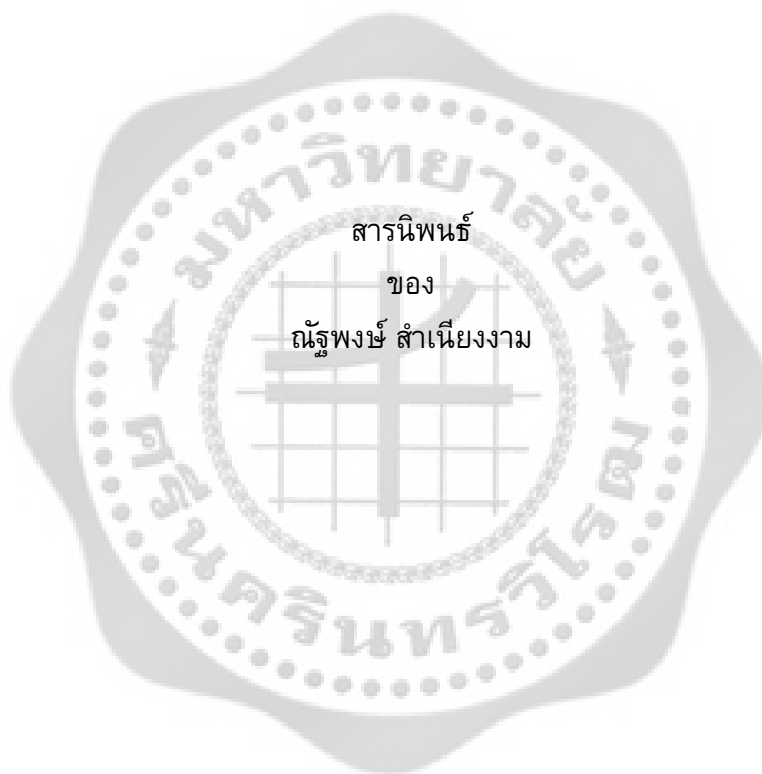
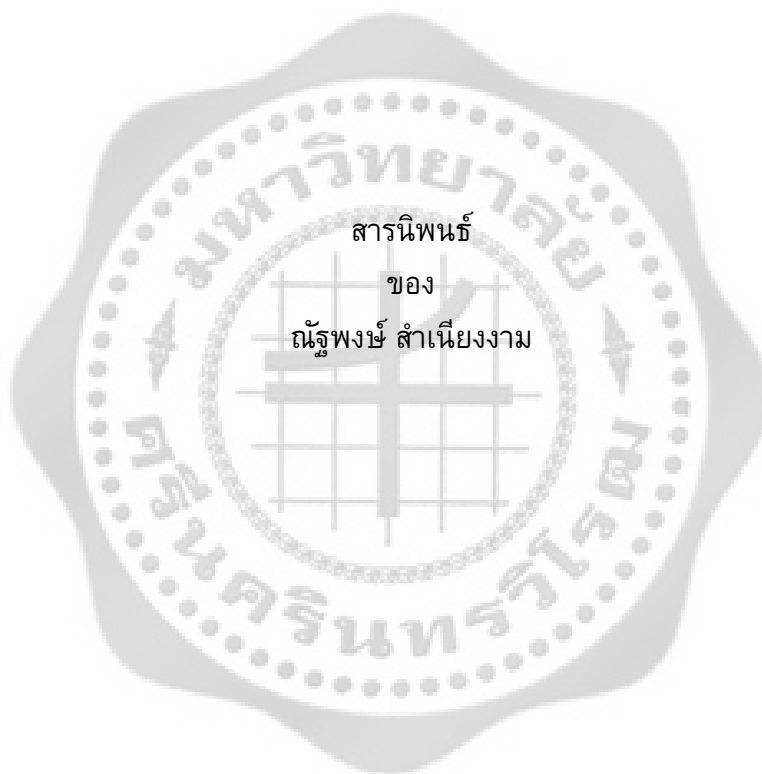


แบบจำลองสถานการณ์สำหรับการประเมินประสิทธิภาพของความปลอดภัยในเครือข่ายไร้สาย
มาตรฐาน IEEE802.11g



เสนอต่อบัณฑิตวิทยาลัย มหาวิทยาลัยศรีนครินทรวิโรฒ เพื่อเป็นส่วนหนึ่งของการศึกษา
ตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต สาขาวิชาการจัดการทางวิศวกรรม
พฤษภาคม 2554

พฤษภาคม 2554แบบจำลองสถานการณ์สำหรับการประเมินประสิทธิภาพของความปลอดภัยใน
เครือข่ายไร้สาย มาตรฐาน IEEE802.11g



เสนอต่อบัณฑิตวิทยาลัย มหาวิทยาลัยศรีนครินทรวิโรฒ เพื่อเป็นส่วนหนึ่งของการศึกษา
ตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต สาขาวิชาการจัดการทางวิศวกรรม

พฤษภาคม 2554

ลิขสิทธิ์เป็นของมหาวิทยาลัยศรีนครินทรวิโรฒ

แบบจำลองสถานการณ์สำหรับการประเมินประสิทธิภาพของความปลอดภัยในเครือข่ายไร้สาย
มาตรฐาน IEEE802.11g



เสนอต่อบัณฑิตวิทยาลัย มหาวิทยาลัยศรีนครินทรวิโรฒ เพื่อเป็นส่วนหนึ่งของการศึกษา
ตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต สาขาวิชาการจัดการทางวิศวกรรม
มีนาคม 2553

ณัฐพงษ์ สำเนียงงาม. (2554). แบบจำลองสถานการณ์สำหรับการประเมินประสิทธิภาพของความปลอดภัยในเครือข่ายไร้สาย มาตรฐาน IEEE802.11g. สารนิพนธ์ วิศวกรรมศาสตรบัณฑิต (วศ.บ.). กรุงเทพมหานคร: บัณฑิตวิทยาลัย มหาวิทยาลัย

(การจัดการทางวิศวกรรม). กรุงเทพฯ: บัณฑิตวิทยาลัย มหาวิทยาลัย

ศรีนครินทร์วิโรฒ. คณะกรรมการควบคุม: ผู้ช่วยศาสตราจารย์ ดร. นำคุณ ศรีสนิท.

งานวิจัยครั้งนี้มีวัตถุประสงค์เพื่อทดสอบแบบจำลองของรูปแบบระบบรักษาความปลอดภัยในเครือข่าย WLAN (Wireless LAN) บนมาตรฐาน IEEE 802.11g โดยระบบที่สร้างขึ้นนั้นสามารถทราบถึงประสิทธิภาพ (throughput) ของชั้นความปลอดภัยในแต่ละแบบจะลอง และยังสามารถใช้เป็นแนวทางเพื่อสนับสนุนการตัดสินใจ ในการนำระบบไปประยุกต์ใช้งาน

แบบจำลองสถานการณ์สำหรับการประเมินประสิทธิภาพของความปลอดภัยในเครือข่ายไร้สาย มาตรฐาน IEEE802.11g ผู้วิจัยได้ทำการทดสอบระบบ ตามสถานการณ์ให้ครอบคลุมการใช้งานได้ 5 แบบการทดสอบ โดยทั้ง 5 กรณีได้ทำการทดสอบกับชั้นความปลอดภัย 7 ชั้นความปลอดภัยด้วยโปรโตคอล TCP และ UDP

เครื่องมือที่ใช้ในการวิจัยคือ โปรแกรม IP Traffic generator, โปรแกรม Wireshark

ผลการวิจัยพบว่า

1. ในขณะรับ-ส่งข้อมูลของโปรโตคอล TCP และ UDP ในทุกรูปแบบทดสอบ พบว่าความเร็วและเวลาในการรับ-ส่งข้อมูล มีประสิทธิภาพต่ำกว่ามาตรฐาน IEEE 802.11g ทุกรูปแบบทดสอบ

2. ความเร็วและเวลาในการรับ-ส่งข้อมูล ของโปรโตคอล UDP มีประสิทธิภาพสูงสุดในรูปแบบทดสอบที่ 3

3. ไม่พบ Data lose บนโปรโตคอล TCP ในขณะรับ-ส่งข้อมูลในทุกรูปแบบการทดสอบทดสอบ

4. Data lose บนโปรโตคอล UDP ในรูปแบบทดสอบที่ 4 มีค่าสูงกว่ารูปแบบทดสอบอื่นๆ โดยค่าที่สูงสุดอยู่ที่ 87%

5. ประสิทธิภาพโดยรวมบนโปรโตคอล TCP ทั้ง 5 รูปแบบการทดสอบ ในแต่ละชั้นความปลอดภัยเป็นไปในทิศทางเดียวกัน คือ รูปแบบการทดสอบที่ 3 มีประสิทธิภาพสูงสุดถึง 23-28Mbps รองลงมาคือ รูปแบบการทดสอบที่ 1, 5, 2 และ 4 ตามลำดับ และชั้นความปลอดภัยที่ 1 มีประสิทธิภาพสูงสุด รองลงมาคือ ชั้นความปลอดภัยที่ 2, 3, 4, 5, 7 และ 6 ตามลำดับ

6. ประสิทธิภาพบนโดยรวมโปรโตคอล UDP ทั้ง 5 รูปแบบการทดสอบ ในแต่ละชั้นความปลอดภัยมีรูปแบบของประสิทธิภาพคล้ายคลึงกัน กล่าวคือ รูปแบบการทดสอบที่ 3 มีประสิทธิภาพสูงสุด ยกเว้นชั้นความปลอดภัยที่ 6 ซึ่ง รูปแบบการทดสอบที่ 4 มีประสิทธิภาพสูงสุด พบว่ารูปแบบการทดสอบที่ 3-5 มีประสิทธิภาพสูงถึง 50-60 Mbps ซึ่งมากกว่าโปรโตคอล TCP ประมาณ 50-85% และ ชั้นความปลอดภัยที่ 1 มีประสิทธิภาพสูงสุด และชั้นความปลอดภัยที่ 6 มีประสิทธิภาพต่ำสุด

THE MODEL FOR EVALUATING THE PERFORMANCE OF SECURITY IN IEEE 802.11G
WIRELESS NETWORK STANDARD



AN ABSTRACT
BY
NATTHAPONG SAMNEANGNGAM

Present in Partial Fulfillment of the Requirements for the
Master of Education Degree in Engineering Management

At Srinakharinwirot University

May 2011

Natthapong Samneangngam.(2011). *The Model for evaluating the performance of security in IEEE 802.11g wireless network standard*. Master Project, M.Eng. (Engineering Management). Bangkok: Graduate School, SrinakSrinakharinwirot University. Advisor Committee: Asst. Prof. Namkhon Srisanit,

Propose of this research project was to create models that have different Infrastructure systems for find performance value of security layers on network system. The direction of this research can use to implement WLAN (Wireless LAN) security network system on IEEE802.11g standard. This system can be providing the results of effectiveness processing (throughput) of the security layers are different and can be used as a approach for decision support on deploy this system.

The Model for evaluating the performance of security in IEEE 802.11g wireless network standard. Researchers have been designed and tested systems to cover situations on five cases that were tested with seven security layers on network system with TCP protocol and UTP protocol.

Tools on this research are IP Traffic generator program and Wireshark program. Statistic analysis used were mean, standard deviation and One-way ANOVA

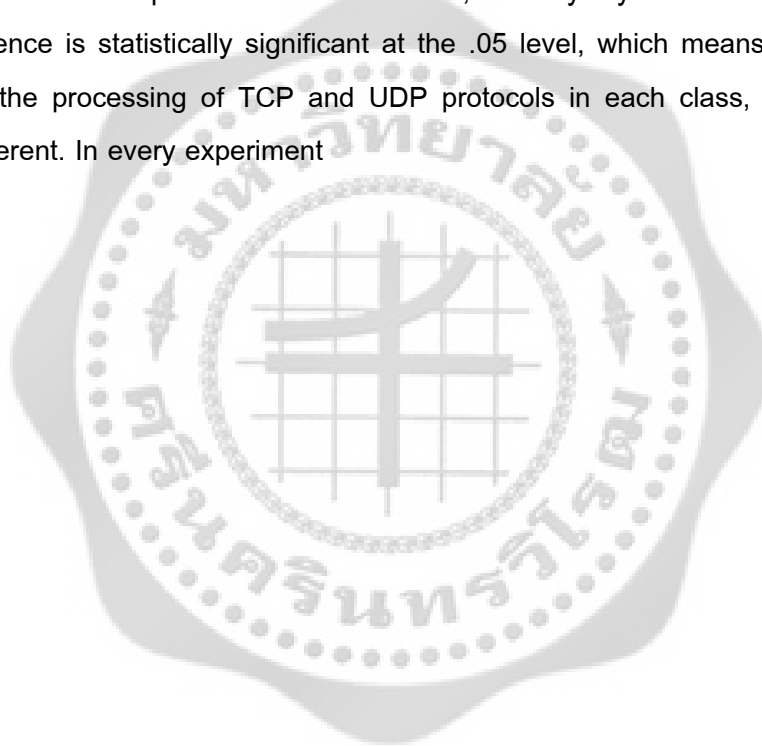
The research revealed that:

1. UDP protocol is more efficient in processing than the protocol TCP.
2. Efficient of TCP protocol on 5 cases in each layer of seven security layers on network system are in the same direction. Case of three effective up to 23-28 Mbps, followed by case of one, case of five, case of two and case of four respectively. Security layers of one is the most effective followed by Security layers of one, Security layers of two, Security layers of three, Security layers of four, Security layers of five, Security layers of seven and Security layers of six respectively.
3. UDP protocol on five cases on each security layers have a similar pattern of performance, which is case of three is the most effective , follow by case of four, case of five , case of one and case of two respectively. Except security layers of six which is case of four that 's the most effective follow by case of three, case of five , case of one and case of two respectively and case of five , case of four and case of five have high effective as 50-60 Mbps more than TCP protocol about 50-85 % and security layers of one is the most effective and security layers of six is the lowest effective.

4. Standard deviation of each security layers on TCP protocol and UDP protocol.

The result of research is TCP protocol has standard deviation of each security layers on each cases have the same direction and less than UDP protocol so TCP protocol has been send and receive data more reliable than UDP protocol and UDP protocol on case of four has the most average standard deviation of each security layers

5. The five value that result from calculated efficiency of processing of TCP protocol and UDP protocol on each security layers of five cases compared with critical values that refer to the table critical value of F. The result is $F_{.05, 4, 45} = 2.58$ so $F_{\text{calculate}} > F_{\text{critical}}$. Therefore reject H_0 and accept H_1 every test result, productivity in the processing of TCP protocol and UDP protocols in each cases, security layers of the 5 cases in each cases. Difference is statistically significant at the .05 level, which means that the average efficiency in the processing of TCP and UDP protocols in each class, secure at least a couple of different. In every experiment



อาจารย์ที่ปรึกษาสารนิพนธ์ ประธานคณะกรรมการบริหารหลักสูตร และคณะกรรมการสอบ
ได้พิจารณาสารนิพนธ์เรื่อง แบบจำลองสถานการณ์สำหรับการประเมินประสิทธิภาพของความ
ปลอดภัยในเครือข่ายไร้สาย มาตรฐาน IEEE802.11g ของ ณัฐพงษ์ สำเนียงงาม ฉบับนี้แล้ว
เห็นสมควรรับเป็นส่วนหนึ่งของการศึกษาตามหลักสูตร ปริญญาวิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชาการจัดการทางวิศวกรรม ของมหาวิทยาลัยศรีนครินทรวิโรฒได้

อาจารย์ที่ปรึกษาสารนิพนธ์

.....
(ผู้ช่วยศาสตราจารย์ ดร.นำคุณ ศรีสนิท)

ประธานคณะกรรมการบริหารหลักสูตร

.....
(ผู้ช่วยศาสตราจารย์ ดร. ปฐมทัศน์ จิระเดชะ)

คณะกรรมการสอบ

..... ประธาน
(รองศาสตราจารย์ธนรัตน์ แต้ววัฒนา)

..... กรรมการสอบสารนิพนธ์
(ผู้ช่วยศาสตราจารย์ ดร. ธนาดล คงสมบูรณ์)

..... กรรมการสอบสารนิพนธ์
(ผู้ช่วยศาสตราจารย์ ดร.นำคุณ ศรีสนิท)

อนุมัติให้รับสารนิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรม
ศาสตรมหาบัณฑิต สาขาวิชาการจัดการทางวิศวกรรม ของมหาวิทยาลัยศรีนครินทรวิโรฒ

..... คณบดีคณะวิศวกรรมศาสตร์
(รองศาสตราจารย์ ดร.เวทิน ปิยรัตน์)

วันที่ เดือน พฤษภาคม พ.ศ. 2554

ประกาศคุณูปการ

สารนิพนธ์ฉบับนี้สำเร็จลุล่วงได้ด้วยความสะดวกช่วยเหลือ และความเอาใจใส่เป็นอย่างดี ตลอดจนการให้คำแนะนำ และข้อคิดเห็นที่เป็นประโยชน์อย่างยิ่งสำหรับการปรับแก้ไขข้อบกพร่องจากคณะกรรมการผู้ควบคุมปริญญานิพนธ์ ผู้วิจัยขอกราบขอบพระคุณ ผู้ช่วยศาสตราจารย์ ดร.นำคุณ ศรีสนิท กรรมการควบคุมปริญญานิพนธ์ ที่ได้ให้ความเมตตากรุณาเป็นที่ปรึกษาและให้ความช่วยเหลือชี้แนะแนวทางในสิ่งที่เป็นประโยชน์ต่อการศึกษาและการทำปริญญานิพนธ์นี้ด้วยความเอาใจใส่ตลอดมา รวมทั้ง รองศาสตราจารย์ ธนรัตน์ แต้วัฒนา และ ผู้ช่วยศาสตราจารย์ ดร.ธนาตล คงสมบูรณ์ กรรมการสอบปริญญานิพนธ์ ที่กรุณาให้ข้อเสนอแนะต่าง ๆ เพิ่มเติมแก่ผู้วิจัย ทำให้ปริญญานิพนธ์ฉบับนี้มีความสมบูรณ์ยิ่งขึ้น ผู้วิจัยขอกราบขอบพระคุณเป็นอย่างสูงไว้ ณ โอกาสนี้

ขอกราบขอบพระคุณคณาจารย์และกรรมการบริหารหลักสูตรสาขาการจัดการทางวิศวกรรม คณะวิศวกรรมศาสตร์ มหาวิทยาลัยศรีนครินทรวิโรฒทุกท่าน ที่ได้กรุณาประสิทธิ์ประสาทความรู้ต่าง ๆ ให้แก่ผู้วิจัย และอบรมสั่งสอนเป็นอย่างดี ตลอดจนให้ความช่วยเหลือในการทำวิจัยครั้งนี้

ขอขอบคุณ สำนักสารสนเทศ บริษัท ไทยเบฟเวอเรจ จำกัด (มหาชน) สำหรับคำแนะนำสถานที่ และอุปกรณ์ ที่ใช้ในการวิจัยนี้และขอขอบคุณผู้เชี่ยวชาญทุกท่าน ซึ่งได้ให้ความอนุเคราะห์ในด้านข้อมูลที่เป็นประโยชน์เพื่อการวิจัย

ขอขอบคุณพี่และเพื่อน ๆ รวมถึงบุคคลอีกหลายท่านที่ไม่ได้กล่าวนามไว้ ณ ที่นี้ที่ได้ให้ความช่วยเหลือและเป็นกำลังใจให้กับผู้วิจัยมาโดยตลอด

สุดท้ายนี้ ผู้วิจัยขอโน้มราลึกถึงคุณของบิดามารดาครูอาจารย์และครอบครัว ที่อบรมสั่งสอนให้ความรู้เป็นกำลังใจและให้การสนับสนุนผู้วิจัยด้วยดีตลอดมา

