEEE International Symposium on Signal Processing and Information Technology, 2008. ISSPIT 2008*. 2008. 369 - 374.
- Khalil, Yehia H., Anup Kumar, and Adel Elmaghraby. "Design considerations for Resilient Distributed Data Centers." *ISCA 20th International Conference on Parallel and Distributed Computing Systems*. Las Vegas, 2007. 51-55.
- Khalil, Yehia H., W. Sheta, and A. S. & Elmaghraby. "Improved Computer Networks Resilience Using Social Behavior." *International Journal of Computer Science and Information Security (IJCSIS)*, 2010: 208-214.
- Kohavi, Ron, Neal J. Rothleder, and Evangelos Simoudis. "Emerging Trends in Business Analytics." *Communications of the ACM*, 2002: 45-48.
- Kohler, Y.C. Chow and W. "Models for Dynamic Load Balancing in a Heterogeneous Multiple Processor System." *IEEE Transactions on Computers*, 1979: 334-361.
- Kvalbein, A., A. F. Hansen, T. Cì'ci'c, S. Gjessing, and O. Lysn. "Fast IP network recovery using multiple routing configurations." *Proceedings of IEEE INFOCOM*. 2006.
- Laboratory, Simula Research. <http://simula.no/>. 2007. (accessed 2011).
- Lei Gao, Mike Dahlin, Amol Nayate, Jiandan Zheng , Arun Iyengar. "Application Specific Data Replication for Edge Services." *12th international conference on World Wide Web*. Budapest, Hungary, 2003. 449 – 460.

- Liu, X. Song and J. W. S. *Performance of Multiversion concurrency Control Algorithms in Maintaining Temporal Consistency*. White paper, Dept. of Computer Science, Uni. of Illinois at Urbana-Champaign, 1990.
- Long, James. *Storage Networking Protocol Fundamentals*. Cisco Press, 2006.
- Macfarlane, James. *Network Routing Basics: Understanding IP Routing in Cisco Systems*. Wiley Publishing , 2006.
- . *Network Routing Basics: Understanding IP Routing in Cisco Systems*. John Wiley and Sons, 2006.
- Marler, R.T., and J.S. Arora. *Review of Multi-Objective Optimization Concepts and Methods for Engineering*. Iowa City, IA: University of Iowa, Optimal Design Laboratory, 2003.
- Maurizio Portolani, Mauricio Arregoces. *Data Center Design Overview*. Cisco Press, 2003.
- McGill, Susan. "Distributed systems: Poor performance: is it the application or the network?" *44th annual Southeast regional conference*. 2006.
- Medh, Deepankari, and Karthikeyan Ramasamy. *Network routing: algorithms, protocols, and architectures*. Morgan Kaufmann, 2007.
- Michael Resch, Sabine Roller, Katharina Benkert. *High Performance Computing on Vector Systems 2009*. Springer, 2010.
- Miller, Rich. "Google Data Center FAQ." 2008. www.datacenterknowledge.com.
- Mohammad, Jabbar, David Hutchison, and James P.G. Sterbenz. "Towards Quantifying Metrics for Resilient and Survivable Networks." *14th IEEE International Conference on Network Protocols*. Santa Barbara, California, 2006.
- Moreno, Victor (CCIE.), Victor Moreno, and Kumar Reddy. *Network virtualization*. Cisco Press, 2006.
- Nicholes, M., and B. Mukherjee. "A survey of security techniques for the border gateway protocol (BGP)." *IEEE Communications Surveys & Tutorials*. 2009. 52-65.
- Patterson, David A., and John L. Hennessy. *Computer organization and design: the hardware/software interface*. Morgan Kaufmann, 2008.
- Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, Jin Li. "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing." *IEEE Transactions on Parallel and Distributed Systems*. 2011. 847 - 859.
- Resilience*. n.d. <http://www.merriam-webster.com/dictionary/resilience> (accessed 2011).
- Ruest, Nelson, and Danielle Ruest. *Virtualization, A Beginner's Guide*. McGraw-Hill Osborne Media, 2009.
- Sarka, P., K. Voruganti, K. Meth, O. Biran, and J. Satran. "Internet Protocol storage area networks." *IBM SYSTEMS JOURNAL*, Vol. 42, 2003.
- SAS. *SAS language reference: concepts*. SAS Publishing, 1999.
- Scott Cato, M. "Green Economics." *Earthscan* (Earthscan), 2009.
- Scott, J. *Social Network Analysis*. Sage, 1992.
- Scott, John. *Social network analysis*. Sage Publications, 1987.
- Seokwoo Song, Sridhar Nerur, and James T.C. Teng. "Research contributions: An exploratory study on the roles of network structure and knowledge processing orientation in work unit knowledge management." *ACM SIGMIS Database*. 2007. Volume 38 Issue 2.

