

Enterprise Network Technology and Internet Security	:العنوان
Saleh, Tamer Mohamed Al Emam Ali	: المؤلف الرئيسي:
Abd Algawad, Ehab. Abd Alrazak, Muneer Mohamed, Abo Alsoud, Mohy Aldin Ahmed(Super.)	: مؤلفين آخرين:
2009	: التاريخ الميلادي:
المنصورة	: موقع:
1 - 167	: الصفحات:
537758	: رقم MD:
رسائل جامعية	: نوع المحتوى:
English	: اللغة:
رسالة ماجستير	: الدرجة العلمية:
جامعة المنصورة	: الجامعة:
كلية الهندسة	: الكلية:
مصر	: الدولة:
Dissertations	: قواعد المعلومات:
الإنترنت، أمن المعلومات، شبكات المعلومات، تأمين الشبكات	: مواضيع:
<a href="https://search.mandumah.com/Record/537758">https://search.mandumah.com/Record/537758</a>	: رابط:

## ملخص البحث

## ملخص البحث

تستخدم الانترنت الآن الإصدار رقم 4 لبروتوكول عناوين الانترنت (IP protocol V4) مما يتيح نظريا عدد من العناوين يصل إلى  $2^{32}$ .

في السنوات الأخيرة زاد استخدام الانترنت بصورة كبيرة في جميع مجالات الحياة بصورة لم تكن متوقعة عند بداية استخدام الانترنت بروتوكول إصدار رقم 4, حيث أدى أضافه كثير من الأجهزة و الخدمات و تطبيقات الانترنت بصورة كبيرة كل يوم إلى زيادة الطلب على عناوين أرقام الانترنت ( IP Address) زيادة كبيرة مما أدى إلى قرب نفاذ هذه العناوين, و قد أعلنت المنظمة المسؤولة عن تنظيم استخدم عناوين الانترنت (IANA) انه بحلول نهاية عام 2010 سوف تنفذ هذه العناوين.

و قد دفعت هذه المشكلة إلى ضرورة تطوير إصدار بروتوكول جديد لعناوين الانترنت و هما ما يعرف بالإصدار رقم 6 لبروتوكول عناوين الانترنت (IPv6) و هو يتيح عدد  $2^{128}$  عنوان انترنت و هو ما يغطي كل الاحتياجات المستقبلية.

الإصدار 6 لبروتوكول عناوين الانترنت لا يحل مشكلة نفاذ العناوين فقط و لكن يقدم مزايا جديدة من ناحية بساطه التركيب البنوي له و زيادة سرعة توجيه حزم البيانات و كفاءته العمل على الخدمات التي تتطلب جوده الخدمة مثل الصوت و الفيديو و بالإضافة إلى انه أفضل من الإصدار السابق في مجال تأمين البيانات حيث أن البروتوكول المعمول به لتأمين الانترنت (IPSEC) يشكل جزء أساسي من أي تنصيب لهذا الإصدار الجديد.

أصبح استخدام هذا الإصدار الجديد من المتطلبات الهامة و الأساسية التي يجب أخذه في الاعتبار من جانب مسؤولي الشبكات في جامعتنا و مؤسساتنا و من هذا المنطلق تم هذا البحث للتعرف على طرق

تنصيب هذا الإصدار الجديد في جامعة المنصورة و دراسة تأثيره على شبكة الجامعة من ناحية التأمين و تأثير الخدمات و التطبيقات المستخدمة بجامعة المنصورة.

تم تنظيم هذا البحث على الوجه التالي:

### الفصل الأول :

يقدم خلفيه عن الإصدار السابق و يقدم أهداف البحث و أسبابه.

### الفصل الثاني:

يقدم وصف تفصيلي للإصدار 6 لبروتوكول عناوين الانترنت و يوضح أهم مميزاته الجديدة .

### الفصل الثالث:

يقدم مقارنة بين كل من الإصدار 4 لبروتوكول عناوين الانترنت و الإصدار 6 لبروتوكول عناوين الانترنت من ناحية التهديدات على مستوى تأمين الشبكات العاملة به و يقدم أيضا مقترحات لمديري الشبكات عند تنصيب الإصدار الجديد.

### الفصل الرابع:

يقدم و صف لطرق التنصيب و التحول لهذا الإصدار الجديد و يقترح خطة لعملية التحول للعمل بالإصدار الجديد و يأخذ شبكة جامعة المنصورة كمثال تطبيقي لذلك.

### الفصل الخامس:

يقدم المحصلة من البحث المقدم، واقتراحات مستقبلية في هذا المجال.

## **ABSTRACT**



## **ABSTRACT**

Over the last few years, the Internet has expanded enormously over what can be imagined; huge number of devices, services, and applications are developed for the internet every day. This represents a great demand for IP addresses. Now, the internet uses IPV4 [1] , which has 32 bit that gives theoretical number of  $2^{32}$  IP addresses. Internet Assigned Numbers Authority (IANA) declared that the IPv4 addresses are expected to be fully allocated by the year 2010.

The next generation Internet protocol; IPv6 [2] has been introduced to overcome the shortage of IPs as it has 128 bit which gives  $2^{128}$  IP addresses. This gives enough IP addresses for any expected future demand. IPv6 does not only solve IP addresses shortage but also provides many improvements over IPv4 considering simplicity, routing speed, quality of service, mobility and security as IPSec [3] is mandatory on the protocol suite.

Using IPv6 becomes an essential requirement that must be considered by the network administrators of universities and organizations. This thesis is concerned studying and identify IPv6 new features and comparing between IPv6 and IPv4 from security point of view

Such thesis also concerned with implementing Mansoura University's transition plan from IPv4 to IPv6, taking into account the complexity of the services, applications and security of the network during the transition.