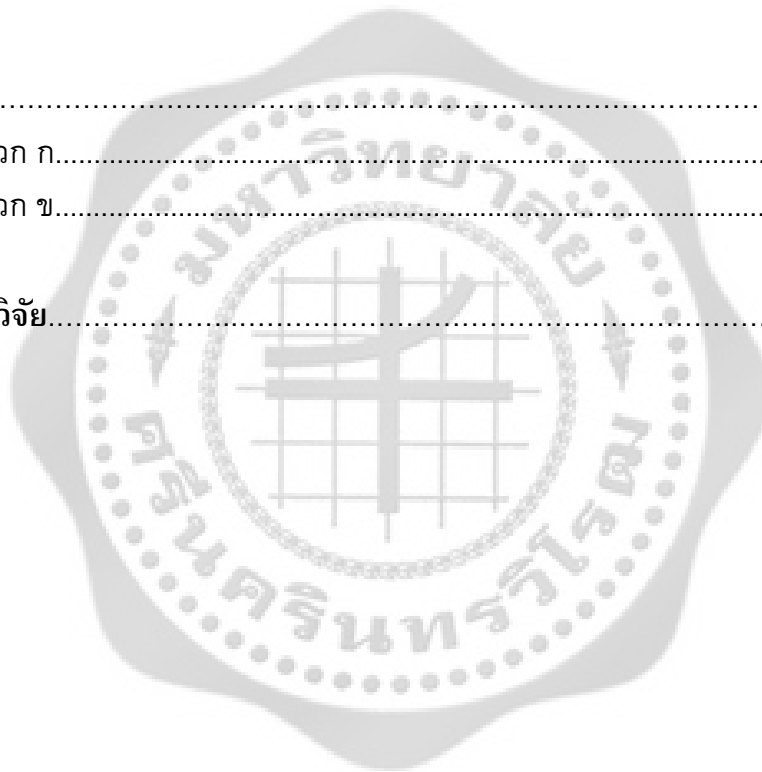
ณัฐพงษ์ สำเนียงงาม

สารบัญ

บทที่	หน้า
1 บทนำ	1
ความเป็นมาและความสำคัญของปัญหา	1
วัตถุประสงค์ของการวิจัย	2
ขอบเขตของการวิจัย	2
วิธีการดำเนินการวิจัยโดยย่อ	2
กรอบแนวคิดในการวิจัย	2
ประโยชน์ที่คาดว่าจะได้รับการวิจัย	3
สมมติฐานในการวิจัย	3
นิยามศัพท์เฉพาะ	3
2 เอกสารและงานวิจัยที่เกี่ยวข้อง	5
มาตรฐานของระบบเครือข่ายไร้สาย IEEE 802.11 ที่นิยมใช้งานในปัจจุบัน	5
การรับ-ส่งข้อมูลของระบบเครือข่ายไร้สายบนมาตรฐาน IEEE 802.11	9
ความปลอดภัยของเครือข่ายไร้สาย IEEE 802.11	12
ประสิทธิภาพบนเครือข่ายไร้สายบนมาตรฐาน IEEE 802.11	19
งานวิจัยที่เกี่ยวข้อง	23
3 วิธีดำเนินการวิจัย	26
ขั้นตอนการดำเนินงานวิจัย	27
การออกแบบและการดำเนินการสร้างแบบจำลองระบบ	27
การทดสอบระบบ	34
การประเมินผลการทดสอบ	36
4 ผลการดำเนินงานวิจัย	37
ผลการทดสอบและประเมินประสิทธิภาพของระบบ	37

สารบัญ (ต่อ)

บทที่	หน้า
5 สรุปผลการวิจัย อภิปรายผล และข้อเสนอแนะ.....	42
สรุปผลการวิจัย.....	42
อภิปรายผลการวิจัย.....	43
ข้อเสนอแนะ.....	44
บรรณานุกรม.....	46
ภาคผนวก.....	48
ภาคผนวก ก.....	49
ภาคผนวก ข.....	71
ประวัติย่อผู้วิจัย.....	88



บัญชีตาราง

ตาราง	หน้า
1 มาตรฐาน IEEE 802.11 WLAN.....	6
2 รูปแบบทดสอบที่ 1: ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยัง เครือข่ายมีสาย (LAN) แบบ หนึ่งต่อหนึ่ง (Single Point) Mbps ของโปรโตคอล TCP และ UDP.....	37
3 รูปแบบทดสอบที่ 2: ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยัง เครือข่ายไร้สาย (WLAN) แบบ หนึ่งจุด (Single Point) ของ TCP และ UDP.....	38
4 รูปแบบทดสอบที่ 3: ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยัง เครือข่ายมีสาย (LAN) แบบ หลายจุด (Multiple Point) ของ TCP และ UDP.....	39
5 รูปแบบทดสอบที่ 4: ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยัง เครือข่ายไร้สาย (WLAN) แบบ หลายจุด (Multiple Point) ของ TCP และ UDP..	40
6 รูปแบบทดสอบที่ 5: เครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่าย มีสาย (LAN) และไร้สาย (WLAN) ของ TCP และ UDP.....	41

บัญชีภาพประกอบ

ภาพประกอบ	หน้า
1 ISM Bands.....	9
2 การส่งข้อมูลแบบ DCF โดยใช้หลักการ MACAW ร่วมกับ Virtual Carrier Sense.	11
3 การเชื่อมWLANโดยใช้ SSID.....	13
4 การควบคุมการใช้งานไวร์เลสด้วย MAC Address Filtering.....	14
5 ข้อมูลที่สื่อสารบนเครือข่ายไวร์เลสโดยผ่านการเข้ารหัส WEP.....	15
6 ผลลัพธ์เอาท์พุตถูก Encrypted Message.....	15
7 ผลลัพธ์เอาท์พุตถูก Decrypted Message.....	16
8 ผ่านกระบวนการเข้ารหัส.....	17
9 แสดง BSS และESS.....	20
10 แสดงการทำงานในโหมด Adhoc หรือ Peer-to-Peer Mode.....	21
11 แสดงHidden Node Problem และ กลไก RTS/CTS Handshake.....	22
12 WLAN to LAN แบบ Single Point.....	29
13 WLAN to WLAN แบบ Single Point.....	29
14 WLAN to LAN แบบ Multiple Point.....	30
15 WLAN to WLAN แบบ Multiple Point.....	30
16 WLAN to LAN and WLAN.....	31
17 IEEE 802.1x model logical flow.....	32
18 ค่าพารามิเตอร์ที่ใช้ทดสอบระบบ.....	34
19 แบบการทดสอบระบบ.....	35

บทที่ 1

บทนำ

ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันเทคโนโลยีเครือข่ายแลนแบบไร้สาย หรือ WLAN (Wireless LAN) ได้รับความนิยมเป็นอย่างมาก โดยเฉพาะ WLAN บนมาตรฐาน IEEE 802.11g เนื่องจากประโยชน์ของ WLAN บนมาตรฐาน IEEE 802.11g มีอยู่มากมาย ทั้งในด้านอำนวยความสะดวกให้แก่ผู้ใช้โดยสามารถนำไปใช้งานในสภาพแวดล้อมหรือสถานที่ที่แตกต่างกันได้ เพิ่มความคล่องตัวในการทำงาน เนื่องจาก ผู้ใช้ไม่จำเป็นต้องต่ออุปกรณ์ต่างๆโดยตรง ทำให้การย้ายอุปกรณ์ไม่ก่อให้เกิดปัญหาในการติดต่อสื่อสาร การติดตั้งทำได้ง่ายและสะดวกเพราะไม่ต้องติดตั้งสายสัญญาณระหว่างอุปกรณ์ของผู้ใช้กับอุปกรณ์เชื่อมต่อต่างๆ ทำให้การขยายเครือข่ายทำได้ง่าย และยังช่วยลดค่าใช้จ่ายได้ในระยะยาว เพราะถ้ามีการเปลี่ยนแปลงเกิดขึ้นก็ไม่ต้องเสียงบประมาณในการติดตั้งระบบใหม่

อย่างไรก็ตามความง่าย, ความสะดวกต่อการติดตั้งและการใช้งาน WLAN (Wireless LAN) ก็นำมาซึ่งการถูกโจมตีมากกว่าระบบเครือข่ายที่ใช้สายสัญญาณ เนื่องจากการติดต่อสื่อสารระหว่างอุปกรณ์ภายในเครือข่ายไร้สายสามารถทำได้ทุกๆบริเวณที่มีสัญญาณครอบคลุม อีกทั้งเทคโนโลยีสำหรับการรักษาความปลอดภัยในอุปกรณ์ WLAN (Wireless LAN) บนมาตรฐาน IEEE 802.11g ที่ใช้อยู่ในปัจจุบันยังมีช่องโหว่ ทำให้ผู้ไม่หวังดีสามารถเข้ามาในระบบเพื่อล้วงข้อมูลหรือทำความเสียหายให้แก่ระบบ ดังนั้นการรักษาความปลอดภัยของ WLAN (Wireless LAN) บนมาตรฐาน IEEE 802.11g จึงต้องทำด้วยความระมัดระวังและให้ความสำคัญที่จะเลือกใช้ระดับความปลอดภัยที่เหมาะสม

นอกจากความปลอดภัยใน WLAN (Wireless LAN) แล้วยังมีเรื่อง ประสิทธิภาพที่คอมพิวเตอร์ประมวลผลได้ (throughput) ก็เป็นสิ่งสำคัญเช่นกัน ทั้งนี้เพื่อที่จะให้การทำงานของผู้ใช้เป็นไปอย่างราบรื่นและรวดเร็ว

งานวิจัยนี้เป็นการทดสอบแบบจำลองในรูปแบบต่างๆ สำหรับการประเมินประสิทธิภาพของความปลอดภัยในเครือข่ายไร้สายบน มาตรฐาน IEEE802.11g ซึ่งแบบจำลองในรูปแบบที่แตกต่างกันนั้นจะทำให้เราสามารถวิเคราะห์ได้ว่าสถานการณ์ใดเหมาะที่จะใช้แบบจำลองและชั้นความปลอดภัยชั้นไหน เพื่อที่จะให้ได้ระบบที่มีประสิทธิภาพและความปลอดภัยที่เหมาะสม โดยในแบบจำลองแต่ละรูปแบบจะบอกถึงผลของประสิทธิภาพในการประมวลผล (throughput) ของระบบรักษาความปลอดภัยบนเครือข่าย WLAN (Wireless LAN) บนมาตรฐาน IEEE 802.11g ในแต่ละชั้นความปลอดภัย

วัตถุประสงค์ของการวิจัย

เพื่อทดสอบแบบจำลองของรูปแบบระบบรักษาความปลอดภัยในเครือข่าย WLAN (Wireless LAN) บนมาตรฐาน IEEE 802.11g

ขอบเขตของการวิจัย

1. หาประสิทธิภาพในการประมวลผล (throughput) ของระบบรักษาความปลอดภัยแต่ละแบบจะลงในเครือข่ายระบบเครือข่าย WLAN (Wireless LAN) บนมาตรฐาน IEEE 802.11g
2. วิเคราะห์ประสิทธิภาพในการประมวลผลของความปลอดภัยในเครือข่าย WLAN (Wireless LAN) บนมาตรฐาน IEEE 802.11g ในแต่ละแบบจำลอง

วิธีการดำเนินการวิจัยโดยย่อ

1. วิเคราะห์ปัญหาที่เกิดขึ้นเพื่อกำหนดขอบเขตการดำเนินงานวิจัย
2. ศึกษาข้อมูลเอกสารและงานวิจัยที่เกี่ยวข้อง
3. ออกแบบและดำเนินการทดสอบแบบจำลองระบบเพื่อให้ครอบคลุมขอบเขตและวัตถุประสงค์ของการวิจัย
4. ส่วนของอุปกรณ์ที่ใช้ในการดำเนินการ
5. ส่วนของโปรแกรมที่ใช้ในการดำเนินการ
6. ส่วนของการตั้งค่าพารามิเตอร์ต่างๆของระบบ
7. ทำการทดสอบระบบ
8. วิเคราะห์และสรุปผลการวิจัย

กรอบแนวคิดในการวิจัย

ในการวิจัยครั้งนี้ ผู้วิจัยได้ทำการสร้างแบบจำลองในลักษณะที่แตกต่างกันเพื่อใช้ทดสอบเครือข่าย WLAN (Wireless LAN) บนมาตรฐาน IEEE 802.11g ในแต่ละชั้นความปลอดภัย ทั้งนี้เพื่อให้บุคคลหรือองค์กรต่างๆได้เลือกใช้ระดับชั้นความปลอดภัยให้เหมาะสมและเกิดประสิทธิภาพมากที่สุด โดยอาศัยกรอบแนวคิดในการวิจัย ดังนี้

1. กระบวนการออกแบบจำลองสถานการณ์ในรูปแบบต่างๆ สำหรับการประเมินประสิทธิภาพในการประมวลผลของความปลอดภัยในเครือข่ายไร้สายบน มาตรฐานIEEE802.11g
2. ทดสอบแบบจำลอง (Test Case)
3. การวิเคราะห์แบบจำลอง

ประโยชน์ที่คาดว่าจะได้รับการวิจัย

1. ทราบถึงประสิทธิภาพในการประมวลผล (throughput) ของระบบรักษาความปลอดภัย แต่ละแบบจะลอง ในระบบเครือข่าย WLAN (Wireless LAN) บนมาตรฐาน IEEE 802.11g
2. สามารถใช้เป็นแนวทางเพื่อสนับสนุนการตัดสินใจ ในการนำระบบไปประยุกต์ใช้ ในระบบเครือข่าย WLAN (Wireless LAN) บนมาตรฐาน IEEE 802.11g

สมมุติฐานการวิจัย

1. ประสิทธิภาพในการประมวลผล (Throughput) แต่ละแบบจำลองของชั้นความปลอดภัย ในเครือข่าย WLAN (Wireless LAN) บนมาตรฐาน IEEE 802.11g มีความแตกต่างกัน

นิยามศัพท์เฉพาะ

1. แลนไร้สาย หรือ WLAN (Wireless LAN) คือระบบที่เชื่อมโยงคอมพิวเตอร์เข้าเข้าด้วยกันเป็นเครือข่ายภายในพื้นที่แบบไร้สาย โดยใช้คลื่นความถี่วิทยุในการเชื่อมต่อหรือสื่อสารกัน การเชื่อมต่อแลนไร้สายมีทั้งแบบเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์ด้วยกัน และเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์ผ่านอุปกรณ์กระจายสัญญาณ (Access Point)
2. throughput คือ ปริมาณงานที่สามารถทำได้ภายในหนึ่งหน่วยเวลาโปรโตคอลที่มีปริมาณงานมากจะมีประสิทธิภาพในการทำงานดี และโปรโตคอลที่มีปริมาณงานต่ำก็จะถือว่ามีประสิทธิภาพในการทำงานที่ไม่ดี (ประสิทธิภาพในการประมวลผล)
3. โปรโตคอล TCP (Transmission Control Protocol) เป็นโปรโตคอลที่มีการรับส่งข้อมูลแบบ stream oriented protocol หมายความว่า การรับส่งข้อมูลจะไม่คำนึงถึงปริมาณข้อมูลที่จะส่งไป แต่จะแบ่งข้อมูลเป็นส่วนย่อย ๆ ก่อน แล้วจึงจะส่งไปยังปลายทางอย่างต่อเนื่องเป็นลำดับข้อมูล ในแบบทดสอบที่ข้อมูลส่วนใดส่วนหนึ่งสูญหายไป ก็จะส่งข้อมูลส่วนนั้นใหม่อีกครั้ง
4. โปรโตคอล UDP (User Datagram Protocol) เป็นโปรโตคอลหลักในชุดโปรโตคอลอินเทอร์เน็ต การส่งข้อมูลผ่าน UDP นั้น คอมพิวเตอร์จะส่งข้อมูลขนาดเล็กที่เรียกว่า เดต้าแกรม (datagram) ผ่านเครือข่ายไปยังเครื่องปลายทาง โดย UDP จะไม่รับประกันความน่าเชื่อถือและลำดับของเดต้าแกรม อย่างที่ TCP รับประกัน ซึ่งหมายความว่าเดต้าแกรมอาจมาถึงไม่เรียงลำดับหรือสูญหายระหว่างทางได้
5. RADIUS (Remote Authentication Dial In User Service) เป็นมาตรฐานในการตรวจสอบความถูกต้องของการล็อกอิน และ RADIUS server คือ เครื่องที่เก็บรายชื่อผู้ใช้งานและรหัสผ่านของผู้ใช้งานในระบบไว้ และคอยทำหน้าที่บอกให้เซิร์ฟเวอร์อื่นทราบว่าผู้ใช้ล็อกอินถูกต้องหรือไม่

6. X.509 Certificate คือ ใบรับรองดิจิทัลจะทำหน้าที่คล้ายกับบัตรประจำตัวประชาชน คือ ยืนยันตัวตนของผู้ที่เป็นเจ้าของ ซึ่งจะบอกข้อมูลทั่วไปของถือใบรับรอง

7. Public Key Infrastructure (PKI) คือระบบป้องกันข้อมูลในการสื่อสารผ่านเครือข่ายอินเทอร์เน็ต โดยจะใช้กุญแจที่เรียกว่า Key pairs คู่ในการเข้ารหัสและถอดรหัสข้อมูล ซึ่งกุญแจคู่นี้จะได้มาพร้อมกับใบรับรอง หรือ Certificate



บทที่ 2

เอกสารและงานวิจัยที่เกี่ยวข้อง

ในการวิจัย เรื่องแบบจำลองสถานการณ์สำหรับการประเมินประสิทธิภาพของความปลอดภัยในเครือข่ายไร้สาย มาตรฐาน IEEE 802.11g ในครั้งนี้ ผู้วิจัยได้ทำการศึกษาและรวบรวมแนวคิด ทฤษฎี เอกสารและงานปริญญานิพนธ์ที่เกี่ยวข้อง โดยนำเสนอตามหัวข้อดังต่อไปนี้

1. มาตรฐานของเครือข่ายไร้สาย IEEE 802.11 ที่นิยมใช้งานในปัจจุบัน
 - 1.1 มาตรฐาน IEEE 802.11a
 - 1.2 มาตรฐาน IEEE 802.11b
 - 1.3 มาตรฐาน IEEE 802.11g
 - 1.4 มาตรฐาน IEEE 802.11n
2. การรับ-ส่งข้อมูลของระบบเครือข่ายไร้สายบนมาตรฐาน IEEE 802.11
 - 2.1 การส่งข้อมูลบนระบบเครือข่ายไร้สาย (Wireless Network Transmission)
 - 2.2 การควบคุมการส่งข้อมูลของเครือข่ายไร้สาย
3. ความปลอดภัยของเครือข่ายไร้สาย IEEE 802.11
 - 3.1 ชั้นความปลอดภัยที่ 1: ไม่มีระบบความปลอดภัย หรือเชื่อมโยงเครือข่ายด้วย SSID
 - 3.2 ชั้นความปลอดภัยที่ 2: กลั่นกรองผู้ใช้ด้วย MAC Address
 - 3.3 ชั้นความปลอดภัยที่ 3 และ 4: Wired Equivalency Privacy (WEP)
 - 3.4 ชั้นความปลอดภัยที่ 5 และ 6: Wi-Fi Protected Access (WPA)
 - 3.5 ชั้นความปลอดภัยที่ 6: PEAP (Protected Extensible Authentication Protocol)
4. ประสิทธิภาพบนเครือข่ายไร้สายบนมาตรฐาน IEEE 802.11
 - 4.1 ลักษณะการเชื่อมต่อของอุปกรณ์
 - 4.2 เข้าใช้ช่องสัญญาณด้วยกลไก CSMA/CA
5. งานวิจัยที่เกี่ยวข้อง

1. มาตรฐานของระบบเครือข่ายไร้สาย IEEE 802.11 ที่นิยมใช้งานในปัจจุบัน

ในปี ค.ศ. 1997 คณะกรรมการของ IEEE ได้ประกาศมาตรฐาน IEEE 802.11 WLAN ในตอนนั้นความเร็วสูงสุดของมาตรฐานอยู่ที่ 2 Mbps ซึ่งค่อนข้างช้าเมื่อเปรียบเทียบกับเครือข่ายแบบใช้สาย เนื่องจากเป็นมาตรฐานแรกเกี่ยวกับเครือข่าย WLAN ดังนั้น จึงมีปัญหาลดสยอย่าง และอาจเป็นผลให้ไม่สามารถรองรับการทำงานร่วมกันได้ของอุปกรณ์ที่ผลิตโดยต่างบริษัทกัน ดังนั้น สถาบัน IEEE จึงได้ตั้งทีมงานขึ้นมา 2 กลุ่ม เพื่อพัฒนามาตรฐาน WLAN โดยกลุ่มแรกคือ TGa (Task Group a) พัฒนามาตรฐาน IEEE 802.11a โดยใช้ความถี่ที่ 5 GHz และสามารถรองรับ

ข้อมูลได้ที่ 6, 9, 12, 18, 24, 36, 48 และ 54 Mbps ส่วนทีม TGb พัฒนามาตรฐาน IEEE 802.11b โดยใช้ความถี่ 2.4 GHz โดยสามารถรองรับอัตราข้อมูล 4 อัตรา คือ 1, 2, 5.5 และ 11 Mbps

ข้อจำกัดของ IEEE 802.11b คือ แบนด์วิธ เนื่องจากมาตรฐานนี้จะรองรับแบนด์วิธได้ 11 Mbps ส่วน IEEE802.11a นั้น สามารถรองรับแบนด์วิธที่สูงกว่า แต่ข้อจำกัดของมาตรฐานนี้คือ ความถี่ เนื่องจากมาตรฐานนี้ใช้ความถี่ที่ 5 GHz ซึ่งบางประเทศนั้นต้องขออนุญาตก่อนจึงจะใช้งานได้ ดังนั้น IEEE จึงตั้งทีมขึ้นอีก 1 กลุ่ม เพื่อพัฒนาอีกมาตรฐานหนึ่งนั่นคือ IEEE 802.11g ซึ่งใช้ความถี่ 2.4 GHz และรองรับแบนด์วิธได้ถึง 54 Mbps

