

# **Evaluation of Performance Analysis And Network Security Using OPNET**

By : Mohammed Seed Ahmed Mohammed Mukhtar  
Supervisor Prof. : Seaf E-deen Fatowh Osman

**Thesis Submitted to the Faculty of Post Graduate Studies and research in Fulfillment of the Requirements for the Doctorate Degree in Information Technology**

Information Technology Department  
Faculty of Applied Science  
Red Sea University

Aug. 2015

## **Abstract**

The Networks security is critical issue and represents a challenge to professional systems developers in protection against diverse attacks. The study deals specifically with network security and exactly evaluate performance analysis of networks.

The objective of study to find good analyzing networks configuration to achieve excellent performance, high throughput, low packets loss rate, decreased re-transmissions data and decreased collisions data.

The study used OPNET analysis system simulator, which is good analyse system, to estimate the performance of new solutions to existing networks, and the simulation can provide the time and effort.

The most important results is to evaluate the performance of the role of firewalls and virtual private networks to provide security for the common public networks such as the Internet. Also the findings of the ringed network under different scenarios where the research examines the impact of asynchronous mode of transmission data and its impact on a range of services and quality.

The study recommended using laboratory results to the output of the program and take advantage of computer networks in real applications. The study also recommended the development of all of its security testing and evaluation of performance of computer networks under Opnet14.0 program environment, which is a good simulation environment and to design models and data analysis are excellent

## المستخلص

إن أمن الشبكات قضية حاسمة وتحدي إلى مطوري النظم المحترفين في الحماية ضد الهجمات المتنوعة وتتناول الأطروحة بشكل محدد أمن الشبكات وبالتحديد تقييم تحليل أداء الشبكات.

استخدمت الدراسة نظام تحليل المحاكاة opnet الذي يعتبر نظام تحليل جيد, فهو يقوم بتخمين أداء الحلول الجديدة للشبكات الحالية، كما ان المحاكاة يُمكن أن توفر الوقت والجهد.

تهدف الدراسة لإيجاد تحليل إعداد الشبكات بصورة جيدة لتحقيق الأداء الامثل والطاقة الإنتاجية العالية ونسبة خسارة حزم منخفضة، وتقليل إعادة إرسال البيانات وايضاً تقليل تصادمات البيانات.

ومن اهم النتائج التي توصل اليها البحث هي تقييم أداء دور الجدران النارية والشبكات الخاصة الافتراضية في توفير الأمن للشبكات العامة المشتركة كالإنترنت. وأيضاً من النتائج الهامة الشبكة الحلقية تحت السيناريوهات المختلفة حيث تم فحص تأثير النمط الغير متزامن لإرسال البيانات وتأثيره على مدى الخدمات وجودتها.

توصي الدراسة باستخدام النتائج المعملية التي توصل اليه البحث لمخرجات البرنامج والاستفادة منها في بناء وتطبيقات شبكات الحاسوب الواقعية . كذلك اوصت الدراسة بوضع كل الاختبارات الامنية وتقييم الأداء لشبكات الحاسوب تحت بيئة برنامج (Opnet14.0) والذي يعتبر بيئة محاكاة جيدة ويقوم بتصميم النماذج وتحليل البيانات بصورة ممتازة.

## Table of contents

Number	Topics	Page
	Dedication	i
	Acknowledgements	ii
	المستخلص	iii
	Abstract	iv
	List of figures	ix
	Abbreviations list	xi
<b>Chapter one : Introduction</b>		
1-1	Introduction	1
1-2	Problems	2
1-3	Objectives	3
1-4	Formulation of hypotheses	3
1-5	Methodology	4
1-6	Chapters review	4
<b>Chapter Two : Literature review</b>		
2-1	Communications Model	6
2-2	Data Communications Model	10
2-3	Signaling	12
2-4	Computer Networks	15
2-4-1	Circuit Switching	17
2-4-2	Packet Switching	17
2-4-3	Frame Relay	17
2-4-4	Asynchronous transfer mode	18
2-5	Model For Network Security	19
2-6	The OSI Security Architecture	21
2-7	Concept Of Security and Performances	24
2-8	Security Attacks	25
2-8-1	Passive Attacks	25
2-8-2	Active Attacks	26
2-8-3	Replay attacks	26
2-9	Network Security and Applications	28
2-9-1	Internet Protocol (IP) Security	29
2-9-2	Web Security	32
2-9-3	Network Management Security	34
2-9-4	Internet Control Message Protocol (ICMP)	34
2-9-5	Session Initiation Protocol (SIP)	35
2-10	System Security	36
2-11	Viruses	36
2-12	Firewalls	37
2-12-1	Packet Filtering Firewalls	37