Such thesis demonstrates using experimental test bed issues regarding address assignment methods, IPv6 performance and security issues. It also and concludes specific recommendations to keep the transition problems as small as possible and provides a road map for transition plan.

Chapter 1: “Introduction” provides an introduction to the thesis, including background and thesis objectives and motivations.

Chapter 2: “IPv6” provide in detailed descriptions of IPv6 features compared to IPv4.

Chapter 3: “IPv6 and IPv4 Security Threats Comparison” provides detailed comparison of the security threats affecting IPv6 and IPv4 and the threats arise from coexisting of the two protocols. It also identifies the threats related to ipv6 only.

Chapter 4: “Transition to IPv6” provides an introduction to the transition mechanism use d to deploy IPv6 and discusses a case study of Mansoura University going through defining the deployment requirements and implementing test bed for deployment and issues arise while deployment.

Chapter 5: “Conclusions and future work” provides the conclusions of this work and the suggestion for the future work.

Enterprise Network Technology and Internet Security	:العنوان
Saleh, Tamer Mohamed Al Emam Ali	: المؤلف الرئيسي:
Abd Algawad, Ehab. Abd Alrazak, Muneer Mohamed, Abo Alsoud, Mohy Aldin Ahmed(Super.)	: مؤلفين آخرين:
2009	: التاريخ الميلادي:
المنصورة	: موقع:
1 - 167	: الصفحات:
537758	: رقم MD:
رسائل جامعية	: نوع المحتوى:
English	: اللغة:
رسالة ماجستير	: الدرجة العلمية:
جامعة المنصورة	: الجامعة:
كلية الهندسة	: الكلية:
مصر	: الدولة:
Dissertations	: قواعد المعلومات:
الإنترنت، أمن المعلومات، شبكات المعلومات، تأمين الشبكات	: مواضيع:
<a href="https://search.mandumah.com/Record/537758">https://search.mandumah.com/Record/537758</a>	: رابط:

## List of Contents

<b>ABSTRACT .....</b>	<b>1</b>
<b>1 CHAPTER 1: INTRODUCTION.....</b>	<b>3</b>
1.1 INTRODUCTION .....	3
1.2 THESIS OBJECTIVES .....	5
1.3 THESIS ORGANIZATION .....	6
1.3.1 Chapter 1: Introduction.....	7
1.3.2 Chapter 2: IPv6 Protocol .....	7
1.3.3 Chapter 3: IPv6 and IPv4 Security Threats Comparison.....	7
1.3.4 Chapter 4: Transition to IPv6 .....	7
1.3.5 Chapter 5: Conclusion and Future Work .....	7
<b>2 CHAPTER 2:IPV6 PROTOCOL.....</b>	<b>8</b>
2.1 IPV6 FEATURES.....	8
2.1.1 New Header Format.....	8
2.1.2 Large Address Space .....	9
2.1.3 Efficient Hierarchical Addressing and Routing Infrastructure .....	9
2.1.4 Stateless and Statefull Address Configuration.....	10
2.1.5 Built-in Security .....	10
2.1.6 Better Support for QoS.....	10
2.1.7 New Protocol for Neighboring Node Interaction .....	11
2.1.8 Extensibility .....	11
2.2 IPV6 HEADER .....	11
2.2.1 IPv6 Packets over LAN Media.....	12
2.2.2 IPv4 Header.....	13
2.2.3 IPv6 Header .....	16
2.2.4 COMPARING SUMMARY the IPv4 and IPv6 Headers .....	18
2.3 IPV6 EXTENSION HEADERS.....	19
2.4 IPV6 ADDRESSING .....	21
2.4.1 IPv6 Address Notation and Syntax.....	21
2.4.2 IPv6 Prefixes .....	22
2.4.3 Types of IPv6 Addresses .....	22
2.4.3.1 Unicast IPv6 Addresses .....	23
2.4.3.2 Multicast IPv6 Addresses .....	28
2.4.3.3 Anycast IPv6 Addresses .....	32
2.4.4 IPv6 Addresses for a Host.....	33



2.4.5	IPv6 Addresses for a Router .....	34
2.4.6	IPv6 Interface Identifiers .....	35
2.4.7	Addresses and Addressing Concept IPv4 Vs IPv6 .....	36
2.5	IPV6 AND DNS .....	36
2.5.1	The Host Address (AAAA) Resource Record .....	37
2.5.2	The IP6.ARPA Domain .....	37
2.6	ICMPV6 .....	38
2.6.1	Types of ICMPv6 Messages .....	39
2.6.2	ICMPv6 Header .....	40
2.6.3	Comparing ICMPv4 and ICMPv6 Error Messages .....	41
2.7	NEIGHBOR DISCOVERY .....	42
2.8	ROUTER DISCOVERY .....	43
2.9	ADDRESS AUTOCONFIGURATION .....	45
2.9.1	Autoconfigured Address States .....	46
2.9.2	Types of Autoconfiguration .....	47
2.10	DIFFERENCES SUMMARY BETWEEN IPV4 AND IPV6 .....	49
<b>3</b>	<b>CHAPTER 3: IPV6 AND IPV4 THREATS COMPARISON .....</b>	<b>51</b>
3.1	1 INTRODUCTION .....	51
3.2	THREATS ANALYSIS .....	51
3.3	ATTACKS CHANGED IN IPV6 NETWORK .....	51
3.3.1	Network Information Gathering – Reconnaissance .....	52
3.3.1.1	Reconnaissance in IPv4 .....	52
3.3.1.2	Reconnaissance in IPv6 .....	53
3.3.1.3	Tools and Technology Capabilities .....	55
3.3.1.4	Mitigation techniques for Reconnaissance .....	55
3.3.2	Unauthorized Access .....	56
3.3.2.1	Unauthorized Access in IPv4 .....	57
3.3.2.2	Unauthorized Access in IPv6 .....	57
3.3.2.3	Mitigation techniques for unauthorized access .....	64
3.3.3	Header Manipulation and Fragmentation .....	64
3.3.3.1	Fragmentation in IPv4 .....	65
3.3.3.2	Fragmentation in IPv6 .....	66
3.3.3.3	Tools and Technology Capabilities .....	68
3.3.3.4	Mitigation techniques for Header Manipulation and Fragmentation .....	68
3.3.4	Layer 3-Layer 4 Spoofing .....	69
3.3.4.1	Layer 3-Layer 4 Spoofing in IPv4 .....	69
3.3.4.2	Layer 3-Layer 4 spoofing in IPv6 .....	70
3.3.4.3	Tools and Technology Capabilities .....	71
3.3.4.4	Mitigation techniques Layer 3-Layer 4 Spoofing .....	71
3.3.5	Subverting Host Initialization and Address-Resolution Attacks .....	73
3.3.5.1	Subverting Host Initialization and Address-Resolution Attacks in IPv4 .....	73