ต่อมาในปี ค.ศ. 2004 IEEE ได้ก่อตั้งคณะทำงานเพื่อพัฒนามาตรฐานใหม่สำหรับพัฒนา มาตรฐาน 802.11 ต่อ โดยตั้งชื่อว่า T Gn (Task Group n) โดยตั้งเป้าเอาไว้ว่ามาตรฐานนี้สามารถรองรับอัตราการส่งข้อมูลได้สูงสุดที่ 50 Mbps หรือ 10 เท่า

เนื่องจาก IEEE เป็นองค์กรที่มีหน้าที่กำหนดและประกาศมาตรฐานเท่านั้นแต่ไม่มีหน้าที่ในการทดสอบอุปกรณ์ที่ผลิตโดยบริษัทต่างๆ ว่าได้มาตรฐานที่กำหนดหรือไม่ ดังนั้น จึงมีกลุ่มที่จัดตั้งขึ้นเพื่อทำหน้าที่นี้เรียกว่า Wi-Fi Alliance ซึ่งเป็นองค์กรที่หน้าที่ตรวจ ทดสอบ และออกใบรับรองอุปกรณ์ที่ผ่านมาตรฐาน IEEE 802.11

ตาราง 1 มาตรฐาน IEEE 802.11 WLAN

มาตรฐาน	ปีที่ประกาศ	ความถี่ที่ใช้	อัตราส่งข้อมูลสูงสุด	ระยะทางโดยประมาณ	Throughput
IEEE802.11a	1999	5GHz	54Mbps	30 m	22Mbps
IEEE802.11b	1999	2.4GHz	11Mbps	50 m	5Mbps
IEEE802.11g	2003	2.4GHz	54Mbps	30 m	20Mbps
IEEE802.11n	2009	2.4GHz/5GHz	108Mbps	50 m	48Mbps

1.1 มาตรฐาน IEEE 802.11a

เป็นมาตรฐานที่ประกาศใช้ในปี 1999 ใช้โปรโตคอล CSMA/CA และใช้ช่วงความถี่ 5GHz โดยใช้เทคโนโลยี OFDM (Orthogonal Frequency-Division Multiplexing) ทำให้สามารถส่งสัญญาณได้ถึง 54 Mbps แต่ด้วยโอเวอร์เฮดต่างๆ ทั้งการต้องรอคอยการตอบรับหลังจากการส่งจากการส่งและการเว้นระยะสำหรับการส่งข้อมูล เพื่อเครื่องอื่นสามารถใช้งานร่วมกันได้ โดยค่าเฉลี่ยของอัตราการรับข้อมูลจริง จึงตกเหลืออยู่ที่ประมาณ 20 Mbps ในกรณีที่มีสัญญาณรบกวนหรือมีสิ่งกีดขวางสัญญาณ WLAN 802.11a ก็จะปรับความเร็วลงเหลือ 48, 36, 24, 18, 12, 9 และ 6 Mbps ตามลำดับโดยอัตโนมัติ มาตรฐาน IEEE 802.11a นี้มีช่องสัญญาณที่เลือกใช้ได้ 12 ช่องสัญญาณ และแต่ละช่องสัญญาณนั้นจะมีความถี่ที่ไม่ทับซ้อนกัน (Non Overlap Channel) โดยมี

8 ช่องสัญญาณที่กำหนดให้ใช้กับการติดตั้งภายในอาคารและอีก 4 ช่องสัญญาณที่เหลือจะใช้กับการเชื่อมต่อแบบจุดต่อจุด ซึ่งส่วนใหญ่จะเป็นการติดตั้งภายนอกอาคาร มาตรฐาน IEEE802.11a จะไม่สามารถทำงานร่วมกับมาตรฐาน IEEE802.11b ได้นอกจากอุปกรณ์นั้นจะรองรับทั้ง 2 มาตรฐาน

เนื่องจากช่วงความถี่ 2.4 GHz มีการใช้งานอย่างแพร่หลายจึงทำให้มีคลื่นรบกวนมากด้วย ในขณะที่ช่วงความถี่ 5 GHz นั้นถูกใช้น้อยกว่าจึงเป็นข้อดีสำหรับมาตรา IEEE 802.11a อย่างไรก็ตามการใช้คลื่นนำสัญญาณที่มีความถี่สูงนั้น ก็มีข้อเสียคือ เมื่อมีสิ่งกีดขวาง เช่น ผนังห้อง ต่ กีดขวางการสื่อสารระหว่างอุปกรณ์ จะทำให้สามารถสื่อสารกันได้ในระยะทางที่ไม่ไกลมากนัก ทำให้จำเป็นต้องใช้แอกเซสพ้อยต์ เพิ่มมากขึ้น

แต่ละประเทศก็จะมีกฎหมายเกี่ยวกับการใช้ช่วงความถี่ที่แตกต่างกัน ที่ใช้งานได้โดยถูกต้องตามกฎหมายก็ได้เฉพาะในประเทศสหรัฐอเมริกาและญี่ปุ่นเท่านั้น ส่วนประเทศอื่นซึ่งรวมถึงประเทศไทยยังไม่ได้รับการอนุญาตให้ใช้ช่วงความถี่นี้

สำหรับ 52 ช่องสัญญาณย่อยที่ใช้ 48 ช่องสัญญาณจะใช้สำหรับดาดำ ในแต่ละช่องสัญญาณจะห่างกัน 0.3125 MHz สัญญาณที่ส่งไปในช่องสัญญาณย่อยนั้น อาจใช้เทคนิคการแปลงสัญญาณแบบ BPSK, QPSK, 16-QAM หรือ 64-QAM โดยช่องความถี่ที่ใช้ทั้งหมดคือ 20 MHz

อุปกรณ์ที่ได้รับรองมาตรฐาน IEEE 802.11a นั้นออกจำหน่ายในปี 2001 หลังจาก IEEE 802.11b วางจำหน่าย เนื่องจากต้องรอการผลิตชิ้นส่วนที่สามารถส่งสัญญาณในช่วงความถี่ 5 GHz ซึ่งยังไม่มีการผลิตที่แพร่หลายเหมือนกับอุปกรณ์ที่ใช้ในช่วงความถี่ 2.4 GHz มาตรฐาน IEEE802.11a นั้น ไม่ได้รับความนิยมนัก เนื่องจากอุปกรณ์ที่ได้รับการรับรองมาตรฐาน IEEE 802.11b นั้นมีราคาถูกกว่า

1.2 มาตรฐาน IEEE 802.11b

มาตรฐาน IEEE 802.11b ได้ประกาศใช้เมื่อปี 1999 โดยกำหนดให้มีแบนด์วิธสูงสุดที่ 11 Mbps และใช้โปรโตคอล CSMA/CA เนื่องจากโปรโตคอลนี้มีโอเวอร์เฮดค่อนข้างมาก ทำให้ค่าเฉลี่ยของอัตราการรับส่งข้อมูลจริงจึงตกเหลืออยู่ที่ประมาณ 5.9 Mbps สำหรับโปรโตคอล TCP และ 7.1 Mbps สำหรับโปรโตคอล UDP

อุปกรณ์ที่ได้รับรองมาตรฐาน IEEE 802.11b นั้น ได้ถูกผลิตออกจำหน่ายสู่ตลาดอย่างรวดเร็ว เนื่องจากใช้เทคนิคโมดูเลชัน แบบ DSSS (Direct-Sequence Spread Spectrum) และ CCK (Complementary Code Keying) ซึ่งเป็นเวอร์ชันหนึ่งของ CDMA ดังนั้นจึงทำให้การผลิตชิปเพื่อใช้งานในอุปกรณ์มาตรฐาน IEEE 802.11b นั้นง่ายและราคาถูก จึงทำให้มาตรฐานนี้ได้รับความนิยมมากกว่ามาตรฐานแรกๆที่ออกมา

มาตรฐาน IEEE 802.11b ปกติจะใช้งานแบบแพร่กระจาย โดยมีแอกเซสพอยต์ที่แพร่กระจายสัญญาณไปโดยรอบเพื่อให้โคเลอนท์ที่อยู่ในระยะครอบคลุมสามารถเชื่อมต่อได้ โดยปกติรัศมีการให้บริการสำหรับภายในอาคารคือ 30 เมตร ที่อัตราข้อมูล 11 Mbps หรือ 90 เมตร ที่อัตราข้อมูล 1 Mbps ถ้าใช้เสาอากาศหรือแอนเทนนาที่การส่งสัญญาณได้ไกลก็สามารถใช้การเชื่อมต่อแบบจุดต่อจุดภายนอกอาคารซึ่งสามารถส่งข้อมูลได้ไกลถึง 8 กิโลเมตร แต่ก็มีบางบริษัทที่สามารถผลิตอุปกรณ์ที่สามารถส่งได้ไกลถึง 80-120 กิโลเมตร แต่แนวสัญญาณนั้นต้องไม่มีสิ่งกีดขวางอย่างไรก็ตามการออกแบบและติดตั้งเสาอากาศนอกอาคารนั้น จำเป็นต้องปฏิบัติตามกฎหมายที่เกี่ยวกับการสื่อสารโทรคมนาคม เช่น ความถี่ที่ใช้และกำลังส่งสัญญาณ ซึ่งแต่ละประเทศก็แตกต่างกันออกไป

มาตรฐาน IEEE 802.11b นั้น สามารถส่งได้ที่ 11 Mbps แต่ก็สามารถลดลงมาที่ 5.5 หรือ 2 หรือ 1 Mbps ซึ่งเป็นการปรับให้เหมาะกับสภาพแวดล้อม ซึ่งอาจมีสัญญาณรบกวนในปริมาณมาก อัตราการรับส่งข้อมูลที่ต่ำกว่าจะมีความน่าเชื่อถือได้มากกว่า มีการปรับปรุงมาตรฐาน IEEE802.11b เพื่อเพิ่มแบนด์วิธเป็น 22, 23 และ 44 Mbps แต่ก็เป็นลิขสิทธิ์เฉพาะของบริษัทผู้ผลิต และไม่ได้รับรองโดย IEEE หลายบริษัทตั้งชื่อให้กับส่วนขยายนี้ว่า IEEE 802.11b+ และส่วนขยายนี้ต่อมาได้พัฒนาเป็นมาตรฐาน IEEE 802.11g ซึ่งมีแบนด์วิธสูงถึง 54 Mbps และยังทำงานร่วมกันได้กับมาตรฐาน IEEE 802.11b

1.3 มาตรฐาน IEEE 802.11g

เมื่อเดือนมิถุนายน 2003 IEEE ได้ประกาศมาตรฐานใหม่คือ IEEE 802.11g โดยใช้ความถี่ 2.4 GHz เหมือนมาตรฐาน IEEE802.11b แต่สามารถส่งข้อมูลได้มากถึง 54 Mbps หรือมีอัตรารับส่งข้อมูลจริงอยู่ที่ประมาณ 24.7 Mbps ใกล้เคียงกับมาตรฐาน IEEE802.11a อุปกรณ์ที่ได้รับรองมาตรฐาน IEEE802.11g นี้ สามารถใช้งานร่วมกับอุปกรณ์ที่ได้รับรองมาตรฐาน IEEE802.11b อย่างไรก็ตาม ถ้าใช้ร่วมกันก็จะทำให้แบนด์วิธนั้นได้เท่ากับของ IEEE802.11b ซึ่งคือ 11 Mbps นั้นเอง

เทคนิคการรวมสัญญาณหรือโมดูเลชันที่ใช้มาตรฐาน IEEE802.11b คือ OFDM สำหรับอัตราข้อมูลที่ 6, 9, 12, 18, 24, 36, 48 หรือ 54 Mbps แต่ก็สามารถใช้เทคนิค CCK หรือมาตรฐาน IEEE802.11b ซึ่งจะรองรับแบนด์วิธที่ 5.5 และ 11 Mbps และ DBPSK/ DQPSK+DSSS สำหรับอัตราข้อมูล 1 และ 2 Mbps มาตรฐาน IEEE802.11g จะทำงานที่ความถี่ 2.4 GHz เหมือน IEEE802.11b แต่ได้ระยะทางที่ไกลกว่าเล็กน้อยถ้าอัตราข้อมูลเท่ากัน อย่างไรก็ตามอัตราข้อมูลสูงสุดคือ 54 Mbps นั้นจะได้ระยะที่สั้นกว่ามาตรฐาน IEEE802.11b ที่อัตราข้อมูล 11 Mbps

โดยส่วนใหญ่บริษัทจะผลิตอุปกรณ์ที่ได้มาตรฐาน IEEE802.11g ก่อนที่จะประกาศใช้งานจริง เนื่องจากผู้ต้องการแบนด์วิธที่มาก โดยส่วนใหญ่จะผลิตอุปกรณ์ที่รองรับ 2 มาตรฐาน หรืออุปกรณ์ Dual-band IEEE 802.11a/b หรือบางบริษัทก็ผลิตอุปกรณ์แบบ Dual-Band/ tri-mode ซึ่ง

จะรองรับมาตรฐาน IEEE 802.11a/b/g อย่างไรก็ตามมาตรฐาน IEEE 802.11g นี้ ก็มีข้อด้อยในเรื่องของคลื่นรบกวน เนื่องจากความถี่ที่ใช้คือ 2.4 GHz นั้นมีอุปกรณ์เครื่องใช้ไฟฟ้าอื่นๆ ที่ใช้ความถี่นี้เช่นกัน เช่น เตาไมโครเวฟ โทรศัพท์บ้านแบบไร้สาย และอุปกรณ์ Bluetooth

1.4 มาตรฐาน IEEE 802.11n

เมื่อปี 2004 IEEE ได้ประกาศจัดตั้งทีม TGn (Task Group n) เพื่อพัฒนามาตรฐาน IEEE 802.11 ใหม่ โดยกำหนดว่าแบนด์วิธสูงสุดอยู่ที่ 540 Mbps หรือเร็วขึ้น 10 เท่าของมาตรฐาน IEEE 802.11a และ g นอกจากนี้ยังให้รัศมีสัญญาณครอบคลุมประมาณ 50 เมตร มาตรฐานนี้พัฒนาต่อจากมาตรฐานเดิมโดยเพิ่มเทคนิค MIMO (Multiple-Input Multiple-Output) ซึ่งจะใช้ตัวส่งสัญญาณ (Transmitter antenna) และตัวรับสัญญาณ (Receiver antenna) หลายตัวเพื่อให้ส่งข้อมูลได้ปริมาณที่มากขึ้น และเมื่อเดือนมกราคม 2007 ทีมงาน TGn ได้ประกาศดราฟต์เวอร์ชัน 2.0 และตามแผนของ IEEE มาตรฐานนี้จะแล้วเสร็จ และประกาศใช้ในปี 2008 โดยอุปกรณ์ที่ได้รับรองมาตรฐานนี้จะต้องทำงานร่วมกับมาตรฐานเดิม โดยแบ่งโหมดการทำงานดังนี้

- **Legacy** (ทำงานเฉพาะกับ 802.11a, b และ g)
- **Mixed** (ทำงานได้กับทั้ง 802.11a, b, g และ n)
- **Greenfield** (ทำงานเฉพาะในโหมด 802.11n)

2. การรับ-ส่งข้อมูลของระบบเครือข่ายไร้สายบนมาตรฐาน IEEE 802.11

2.1 การส่งข้อมูลบนระบบเครือข่ายไร้สาย (Wireless Network Transmission)

เทคนิคการส่งข้อมูลบนเครือข่าย WLAN แบ่งได้ 2 วิธี คือ การส่งข้อมูลด้วยคลื่นวิทยุ และส่งข้อมูลด้วยอินฟราเรด โดยมีรายละเอียดดังนี้

2.1.1 การส่งข้อมูลด้วยคลื่นวิทยุ (Radio Frequency Transmission)

คลื่นวิทยุมีความถี่ตั้งแต่ 1-20 GHz โดยองค์กร Federal Communication Commission (FCC) ของประเทศสหรัฐอเมริกา ได้กำหนด Industrial, Scientific or Medical Bands ขึ้น เพื่อกำหนดช่วงความถี่สาธารณะของคลื่นวิทยุให้ใช้ในงานด้านอุตสาหกรรม ด้านวิทยาศาสตร์ และด้านการแพทย์ โดยมีช่วงความถี่ระหว่าง 902 MHz-5.85 GHz ดังภาพประกอบ 1

2.4 GHz		2.48 GHz		
Industrial Band I-Band		Scientific Band S-Band		Medica Band M-Band
902 MHz	928 MHz	5.725 GHz		5.85 GHz

ภาพประกอบ 1 ISM Bands

ประเทศต่างๆ จะมีการกำหนดคลื่นความถี่สาธารณะแตกต่างกันไป แต่สำหรับคลื่นความถี่ 2.4 GHz เป็นคลื่นสาธารณะที่อนุญาตให้ใช้ได้ทั่วโลก

การส่งข้อมูลด้วยคลื่นวิทยุมี 4 เทคนิค คือ เทคนิค Frequency Hopping Spread Spectrum (FHSS), เทคนิค Direct Sequence Spread Spectrum (DSSS), เทคนิค Orthogonal Frequency Division Multiplex (OFDM) และเทคนิค High Rate Direct Sequence Spread Spectrum (HR-DSSS) โดยมีรายละเอียดดังนี้

2.1.1.1 เทคนิค Frequency Hopping Spread Spectrum (FHSS)

เป็นการส่งสัญญาณข้อมูลที่มีความถี่ 2.4 GHz ISM Band โดยมีจำนวนช่องสำหรับส่งข้อมูล 79 ช่อง และแต่ละช่องมีความกว้าง 1 MHz ข้อเสียของการส่งแบบนี้คือ Bandwidth แคบ นอกจากนี้ที่ความถี่ 2.4 GHz ยังตรงกับโทรศัพท์ไร้สายและคลื่นวิทยุบังคับ ดังนั้นอาจถูกสัญญาณดังกล่าวรบกวนได้ สำหรับข้อดีคือ สามารถส่งได้ในระยะไกล

2.1.1.2 เทคนิค Direct Sequence Spread Spectrum (DSSS)

เป็นเทคนิคที่ใช้ในการมอดูเลชัน (Modulation) ซึ่งข้อมูลที่ได้รับจริงขึ้นอยู่กับจำนวนบิตที่ Chip Code แทนค่า เช่น Chip Code แทนค่าด้วยข้อมูล 8 บิต ดังนั้นอัตราเร็วในการขนส่ง Chip Code คือ 1 Mbps และอัตราเร็วในการส่งข้อมูลจริง คือ $1 \text{ Mbps} \times 8 = 8 \text{ Mbps}$

2.1.1.3 เทคนิค Orthogonal Frequency Division Multiplex (OFDM)

เป็นเทคนิคที่คิดขึ้นมาเพื่อเพิ่มความเร็วในการส่งข้อมูลของระบบเครือข่ายไร้สาย โดยถูกนำไปใช้ IEEE 802.11a ซึ่งช่วยให้มีอัตราเร็วในการส่งข้อมูลถึง 54 Mbps ที่ความถี่ 5 GHz ISM Band และนำไปใช้กับ IEEE 802.11g โดยมีอัตราเร็วในการส่งข้อมูล 54 Mbps ที่ความถี่ 2.4 GHz SM Band

2.1.1.4 เทคนิค High Rate Direct Sequence Spread Spectrum (HR-DSSS)

เป็นเทคนิคที่มีการส่งข้อมูลที่มีความถี่ 2.4 GHz ซึ่งมีอัตราเร็วในการส่งข้อมูล 11 Mbps และนำไปใช้กับมาตรฐาน IEEE 802.11b

2.1.2 การส่งข้อมูลด้วยอินฟราเรด (Infrared)

นอกจากคลื่นวิทยุสามารถนำมาใช้ส่งข้อมูลกับ WLAN แล้ว สื่อไร้สายอีกประเภทหนึ่งที่น่ามาใช้กับระบบนี้ คือ อินฟราเรด

ข้อดีของการใช้อินฟราเรดในการส่งข้อมูลมีหลายประการ ดังนี้

- ระบบเครือข่ายมีความปลอดภัย นั่นคือ สามารถควบคุมผู้ใช้ระบบเครือข่ายให้อยู่ภายในห้องที่กำหนดไว้ได้ ทำให้มั่นใจได้ว่าจะไม่มีการลักลอบใช้เครือข่ายจากนอกห้อง เนื่องจากอินฟราเรดไม่สามารถผ่านทะลุวัตถุทึบแสงจำพวกอาคาร กำแพง และผนังห้องได้
- อินฟราเรดทนต่อการรบกวนจากคลื่นแม่เหล็กไฟฟ้าบางชนิดได้ เช่น คลื่นวิทยุ และคลื่นไมโครเวฟ เป็นต้น