- Shoukat Ali, Anthony A. Maciejewski, Howard Jay Siegel, and Jong-Kook Kim. "Measuring the Robustness of a Resource Allocation." *IEEE Transactions on Parallel And Distributed Systems*, 2004.
- Snevely, Rob. *Enterprise Data Center Design and Methodology*. Sun Microsystems Press, 2003.
- Souza, Randy, Harley Manning, and Katharine M. Gardiner. *How to measure what matters*. The Forrester, 2001.
- Swaminathan Sivasubramanian, Guillaume Pierre, Maarten van Steen. *Web content caching and distribution*. Kluwer Academic Publishers, 2004.
- Thing, V.L.L., M. Sloman, and N. Dulay. "Adaptive response system for distributed denial-of-service attacks." *IEEE International Symposium on Integrated Network Management, 2009. IM '09. IFIP*. 2009. 809-814.
- Traffic-Shaper-XP. *www.cnet.com*. 2005. (accessed 2008).
- Trivedi, K.S., Dong Seong Kim, and R. Ghosh. "Resilience in computer systems and networks." *IEEE/ACM International Conference on Computer-Aided Design - Digest of Technical Papers, 2009. ICCAD 2009*. . 2009. 74 - 77 .
- Vaidyanathan, K., S. Narravula, P. Balaji, and D. K. Panda. "Designing Efficient Systems Services and Primitives for Next-Generation Data-Centers." *NSF Next Generation Software (NGS '07) Program, IPDPS*. 2007.
- Villars, L. *IBM Total Storage Software: Building Storage Solutions in Alignment with Current and Future Business Requirement*. White paper sponsored by IBM, 2004.
- Wasserman, S., and K Faust. *Social Network Analysis*. Cambridge University Press, 1994.
- Wenzheng, Li, and Shi Hongyan. "Novel algorithm for load balancing in cluster systems." *2010 14th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*. 2010. 413 - 416 .
- Wilson, Steven. *Managing a Fibre Channel Storage Area Network*. Storage Networking Industry Association, 1998.
- Wolf, Chris, and Erick M. Halter. *Virtualization: from the desktop to the enterprise*. Apress, 2005.
- www.opnet.com*. 2005. (accessed 2010).
- www.sas.com*. 2005. (accessed 2010).
- Yun, YE. "Design and Implementation of a Distributed Data Backup and Recovery System." *JOURNAL OF NATIONAL UNIVERSITY OF DEFENSE TECHNOLOGY*, 2003: 76-80.
- Zeeshan Naseh, Zeeshan Naseh. *Designing Content Switching Solutions*. Cisco Press , 2006.
- Zhu, Ying-Guo. "Design and realization of data center based on SAN." *The 2nd IEEE International Conference on Information Management and Engineering (ICIME), 2010* . 2010. 539-541.

CURRICULUM VITAE

YEHIA H. KHALIL MOHAMED

Cell phone: 502-407-0384

yh.khalil@gmail.com

Highlights

- SAS Student Ambassador.
- IEEE & CECS of U of Louisville Outstanding Student Award (2008-2009).
- Travel Grant Awards for 2008 & 2009
- MWSUG 2010 Student Scholars

Professional Experience

University of Louisville, Louisville KY

08/2005- Now

As a Graduate Research Assistant, I worked on several projects detailed below:

- **Financial Data Center Resilience project funded by Department of the US-Treasury**
Analyzed and evaluated the data center resilience requirements, developed a practical solution for resilience analysis (Resilience is the ability of Data Centers to provide acceptable service levels during server operational conditions). Several publications resulted.
- **Computer Network resilience analysis using social network Analysis**
The main objective of this work is to use social network analysis to identify the important or prestige nodes based on their social activity.
- **Faculties Load Balancing Evaluation Using Data Mining**
Collected and analyzed data from faculties work plans and resumes, for two departments, Math & Biology, for social network analysis. Text mining was used to discover frequent faculty tasks and activity. Earned the SAS Ambassador Award for this work.
- **Health Care Cost Reduction Opportunities**
Used the Medical Expenditure Panel Survey (MEPS) data sets to study the impact of medical personnel levels at clinics looking at the overall clinic visit cost in terms of the number of visits, procedures, etc. Resulted in a poster presentation at M2010.
"Investigate the Consequence of Medical Personnel Level on Health Care Expenses Using SAS Enterprise Guide"
- **Teaching Activity**
I have been teaching several introductory and advance classes for undergraduate and graduate students at the Schools of Engineering and Business.

Participated in several projects:

- **Web based System for Sales Analysis and Monitoring**
It is a business Integrated System that helps the decision makers to make their decisions in a fast and easy way based on historical data. It provides a powerful and Interactive Interface.
- **Geographical Information Systems (GIS) for Environment Planning and Healthcare**
This project was funded by the British Council Cairo office; we developed training materials for health care workers on how to use GIS and associated peripherals to build a public medical infrastructure.
- **Enhancement of Pharmaceutical Warehouse Database**
Historical data of pharmaceutical sales and on-line orders were analyzed to redesign an enhanced user interface.

Operational IT activities

- **Network Administration management group manger**
 - Develop security policy and operations
 - Solve daily problems as they appear and maintain regular daily and weekly activity.

Education

- **Ph.D. Computer Science and Engineering Program CECS**
University of Louisville,
Louisville, KY USA.
- **M.S. Computer Science & Operation Research (2001)**
Faculty of Engineering & Technology
Arab Academy for Science and Technology, Egypt.
- **B.S. of Computer Science and statistics (1994)**
Faculty of Science Alexandria University, Egypt.

Training

- **Advanced Techniques in the SAS® Macro Language By Art Carpenter**
The main course topics: Macro Functions, Using and Creating, Writing Dynamic Code, Controlling Environment, Working with SAS data sets, Using SAS Macro Libraries, Miscellaneous Macro Topics

Certifications

- **Graduate Data Mining Certification, U. of Louisville, Spring 2010**
The Department of Computer Engineering and Computer Science (CECS) and the Department of Mathematics at the U. of Louisville have developed this joint certificate in data mining to address the need for trained professionals in the interdisciplinary field of data mining.
- **Graduate Teaching Academy Certification**

The Graduate Student Teaching Academy is designed to assist second year graduate students who serve as graduate teaching assistants to develop knowledge, skills and excellence in pedagogy and classroom teaching skills.

Awards

- **SAS Student Ambassador**

The SAS Student Ambassador Program is a competitive program that recognizes and supports students who use SAS technologies in innovative ways that benefit their respective industries and fields of study. Select students were named SAS Student Ambassadors and earn the opportunity to present their research at the 2011 SAS Global Forum in Las Vegas, Nevada on April 4-7

- **MWSUG 2010 Student Scholars**

MidWest SAS® Users Group (MWSUG) grants support to present at the MWSUG, 2010 meeting.

- **IEEE & CECS of U of Louisville Outstanding Student Award (2008-2009)**

The IEEE Louisville Chapter honors two outstanding students upon the recommendation of CECS faculty.

- **Travel Grant Awards for 2008 & 2009**

Grants are supported by the National Science Foundation (NSF), the Office of Navy Research (ONR), and the U.S. Army Research Office (ARO) awarded for students and junior researcher to attend the IEEE Symposium on Security and Privacy.