3.3.5.2	Subverting Host Initialization and Address-Resolution Attacks in IPv6 .....	75
3.3.5.3	Tools and Technology Capabilities.....	76
3.3.5.4	Mitigation techniques for Subverting Host Initialization and Address-Resolution Attacks Attacks.....	77
<b>3.3.6</b>	<b><i>Broadcast Amplification Attacks (smurf)</i></b> .....	<b>78</b>
3.3.6.1	Smurf attack in IPv4 .....	78
3.3.6.2	Smurf attack in IPv6 .....	78
3.3.6.3	Tools and Technology Capabilities.....	79
3.3.6.4	Mitigation techniques for Broadcast Amplification Attacks (smurf).....	80
<b>3.3.7</b>	<b><i>Routing Attacks</i></b> .....	<b>81</b>
3.3.7.1	Routing Attacks in IPv4 .....	81
3.3.7.2	Routing Attacks in IPv6 .....	82
3.3.7.3	Tools and Technology Capabilities.....	83
3.3.7.4	Mitigation techniques for Routing Attacks .....	83
<b>3.3.8</b>	<b><i>Viruses and Worms</i></b> .....	<b>83</b>
3.3.8.1	Viruses and Worms in IPv4 .....	84
3.3.8.2	Viruses and Worms in IPv6 .....	85
3.3.8.3	Tools and Technology Capabilities.....	87
3.3.8.4	Mitigation techniques for Viruses and Worms .....	88
<b>3.3.9</b>	<b><i>Translation, Transition, and Tunneling Mechanisms</i></b> .....	<b>88</b>
3.3.9.1	Dual stack security issues .....	89
3.3.9.2	Tunneling Issues .....	90
3.3.9.3	Translation security Issues.....	92
3.3.9.4	Mitigation techniques.....	92
<b>3.4</b>	<b>SIMILAR ATTACKS FOR IPV4 AND IPV6</b> .....	<b>93</b>
3.4.1	<i>Capturing Data in Transit (Sniffing)</i> .....	94
3.4.2	<i>Application Layer Attacks</i> .....	94
3.4.3	<i>Rogue Devices</i> .....	95
3.4.4	<i>Man-in-the-Middle Attacks</i> .....	95
3.4.5	<i>Flooding, Denial of Service Attacks and Botnets</i> .....	96
<b>3.5</b>	<b>MITIGATION TECHNIQUES SUMMARY</b> .....	<b>97</b>
<b>4</b>	<b>CHAPTER4: TRANSITION TO IPV6</b> .....	<b>101</b>
<b>4.1</b>	<b>IPV6 TRANSITION MECHANISM</b> .....	<b>101</b>
4.1.1	<i>Dual Stack</i> .....	101
4.1.2	<i>NAT-PT</i> .....	102
4.1.3	<i>Tunneling</i> .....	103
4.1.3.1	Basic Tunneling Strategies .....	103
4.1.3.2	Configured Tunneling .....	104
4.1.3.3	Automatic Tunneling .....	105
4.1.3.4	Tunneling Implementations.....	106
<b>4.2</b>	<b>TRANSITION TO IPV6</b> .....	<b>109</b>
4.2.1	<i>Identify the network infrastructure</i> .....	110
4.2.2	<i>Inventory network equipment and operating systems:</i> .....	111
4.2.3	<i>Identify Software and applications and how they need to be changed:</i> .....	111



4.2.4	Developing an address plan.....	112
4.2.5	Set up an IPv6 Test environment.....	112
4.2.6	Devise and implementing a security policy.....	112
4.2.7	Establish an IPv6 education and awareness plan for IT staff & users.....	113
4.2.8	Case study Mansoura University Network.....	113
4.2.9	Mansoura University Network Infrastructure.....	114
4.2.9.1	Network Main Features.....	114
4.2.9.2	Services Provided.....	118
4.2.9.3	Host and device platforms.....	121
4.2.9.4	User tools/systems.....	123
4.2.9.5	IP Address plan and Assignment management.....	124
4.2.10	Setting up pilot test environment.....	126
4.2.10.1	Test bed discussed issues.....	127
4.2.10.2	Address assignment methods test.....	128
4.2.10.3	Security threats test.....	137
4.2.11	IPv6 Transition Road Map.....	157
4.2.12	Transition Gap Analysis and Outcomes results.....	158
4.2.13	IPv6 Security Considerations.....	159
<b>5</b>	<b>CHAPTER 5: CONCLUSIONS AND FUTURE WORK.....</b>	<b>160</b>
5.1	CONCLUSIONS.....	160
5.2	RECOMMENDED FUTURE WORK.....	162
5.2.1	Voice Over IPV6.....	162
5.2.2	IPv6 and mobility.....	163
<b>6</b>	<b>PUBLICATION.....</b>	<b>164</b>
<b>7</b>	<b>REFERENCES.....</b>	<b>165</b>