- อินฟราเรดมี Bandwidth กว้างทำให้สามารถส่งข้อมูลที่มีอัตราเร็วสูงได้
ข้อเสียของการใช้อินฟราเรดมีดังนี้
- รัศมีการส่งข้อมูลแคบ จึงไม่เหมาะกับระบบที่ต้องการส่งข้อมูลระยะไกล เช่น ระบบโทรศัพท์มือถือ
- แม้ว่าอินฟราเรดจะมีความปลอดภัย เนื่องจากสามารถทะลุผ่านวัตถุทึบแสงได้ แต่ลักษณะดังกล่าวทำให้สัญญาณครอบคลุมในพื้นที่จำกัด
- ลักษณะของอากาศ เช่น ฝนตก หมอก และฝุ่น เป็นสิ่งรบกวนที่สำคัญของการส่งข้อมูลด้วยอินฟราเรด ซึ่งทำให้ไม่สามารถนำอินฟราเรดไปใช้นอกอาคารได้

2.2 การควบคุมการส่งข้อมูลของเครือข่ายไร้สาย

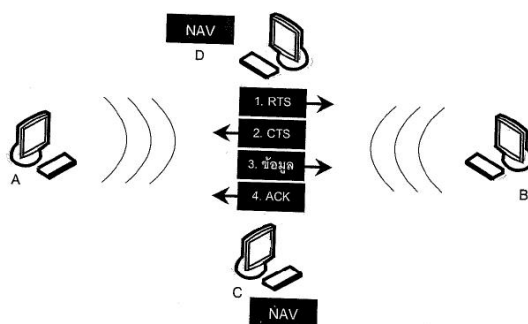
การควบคุมการส่งข้อมูลของ WLAN มี 2 ลักษณะคือ Distributed Coordination Function (DCF) และ Point Coordination Function (PCF) โดยทั่วไปจะใช้วิธีควบคุมการส่งข้อมูลแบบ DCF เป็นหลัก สำหรับ PCF เป็นเพียงทางเลือกหนึ่งเท่านั้น

2.2.1 Distributed Coordination Function (DCF)

DCF ใช้หลักการของ CSMA/CA ในการควบคุมข้อมูลซึ่งมี 2 วิธี คือ Physical Carrier Sense และการใช้ MACAW (Multiple Access with Collision Avoidance for Wireless) ร่วมกับ Virtual Carrier Sense โดยมีรายละเอียดดังนี้

2.2.1.1 การใช้ Physical Carrier Sense เมื่อสถานีใดต้องการส่งข้อมูลจะตรวจสอบว่าสัญญาณคลื่นว่างหรือไม่ ถ้าว่างจะเริ่มส่งข้อมูล ถ้าไม่ว่างจะต้องรอ ในการที่มีข้อมูลชนกัน สถานีที่ส่งข้อมูลไปที่หลังจะต้องรอเป็นระยะเวลาหนึ่งแล้วค่อยส่งข้อมูลใหม่

2.2.1.2 การใช้ MACAW (Multiple Access with Collision Avoidance for Wireless) ร่วมกับ Virtual Carrier Sense ปัญหาที่สำคัญของ Physical Carrier Sense คือ คอมพิวเตอร์อาจตรวจสอบไม่ได้ว่ามีการส่งข้อมูลอยู่ เนื่องจากรัศมีของคลื่นที่ส่งข้อมูลไม่ครอบคลุมคอมพิวเตอร์ทุกเครื่อง ดังนั้นข้อมูลอาจเกิดการชนกันได้ เรียกปัญหานี้ว่า Hidden Node Problem ซึ่งสามารถแก้ไขได้ด้วยการใช้ MACAW ร่วมกับ Virtual Carrier Sense โดยมีหลักการดังนี้



ภาพประกอบ 2 การส่งข้อมูลแบบ DCF โดยใช้หลักการ MACAW ร่วมกับ Virtual Carrier Sense

จากภาพประกอบจะเห็นว่า A ต้องการส่งข้อมูลให้ B โดยมีขั้นตอนดังนี้

ขั้นที่ 1 A ส่ง RTS (Request to Send) ซึ่งประกอบด้วยที่อยู่ของ B และความยาวของข้อมูลที่ต้องการส่งไปยัง B โดยทุกสถานีที่อยู่ในรัศมีของ A จะได้รับ RTS ที่ถูกกระจายสัญญาณมาจาก A และกำหนดให้หยุดส่งข้อมูลตามระยะเวลาที่ระบุใน CTS (Clear to Send)

ขั้นที่ 2 B ตรวจสอบว่ามีการส่งข้อมูลอยู่หรือไม่ ถ้าสัญญาณว่าง ก็จะส่ง CTS (Clear to Send) ซึ่งประกอบด้วยความยาวของข้อมูลที่ A ต้องการส่ง (คัดลอกมาจาก RTS) ให้กับ A โดยทุกสถานีที่อยู่ในรัศมีของ B จะได้รับ CTS ที่ถูกกระจายสัญญาณมาจาก B และจะกำหนดให้หยุดส่งข้อมูลตามระยะเวลาที่ระบุใน CTS ซึ่งค่าระยะเวลาที่กำหนดให้นั้นเรียกว่า NAV (Network Allocation Vector) โดยเครื่องอื่นๆ จะส่งข้อมูลได้ก็ต่อเมื่อระยะเวลาตามค่า NAV สิ้นสุดลง

ขั้นที่ 3 A ส่งข้อมูลให้ B

ขั้นที่ 4 เมื่อได้รับข้อมูลเรียบร้อยแล้ว B จะส่ง ACK (Acknowledge) กลับไปยัง A เพื่อแจ้งให้ทราบว่าได้รับข้อมูลเรียบร้อยแล้ว

2.2.2 Point Coordination Function (PCF)

เป็นเทคนิคที่ใช้วิธีการ Polling กล่าวคือ จะใช้ Access Point เป็นศูนย์กลางในการควบคุมการส่งข้อมูล โดย Access Point จะมีหน้าที่ในการสอบถามสถานีต่างๆ ที่อยู่ภายในรัศมีว่าต้องการส่งข้อมูลหรือไม่ วิธีนี้จะช่วยลดความเสี่ยงให้ข้อมูลชนกัน เนื่องจาก Access Point เป็นผู้ดูแลการส่งข้อมูลทั้งหมดนั่นเอง

3. ความปลอดภัยของเครือข่ายไร้สาย IEEE 802.11

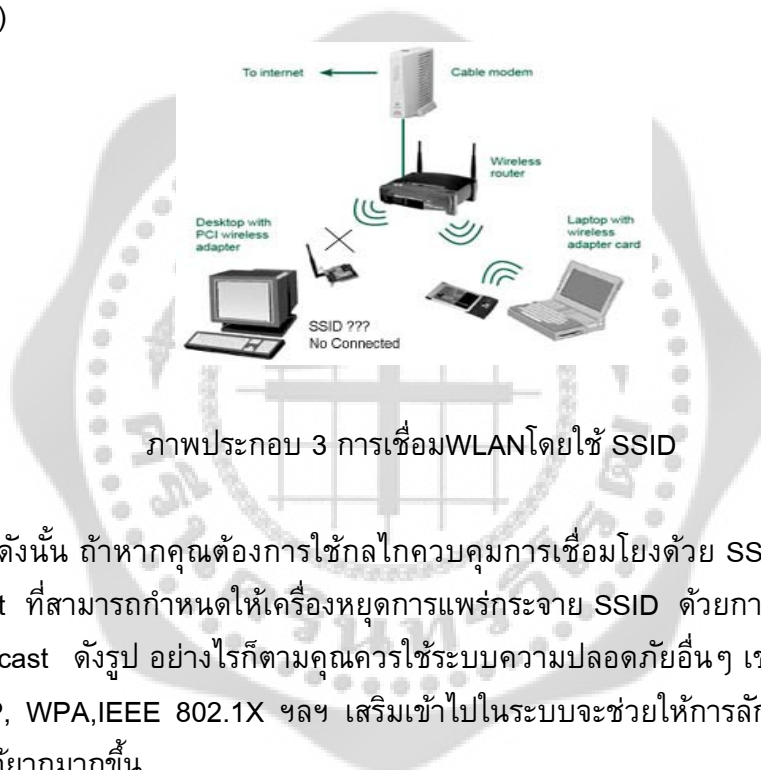
ประเด็นสำคัญอีกประการหนึ่งสำหรับการตัดสินใจเลือกใช้งานเครือข่ายไร้สายคงหนีไม่พ้นเรื่องความปลอดภัยของข้อมูล สืบเนื่องจากอุปกรณ์ต่างๆ ของเครือข่ายไร้สายรับ-ส่งข้อมูลโดยใช้คลื่นวิทยุสื่อสารข้อมูลระหว่างกัน ซึ่งเราไม่สามารถมองเห็นการแพร่กระจายคลื่นวิทยุและขอบเขตพื้นที่ให้บริการได้ด้วยตาเปล่า ทำให้ยากแก่การป้องกันและตรวจสอบผู้บุกรุก (Hacker) เข้ามาโจรกรรมข้อมูลและลักลอบเข้าใช้งานเครือข่าย จริงๆ แล้วเครือข่ายไร้สายเองมีโซลูชันของความปลอดภัยให้เลือกใช้งานตั้งแต่ระดับพื้นฐานจนถึงระดับสูงขึ้นอยู่กับอุปกรณ์ Access Point ว่ารองรับได้มากน้อยแค่ไหน โดยระดับชั้นความปลอดภัยที่นิยมใช้กันตามบ้าน ธุรกิจขนาดเล็กถึงขนาดกลางมีดังนี้

3.1 ชั้นความปลอดภัยที่ 1: ไม่มีระบบความปลอดภัย หรือเชื่อมโยงเครือข่ายด้วย SSID (Service Set Identifier)

SSID (Service Set Identifier) นอกจากจะใช้เป็นชื่ออ้างอิง Service Set ของเครือข่ายไวร์เลสแลนแล้ว ยังสามารถใช้เป็นกลไกควบคุมการเชื่อมโยงเข้าสู่เครือข่ายไวร์เลสแลนของเครื่อง

คอมพิวเตอร์ไร้สายแต่ละเครื่องได้อีกด้วย เครื่องคอมพิวเตอร์ไร้สายที่ต้องการเชื่อมโยงเข้าเครือข่าย จะต้องกำหนด SSID ของตนเองให้เป็นชื่อเดียวกันกับชื่อ SSID ของ Access Point ที่ให้บริการในพื้นที่นั้นๆ บุคคลภายนอกที่มีเครื่องคอมพิวเตอร์ไร้สายแต่ไม่ทราบ SSID ก็ไม่สามารถเชื่อมโยงเข้าสู่เครือข่ายไร้เลสได้

การใช้ SSID สำหรับสร้างความปลอดภัยให้กับเครือข่ายไร้เลสแลน ก็ยังถือว่าเป็นระดับพื้นฐานอยู่ เพราะปัจจุบันได้มีโปรแกรม Utility ของอุปกรณ์ไร้เลสหลายยี่ห้อที่สามารถที่จะ scan ตัว SSID ได้เลย ยิ่งไปกว่านั้น สำหรับผู้ที่ใช้ระบบปฏิบัติการ Windows XP สามารถใช้ Windows Zero ตรวจจับ SSID ของ Access Point ที่ให้บริการในพื้นที่นั้นๆ คนภายนอกก็จะสามารถใช้คอมพิวเตอร์ไร้สายเชื่อมโยงเข้าสู่เครือข่ายได้ทันที (ในกรณีที่ไม่ได้ติดตั้งระบบความปลอดภัยอื่นๆ)



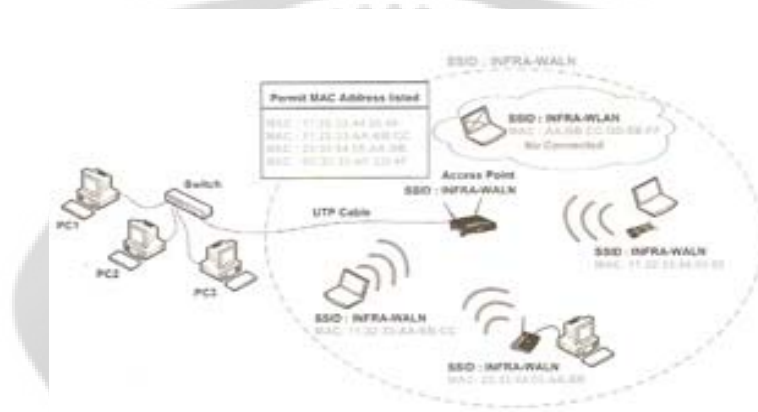
ภาพประกอบ 3 การเชื่อมWLANโดยใช้ SSID

ดังนั้น ถ้าหากคุณต้องการใช้กลไกควบคุมการเชื่อมโยงด้วย SSID ควรจะเลือก Access Point ที่สามารถกำหนดให้เครื่องหยุดการแพร่กระจาย SSID ด้วยการ Disable ฟังก์ชัน SSID Broadcast ดังรูป อย่างไรก็ตามคุณควรใช้ระบบความปลอดภัยอื่นๆ เช่น MAC Address Filtering, WEP, WPA, IEEE 802.1X ฯลฯ เสริมเข้าไปในระบบจะช่วยให้การลักลอบเชื่อมโยงเข้าสู่เครือข่ายทำได้ยากมากขึ้น

3.2 ชั้นความปลอดภัยที่ 2: กลั่นกรองผู้ใช้ด้วย MAC Address

MAC Address เป็นชุดตัวเลขฐานสิบหกขนาด 6 bytes เช่น OC:14:3A:29:2F:AA คำนี้ใช้สำหรับอ้างอิงที่อยู่กายภาพ (Physical Address) ของแลนการ์ดไร้สาย ซึ่งแลนการ์ดไร้สายที่ผลิตออกมาจำหน่ายจะมีค่า MAC Address ประจำตัวที่ไม่เหมือนกัน เราจึงสามารถใช้วิธีตรวจสอบและกลั่นกรอง MAC Address ของแลนการ์ดไร้สายของเครื่องคอมพิวเตอร์ก่อนที่จะเชื่อมโยงเข้าสู่เครือข่ายไร้เลสแลน

Access Point จะทำหน้าที่เป็นผู้ตรวจสอบและกลั่นกรองเครื่องคอมพิวเตอร์ไร้สายบนเครื่องใดบ้างที่อยู่ใน List ที่ได้รับอนุญาต โดยการนำ MAC Address ของแลนการ์ดไร้สายบนเครื่องคอมพิวเตอร์ที่ต้องการเชื่อมโยงมาเปรียบเทียบกับค่า MAC Address ในฐานข้อมูลบนตัว Access Point หากฐานข้อมูลตรงกับฐานข้อมูลของตัว Access Point ตัว Access Point ก็จะอนุญาตให้เครื่องคอมพิวเตอร์ไร้สายเครื่องนั้นสื่อสารข้อมูลผ่านตัว access point ไปยังเครือข่าย ในทำนองกลับกันหากค้นหา MAC Address แล้วไม่พบ Access Point ก็จะยกเลิกการสื่อสารกับเครื่องคอมพิวเตอร์เครื่องนั้นทันที การทำ MAC Address Filtering เหมาะสำหรับเครือข่ายไร้สายขนาดเล็กเนื่องจากขนาดฐานข้อมูลที่เก็บ MAC Address บนตัว Access Point มีค่อนข้างจำกัดคือเก็บได้ประมาณ 50-255 address ทำให้ access point สามารถตรวจสอบกลั่นกรองเครื่องคอมพิวเตอร์ไร้สายได้ประมาณ 50-255 เครื่องเท่านั้น หากเกินจากนี้ access point ก็จะสามารถรองรับได้

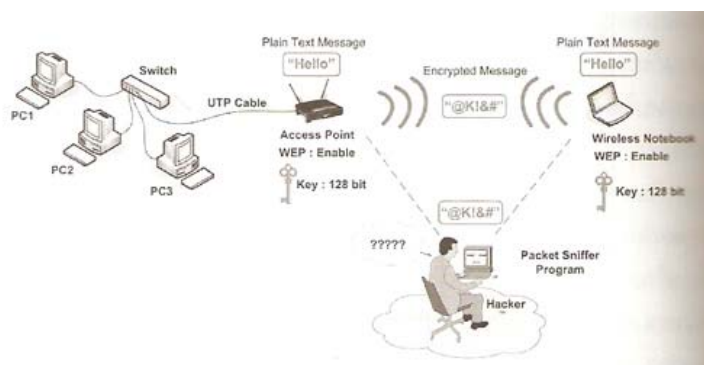


ภาพประกอบ 4 การควบคุมการใช้งานไร้สายด้วย MAC Address Filtering

3.3 ชั้นความปลอดภัยที่ 3และ4: Wired Equivalency Privacy (WEP)

ข้อมูลที่สื่อสารกันระหว่างอุปกรณ์บนเครือข่ายไร้สายแลนมักจะอยู่ในรูปของข้อมูลที่ไม่มีการเข้ารหัสหรือเรียกว่า "Plain Text Message" หรือ "Clear Text" ทำให้ผู้บุกรุกสามารถโจรกรรมข้อมูลที่กำลังสื่อสารโดยใช้โปรแกรมประเภท Packet Sniffer ดักจับข้อมูลที่แพร่กระจายออกมาในอากาศ

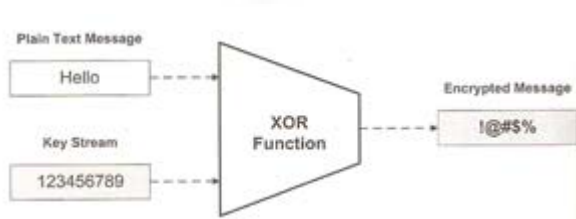
มาตรฐาน IEEE802.11 จึงได้มีการกำหนดเรื่องความปลอดภัยในการสื่อสารข้อมูลบนเครือข่ายไร้สายแลนขึ้นมา เพื่อให้อุปกรณ์ไร้สายที่สนับสนุนมาตรฐาน IEEE802.11 สามารถใช้ WEP(Wired Equivalency Privacy) เพื่อการสร้างความปลอดภัยแก่ข้อมูลที่สื่อสารโดยอาศัยกลไกการเข้ารหัส/ถอดรหัสแบบ RC4 ก่อนส่งและรับข้อมูล การใช้งาน WEP ผู้ใช้จะต้อง Enable ฟังก์ชัน WEP และกำหนดคีย์ (Key Stream) ที่มีขนาด 64 บิต (40 bit) หรือ 128 บิต (104 bit) บนตัวอุปกรณ์ไร้สายแลน เช่น แอ็กเซสพอยน์และเครื่องคอมพิวเตอร์ไร้สาย ซึ่งอุปกรณ์ทุกเครื่องบนเครือข่ายต้องกำหนดคีย์เป็นค่าเดียวกัน



ภาพประกอบ 5 ข้อมูลที่สื่อสารบนเครือข่ายไร้เลสโดยผ่านการเข้ารหัส WEP

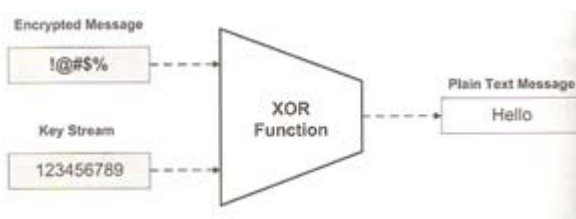
หลังจากที่ได้ enable ฟังก์ชัน WEP และใส่คีย์เข้ารหัสบนตัวอุปกรณ์ไร้เลสแล้ว ข้อมูลที่ส่งออกไปแพร่กระจายในอากาศจะเป็นข้อมูลที่ถูกรหัสไว้แล้วไม่ใช่ข้อมูลต้นฉบับจริง ดังนั้น หากมีผู้บุกรุกเข้ามาโจมตีข้อมูลที่กำลังแพร่กระจายอยู่ก็จะได้รับข้อมูลที่ผิดไป อุปกรณ์ปลายทางที่มีคีย์ถอดรหัสเท่านั้นจึงจะได้รับข้อมูลที่ถูกต้อง แต่ก็มีรายงานว่า WEP ที่ใช้คีย์ขนาด 64 บิต ถูกรหัสข้อมูลได้แล้วจากโปรแกรมถอดรหัส WEP ที่สามารถดาวน์โหลดได้ฟรีบนเว็บไซต์ ดังนั้น หากคุณต้องการความปลอดภัยในระดับสูงควรจะ เข้า/ถอดรหัสด้วย WEP 128 bit การเข้า/ถอดรหัสข้อมูล WPA หรือการใช้ Radius Server แทน