<b>Number</b>	<b>Topics</b>	<b>Page</b>
2-12-2	Stateful Inspection Firewalls	38
2-12-3	Application Firewalls	38
2-13	Virtual Private Networks	39
2-13-1	Tunneling	39
2-13-2	Types of Tunneling	40
2-13-3	Types of VPNs	40
2-14	Cryptographic	41
2-14-1	Cryptographic goals	41
2-14-2	Conventional encryption	42
2-14-3	Public key cryptography	43
2-14-4	Encryption/decryption	43
2-14-5	Digital signature	44
2-14-6	Key exchange	44
2-15	Related Works	45
<b>Chapter Three : Materials and Methods</b>		
3-1	Introduction	46
3-2	Simulation	46
3-3	Simulation in Real Environments	47
3-4	The OPNET Simulation Environment	47
3-5	Why OPNET Modeler for Research?	49
3-5-1	OPNET Advantages	49
3-5-2	OPNET Disadvantages	49
3-6	Methods	49
3-7	Simulation Analysis Methods with OPNET	51
3-7-1	Recommended system configuration, platforms, and software	51
3-7-2	Performance of Real Networks	51
3-7-3	Understanding performance of the network	51
3-8	Procedures	52
3-8-1	Start OPNET IT Guru Academic Edition	52
3-8-2	Network topology Editor	53
3-8-3	The Node Editor	54
3-8-4	The Process Model Editor	55
3-8-5	The Link Model Editor	56
3-8-6	The Path Editor	57
3-8-7	Configure Nodes and protocols	58
3-8-8	Specify traffic from users	59
3-8-9	Select statistics to measure	60
3-8-10	The Simulation Sequence Editor	61
3-8-11	Analyze the results	62
3-9	OPNET Modeling Hierarchy	63
<b>Number</b>	<b>Topics</b>	<b>Page</b>

3-10	Model Library	63
3-11	Internal Structure of OPNET	63
3-12	States and Events	64
4-1	Introduction	65
<b>Chapter Four: Design and Results</b>		
4-2	Firewalls and VPN (Network Security and Virtual Private Networks)	65
4-2-1	Objective	65
4-2-2	Overview	65
4-2-3	The No_Firewall scenario	67
4-2-4	Configure the nodes of scenario	68
4-2-5	Choose the Statistics of scenario	68
4-2-6	The Firewall Scenario	68
4-2-7	Simulating encryption of scenario	71
4-2-8	Run the Simulation of scenarios	73
4-2-9	View the Results of scenarios	73
4-2-10	Result analysis of scenarios	78
4-3	Virtual Local Area Networks (VLANs)	79
4-3-1	Objective	79
4-3-2	Overview	79
4-3-3	No_VLAN scenario	80
4-3-4	Configure the traffic demands of No_VLAN scenario	81
4-3-5	Configure the links ports of No_VLAN scenario	81
4-3-6	Choose the Statistics of scenario	82
4-3-7	The VLAN Scenario	82
4-3-8	The VLAN_Comm Scenario	83
4-3-9	View the Results of all scenario	85
4-4	Web Caching and Data Compression Improving Web Access and Server Performance	88
4-4-1	Objective	88
4-4-2	Overview	88
4-4-3	NoCache_NoComp scenario	89
4-4-4	Configuring the UN sub-network	90
4-4-5	Configuring the Africa sub-network	91
4-4-6	Choose the Statistics of the UN sub-network	91
4-4-7	The NoCache_Comp Scenario	92
4-4-8	The Cache_NoComp Scenario	92
4-4-9	View the Results of all scenarios	93
4-5	Internet Control Message Protocol (ICMP)	95
4-5-1	Objective	95
4-5-2	Overview	95
4-5-3	Link_UP Scenario Procedure	95

4-5-4	Configuration	96
4-5-5	Configuring Simulation of ICMP	96
4-5-6	Result Analysis of all scenarios	97
4-6	Switched LANs	103
4-6-1	Objective	103
4-6-2	Overview	103
4-6-3	The OnlyHub Scenario Procedure	104
4-6-4	Configure the Network Nodes	104
4-6-5	Choose the Statistics	105
4-6-6	Hub And Switch Scenario	105
4-6-7	View the Results	106
Conclusion		110
Recommendations		111
References		112

## **Conclusion**

The experiments discuss a variety of Evaluate Performance Analysis and Network Security, networking designs and protocols. They do not require programming skills as a prerequisite. They are generic and can be easily expanded to utilize new technologies and networking standards. With the free, easy-to-install software, the OPNET IT Guru Academic Edition.

This thesis discusses 5 cases which intend to be an approach to Evaluate Performance Analysis and Network Security. It has a special focus on security issues.

OPNET IT Guru is a complete tool for this purpose and has been proved to simulate Firewalls and VPN (Network Security and Virtual Private Networks), internet Control Message Protocol (ICMP), Web Caching and Data Compression Improving Web Access and Server Performance, Switched LANs, VLANs: Virtual Local Area Networks.

The scenario duplication mechanism has shown itself a powerful feature to construct the three security schemes using a common root scenario.

Statistics and Simulation Logs compared between multiple scenarios within a same project has demonstrated to be a pedagogical way to show whether a connection is available between peers or not, which was a requirement to assure the correct implementation of the security schemes.

### **Recommendations**

The researcher recommended:

- Using laboratory results to the output of the program and take advantage of computer networks in real applications.
- The development of all of its security testing and evaluation of performance of computer networks under Opnet program environment, which is a good simulation environment and to design models and data analysis are excellent .
- Developed all laboratories in OPNET Modeler 14.5 simulation environment which is a network simulator that offers the tools for model design, simulation, data mining and analysis.

Newer version of Opnet software should be considered. This is due to the limitation of blocks in communication toolbox and block set. Even though the numbers of block in communication block set are many, more designs of block set using opnet, especially advance opnet software technologies are needed in that's labs .