Enterprise Network Technology and Internet Security	العنوان:
Saleh, Tamer Mohamed Al Emam Ali	المؤلف الرئيسي:
Abd Algawad, Ehab, Abd Alrazak, Muneer Mohamed, Abo Alsoud, Mohy Aldin Ahmed(Super.)	مؤلفين آخرين:
2009	التاريخ الميلادي:
المنصورة	موقع:
1 - 167	الصفحات:
537758	رقم MD:
رسائل جامعية	نوع المحتوى:
English	اللغة:
رسالة ماجستير	الدرجة العلمية:
جامعة المنصورة	الجامعة:
كلية الهندسة	الكلية:
مصر	الدولة:
Dissertations	قواعد المعلومات:
الإنترنت، أمن المعلومات، شبكات المعلومات، تأمين الشبكات	مواضيع:
<a href="https://search.mandumah.com/Record/537758">https://search.mandumah.com/Record/537758</a>	رابط:



Mansoura University  
Faculty of Engineering  
Electronics and Communications  
Engineering Department

# Enterprise Network Technology and Internet Security

A Thesis Submitted in Partial Fulfillment of the requirements for the  
Master of Science Degree

*In*

Electrical Communications Engineering

*By*

**Eng. Tamer Mohamed Elemam Ali Saleh**

B. S. Electronics and Communications Engineering  
Mansoura University – Faculty of Engineering

## *Supervisors*

**Prof. Mohy Eldin ahmed  
abo-Elsoud**  
Electronics and  
Communications  
Engineering Dept  
Faculty of Engineering  
Mansoura University

**Assoc. Prof. Muneer  
Mohamed Abdel Razak**  
Electronics and  
Communications  
Engineering Dept  
Faculty of Engineering  
Mansoura University

**Dr. Ehab Abdel Gawad**  
Electronics and  
Communications  
Engineering Dept  
Faculty of Engineering  
Helwan University

2009



Mansoura University  
Faculty of Engineering  
Electronics and Communications  
Engineering Department

# Enterprise Network Technology and Internet Security

A Thesis Submitted in Partial Fulfillment of the requirements for the  
Master of Science Degree

*In*

Electrical Communications Engineering

*By*

**Eng. Tamer Mohamed Elemam Ali Saleh**

B. S. Electronics and Communications Engineering  
Mansoura University – Faculty of Engineering

## *Supervisors*

**Prof. Mohy Eldin ahmed  
abo-Elsoud**

Electronics and  
Communications  
Engineering Dept  
Faculty of Engineering  
Mansoura University

**Assoc. Prof. Muneer  
Mohamed Abdel Razak**

Electronics and  
Communications  
Engineering Dept  
Faculty of Engineering  
Mansoura University

**Dr. Ehab Abdel Gawad**

Electronics and  
Communications  
Engineering Dept  
Faculty of Engineering  
Helwan University

2009



## SUPERVISORS

### THISIS TITLE:

**ENTERPRISE NETWORK TECHNOLOGY AND INTERNET  
SECURITY**

### RESHERSHER NAME:

**TAMER MOHAMED ELEMAM ALI SALEH**

### SUPERVISORS:

Name	Position	Signature
<b>Prof. MOHY ELDIN AHMED ABO-ELSOUD</b>	Prof of Electronics and Communications Engineering, Faculty of Engineering Mansoura University	<i>M.A. Abo- Elsoud</i>
<b>Assoc. Prof. MUNEER MOHAMED ABDEL RAZAK</b>	Associate Prof. Electronics and Communications Engineering Faculty of Engineering, Mansoura University	<del><i>[Signature]</i></del>
<b>Dr. EHAB ABDEL GAWAD</b>	Electronics and Communications Engineering, Faculty of Engineering Helwan University	<i>Ehab</i>

Head of Department

*Fatma E.Z. Abou-Chadi*  
Prof. Fatma E.Z. Abou-Chadi

Vice Dean

Prof. **M.ELshabrawy**

Dean

**M.ELshabrawy**  
Prof. Mohamed El-Shabrawy M.Ali





## SUPERVISORS & JUDGES

**THISIS TITLE:**

**ENTERPRISE NETWORK TECHNOLOGY AND INTERNET  
SECURITY**

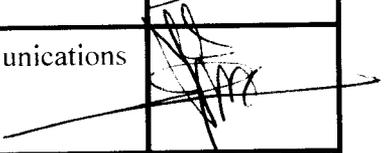
**RESHERSHER NAME:**

**TAMER MOHAMED EL-EMAM ALI SALEH**

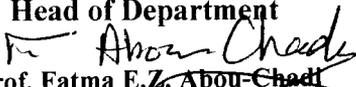
**SUPERVISORS:**

Name	Position	Signature
<b>Prof. MOHY ELDIN AHMED ABO-ELSOUD</b>	Prof of Electronics and Communications Engineering, Faculty of Engineering Mansoura University	M.A. Abo-ElSoud
<b>Assoc. Prof. MUNEER MOHAMED ABDEL RAZAK</b>	Associate Prof. Electronics and Communications Engineering Faculty of Engineering, Mansoura University	
<b>Dr. EHAB ABDEL GAWAD</b>	Electronics and Communications Engineering, Faculty of Engineering Helwan University	Ehab