การสร้าง Encrypted Message ตามกลไกของ RC4 ข้อมูลต้นฉบับ (Plain Text Message) ที่ต้องการส่งและคีย์เข้ารหัส (Key Stream) ถูกนำมาเป็นอินพุตผ่านกระบวนการทางตรรกะด้วยฟังก์ชัน XOR (Exclusive OR) ซึ่งผลลัพธ์เอาต์พุตที่ได้จากกระบวนการนี้กลายเป็น Encrypted Message หรือข้อมูลที่ถูกรหัสแล้วสามารถดำเนินการส่งต่อไปยังอุปกรณ์ไร้เลสปลายทางได้ทันที



ภาพประกอบ 6 ผลลัพธ์เอาต์พุตถูก Encrypted Message

เมื่ออุปกรณ์ไร้เลสแลนปลายทางได้รับ Encrypted Message กลไก RC4 ก็นำเอาข้อมูลดังกล่าวพร้อมคีย์ถอดรหัส (เป็นคีย์เดียวกับที่ใช้เข้ารหัสในอุปกรณ์ไร้เลสต้นทาง) มาใช้เป็นอินพุตผ่านกระบวนการทางตรรกะด้วยฟังก์ชัน XOR (Exclusive OR) เอาต์พุตที่ได้จะเป็นข้อมูลต้นฉบับเหมือนกับที่อุปกรณ์ไร้เลสแลนต้นทางต้องการส่งให้



ภาพประกอบ 7 ผลลัพธ์เอาท์พุตถูก Decrypted Message

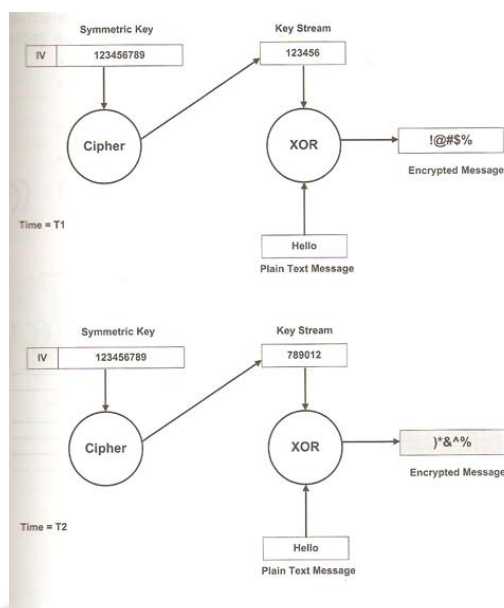
จากที่ได้กล่าวมาข้างต้นกลไก RC4 จะอาศัย Key Stream สำหรับใช้ในการเข้ารหัสข้อมูล เพื่อสร้าง Encrypted Message ซึ่ง Key Stream ประกอบด้วยข้อมูลสองส่วนคือ IV ขนาด 24-bit (Initialization Vector) และคีย์แบบสมมาตรขนาด 40-bit/104-bit ได้จากการใส่ของผู้ใช้ผ่าน Windows Zero หรือโปรแกรม Configuration Utility ของอุปกรณ์ไร้สายแลน

$$\text{Key Stream} = \text{IV} + \text{Symmetric Key}$$

$$64 \text{ bits} = 24 \text{ bits} + 40 \text{ bits}$$

$$128 \text{ bits} = 24 \text{ bits} + 104 \text{ bits}$$

เพื่อให้การคาดเดาคีย์เข้ารหัส/ถอดรหัสทำได้ยากลำบาก ทางมาตรฐาน IEEE802.11 จึงกำหนดให้ข้อมูลใน IV เปลี่ยนค่าทุกๆ ครั้งเมื่อมีการส่งเฟรมข้อมูลใหม่ลงไป ทำให้ key stream (ได้จากการรวมกันระหว่าง IV + Symmetric Key) เปลี่ยนแปลงค่าเป็นคีย์อันใหม่ตาม IV ด้วย ดังนั้น หากผู้ใช้งานส่งข้อมูลฉบับซ้ำ (Hello) กลไก WEP ในอุปกรณ์ไร้สายก็จะสามารถสร้าง Encrypted Message แตกต่างกันไป ซึ่งในรูปด้านล่างจะแสดงให้เห็นว่าเมื่อเวลาผ่านไปจาก T1 ไปเป็น T2 ค่า IV นั้นก็ถูกเปลี่ยนไปทำให้ค่า Key Stream ที่ถูกสร้างขึ้นเปลี่ยนไป เมื่อนำมาผ่านกระบวนการเข้ารหัสก็จะทำให้ได้ Encrypted Message ที่เปลี่ยนไปตามคาบเวลาด้วย



ภาพประกอบ 8 ผ่านกระบวนการเข้ารหัส

3.4 ชั้นความปลอดภัยที่ 5และ6: Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access (WPA) เป็นมาตรฐานความปลอดภัยข้อมูลที่พัฒนาขึ้นมาโดยองค์กร Wi-Fi Alliance (WECA) เพื่อแก้ไขจุดอ่อนของ WEP ในเรื่องการเข้ารหัสข้อมูล ถูกประกาศให้เป็นมาตรฐานในเดือนพฤศจิกายน ค.ศ.2002 การพัฒนา WPA อยู่บนพื้นฐานเดียวกับมาตรฐาน IEEE802.11i ของสถาบันวิศวกรรมไฟฟ้าและอิเล็กทรอนิกส์ (IEEE) WPA จะถูกนำมาใช้ทดแทน WEP เพื่อแก้ไขจุดอ่อนในเรื่องการเข้ารหัส/ถอดรหัสข้อมูลด้วย WEP Key โดยการนำเอา Dynamic Key Distribution และการตรวจสอบและพิสูจน์สิทธิ์ผู้ใช้งาน IEEE802.1X มารวมไว้เป็นกลไกของ WPA อุปกรณ์ไร้เลสที่สนับสนุนมาตรฐาน WPA จะมีโหมดการทำงานให้เลือก 2 โหมด ดังนี้

3.4.1 WPA Pre-Shared Key: โหมดการทำงาน Pre-Shared Key ออกแบบมาสำหรับเครือข่ายไร้เลสแลนที่ใช้ภายในบ้านหรือในสำนักงานขนาดเล็ก (Home Office Small Office : SOHO) เพื่อสร้างความปลอดภัยให้แก่ข้อมูล เนื่องจากโหมดนี้ไม่ต้องการ RADIUS Server สำหรับการตรวจสอบและพิสูจน์สิทธิ์ของผู้ใช้งาน Pre-Shared Key จะใช้กลไกการเข้ารหัส/ถอดรหัสข้อมูลสองแบบคือ แบบแรกใช้ TKIP(Temporal Key Integrity Protocol) ร่วมกับ MIC(Message Integrity Code หรือเรียกว่า Michael) และแบบที่สอง AES (Advanced Encryption Standard) ทั้งสองกลไกมีระดับความปลอดภัยสูงกว่า WEP หลายเท่า

3.4.1.2 Temporal Key Integrity Protocol : เทคนิคการใช้คีย์ชั่วคราวเพื่อเข้ารหัส

TKIP เป็นกลไกการเข้ารหัสที่ยังคงใช้เทคนิค RC4 เช่นเดียวกับ WEP แต่ได้มีการปรับปรุงการทำงานให้มีประสิทธิภาพที่เหนือกว่า WEP ดังนี้

- ทุกๆ แพ็กเก็ตข้อมูลที่สร้างขึ้นจากการสื่อสารระหว่าง AP กับเครื่องคอมพิวเตอร์ไร้สายจะถูกเข้ารหัสด้วยคีย์ที่แตกต่างกันออกไป (Dynamic Ciphering Keys) ทำให้ยากแก่การเดาคีย์ที่ต้องการ
- ใช้กลไก Message Integrity Checking (MIC) เพื่อให้มั่นใจว่าข้อมูลที่อยู่ระหว่างการสื่อสารจะไม่ถูกปลอมแปลงจากผู้บุกรุก
- จำนวนบิต Initialization Vector (IV) hashing ขนาด 48 บิต ซึ่งสูงกว่า IV ของ WEP ที่มีจำนวนแค่ 24 บิต (ค่า IV นี้ถูกนำไปรวมกับคีย์ที่ผู้ใช้ต้องใส่เพื่อใช้สำหรับการเข้ารหัสและถอดรหัส) การที่มีจำนวนบิตมากกว่าทำให้การเดาคีย์ทำได้ยากขึ้น

3.4.1.2 Advance Encryption Standard (AES)

กลไกการเข้ารหัสข้อมูล Advance Encryption Standard (AES) เป็นมาตรฐานที่พัฒนาขึ้นโดยสถาบันมาตรฐานและเทคโนโลยีแห่งชาติอเมริกา (National Institute of Standard and Technology : NIST) ถือว่าเป็นกลไกการเข้ารหัสข้อมูลที่แข็งแกร่งที่สุดในปัจจุบัน วิธีนี้จะใช้การเข้ารหัสข้อมูลขนาด 128-bit 192-bit และ 256-bit

3.4.2 WPA RADIUS/IEEE802.1X

โหมดการทำงานนี้จะคล้ายกับการใช้ WEP ร่วมกับ IEEE802.1X เพียงแต่เปลี่ยนกลไกการเข้ารหัส/ถอดรหัสข้อมูลจาก WEP เป็น TKIP หรือ AES เท่านั้น หลักการก็คือใช้ Radius Server ทำหน้าที่คอยตรวจสอบและพิสูจน์สิทธิผู้ใช้งานก่อนการเชื่อมโยงเครื่องคอมพิวเตอร์ไร้สายเข้าสู่ระบบและในระหว่างการสื่อสารข้อมูลของ Access Point กับเครื่องคอมพิวเตอร์ไร้สาย ข้อมูลถูกเข้ารหัสข้อมูลด้วยคีย์ที่แตกต่างกัน และคีย์เข้ารหัสจะถูกเปลี่ยนไปเรื่อยๆ อัตโนมัติ ทำให้ผู้บุกรุกคาดเดาคีย์ได้ยากลำบากและยังต้องเจอการพิสูจน์สิทธิผู้ใช้งานก่อนผ่านเข้าระบบอีกด้วย

3.5 ชั้นความปลอดภัยที่ 7: PEAP (protected Extensible Authentication Protocol)

PEAP (Protected Extensible Authentication Protocol) เป็นมาตรฐานที่เปิดใช้อย่างกว้างขวางในผลิตภัณฑ์ของ Cisco และ Microsoft และ จัดเตรียมความปลอดภัยที่ดีมาก มันซึ่งคล้ายในการออกแบบของ EAP -TTLS ซึ่งจะต้องมี Radius Server ที่มี PKI หรือใบรับรองเท่านั้น เพื่อที่จะสร้าง TLS ที่ปลอดภัยเพื่อใช้ในการตรวจสอบผู้เข้า หลังจาก EAP - TTLS ได้มีวางขายเรียบร้อยแล้วบนตลาด ซึ่ง Microsoft และ Cisco ทำให้มาตรฐานนี้ตามทันมาตรฐาน EAP - TTLS ในตลาดได้อย่างรวดเร็ว ซึ่ง Microsoft และ Cisco แบ่งออกเป็นส่วนๆเมื่อ Microsoft สนับสนุนเพียงแค่มาตรฐาน PEAPv0 ขณะที่ Cisco สนับสนุนทั้ง 2 มาตรฐานทั้ง PEAPv1 และ PEAPv0 ซึ่งทั้ง 2 มาตรฐานนี้อ้างถึงวิธีการตรวจสอบผู้เข้าใช้คือกลไกที่จะสร้าง TLS ที่ปลอดภัยทำเพื่อปกป้องและป้องกันระบบ รายการนำเชื่อถือต่อมาคือ EAP -MSCHAPv2, EAP -GTC, และ

EAP - SIM จะอ้างถึงวิธีการตรวจสอบผู้เข้าใช้ที่ทำให้สะดวกต่อผู้ใช้หรือความน่าเชื่อถือของอุปกรณ์ เทคนิค PEAPv0 จะสนับสนุนวิธี EAP ภายใน EAP - MSCHAPv2 และ EAP - SIM ขณะที่ PEAPv1 จะสนับสนุนวิธี EAP ภายใน EAP - GTC และ EAP -SIM เพราะว่า Microsoft สนับสนุนแค่ PEAPv0 เท่านั้น และไม่มีการสนับสนุน PEAPv1 ซึ่ง Microsoft เรียก PEAPv0 ง่ายกว่า PEAP โดยปราศจาก v0 หรือ v1 ความแตกต่างอื่นๆระหว่าง Microsoft และ Cisco คือ Microsoft จะการสนับสนุน PEAPv0 / EAP - MSCHAPv2 โหมดเท่านั้น แต่จะไม่สนับสนุน PEAPv0 / EAP - SIM โหมด อย่างไรก็ตาม Microsoft สนับสนุนรูปแบบอื่นๆของ PEAPv0 คือ PEAP - EAP - TLS ซึ่ง Cisco's Radius Server และ ซอฟต์แวร์ไคลเอ็นท์ไม่มีการสนับสนุน PEAP - EAP - TLS แต่จะต้องการไคลเอ็นท์-ด้านไบบรอนดิจิตอลซึ่งจะค้นหาที่ตั้งบนฮาร์ดไดรฟ์ หรือ ที่ปลอดภัยมากกว่า smartcard จริงๆ แต่ PEAP - EAP - TLS ซึ่งมีความคล้ายคลึง EAP - TLS ที่เป็นต้นฉบับมาก คือ จะไม่มีจัดเตรียมการป้องกันมากกว่าแต่อย่างใดเนื่องจากข้อเท็จจริงส่วนของไบบรอนดิไคลเอ็นท์คือ ไม่มีการนำข้อความมาเข้ารหัสใน EAP - TLS แต่จะถูกการนำข้อความมาเข้ารหัสใน PEAP - EAP -TLS แทน เพราะว่าไคลเอ็นท์รายอื่นและการสนับสนุนเครื่องแม่ข่าย PEAP - EAP -TLS ซึ่งผู้ใช้ อาจจะหลีกเลี่ยงซึ่งเป็นไปได้มากมันถ้าเขาไม่เพียงแต่ตั้งใจเพื่อใช้ไคลเอ็นท์เดสค์ทอป และ เครื่องแม่ข่าย ของ Microsoft ทำยที่สุด PEAPv0 / EAP - MSCHAPv2 คือรูปแบบของ PEAP ซึ่งผู้คนส่วนมากที่นั้นจะเคยรู้จัก PEAP แม้กระทั่งในรูปแบบของ Funk Software ซึ่ง Funk Soft นี้คือ ผู้สนับสนุนของ EAP -TTLS

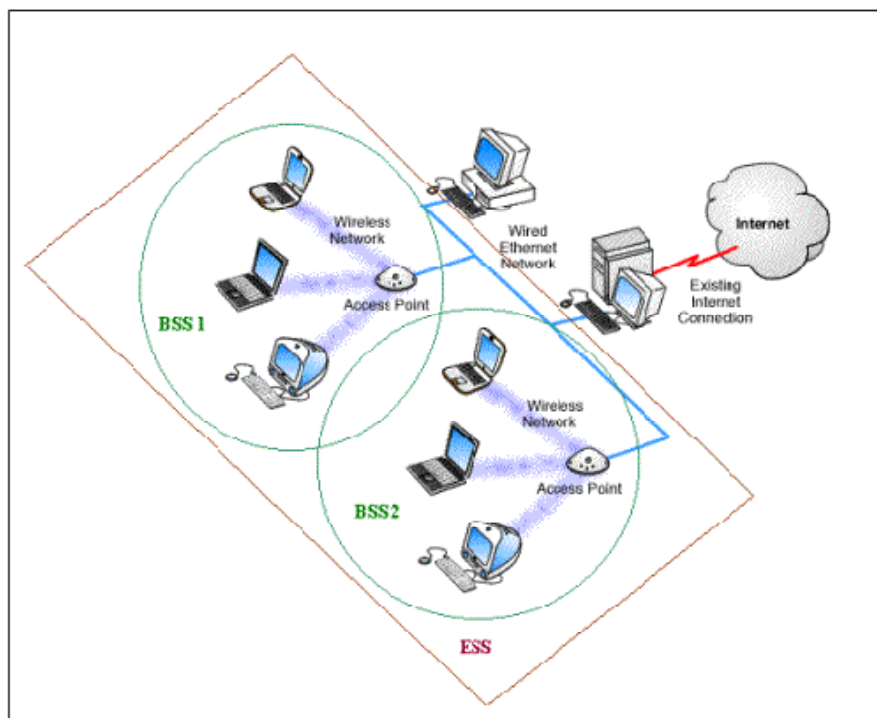
4. ประสิทธิภาพบนเครือข่ายไร้สายบนมาตรฐาน IEEE 802.11

4.1 ลักษณะการเชื่อมต่อของอุปกรณ์

มาตรฐาน IEEE 802.11 ได้กำหนดลักษณะการเชื่อมต่อของอุปกรณ์ภายในเครือข่าย WLAN ไว้ ลักษณะคือโหมด Infrastructure และโหมด Ad-Hoc หรือ Peer-to-Peer

4.1.1 โหมด Infrastructure

โดยทั่วไปแล้วอุปกรณ์ในเครือข่าย IEEE 802.11 WLAN จะเชื่อมต่อกันในลักษณะของโหมด Infrastructure ซึ่งเป็นโหมดที่อนุญาตให้อุปกรณ์ภายใน WLAN สามารถเชื่อมต่อกับเครือข่ายอื่นได้ ในโหมด Infrastructure นี้เครือข่าย IEEE 802.11 WLAN จะประกอบไปด้วยอุปกรณ์ 2 ประเภทได้แก่ สถานีผู้ใช้ (Client Station) ซึ่งก็คืออุปกรณ์คอมพิวเตอร์ (Desktop, Laptop, หรือ PDA ต่างๆ) ที่มีอุปกรณ์ Client Adapter เพื่อใช้รับส่งข้อมูลผ่าน IEEE 802.11 WLAN และสถานีแม่ข่าย (Access Point) ซึ่งทำหน้าที่ต่อเชื่อมสถานีผู้ใช้เข้ากับเครือข่ายอื่น (ซึ่งโดยปกติจะเป็นเครือข่าย IEEE 802.3 Ethernet LAN) การทำงานในโหมด Infrastructure มีพื้นฐานมาจากระบบเครือข่ายโทรศัพท์มือถือ กล่าวคือสถานีผู้ใช้จะสามารถรับส่งข้อมูลโดยตรงกับสถานีแม่ข่ายที่ให้บริการแก่สถานีผู้ใช้นั้นอยู่เท่านั้น ส่วนสถานีแม่ข่ายจะทำหน้าที่ส่งต่อ (forward) ข้อมูลที่ได้รับจากสถานีผู้ใช้ไปยังจุดหมายปลายทางหรือส่งต่อข้อมูลที่ได้รับจากเครือข่ายอื่นมายังสถานีผู้ใช้



ภาพประกอบ 9 แสดง BSS และ ESS

4.1.1.1 Basic Service Set (BSS)

Basic Service Set (BSS) หมายถึงบริเวณของเครือข่าย IEEE 802.11 WLAN ที่มีสถานีแม่ข่าย 1 สถานี ซึ่งสถานีผู้ใช้ภายในขอบเขตของ BSS นี้ทุกสถานีจะต้องสื่อสารข้อมูลผ่านสถานีแม่ข่ายดังกล่าวเท่านั้น

4.1.1.2 Extended Service Set (ESS)

Extended Service Set (ESS) หมายถึงบริเวณของเครือข่าย IEEE 802.11 WLAN ที่ประกอบด้วย BSS มากกว่า 1 BSS ซึ่งได้รับการเชื่อมต่อเข้าด้วยกัน สถานีผู้ใช้สามารถเคลื่อนย้ายจาก BSS หนึ่งไปอยู่ในอีก BSS หนึ่งได้โดย BSS เหล่านี้จะทำการ Roaming หรือติดต่อสื่อสารกันเพื่อทำการโอนย้ายการให้บริการสำหรับสถานีผู้ใช้ดังกล่าว

4.1.2 โหมด Ad-Hoc หรือ Peer-to-Peer

เครือข่าย IEEE 802.11 WLAN ในโหมด Ad-Hoc หรือ Peer-to-Peer เป็นเครือข่ายที่ปิดคือไม่มีสถานีแม่ข่ายและไม่มีการเชื่อมต่อกับเครือข่ายอื่น บริเวณของเครือข่าย IEEE 802.11 WLAN ในโหมด Ad-Hoc จะถูกเรียกว่า Independent Basic Service Set (IBSS) ซึ่งสถานีผู้ใช้หนึ่งสามารถติดต่อสื่อสารข้อมูลกับสถานีผู้ใช้อื่นๆในเขต IBSS เดียวกันได้โดยตรงโดยไม่ต้องผ่านสถานีแม่ข่าย แต่สถานีผู้ใช้จะไม่สามารถรับส่งข้อมูลกับเครือข่ายอื่นๆได้