Computer Skills

- Operating Systems: Windows all versions and Linux
- Applications/Software: MS. Office, SAS, Visio, SQL Servers, Rapid Miner.
- Computer Networks: TCP/IP protocols, Cisco routers, IIS and DNS.
- Programming languages: C& C++ and java.
- Specialized tools and packages: SAS, EM, OPNET

Presentations & Posters

- Yehia H. Khalil, “Data Center Resilience Assessment”, presented at INFORMS Computing Society Conference held in Monterey, California, 9-11 January 2011.
- Yehia H. Khalil, “Investigate the Consequence of Medical Personnel Level on Health Care Expenses Using SAS Guide”, Poster to be presented on M2010 the 13th Data Mining conference, Las Vegas, Oct 2010.
- Yehia H. Khalil, “DRG-Based Hospital Payment System Impact On Medical Decision Making”, Poster presented at the ISPOR 15th Annual International Meeting, May 15-19, 2010 at the Hilton Atlanta in Atlanta, GA, USA
- Yehia H. Khalil, “Business Success: Using Social Networks for Team Building and Team Productivity Analysis”, Poster presented on M2009 the 12th Data Mining conference, Las Vegas, Oct 2009.

- Yehia H. Khalil, “Data Center: Threats & Resilience Evaluation”, Poster presented on E-Expo 2008, J.B. Speed School, University of Louisville, Louisville, KY.
- Yehia H. Khalil, “Parameter Reduction for Data Center Resilience Evaluation”, Poster presented on M2007 the 10th Data Mining conference, Las Vegas, Oct 2007.

Book Chapter

- Yehia H. Khalil, Adel S. Elmaghraby, “Data Center Resilience”, Cyber Infrastructure Protection; Policy and Strategy, New York USA, June 4-5, 2009. Printed as book Chapter to be published by the Strategic Studies Institute, U.S. Army War College 2010.

Journal Papers

- Yehia H. Khalil, Walaa M. Sheta, Adel S. Elmaghraby, “Improved Computer Networks resilience Using Social Behavior”, International Journal of Computer Science and Information Security, October 2010, Vol. 8 No. 7, pp. 208-214.

Conference’s Papers

- Yehia H. Khalil, “A Detailed Examination of Workload Assigned and Faculty Productivity: Social Networks Using SAS® Enterprise Guide® and SAS® Text Miner”, SAS Global Forum, Las Vegas, 2011.
- Yehia H. Khalil, Adel Elmaghraby, “Data Center Resilience Evaluation Test-bed Design and Implementation”, ISSPIT 2008, Sarajevo, Bosnia and Herzegovina, December 2008, pp. 369-374.
- Yehia H. Khalil, Adel Elmaghraby, “Evaluating Server Load Balancing Algorithms For Data Center’s Resilience Enhancement”, ISCA 21st International Conference on Parallel and Distributed Computing and Communication Systems, New Orleans, Louisiana, September 2008, pp. 111-116.
- Yehia H. Khalil, Adel Elmaghraby, Anup Kumar, “Evaluation of Resilience for Distributed Data Centers”, to be published on IEEE Symposium on Computers and Communications (ISCC'08) Marrakech, Morocco, July 2008, pp. 340-345.
- Viktoria Rojkova, Yehia Khalil, Adel Elmaghraby, Mehmed Kantardzic: “Use of Simulation and Random Matrix Theory to Identify the State of Network Traffic” The 7th IEEE International Symposium on Signal Processing and Information Technology (ISSPIT2007), Cairo, Egypt, Dec. 2007, pp. 647-652.
- Yehia H. Khalil, Anup Kumar, Adel Elmaghraby: “Design considerations for Resilient Distributed Data Centers”, ISCA 20th International Conference on Parallel and Distributed Computing Systems (PDCS 2007), Las Vegas, September 2007, pp. 51-55.
- Yehia H. Khalil, Walaa M. Sheta, Saleh El-Shehaby, Adel S. Elmaghraby: “Network Performance Requirement for Online Games”, CGAMES 10th

International Conference on Computer Games (CGAMES'2007), Louisville, KY, 2007, pp. 51-56.

- Yehia H. Khalil, Anup Kumar, Adel S. Elmaghraby, James H. Graham, "Performance Modeling of Resilient Information System for Remote Data Storage", SoutheastCon, 2007. Proceedings. IEEE, March 2007, pp. 346-346.
- Yehia H. Khalil, Abaith Mohamed, Ayman El Desouki, "Using Expert System for solving LAN management performance problem", ICAIA, 2001.