**JUDGES:**

Name	Position	Signature
<b>Prof. MOHAMED EL-SAID NASR</b>	Prof. of Electronics and Communications Engineering, Faculty of Engineering Tanta University	
<b>Prof. MOHY ELDIN AHMED ABO-ELSOUD</b>	Prof of Electronics and Communications Engineering, Faculty of Engineering Mansoura University	M.A. Abo-ElSoud
<b>Assoc. Prof. MUNEER MOHAMED ABDEL RAZAK</b>	Associate Prof. Electronics and Communications Engineering, Faculty of Engineering Mansoura University	
<b>Assoc. Prof. SAMEH IBRAHIM REHAN</b>	Associate Prof. Electronics and Communications Engineering, Faculty of Engineering Mansoura University	Sameh Rehan

Head of Department

  
Prof. Fatma E.Z. Abou-Chadi

Vice Dean



Dean

M.ELshabrawy

Prof. Mohamed El-Shabrawy M.Ali



## **ACKNOWLEDGMENTS**

First of all, I must thank Allah for everything, Without Allah I would not complete this work.

My sincere and deepest gratitude to my supervisors **Prof. Mohy Eldin Ahmed Abo-Elsoud** and **Ass. Prof. Muneer Mohamed Abdel Razak**, for their invaluable support, unique inspiration and fruitful discussions during this work. I have benefited greatly from their experience and directions at every step of this research.

Heart gratitude is due to my family, my father, my mother and my wife who granted me every thing.

My deepest Grateful to all Staff of Communications and Information Technology Center (CITC), Mansoura University for the facilities that were given.

*Eng. Tamer Mohamed Elmam*



## List of Contents

<b>ABSTRACT .....</b>	<b>1</b>
<b>1 CHAPTER 1: INTRODUCTION.....</b>	<b>3</b>
1.1 INTRODUCTION .....	3
1.2 THESIS OBJECTIVES .....	5
1.3 THESIS ORGANIZATION .....	6
1.3.1 Chapter 1: Introduction.....	7
1.3.2 Chapter 2: IPv6 Protocol .....	7
1.3.3 Chapter 3: IPv6 and IPv4 Security Threats Comparison.....	7
1.3.4 Chapter 4: Transition to IPv6 .....	7
1.3.5 Chapter 5: Conclusion and Future Work .....	7
<b>2 CHAPTER 2:IPV6 PROTOCOL.....</b>	<b>8</b>
2.1 IPV6 FEATURES.....	8
2.1.1 New Header Format.....	8
2.1.2 Large Address Space .....	9
2.1.3 Efficient Hierarchical Addressing and Routing Infrastructure .....	9
2.1.4 Stateless and Statefull Address Configuration.....	10
2.1.5 Built-in Security .....	10
2.1.6 Better Support for QoS.....	10
2.1.7 New Protocol for Neighboring Node Interaction .....	11
2.1.8 Extensibility .....	11
2.2 IPV6 HEADER .....	11
2.2.1 IPv6 Packets over LAN Media.....	12
2.2.2 IPv4 Header.....	13
2.2.3 IPv6 Header .....	16
2.2.4 COMPARING SUMMARY the IPv4 and IPv6 Headers .....	18
2.3 IPV6 EXTENSION HEADERS.....	19
2.4 IPV6 ADDRESSING .....	21
2.4.1 IPv6 Address Notation and Syntax.....	21
2.4.2 IPv6 Prefixes .....	22
2.4.3 Types of IPv6 Addresses .....	22
2.4.3.1 Unicast IPv6 Addresses .....	23
2.4.3.2 Multicast IPv6 Addresses .....	28
2.4.3.3 Anycast IPv6 Addresses .....	32
2.4.4 IPv6 Addresses for a Host.....	33



2.4.5	IPv6 Addresses for a Router .....	34
2.4.6	IPv6 Interface Identifiers .....	35
2.4.7	Addresses and Addressing Concept IPv4 Vs IPv6 .....	36
2.5	IPV6 AND DNS .....	36
2.5.1	The Host Address (AAAA) Resource Record .....	37
2.5.2	The IP6.ARPA Domain .....	37
2.6	ICMPV6 .....	38
2.6.1	Types of ICMPv6 Messages .....	39
2.6.2	ICMPv6 Header .....	40
2.6.3	Comparing ICMPv4 and ICMPv6 Error Messages .....	41
2.7	NEIGHBOR DISCOVERY .....	42
2.8	ROUTER DISCOVERY .....	43
2.9	ADDRESS AUTOCONFIGURATION .....	45
2.9.1	Autoconfigured Address States .....	46
2.9.2	Types of Autoconfiguration .....	47
2.10	DIFFERENCES SUMMARY BETWEEN IPV4 AND IPV6 .....	49
<b>3</b>	<b>CHAPTER 3: IPV6 AND IPV4 THREATS COMPARISON .....</b>	<b>51</b>
3.1	1 INTRODUCTION .....	51
3.2	THREATS ANALYSIS .....	51
3.3	ATTACKS CHANGED IN IPV6 NETWORK .....	51
3.3.1	Network Information Gathering – Reconnaissance .....	52
3.3.1.1	Reconnaissance in IPv4 .....	52
3.3.1.2	Reconnaissance in IPv6 .....	53
3.3.1.3	Tools and Technology Capabilities .....	55
3.3.1.4	Mitigation techniques for Reconnaissance .....	55
3.3.2	Unauthorized Access .....	56
3.3.2.1	Unauthorized Access in IPv4 .....	57
3.3.2.2	Unauthorized Access in IPv6 .....	57
3.3.2.3	Mitigation techniques for unauthorized access .....	64
3.3.3	Header Manipulation and Fragmentation .....	64
3.3.3.1	Fragmentation in IPv4 .....	65
3.3.3.2	Fragmentation in IPv6 .....	66
3.3.3.3	Tools and Technology Capabilities .....	68
3.3.3.4	Mitigation techniques for Header Manipulation and Fragmentation .....	68
3.3.4	Layer 3-Layer 4 Spoofing .....	69
3.3.4.1	Layer 3-Layer 4 Spoofing in IPv4 .....	69
3.3.4.2	Layer 3-Layer 4 spoofing in IPv6 .....	70
3.3.4.3	Tools and Technology Capabilities .....	71
3.3.4.4	Mitigation techniques Layer 3-Layer 4 Spoofing .....	71
3.3.5	Subverting Host Initialization and Address-Resolution Attacks .....	73
3.3.5.1	Subverting Host Initialization and Address-Resolution Attacks in IPv4 .....	73