ภาพประกอบ 10 แสดงการทำงานในโหมด Adhoc หรือ Peer-to-Peer Mode

4.2 การเข้าใช้ช่องสัญญาณด้วยกลไก CSMA/CA

บทบาทหนึ่งของ MAC Layer ในมาตรฐาน IEEE 802.11 คือการจัดสรรการเข้าใช้ช่องสัญญาณซึ่งแต่ละสถานีใน BSS หรือ IBSS จะต้องแบ่งกันใช้ช่องสัญญาณที่ถูกกำหนดมาสำหรับใช้งานร่วมกันอย่างเป็นธรรมชาติ มาตรฐาน IEEE 802.11 ได้กำหนดให้ใช้กลไก CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) เพื่อจัดสรรการใช้ช่องสัญญาณร่วมกันดังกล่าว

4.2.1 CSMA with Random Back-Off

กลไก CSMA (Carrier Sense Multiple Access) with Random Back-Off เป็นเทคนิคอย่างง่ายสำหรับจัดสรรการเข้าใช้ช่องสัญญาณของผู้ใช้แต่ละคน (ซึ่งต้องแบ่งกันใช้ช่องสัญญาณร่วมกัน) อย่างยุติธรรม กลไกนี้เป็นที่ยอมรับและนิยมใช้กันอย่างแพร่หลาย เช่น ในมาตรฐาน IEEE 802.3 Ethernet LAN หลักการทำงานของกลไก CSMA คือ เมื่อสถานีหนึ่งต้องการเข้าใช้ช่องสัญญาณ สถานีดังกล่าวจะต้องตรวจสอบช่องสัญญาณก่อนว่ามีสถานีอื่นทำการรับส่งสัญญาณข้อมูลอยู่หรือไม่และรอจนกว่าช่องสัญญาณจะว่าง เมื่อช่องสัญญาณว่างแล้วสถานีที่ต้องการเข้าใช้ช่องสัญญาณจะต้องรอต่อไปอีกระยะหนึ่ง (Random Back-Off) ซึ่งแต่ละสถานีได้กำหนดระยะเวลาในการรอดังกล่าวไว้แล้วด้วยการสุ่มค่าหลังจากเสร็จการใช้ช่องสัญญาณครั้งก่อน สถานีที่สุ่มได้ระยะเวลาในการรอน้อยกว่าก็จะมีสิทธิในการเข้าใช้ช่องสัญญาณก่อนแต่อย่างไรก็ตามในบางกรณีกลไกดังกล่าวอาจจะกำหนดให้สถานีมากกว่าหนึ่งสถานีส่งข้อมูลในเวลาพร้อมๆ กันซึ่งจะทำให้เกิดการชนกันของสัญญาณได้ ซึ่งหากเกิดการชนกันของสัญญาณขึ้นจะต้องมีการส่งสัญญาณข้อมูลเดิมซ้ำอีกครั้งด้วยกลไกที่กล่าวมาแล้วข้างต้น

4.2.2 CSMA/CD

กลไก CSMA/CD (Collision Detection) เป็นเทคนิคที่รู้จักกันดีซึ่งถูกนำมาใช้ในมาตรฐาน IEEE 802.3 Ethernet LAN ซึ่งการทำงานของกลไก CSMA/CD โดยหลักแล้วเป็นเช่นเดียวกับที่กล่าวไว้ในส่วนของ CSMA with Random Back-Off แต่จะมีรายละเอียดเพิ่มเติมเกี่ยวกับการตรวจสอบว่าเกิดการชนกันของสัญญาณหรือไม่ ในกรณีนี้สถานีที่กำลังทำการส่งสัญญาณข้อมูลอยู่จะต้องคอยตรวจสอบด้วยว่ามีการชนกันของสัญญาณเกิดขึ้นหรือไม่

(ในขณะที่เดียวกันกับการทำการส่งสัญญาณข้อมูล) โดยการตรวจวัดระดับ voltage ของสัญญาณในสายสัญญาณว่ามีค่าสูงกว่าปกติหรือไม่ ซึ่งหากระดับ voltage ของสัญญาณในสายสัญญาณในสายสัญญาณมีค่าสูงกว่าค่าที่กำหนดแสดงว่าเกิดการชนกันของสัญญาณขึ้น ในกรณีดังกล่าวสถานีที่กำลังส่งสัญญาณข้อมูลอยู่จะต้องยกเลิกการส่งสัญญาณทันทีและปฏิบัติตามกลไกที่กล่าวมาแล้วข้างต้นเพื่อทำการส่งข้อมูลเดิมซ้ำอีกต่อไป

4.2.3 CSMA/CA with Acknowledgement

เป็นที่ควรสังเกตว่าเทคนิค CSMA/CD ไม่สามารถนำมาใช้กับ WLAN ซึ่งใช้การสื่อสารแบบไร้สายได้ สาเหตุหลักๆ ก็คือการตรวจสอบการชนกันของสัญญาณในระหว่างที่ทำการส่งสัญญาณจะต้องใช้อุปกรณ์รับส่งคลื่นวิทยุที่เป็น Full Duplex (สามารถรับและส่งสัญญาณในเวลาเดียวกันได้) ซึ่งจะมีราคาแพงกว่าอุปกรณ์รับส่งคลื่นวิทยุที่ไม่สามารถรับและส่งสัญญาณในเวลาเดียวกัน นอกจากนี้แต่ละสถานีใน BSS หรือ IBSS อาจไม่ได้ยินสัญญาณจากสถานีอื่นทุกสถานีหรือปัญหาที่เรียกว่า Hidden Node Problem (ดังในภาพประกอบ 4: สถานี A ได้ยินสัญญาณจากสถานีแม่ข่าย (Access Point) แต่ไม่ได้ยินสัญญาณจากสถานี C และในทางกลับกันสถานี C ไม่ได้ยินสัญญาณจากสถานี A แต่ได้ยินสัญญาณจากสถานีแม่ข่าย ซึ่งสถานการณ์ดังกล่าวนี้เป็นสถานการณ์เกิดขึ้นใน WLAN โดยทั่วไป) ดังนั้นการตรวจสอบการชนกันของสัญญาณโดยตรงเป็นไปได้ยากหรือเป็นไปได้เลย มาตรฐาน IEEE 802.11 จึงได้กำหนดให้ใช้เทคนิค CSMA/CA with Acknowledgement สำหรับการจัดการการเข้าใช้ช่องสัญญาณของแต่ละสถานีเพื่อแก้ไขปัญหาเหล่านี้ ซึ่งการทำงานของกลไก CSMA/CA โดยหลักแล้วเป็นเช่นเดียวกับที่กล่าวไว้ในส่วนของ CSMA with Random Back-Off แต่จะมีรายละเอียดเพิ่มเติมเกี่ยวกับการหลีกเลี่ยงไม่ให้เกิดการชนกันของสัญญาณและเทคนิคสำหรับการตรวจสอบว่าเกิดการชนของสัญญาณหรือไม่แบบเป็นนัย โดยสถานีผู้ส่งสัญญาณข้อมูลจะต้องรอรับ Acknowledgement จากสถานีที่ส่งข้อมูลไปให้ หากไม่ได้รับ Acknowledgement กลับมาภายในเวลาที่กำหนดจะถือว่าเกิดการชนของสัญญาณขึ้นและต้องทำการส่งข้อมูลเดิมซ้ำอีกต่อไป



ภาพประกอบ 11 แสดง Hidden Node Problem และ กลไก RTS/CTS Handshake

สำหรับการหลีกเลี่ยงไม่ให้เกิดการชนกันของสัญญาณนั้น มาตรฐาน IEEE 802.11 ได้ใช้กลไกที่เรียกว่า Virtual Carrier Sense เพื่อแก้ไขปัญหาที่แต่ละสถานีใน BSS หรือ IBSS อาจไม่ได้ยินสัญญาณจากสถานีอื่นบางสถานี (Hidden Node Problem) กลไกดังกล่าวมีการทำงานดังนี้ เมื่อสถานีที่ต้องการจะส่งแพ็กเก็ตข้อมูลได้รับสิทธิในการเข้าใช้ช่องสัญญาณแล้วจะทำการส่งแพ็กเก็ตสั้นๆ ที่เรียกว่า RTS (Request To Send) เพื่อเป็นการจองช่องสัญญาณ ก่อนที่จะส่งแพ็กเก็ตข้อมูลจริง ซึ่งแพ็กเก็ต RTS ประกอบไปด้วย ระยะเวลาที่คาดว่าจะใช้ช่องสัญญาณจนแล้วเสร็จ (Duration ID) รวมถึง Address ของสถานีผู้ส่งและผู้รับ เมื่อสถานีผู้รับได้ยินสัญญาณ RTS ก็จะตอบรับกลับมาด้วยการส่งสัญญาณ CTS (Clear To Send) ซึ่งจะบ่งบอกข้อมูลระยะเวลาที่คาดว่าจะสถานีที่กำลังจะทำการส่งข้อมูลนั้นจะใช้ช่องสัญญาณจนแล้วเสร็จ หลักการก็คือทุกๆ สถานีใน BSS หรือ IBSS ควรจะได้ยินสัญญาณ RTS หรือไม่ก็ CTS อย่างใดอย่างหนึ่งหรือทั้งสองอย่าง เมื่อได้รับ RTS หรือ CTS ทุกๆ สถานีจะทราบถึงว่าช่วงเวลาที่จะระบุไว้ใน Duration ID ซึ่งช่องสัญญาณจะถูกใช้และทุกสถานีที่ยังไม่ได้รับสิทธิในการเข้าใช้ช่องสัญญาณจะตั้งค่า NAV (Network Allocation Vector) ให้เท่ากับ Duration ID ซึ่งแสดงถึงช่วงเวลาที่ยังไม่สามารถเข้าใช้ช่องสัญญาณได้ ทุกๆ สถานีจะใช้กลไก Virtual Carrier Sense ดังกล่าวผนวกกับการฟังสัญญาณในช่องสัญญาณจริงๆ ในการตรวจสอบว่าช่องสัญญาณว่างอยู่หรือไม่

5. งานวิจัยที่เกี่ยวข้อง

5.1 งานวิจัยในประเทศ

ศาลทัส พัตพุททรัพย์ (2549) ได้วิจัยถึงความปลอดภัยบนระบบเครือข่ายไร้สาย โดยเครือข่ายไร้สายมีการเข้ารหัสแบบ WEP (Wired Equivalent Privacy) เพื่อเข้ารหัสลับของผู้ใช้งาน และมีการตั้งชื่อเครือข่าย SSID (Service Set Identifier) เป็นค่าที่กำหนดขึ้นเอง WEP เป็นรูปแบบความปลอดภัยพื้นฐานที่ติดมากับมาตรฐาน 802.11 โดยได้มีขั้นตอนการดำเนินงานได้แก่ การจำลองเครือข่ายไร้สายเพื่อทำการทดสอบถึงภัยคุกคามที่อาจเกิดขึ้นบนเครือข่ายไร้สาย โดยได้จัดตั้ง APs (Access Point) จำนวน 1 เครื่อง เครื่องลูกข่ายจำนวน 2 เครื่อง และเครื่องที่ใช้ดักจับแพ็กเก็ตข้อมูลและแกะรอยกุญแจที่เข้ารหัสแบบ WEP 64 บิต และ 128 บิต จำนวน 1 เครื่อง ผลการวิเคราะห์เปรียบเทียบจำนวนแพ็กเก็ตและเวลาที่ใช้ในการแกะรอยกุญแจ สรุปได้ว่า การเข้ารหัสแบบ WEP 128 บิต มีความปลอดภัยในการแกะรอยกุญแจมากกว่าการเข้ารหัสแบบ WEP 64 บิต เนื่องจากจำนวนแพ็กเก็ตที่ดักจับที่มีการเข้ารหัสแบบ WEP 128 บิต ต้องใช้จำนวนแพ็กเก็ตมากกว่าการเข้ารหัสแบบ WEP 64 บิต ถึง 2.17 เท่า แสดงให้เห็นถึงความสามารถในการรักษาความปลอดภัยบนเครือข่ายไร้สายที่สูงกว่า ผลการสำรวจเครือข่ายไร้สายทั่วไปจำนวน 77 APs พบ 58% เปิดใช้งาน WEP และผลการสำรวจจุดบริการอินเทอร์เน็ตไร้สายจำนวน 41 APs พบ 31.7% เปิดใช้งาน WEP

5.2 งานวิจัยต่างประเทศ

อาเหม็ด เอ จาฮา, ฟาติ เบน ชัทวาน, เมจดี อชิบानी (Ahmed A. Jaha, Fathi Ben Shatwan, Majdi Ashibani. 2008) ได้วิจัยถึงประสิทธิภาพบนเครือข่ายที่ทำการเชื่อมต่อโดยใช้ Remote Access VPN (Virtual Private Network) ผ่านทางเครือข่ายที่ใช้สาย(Wired LAN)และเครือข่ายไร้สาย(Wireless LAN) ซึ่งเป็นโครงสร้างพื้นฐานของความปลอดภัยในการติดต่อสื่อสารระหว่างภายนอกกับภายในองค์กร ซึ่งทางผู้วิจัยได้ทำการจำลองระบบและ ทำการวัดหาค่าประสิทธิภาพ ทูพุท(Throughput) บนโปรโตคอล TCP และ UDP, ราวด์ ทริป ทาม (Round Trip Time), จิสเตอร์ (Jitter) และ แพคเก็ต ลอสส์ (Packet loss) ของระบบที่เชื่อมต่อVPNโดยใช้ โปรโตคอล Point to Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), Internet Protocol Security (IPsec) และ Secure Socket Layer (SSL) บน Open VPN จากผลการวิจัยสรุปได้ว่า เครือข่ายที่ใช้สาย(Wired LAN) ที่เชื่อมต่อแบบ PPTP ให้ ทูพุท (Throughput) บนโปรโตคอลTCP และ UDP สูงที่สุด, ราวด์ ทริป ทาม (Round Trip Time) เร็วที่สุด, จิสเตอร์ (Jitter) ต่ำที่สุด และ แพคเก็ต ลอสส์ (Packet loss) ต่ำที่สุด ส่วนเครือข่ายไร้สาย (Wireless LAN) ที่เชื่อมต่อแบบ Open VPN ให้ ทูพุท(Throughput) บนโปรโตคอล TCP และ UDP น้อยที่สุด, ราวด์ ทริป ทาม (Round Trip Time) ช้าที่สุด, จิสเตอร์ (Jitter) สูงที่สุด และ แพคเก็ต ลอสส์ (Packet loss) สูงที่สุด

อีซีดีน บราก้า และ มุฮัมหมัด โบลมัลฟ (Ezedin Barka & Mohammed Boulmalf. 2007) ได้วิจัยถึงประสิทธิภาพที่คอมพิวเตอร์ประมวลผลได้ ทูพุท (throughput) ของเครือข่ายไร้สาย (WLAN) บนมาตรฐาน IEEE 802.11g บนชั้นความปลอดภัย Wired Equivalent Privacy 64 บิต และ 128 บิต (WEP 64bit & 128bit) บนโปรโตคอล TCP และ UDP โดยขนาดข้อมูลที่ใช้ในการส่งคือ 1460 bytes ผู้วิจัยได้จัดเหตุการณ์สองเหตุการณ์ คือ เหตุการณ์แรก มีคอมพิวเตอร์ที่มีการ์ด Wireless มาตรฐาน IEEE 802.11g สอง เครื่อง, Access Point หนึ่งเครื่อง ส่งข้อมูลจากเครื่อง A ไป B เหตุการณ์ที่สอง เครื่อง B เปลี่ยนจากไร้สาย (Wireless) เป็น ใช้สาย (Wired) จากผลการวิจัยสรุปได้ว่า เหตุการณ์ที่หนึ่ง ทูพุท(Throughput) ของ TCP คือ 9400 Kbps สำหรับ WEP 64 บิต และ 9100 Kbps สำหรับ WEP 128 บิต ทูพุท(Throughput) ของ UDP คือ 10390 Kbps สำหรับ WEP 64 บิต และ 13000 Kbps สำหรับ WEP 128 ส่วนเหตุการณ์ที่สอง ทูพุท (Throughput) ของ TCP คือ 5141 Kbps สำหรับ WEP 64 บิต และ 5071 Kbps สำหรับ WEP 128 บิต ทูพุท(Throughput) ของ UDP คือ 7000 Kbps สำหรับ WEP 64 บิต และ 7198 Kbps สำหรับ WEP 128

ราโซล เบค และ อเจส ฮัสเซียน เมียร์ (Gh. Rasool Begh & Ajaz Hussain Mir. 2009) ได้วิจัยถึงผลกระทบของประสิทธิภาพของความปลอดภัยในเครือข่ายไร้สาย (WLAN) ที่ แบนวิธ 11 Mbps โดยหา ทูพุท (throughput), ดีเลย์ (delay) และ แพคเก็ต ลอส (packet loss) ภายใต้ชั้นความปลอดภัยที่แตกต่างกันของโปรโตคอล TCP และ UDP เหตุการณ์ที่ทำการวิจัยคือ มี

คอมพิวเตอร์ที่มีการ์ด Wireless มาตรฐาน IEEE 802.11g หนึ่งเครื่อง(เครื่อง A), คอมพิวเตอร์ที่มีสายแลนค์ หนึ่งเครื่อง(เครื่อง B), Access Point หนึ่งเครื่อง ส่งข้อมูลจากเครื่อง A ไป B จากผลการวิจัยสรุปได้ว่า เมื่อปล่อย ทราฟฟิกขนาด 12 Mb จะทำให้ ทรูพุท(throughput) ลดลงถึงประมาณ 54%ของทุกโปรโตคอลและทุกชั้นความปลอดภัยที่ทดลอง ส่วนทราฟฟิกที่เหลือ (1Mb กับ 5Mb) เมื่อปล่อยออกไปแทบจะไม่ทำให้ทรูพุท(throughput) ลดลง

จากการศึกษางานวิจัยที่เกี่ยวข้องพบว่า ส่วนของการวิจัยภายในประเทศนั้นได้ทำการวิจัยถึงความปลอดภัยบนระบบเครือข่ายไร้สาย โดยเครือข่ายไร้สายมีการเข้ารหัสแบบ WEP (Wired Equivalent Privacy) และทำการหาจำนวน แพคเก็ตและเวลาในการแกะรอยกุญแจ ในส่วนของงานวิจัยในต่างประเทศนั้นได้มีการจำลองระบบในการหาประสิทธิภาพ ทรูพุท (throughput) ของโปรโตคอล TCP และ UDP ซึ่งช่วยสนับสนุนแบบจำลองระบบที่ผู้วิจัยจำลองขึ้นมา