3.3.5.2	Subverting Host Initialization and Address-Resolution Attacks in IPv6 .....	75
3.3.5.3	Tools and Technology Capabilities.....	76
3.3.5.4	Mitigation techniques for Subverting Host Initialization and Address-Resolution Attacks Attacks.....	77
<b>3.3.6</b>	<b>Broadcast Amplification Attacks (smurf) .....</b>	<b>78</b>
3.3.6.1	Smurf attack in IPv4 .....	78
3.3.6.2	Smurf attack in IPv6 .....	78
3.3.6.3	Tools and Technology Capabilities.....	79
3.3.6.4	Mitigation techniques for Broadcast Amplification Attacks (smurf).....	80
<b>3.3.7</b>	<b>Routing Attacks .....</b>	<b>81</b>
3.3.7.1	Routing Attacks in IPv4 .....	81
3.3.7.2	Routing Attacks in IPv6 .....	82
3.3.7.3	Tools and Technology Capabilities.....	83
3.3.7.4	Mitigation techniques for Routing Attacks .....	83
<b>3.3.8</b>	<b>Viruses and Worms .....</b>	<b>83</b>
3.3.8.1	Viruses and Worms in IPv4 .....	84
3.3.8.2	Viruses and Worms in IPv6 .....	85
3.3.8.3	Tools and Technology Capabilities.....	87
3.3.8.4	Mitigation techniques for Viruses and Worms .....	88
<b>3.3.9</b>	<b>Translation, Transition, and Tunneling Mechanisms.....</b>	<b>88</b>
3.3.9.1	Dual stack security issues .....	89
3.3.9.2	Tunneling Issues .....	90
3.3.9.3	Translation security Issues.....	92
3.3.9.4	Mitigation techniques.....	92
<b>3.4</b>	<b>SIMILAR ATTACKS FOR IPV4 AND IPV6 .....</b>	<b>93</b>
3.4.1	<i>Capturing Data in Transit (Sniffing) .....</i>	<i>94</i>
3.4.2	<i>Application Layer Attacks .....</i>	<i>94</i>
3.4.3	<i>Rogue Devices .....</i>	<i>95</i>
3.4.4	<i>Man-in-the-Middle Attacks.....</i>	<i>95</i>
3.4.5	<i>Flooding, Denial of Service Attacks and Botnets.....</i>	<i>96</i>
<b>3.5</b>	<b>MITIGATION TECHNIQUES SUMMARY.....</b>	<b>97</b>
<b>4</b>	<b>CHAPTER4: TRANSITION TO IPV6.....</b>	<b>101</b>
4.1	IPV6 TRANSITION MECHANISM .....	101
4.1.1	<i>Dual Stack .....</i>	<i>101</i>
4.1.2	<i>NAT-PT .....</i>	<i>102</i>
4.1.3	<i>Tunneling.....</i>	<i>103</i>
4.1.3.1	Basic Tunneling Strategies .....	103
4.1.3.2	Configured Tunneling .....	104
4.1.3.3	Automatic Tunneling .....	105
4.1.3.4	Tunneling Implementations.....	106
4.2	TRANSITION TO IPV6 .....	109
4.2.1	<i>Identify the network infrastructure.....</i>	<i>110</i>
4.2.2	<i>Inventory network equipment and operating systems:.....</i>	<i>111</i>
4.2.3	<i>Identify Software and applications and how they need to be changed: .....</i>	<i>111</i>



4.2.4	Developing an address plan.....	112
4.2.5	Set up an IPv6 Test environment.....	112
4.2.6	Devise and implementing a security policy.....	112
4.2.7	Establish an IPv6 education and awareness plan for IT staff & users.....	113
4.2.8	Case study Mansoura University Network.....	113
4.2.9	Mansoura University Network Infrastructure.....	114
4.2.9.1	Network Main Features.....	114
4.2.9.2	Services Provided.....	118
4.2.9.3	Host and device platforms.....	121
4.2.9.4	User tools/systems.....	123
4.2.9.5	IP Address plan and Assignment management.....	124
4.2.10	Setting up pilot test environment.....	126
4.2.10.1	Test bed discussed issues.....	127
4.2.10.2	Address assignment methods test.....	128
4.2.10.3	Security threats test.....	137
4.2.11	IPv6 Transition Road Map.....	157
4.2.12	Transition Gap Analysis and Outcomes results.....	158
4.2.13	IPv6 Security Considerations.....	159
<b>5</b>	<b>CHAPTER 5: CONCLUSIONS AND FUTURE WORK.....</b>	<b>160</b>
5.1	CONCLUSIONS.....	160
5.2	RECOMMENDED FUTURE WORK.....	162
5.2.1	Voice Over IPV6.....	162
5.2.2	IPv6 and mobility.....	163
<b>6</b>	<b>PUBLICATION.....</b>	<b>164</b>
<b>7</b>	<b>REFERENCES.....</b>	<b>165</b>



## List of Figures

FIGURE 2.1 THE STRUCTURE OF AN IPV6 PACKET .....	12
FIGURE 2.2 IPV6 PACKETS AT THE LINK LAYER .....	12
FIGURE 2.3 THE IPV4 HEADER .....	13
FIGURE 2.4 IPV6 HEADER .....	16
FIGURE 2.5 IPV6 EXTENSION HEADERS .....	20
FIGURE 2.6 THE GLOBAL UNICAST ADDRESS AS DEFINED IN RFC 3587 .....	24
FIGURE 2.7 THE LINK-LOCAL ADDRESS STRUCTURE .....	26
FIGURE 2.8 THE SITE-LOCAL ADDRESS STRUCTURE.....	26
FIGURE 2.9 THE IPV6 MULTICAST ADDRESS STRUCTURE .....	29
FIGURE 2.10 THE MODIFIED IPV6 MULTICAST ADDRESS USING A 32-BIT GROUP ID .....	31
FIGURE 2.11 THE SOLICITED-NODE MULTICAST ADDRESS .....	32
FIGURE 2.12 THE ICMPV6 MESSAGE STRUCTURE.....	40
FIGURE 2.13 THE STATES AND LIFETIMES FOR AN AUTOCONFIGURED ADDRESS.....	47
FIGURE 3.1 EXTENSION HEADER ROUTING ATTACKS.....	59
FIGURE 3.2 ICMP FILTER IN IPV6 .....	61
FIGURE 4.1 TEST BID NETWORK LAY OUT .....	128
FIGURE 4.2 WINDOWS XP IPCONFIG OUTPUT FOR STATELESS AUTOCONFIGURATION .....	129
FIGURE 4.3 WINDOWS 2003 IPCONFIG OUTPUT FOR STATELESS AUTOCONFIGURATION .....	129
FIGURE 4.4 WINDOWS 2008 IPCONFIG OUTPUT FOR STATELESS AUTOCONFIGURATION .....	130
FIGURE 4.5 WINDOWS VISTA IPCONFIG OUTPUT FOR STATELESS AUTOCONFIGURATION.....	131
FIGURE 4.6 WINDOWS 7 BETA IPCONFIG OUTPUT FOR STATELESS AUTOCONFIGURATION.....	131
FIGURE 4.7 LINUX IFCONFIG OUTPUT FOR STATELESS AUTOCONFIGURATION.....	131
FIGURE 4.8 RESERVE IPV6 FOR SPECIFIC PC .....	133
FIGURE 4.9 MS DHCPV6 DYNAMIC DNS UPDATE .....	133
FIGURE 4.10 DHCPV6 SERVER ASSIGNEE IPV6 .....	134
FIGURE 4.11 USING TOOLS ALIVE6 .....	139
FIGURE 4.12 WIRE SHARK SNIFFING THE ALIVE6 ATTACK.....	139
FIGURE 4.13 WIRE SHARK STIFFENING OF SMURF6 ECHO REQUEST.....	141
FIGURE 4.14 WIRE SHARK STIFFENING OF SMURF6 ECHO REPLY .....	141
FIGURE 4.15 CASH ENTRIES BEFORE ND ATTACK.....	142
FIGURE 4.16 CASH ENTRIES AFTER ND ATTACK.....	143
FIGURE 4.17 WIRE SHARK SNIFFING ND ATTACK.....	143
FIGURE 4.18 DEFAULT ROUTER BEFORE RA ATTACK.....	144
FIGURE 4.19 DEFAULT ROUTER AFTER RA ATTACK.....	145
FIGURE 4.20 WIRE SHARK SNIFFING OF FAKED RA .....	146



*List of Figures*

---

FIGURE 4.21 WIRE SHARK SNIFFING ATTACK AGAINST DAD .....	148
FIGURE 4.22 WINDOWS VISTA AFTER DAD ATTACK.....	148
FIGURE 4.23 SQUID LOG FILE ANALYZED BY THIRD PART PROGRAMS .....	151
FIGURE 4.24 SQUID LOGS DIRECTED TO SYSLOG SERVER .....	152
FIGURE 4.25 PROXY SETTING IN INTERNET EXPLORER .....	153
FIGURE 4.26 IPREF RESULT FOR IPV6.....	155
FIGURE 4.27 IPREF RESULTS FOR IPV4 .....	156



## List of Tables

TABLE 2-1 IPV6 VERSES IPV4 ADDRESS SIZE .....	9
TABLE 2-2 VALUES OF THE NEXT HEADER FIELD .....	17
TABLE 2-3 IPV4 HEADER FIELDS AND CORRESPONDING IPV6 EQUIVALENTS .....	18
TABLE 2-4 IPV4 ADDRESSING CONCEPTS AND THEIR IPV6 EQUIVALENTS.....	36
TABLE 2-5 IPV6 Vs IPV4 DNS RECOREDS .....	38
TABLE 2-6 ICMPV4 ERROR MESSAGES AND THEIR CORRESPONDING ICMPV6 EQUIVALENTS .....	41
TABLE 2-7 DIFFERENCES SUMMARY BETWEEN IPV4 AND IPV6 .....	49
TABLE 3-1 COMMON MULTICAST ADDRESS .....	55
TABLE 3-2 EXTENSION HEADER ROUTING ATTACKS .....	59
TABLE 3-3 BOGON FILTER .....	60
TABLE 3-4 ICMP DEPENDENCY IN IPV6 & IPV4.....	61
TABLE 3-5 FILTERING ICMP IN IPV4.....	62
TABLE 3-6 FILTERING ICMP IN IPV6.....	62
TABLE 3-7 IPV6 AGGREGATION ADDRESS .....	70
TABLE 3-8 SUMMARY OF MITIGATION TECHNIQUES .....	98
TABLE 4-1MANSOURA UNIVERSITY SWITCHES SUPPORTING IPV6 .....	116
TABLE 4-2MANSOURA UNIVERSITY CLIENT OPERATING SYSTEM DISTRIBUTION RATIO .....	122