บทที่ 3

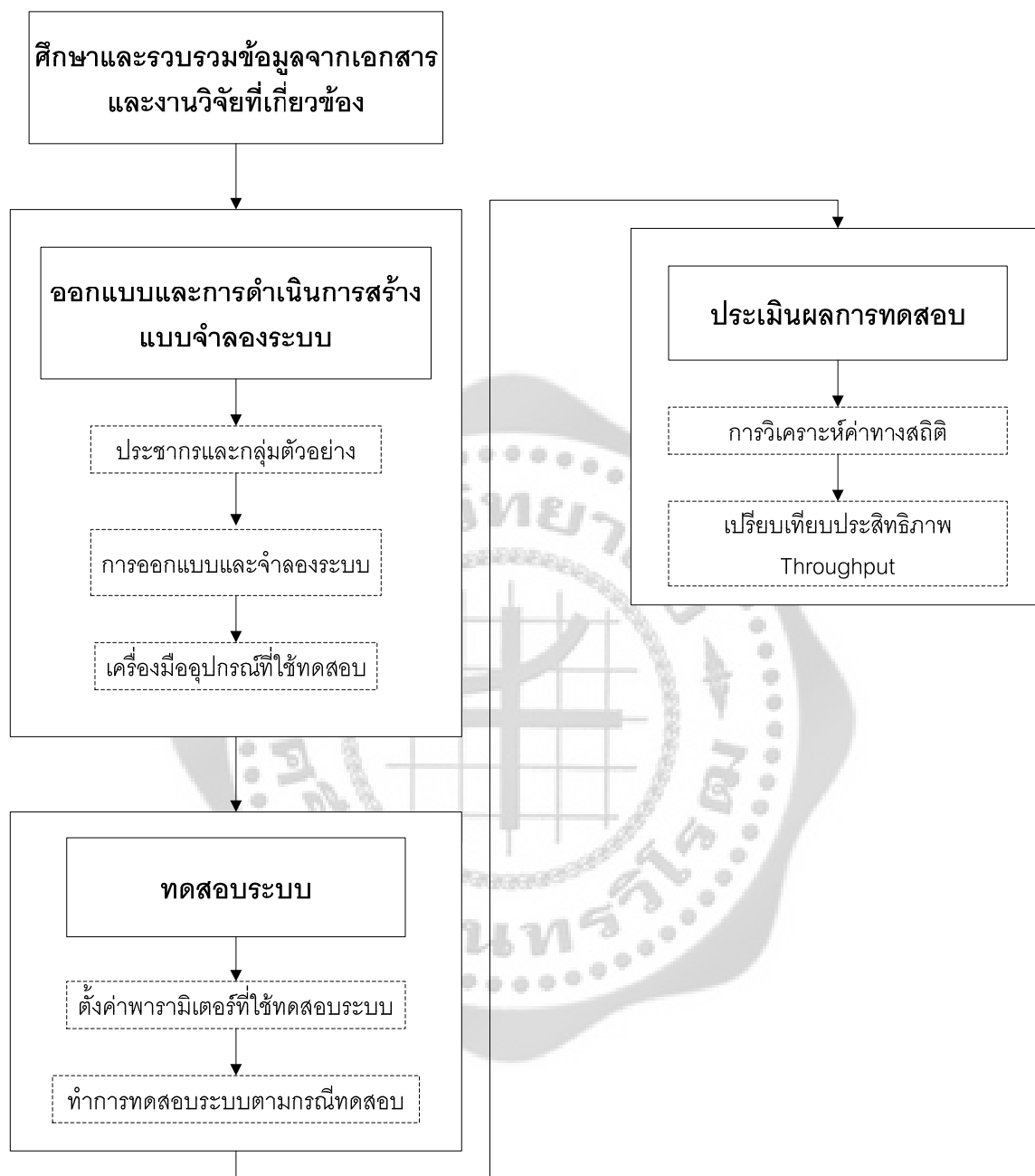
วิธีดำเนินการวิจัย

การดำเนินการวิจัยเรื่องแบบจำลองสถานการณ์สำหรับการประเมินประสิทธิภาพของ
ความปลอดภัยในเครือข่ายไร้สาย มาตรฐาน IEEE802.11g ผู้วิจัยได้ดำเนินการตามขั้นตอน
ดังต่อไปนี้

1. ขั้นตอนการดำเนินงานวิจัย
2. การออกและการดำเนินการสร้างแบบจำลองระบบ
3. การทดสอบระบบ
4. การประเมินผลการทดสอบ



ขั้นตอนการดำเนินงานวิจัย



การออกแบบและดำเนินการสร้างแบบจำลองระบบ

ประชากรและกลุ่มตัวอย่าง

ประชากร

ประชากรในงานวิจัยนี้คือ ประสิทธิภาพในการประมวลผลของโปรโตคอล TCP และ UDP ในชั้นความปลอดภัย 7 ชั้น ได้แก่

- ชั้นความปลอดภัยที่ 1: ไม่มีระบบรักษาความปลอดภัยหรือ เชื่อมโยงเครือข่าย ด้วย SSID เพียงอย่างเดียว

- ชั้นความปลอดภัยที่ 2: ตรวจสอบโดยใช้ MAC Address
- ชั้นความปลอดภัยที่ 3: ตรวจสอบโดยใช้ WEP 64 บิต
- ชั้นความปลอดภัยที่ 4: ตรวจสอบโดยใช้ WEP 128 บิต
- ชั้นความปลอดภัยที่ 5: ตรวจสอบโดยใช้ WPA-PSK Version1
- ชั้นความปลอดภัยที่ 6: ตรวจสอบโดยใช้ WPA-PSK Version2
- ชั้นความปลอดภัยที่ 7: ตรวจสอบโดยใช้ PEAP

กลุ่มตัวอย่าง

กลุ่มตัวอย่างในงานวิจัยนี้คือ ชั้นความปลอดภัยของแบบจำลองระบบทั้ง 5 กรณี ได้แก่

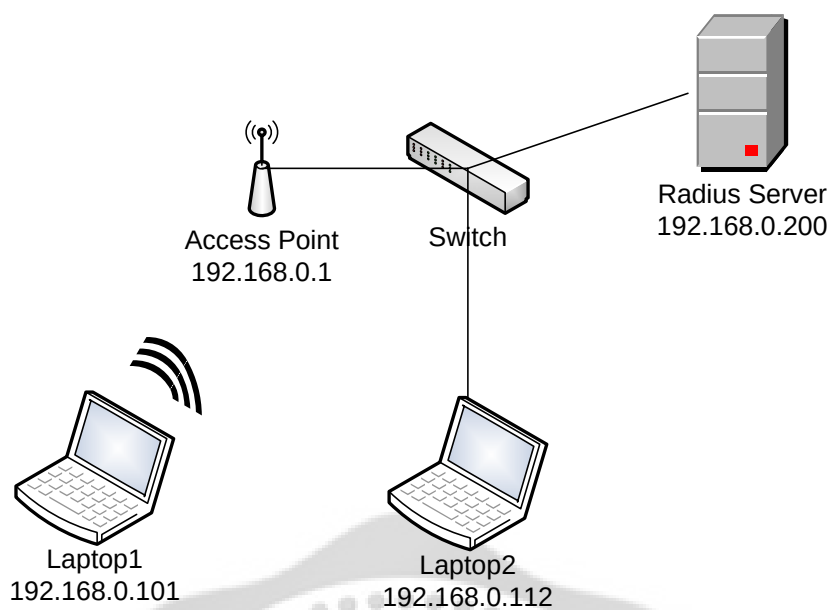
- ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายมีสาย (LAN) แบบ หนึ่งต่อหนึ่ง (Single Point)
- ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายไร้สาย (WLAN) แบบ หนึ่งจุด (Single Point)
- ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายมีสาย (LAN) แบบ หลายจุด (Multiple Point)
- เครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายไร้สาย (WLAN) แบบ หลายจุด (Multiple Point)
- เครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายมีสาย (LAN)และไร้สาย (WLAN)

การออกแบบและการจำลองระบบ

ในการออกแบบระบบผู้วิจัยได้ทำการศึกษาทฤษฎีและรูปแบบการใช้งานของระบบเครือข่ายไร้สาย (WLAN) บนมาตรฐาน IEEE 11g ซึ่งได้คำนึงถึงการรองรับของระบบกับอุปกรณ์ในการเชื่อมต่อ และได้ออกแบบระบบตามสถานการณ์ให้ครอบคลุมการใช้งานดังต่อไปนี้

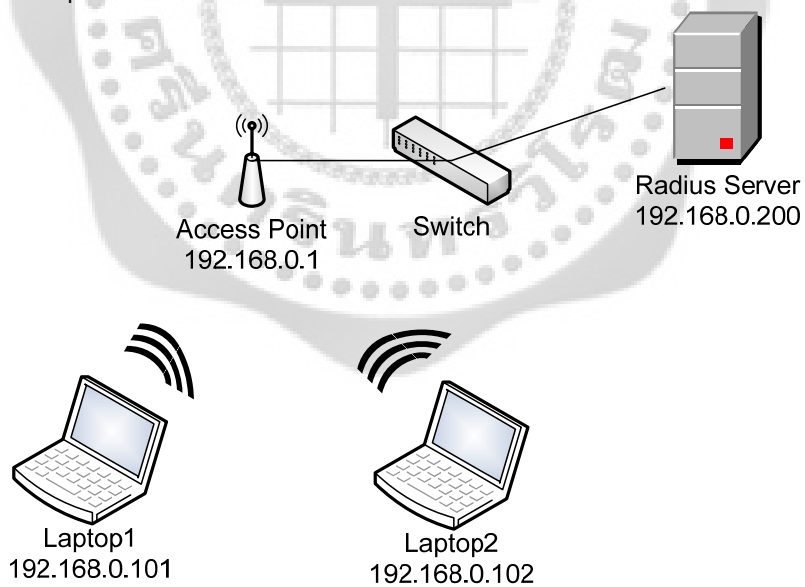
1. รูปแบบจำลองของระบบ

- 1.1 ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายมีสาย (LAN) แบบ หนึ่งต่อหนึ่ง (Single Point)



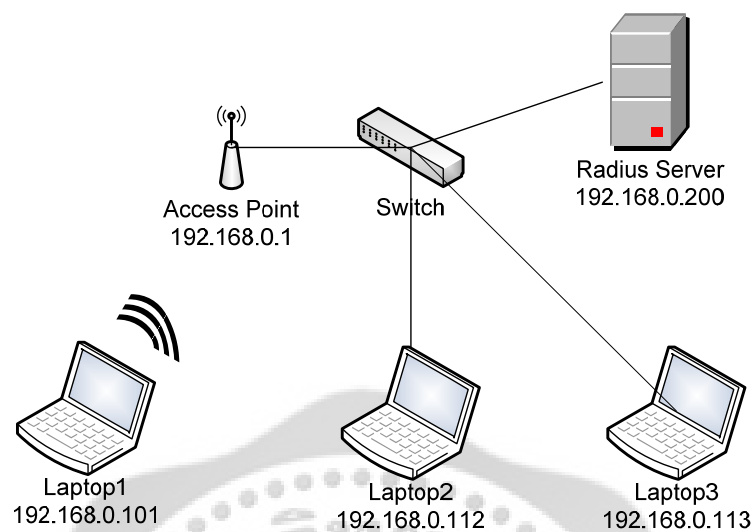
ภาพประกอบ 12 WLAN to LAN แบบ Single Point

1.2 ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายไร้สาย (WLAN) แบบ หนึ่งจุด (Single Point)



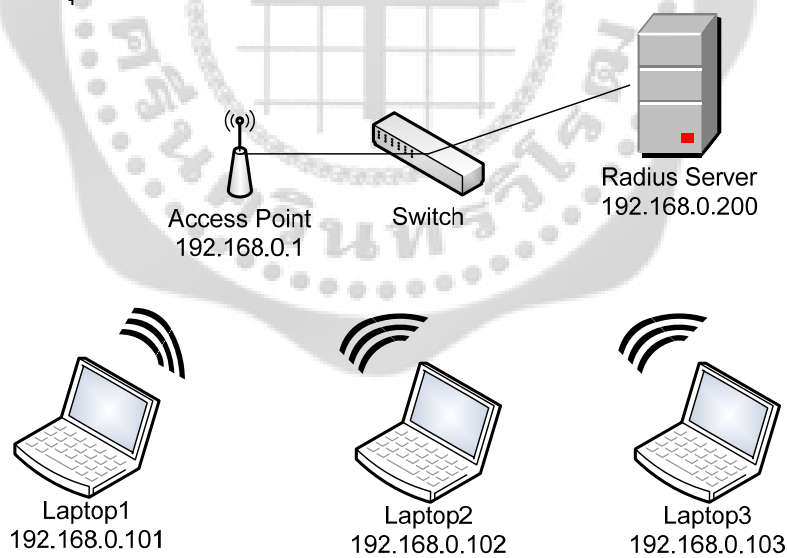
ภาพประกอบ 13 WLAN to WLAN แบบ Single Point

1.3 ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายมีสาย (LAN) แบบ หลายจุด (Multiple Point)



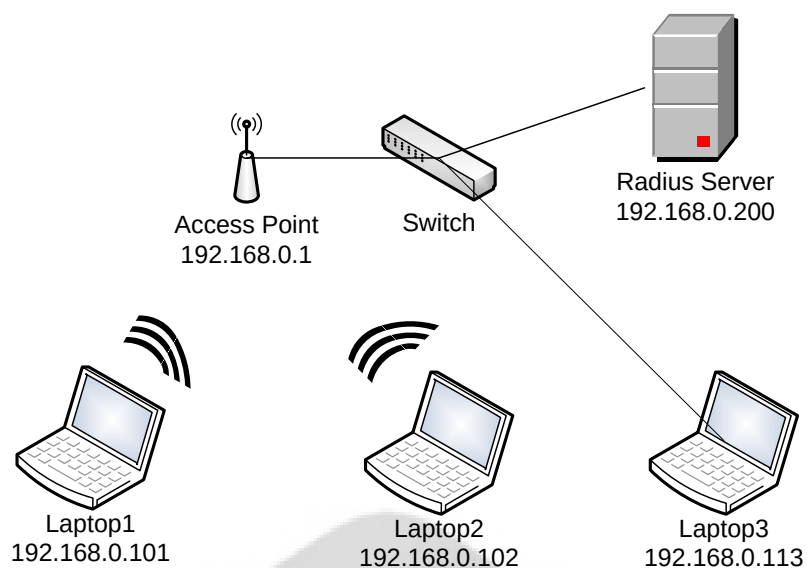
จากภาพประกอบ 14 WLAN to LAN แบบ Multiple Point

1.4 ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายไร้สาย (WLAN) แบบ หลายจุด (Multiple Point)



ภาพประกอบ 15 WLAN to WLAN แบบ Multiple Point

1.5 ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายมีสาย (LAN)และไร้สาย (WLAN)



ภาพประกอบ 16 WLAN to LAN and WLAN

2. ชั้นความปลอดภัยที่ใช้ในการทดสอบ มีดังนี้

2.1 ชั้นความปลอดภัยที่ 1: ไม่มีระบบรักษาความปลอดภัยหรือ เชื่อมโยง
เครือข่ายด้วย SSID เพียงอย่างเดียว

2.2 ชั้นความปลอดภัยที่ 2: ตรวจสอบโดยใช้ MAC Address

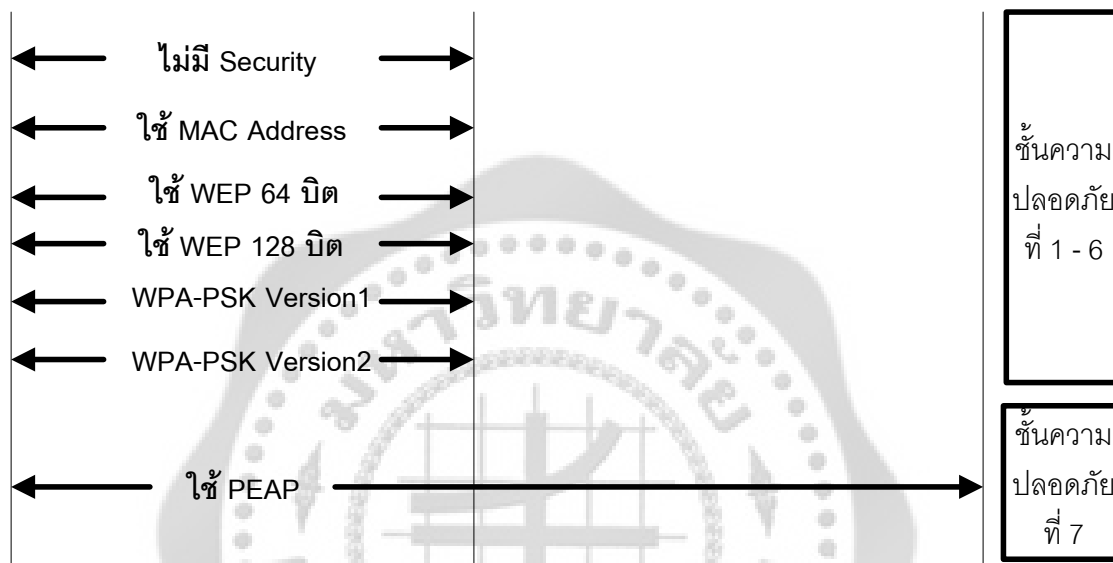
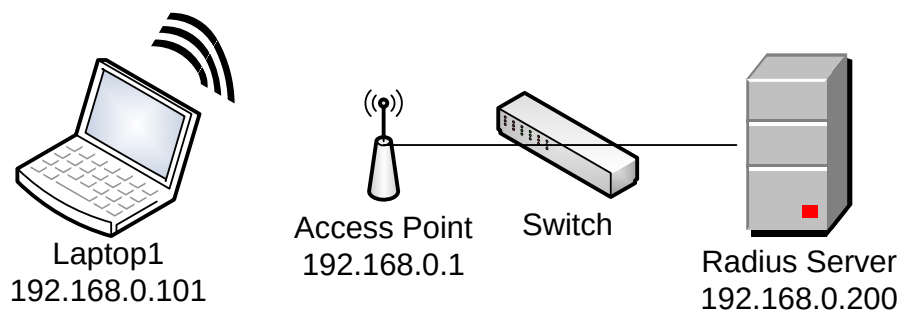
2.3 ชั้นความปลอดภัยที่ 3: ตรวจสอบโดยใช้ WEP 64 บิต

2.4 ชั้นความปลอดภัยที่ 4: ตรวจสอบโดยใช้ WEP 128 บิต

2.5 ชั้นความปลอดภัยที่ 5: ตรวจสอบโดยใช้ WPA-PSK Version1

2.6 ชั้นความปลอดภัยที่ 6: ตรวจสอบโดยใช้ WPA-PSK Version2

2.7 ชั้นความปลอดภัยที่ 7: ตรวจสอบโดยใช้ PEAP



ภาพประกอบ 17 IEEE 802.1x model logical flow

3. ชนิดของทราฟฟิก (Traffic)

ชนิดของทราฟฟิก (Traffic) ได้เลือก โปรโตคอล TCP และ UDP เพราะทั้งสองโปรโตคอล เป็นพื้นฐานในการรับส่งข้อมูลระหว่างระบบคอมพิวเตอร์

4. ผลรวมจำนวนของแพ็คเกจ (Packet)

จากการประเมินและทดสอบเบื้องต้นพบว่า ช่วงระหว่าง 10,000 ถึง 60,000 เป็นช่วงที่เหมาะสมที่จะใช้ทดสอบ (Baghaei & Hunt. 2004) ดังนั้นจึงเลือกค่าที่สูงที่สุดคือ 60,000 สำหรับการทดสอบในครั้งนี้

5. ความยาวของแพ็คเกจ (Packet)

ผู้วิจัยจะสุ่มความยาวของแพ็คเกจ (Packet) จนเต็มช่วง 40-3550 เนื่องจากเป็นช่วงนี้มีความเหมาะสมของไอพีแพ็คเกจ (IP Packet), มีการกระจายตัวดี และสามารถวิเคราะห์แบบเต็มความยาวของขนาดของแพ็คเกจ (Packet) ได้ ซึ่งในช่วงดังกล่าวจะใช้ขนาดข้อมูลในการส่ง 100 MB

เครื่องมืออุปกรณ์ที่ใช้ทดสอบ

ในการทดสอบระบบผู้วิจัยได้ทำการใช้เครื่องมือทั้งที่เป็น ฮาร์ดแวร์ (Hardware) และ ซอฟต์แวร์ (Software) โดยมีรายละเอียดดังนี้

1. ฮาร์ดแวร์ (Hardware)

1.1 เครื่องคอมพิวเตอร์โน้ตบุ๊ก IBM รุ่น R400 ใช้สำหรับการส่งข้อมูล จำนวน 1

เครื่อง

- Intel® Core™2 Duo CPU P7370 @ 2.00GHz 1.99GHz
- 2.00 GB of RAM
- Windows XP Service Pack3
- 11b/g/n Wireless LAN Mini-PCI Express Adapter II

1.2 เครื่องคอมพิวเตอร์โน้ตบุ๊ก IBM รุ่น T400 ใช้สำหรับการรับข้อมูล จำนวน 2

เครื่อง

- Intel® Core™2 Duo CPU P8600 @ 2.40GHz 2.40GHz
- 2.00 GB of RAM
- Windows 7 Service Pack1
- Intel® WiFi Link 5300 AGN

1.3 เครื่องคอมพิวเตอร์เซิร์ฟเวอร์ ใช้สำหรับทำ RADIUS Server

- Windows Server 2003
- 1 GB of RAM

1.4 Wireless Access Point Linksys WAP54G

1.5 สายแลนรองรับการรับส่งข้อมูล 100 Mbps

2. ซอฟต์แวร์ (Software)

2.1 IP Traffic generator เป็นซอฟต์แวร์ที่ใช้ในการทดสอบระบบ เหตุที่เลือกซอฟต์แวร์นี้เนื่องจาก

- เหมาะสำหรับเครือข่ายไร้สาย
- สามารถรองรับเครือข่ายมาตรฐาน IEEE 802.11g
- เลือกโปรโตคอล TCP และ UDP ในการทดสอบได้

2.2 Wireshark เป็นซอฟต์แวร์ที่ใช้ในการวัดทราฟฟิกของระบบ

การทดสอบระบบ

ในการทดสอบระบบจะใช้แบบจำลองระบบที่ผู้วิจัยได้ทำการออกแบบมาแล้วในการทดสอบ โดยในแต่ละแบบจำลองจะมีรายละเอียดในการทดสอบดังนี้