### **List of Abbreviations**

<b>ACL:</b>	Access Control List
<b>AH:</b>	Authentication Header
<b>APIPA:</b>	Automatic Private IP Addressing
<b>ARP:</b>	Address Resolution Protocol
<b>BGB:</b>	Border Gateway Protocol
<b>CIDR:</b>	Classless Inter-Domain Routing
<b>CITC:</b>	Communications and Information Technology Center
<b>DAD:</b>	Duplicate Address Detection
<b>DDoS:</b>	Distributed denial of service
<b>DHCP:</b>	Dynamic Host Configuration Protocol
<b>DNS:</b>	Domain Name System
<b>DoS:</b>	Denial-of-Service
<b>EH:</b>	Extension Headers
<b>EUN</b>	Egyptian University Network
<b>EIGRP:</b>	Enhanced Interior Gateway Routing Protocol
<b>ESP:</b>	Encapsulating Security Payload
<b>EUI:</b>	Extended Universal Identifier
<b>IANA:</b>	Internet Assigned Numbers Authority
<b>ICMPv6:</b>	Internet Control Message Protocol for IPv6
<b>IDS:</b>	Intrusion Detection System
<b>IETF:</b>	Internet Engineering Task Force

Enterprise Network Technology and Internet Security	:العنوان
Saleh, Tamer Mohamed Al Emam Ali	: المؤلف الرئيسي:
Abd Algawad, Ehab. Abd Alrazak, Muneer Mohamed, Abo Alsoud, Mohy Aldin Ahmed(Super.)	: مؤلفين آخرين:
2009	: التاريخ الميلادي:
المنصورة	: موقع:
1 - 167	: الصفحات:
537758	: رقم MD:
رسائل جامعية	: نوع المحتوى:
English	: اللغة:
رسالة ماجستير	: الدرجة العلمية:
جامعة المنصورة	: الجامعة:
كلية الهندسة	: الكلية:
مصر	: الدولة:
Dissertations	: قواعد المعلومات:
الإنترنت، أمن المعلومات، شبكات المعلومات، تأمين الشبكات	: مواضيع:
<a href="https://search.mandumah.com/Record/537758">https://search.mandumah.com/Record/537758</a>	: رابط:



جامعة المنصورة – كلية الهندسة  
قسم هندسة الإلكترونيات و الإتصالات

# شبكات الحاسب و تأمين شبكة المعلومات الدولية الانترنت

رسالة مقدمة من

**المهندس / تامر محمد الامام على صالح**

بكالوريوس هندسة الإلكترونيات و الإتصالات كلية الهندسة – جامعة المنصورة

توطئة للحصول على

درجة الماجستير

فى

هندسة الإتصالات الكهربائية

**لجنة الإشراف**

د.ايهاب عبد الجواد  
مدرس بقسم هندسة الإلكترونيات  
و الإتصالات – كلية الهندسة  
جامعة حلوان

أ.م.د/ منير محمد عبد الرزاق  
أستاذ مساعد بقسم هندسة هندسة  
الإلكترونيات و الإتصالات  
كلية الهندسة – جامعة المنصورة

أ.د / محى الدين احمد ابو السعود  
أستاذ بقسم هندسة الإلكترونيات  
و الإتصالات – كلية الهندسة  
جامعة المنصورة

2009



جامعة المنصورة – كلية الهندسة  
قسم هندسة الإلكترونيات و الإتصالات

# شبكات الحاسب و تأمين شبكة المعلومات الدولية الانترنت

رسالة مقدمة من

**المهندس / تامر محمد الامام على صالح**

بكالوريوس هندسة الإلكترونيات و الإتصالات كلية الهندسة – جامعة المنصورة

توطئة للحصول على

درجة الماجستير

في

هندسة الإتصالات الكهربائية

**لجنة الإشراف**

د.ايهاب عبد الجواد  
مدرس بقسم هندسة الإلكترونيات  
و الإتصالات – كلية الهندسة  
جامعة حلوان

أ.م.د/ منير محمد عبد الرزاق  
أستاذ مساعد بقسم هندسة هندسة  
الإلكترونيات و الإتصالات  
كلية الهندسة – جامعة المنصورة

أ.د / محي الدين احمد ابو السعود  
أستاذ بقسم هندسة الإلكترونيات  
و الإتصالات – كلية الهندسة  
جامعة المنصورة

2009



Mansoura University  
Faculty of Engineering  
Electronics and Communications  
Engineering Department

# Enterprise Network Technology and Internet Security

A Thesis Submitted in Partial Fulfillment of the requirements for the  
Master of Science Degree

*In*

Electrical Communications Engineering

*By*

**Eng. Tamer Mohamed Elemam Ali Saleh**

B. S. Electronics and Communications Engineering  
Mansoura University – Faculty of Engineering

## *Supervisors*

**Prof. Mohy Eldin ahmed  
abo-Elsoud**

Electronics and  
Communications  
Engineering Dept  
Faculty of Engineering  
Mansoura University

**Assoc. Prof. Muneer  
Mohamed Abdel Razak**

Electronics and  
Communications  
Engineering Dept  
Faculty of Engineering  
Mansoura University

**Dr. Ehab Abdel Gawad**

Electronics and  
Communications  
Engineering Dept  
Faculty of Engineering  
Helwan University

2009