ตั้งค่าพารามิเตอร์ที่ใช้ทดสอบระบบ

1. จำนวนของแพ็คเกจ (Packet Generator Parameters) 60,000
2. ยาวของแพ็คเกจ (Packet Data size) 40 – 3550 byte

The screenshot shows the 'IP Traffic - Test & Measure' software interface in 'Parameters in unitary testing mode'. The interface is divided into several sections:

- Mode 1: Using the Internal Data Generator**
 - Step 1: Select the traffic generator type**
 - Packets number (0 to 99,999,999): 60000
 - Packet Contents (00 to FF hexa byte):
 - Fix: 5A
 - Random: 41 min, 7A max
 - Alternate: 30 value-1, 31 value-2
 - Increasing / Decreasing: 30 min, 39 max, 01 step
 - Law: data volume to send: Default
 - Mathematical law: Uniform law, Range: [9.77 KB, 2.38 MB]
 - File to send: Browse
 - Loop counter (1 to 99): 1
 - Idle time between each loop (0 to 99 s): 0
 - Step 2: Specify Data Size and packets parameters**
 - UDP Data Size (1 to 65,507 bytes):
 - Fix: 1460
 - Random: 40 min, 3550 max
 - Alternate: 128 size-1, 1460 size-2
 - Increasing / Decreasing: 1 min, 1460 max, 1 step
 - Inter Packet Delay (0 to 9,999 ms):
 - Fix: 0 (See Forewarnings menu please)
 - Random: 10 min, 500 max
 - Alternate: 10 value-1, 100 value-2
 - Increasing / Decreasing: 10 min, 200 max, 10 step
 - Mathematical law: Default
 - Step 3 (Optional): Activate a throughput limit**
 - When one of these two options is selected, "IP Traffic - Test & Measure" generates the traffic in best effort to respect the throughput chosen.
 - Use value: 54000
 - Mean Throughput (8 to 999,999 Kb/s): Inter Packet Delay automatically adjusted by IP Traffic
 - Mean Packet Throughput (1 to 99,999 Pkts/s): Use value (except for TCP connection): 10
- Mode 2: Using the External Data Source Generator**
 - Filename: Browse
 - Loop counter: 1
 - Idle time between each loop (sec.): 0
- Options**
 - Timecode (RTT) option: If enabled, IP Traffic adds 14 bytes to the "Data Size" defined by the Mode 1 or Mode 2 settings. Yes No
 - DSCP (1 hexa byte): Value (0x00 to 0xF): 00
 - Time To Live (TTL): Value: 00
 - Save incoming data traffic (needs remote in echo mode): Browse
 - Save generated traffic into file (only data are saved): C:\Documents and Settings\1016158\Desktop\WEP_Send.t Browse

ภาพประกอบ 18 ค่าพารามิเตอร์ที่ใช้ทดสอบระบบ

ทำการทดสอบระบบตามกรณีทดสอบ

ในการจำลองระบบเครือข่ายไร้สายมาตรฐาน IEEE802.11g เพื่อทำการทดสอบหา throughput ผู้วิจัยได้แบ่งแบบจำลองออกเป็น 5 กรณี ดังนี้

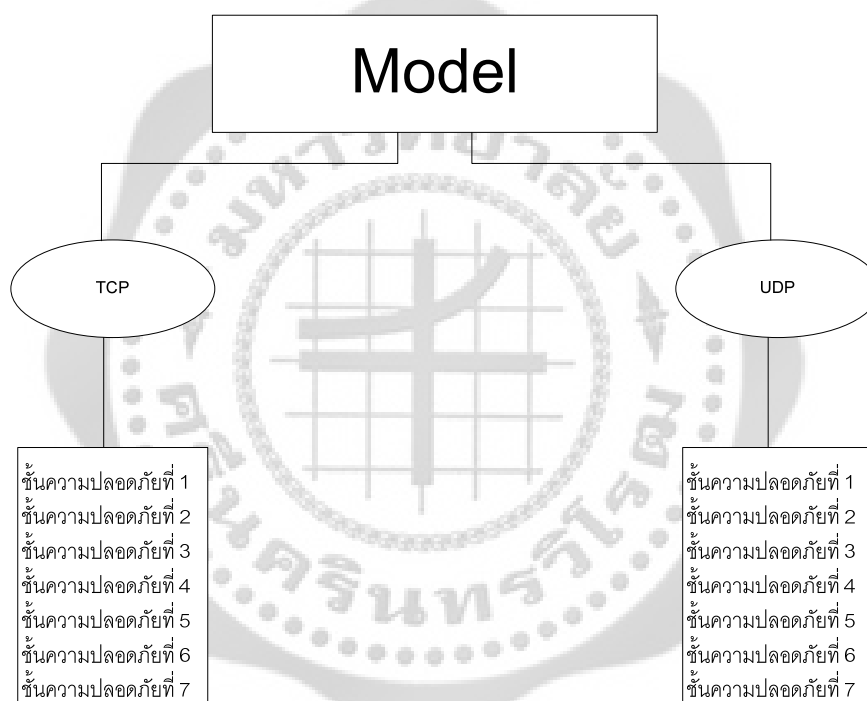
1. ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายมีสาย (LAN) แบบ หนึ่งต่อหนึ่ง (Single Point)
2. ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายไร้สาย (WLAN) แบบ หนึ่งจุด (Single Point)

3. ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายมีสาย (LAN) แบบ หลายจุด (Multiple Point)

4. ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายไร้สาย (WLAN) แบบ หลายจุด (Multiple Point)

5. ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายมีสาย (LAN) และ ไร้สาย (WLAN)

วิเคราะห์ประสิทธิภาพในการประมวลผล (throughput) ในแต่ละกรณีทดสอบ โดย เปรียบเทียบระหว่างโปรโตคอล TCP และ UDP ในแต่ละชั้นความปลอดภัยทั้ง 7 ชั้นความปลอดภัย ทำการทดสอบซ้ำกัน 10 ครั้ง บันทึกผลการทดสอบ



ภาพประกอบ 19 แบบการทดสอบระบบ

การประเมินผลการทดสอบ

นำผลการทดสอบจากข้อ 3.2 มาประเมินผลการทดสอบดังนี้

1. การวิเคราะห์ค่าทางสถิติ

สถิติพื้นฐาน

การวิเคราะห์ข้อมูลทางสถิติจะมุ่งเน้นสถิติเชิงพรรณนาในการวัดค่ากลางของข้อมูล โดยใช้ค่าเฉลี่ยเลขคณิต (Arithmetic Mean) หรือค่าเฉลี่ย (Mean) วัดการกระจายของข้อมูลโดยใช้ส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation) โดยมีขั้นตอนดังต่อไปนี้

การหาค่าเฉลี่ยเลขคณิต ดังสมการที่ 3.1

$$\bar{X} = \frac{\sum_{i=1}^n Xi}{n}$$

$\bar{X}$	=	ค่าเฉลี่ยของประสิทธิภาพในแต่ละกรณีของชั้นความปลอดภัยในแต่ละครั้ง
$\sum_{i=1}^n Xi$	=	ผลรวมของประสิทธิภาพในแต่ละกรณีของชั้นความปลอดภัยในแต่ละครั้ง
n	=	จำนวนครั้งของการทดสอบในแต่ละกรณี

2. เปรียบเทียบประสิทธิภาพในการประมวลผล (Throughput)

นำผลที่ได้มาวิเคราะห์ หาประสิทธิภาพของระบบ โดยวัดผลจาก ความเร็วในการรับ-ส่งข้อมูล เวลาที่ใช้ในการส่งข้อมูลจำนวน 100 MB และปริมาณการสูญหายของข้อมูลในขณะส่งข้อมูล (Data lose) บนโปรโตคอล TCP และ UDP ที่ชั้นความปลอดภัยทั้ง 7 ชั้น

บทที่ 4

ผลการดำเนินงานวิจัย

งานวิจัยนี้มีวัตถุประสงค์เพื่อทดสอบแบบจำลองของรูปแบบระบบรักษาความปลอดภัยในเครือข่าย WLAN (Wireless LAN) บนมาตรฐาน IEEE 802.11g ซึ่งจากการดำเนินการวิจัยสามารถแสดงผลและประเมินผลการทดสอบประสิทธิภาพของระบบบนแบบจำลองของรูปแบบระบบรักษาความปลอดภัยในเครือข่าย WLAN (Wireless LAN) บนมาตรฐาน IEEE 802.11g

ผลการทดสอบและประเมินประสิทธิภาพของระบบ

จากการทดสอบแบบจำลองระบบทั้ง 5 รูปแบบ โดยใช้ ซอร์ฟแวร์ Traffic generator ในการทดสอบระบบและ ซอร์ฟแวร์ Wireshark ในการหาประสิทธิภาพของระบบ โดยวัดผลจากความเร็วในการรับ-ส่งข้อมูล เวลาที่ใช้ในการส่งข้อมูลจำนวน 100 MB และปริมาณการสูญหายของข้อมูลในขณะส่งข้อมูล (Data lose) บนโปรโตคอล TCP และ UDP ที่ชั้นความปลอดภัยทั้ง 7 ชั้น โดยวัดได้ผลการทดสอบดังนี้

4.1 ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายมีสาย (LAN) แบบหนึ่งต่อหนึ่ง (Single Point)

ตาราง 2 รูปแบบทดสอบที่ 1: ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายมีสาย (LAN) แบบ หนึ่งต่อหนึ่ง (Single Point) Mbps ของโปรโตคอล TCP และ UDP

รูปแบบทดสอบที่ 1	TCP			UDP		
	Speed (Mbps)	Time (s)	Lose (%)	Speed (Mbps)	Time (s)	Lose (%)
ชั้นความปลอดภัยที่ 1: ไม่มีระบบรักษาความปลอดภัยหรือ เชื่อมโยงเครือข่ายด้วยSSID	27.83	28.74	0.00	30.59	26.15	0.00
ชั้นความปลอดภัยที่ 2: ตรวจสอบโดยใช้ MAC Address	24.85	32.19	0.00	27.43	29.16	0.11
ชั้นความปลอดภัยที่ 3: ตรวจสอบโดยใช้ WEP 64 บิต	23.60	33.90	0.00	25.99	30.78	0.07
ชั้นความปลอดภัยที่ 4: ตรวจสอบโดยใช้ WEP 128 บิต	23.50	34.04	0.00	25.51	31.37	0.35
ชั้นความปลอดภัยที่ 5: ตรวจสอบโดยใช้ WPA-PSK Version1	23.42	34.16	0.00	25.16	31.80	0.38
ชั้นความปลอดภัยที่ 6: ตรวจสอบโดยใช้ WPA-PSK Version2	20.91	38.25	0.00	24.33	32.88	0.12
ชั้นความปลอดภัยที่ 7: ตรวจสอบโดยใช้ PEAP	21.14	37.85	0.00	24.93	32.10	0.37

จากผลการทดสอบประสิทธิภาพของระบบในรูปแบบที่ 1 ในขณะที่รับ-ส่งข้อมูลของโปรโตคอล TCP พบว่าความเร็วและเวลาในการรับ-ส่งข้อมูล มีประสิทธิภาพต่ำกว่ามาตรฐาน IEEE 802.11g และโปรโตคอล UDP มีประสิทธิภาพโดยรวมต่ำกว่ามาตรฐาน IEEE 802.11g ยกเว้นประสิทธิภาพของ Data lose บนชั้นความปลอดภัยที่ 1 ของโปรโตคอล UDP ที่ได้ตามมาตรฐาน

ถ้าเปรียบเทียบในแต่ละชั้นความปลอดภัยของระบบในรูปแบบที่ 1 โปรโตคอล TCP ของชั้นความปลอดภัยที่ 1 มีประสิทธิภาพโดยรวมสูงสุด รองลงมาคือ ชั้นความปลอดภัยที่ 2, 3, 4, 5, 7 และ 6 ตามลำดับ ส่วนโปรโตคอล UDP ได้ผลประสิทธิภาพโดยรวมไปในทางเดียวกันกับโปรโตคอล TCP และโปรโตคอล UDP มีประสิทธิภาพโดยรวมของระบบสูงกว่าโปรโตคอล TCP ทุกระดับชั้นความปลอดภัย ยกเว้นประสิทธิภาพของ Data lose ที่มีประสิทธิภาพต่ำกว่าโปรโตคอล TCP

4.2 ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายไร้สาย (WLAN) แบบ หนึ่งจุด (Single Point)

ตาราง 3 รูปแบบทดสอบที่ 2: ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายไร้สาย (WLAN) แบบ หนึ่งจุด (Single Point) ของ TCP และ UDP

รูปแบบทดสอบที่ 2	TCP			UDP		
	Speed (Mbps)	Time (s)	Lose (%)	Speed (Mbps)	Time (s)	Lose (%)
ชั้นความปลอดภัยที่ 1: ไม่มีระบบรักษาความปลอดภัยหรือ เชื่อมโยงเครือข่ายด้วยSSID	12.46	64.20	0.00	28.80	27.78	10.03
ชั้นความปลอดภัยที่ 2: ตรวจสอบโดยใช้ MAC Address	12.40	64.50	0.00	15.02	53.28	13.67
ชั้นความปลอดภัยที่ 3: ตรวจสอบโดยใช้ WEP 64 บิต	11.50	69.55	0.00	14.38	55.62	18.38
ชั้นความปลอดภัยที่ 4: ตรวจสอบโดยใช้ WEP 128 บิต	11.01	72.69	0.00	13.84	57.81	17.21
ชั้นความปลอดภัยที่ 5: ตรวจสอบโดยใช้ WPA-PSK Version1	10.37	77.18	0.00	12.79	62.55	16.06
ชั้นความปลอดภัยที่ 6: ตรวจสอบโดยใช้ WPA-PSK Version2	7.84	102.04	0.00	11.10	72.10	14.96
ชั้นความปลอดภัยที่ 7: ตรวจสอบโดยใช้ PEAP	10.34	77.37	0.00	12.09	66.18	14.92

จากผลการทดสอบประสิทธิภาพของระบบในรูปแบบที่ 2 ในขณะรับ-ส่งข้อมูลของโปรโตคอล TCP และ UDP พบว่าประสิทธิภาพโดยรวมในการรับ-ส่งข้อมูลมีประสิทธิภาพต่ำกว่ามาตรฐาน IEEE 802.11g ยกเว้นประสิทธิภาพของ Data lose บนทุกชั้นความปลอดภัย ของโปรโตคอล TCP ที่ได้ตามมาตรฐาน

ถ้าเปรียบเทียบในแต่ละชั้นความปลอดภัยของระบบในรูปแบบที่ 2 คล้ายกับ รูปแบบที่ 1 ทั้งในโปรโตคอล TCP และ UDP คือ ชั้นความปลอดภัยที่ 1 มีประสิทธิภาพสูงสุด และชั้นความปลอดภัยที่ 6 ต่ำที่สุด ยกเว้นประสิทธิภาพของ Data lose 10-18% ซึ่งที่มีประสิทธิภาพต่ำกว่าโปรโตคอล TCP

4.3 ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายมีสาย (LAN) แบบ หลายจุด (Multiple Point)

ตาราง 4 รูปแบบทดสอบที่ 3: ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายมีสาย (LAN) แบบ หลายจุด (Multiple Point) ของ TCP และ UDP

รูปแบบทดสอบที่ 3	TCP			UDP		
	Speed (Mbps)	Time (s)	Lose (%)	Speed (Mbps)	Time (s)	Lose (%)
ชั้นความปลอดภัยที่ 1: ไม่มีระบบรักษาความปลอดภัยหรือ เชื่อมโยงเครือข่ายด้วยSSID	14.12	56.66	0.00	29.96	26.70	68.17
ชั้นความปลอดภัยที่ 2: ตรวจสอบโดยใช้ MAC Address	13.06	61.27	0.00	29.30	27.30	67.87
ชั้นความปลอดภัยที่ 3: ตรวจสอบโดยใช้ WEP 64 บิต	12.69	63.05	0.00	27.93	28.64	73.84
ชั้นความปลอดภัยที่ 4: ตรวจสอบโดยใช้ WEP 128 บิต	24.49	32.67	0.00	27.63	28.96	67.95
ชั้นความปลอดภัยที่ 5: ตรวจสอบโดยใช้ WPA-PSK Version1	12.23	65.40	0.00	27.75	28.83	70.56
ชั้นความปลอดภัยที่ 6: ตรวจสอบโดยใช้ WPA-PSK Version2	11.22	71.33	0.00	23.59	33.91	70.10
ชั้นความปลอดภัยที่ 7: ตรวจสอบโดยใช้ PEAP	11.48	69.67	0.00	27.83	28.74	69.36

จากผลการทดสอบประสิทธิภาพของระบบในรูปแบบที่ 3 ในขณะที่รับ-ส่งข้อมูลของโปรโตคอล TCP และ UDP พบว่าประสิทธิภาพโดยรวมในการรับ-ส่งข้อมูลมีประสิทธิภาพเป็นไปในทิศทางเดียวกันกับรูปแบบที่ 2 แต่ประสิทธิภาพของ Data lose 67-74% ซึ่งสูงมากกว่า โปรโตคอล TCP

4.4 ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายไร้สาย (WLAN) แบบ หลายจุด (Multiple Point)

ตาราง 5 รูปแบบทดสอบที่ 4: ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายไร้สาย (WLAN) แบบ หลายจุด (Multiple Point) ของ TCP และ UDP

รูปแบบทดสอบที่ 4	TCP			UDP		
	Speed (Mbps)	Time (s)	Lose (%)	Speed (Mbps)	Time (s)	Lose (%)
ชั้นความปลอดภัยที่ 1: ไม่มีระบบรักษาความปลอดภัยหรือ เชื่อมโยงเครือข่ายด้วยSSID	5.80	138.05	0.00	27.62	28.97	77.56
ชั้นความปลอดภัยที่ 2: ตรวจสอบโดยใช้ MAC Address	5.67	141.03	0.00	26.95	29.68	79.57
ชั้นความปลอดภัยที่ 3: ตรวจสอบโดยใช้ WEP 64 บิต	5.52	144.82	0.00	25.60	31.25	87.00
ชั้นความปลอดภัยที่ 4: ตรวจสอบโดยใช้ WEP 128 บิต	5.30	150.86	0.00	24.53	32.62	82.62
ชั้นความปลอดภัยที่ 5: ตรวจสอบโดยใช้ WPA-PSK Version1	5.25	152.45	0.00	25.41	31.49	82.32
ชั้นความปลอดภัยที่ 6: ตรวจสอบโดยใช้ WPA-PSK Version2	3.62	220.75	0.00	23.94	33.41	85.47
ชั้นความปลอดภัยที่ 7: ตรวจสอบโดยใช้ PEAP	4.95	161.63	0.00	26.42	30.28	81.08

จากผลการทดสอบประสิทธิภาพของระบบในรูปแบบที่ 4 ในขณะที่รับ-ส่งข้อมูลของโปรโตคอล TCP และ UDP พบว่าประสิทธิภาพโดยรวมในการรับ-ส่งข้อมูลมีประสิทธิภาพเป็นไปในทิศทางเดียวกันกับรูปแบบที่ 2 แต่ประสิทธิภาพของ Data lose 77-87% ซึ่งสูงมากกว่า โปรโตคอล TCP

4.5 เครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายมีสาย (LAN)และไร้สาย (WLAN)

ตาราง 6 รูปแบบทดสอบที่ 5: เครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายมีสาย (LAN) และไร้สาย (WLAN) ของ TCP และ UDP

รูปแบบทดสอบที่ 5	TCP			UDP		
	Speed (Mbps)	Time (s)	Lose (%)	Speed (Mbps)	Time (s)	Lose (%)
ชั้นความปลอดภัยที่ 1: ไม่มีระบบรักษาความปลอดภัยหรือ เชื่อมโยงเครือข่ายด้วยSSID	8.68	92.12	0.00	27.37	29.23	67.05
ชั้นความปลอดภัยที่ 2: ตรวจสอบโดยใช้ MAC Address	8.51	94.06	0.00	26.09	30.67	67.05
ชั้นความปลอดภัยที่ 3: ตรวจสอบโดยใช้ WEP 64 บิต	8.18	97.76	0.00	24.82	32.23	71.03
ชั้นความปลอดภัยที่ 4: ตรวจสอบโดยใช้ WEP 128 บิต	7.66	104.49	0.00	22.87	34.98	66.74
ชั้นความปลอดภัยที่ 5: ตรวจสอบโดยใช้ WPA-PSK Version1	7.56	105.79	0.00	24.60	32.53	68.73
ชั้นความปลอดภัยที่ 6: ตรวจสอบโดยใช้ WPA-PSK Version2	6.01	133.13	0.00	22.50	35.55	68.58
ชั้นความปลอดภัยที่ 7: ตรวจสอบโดยใช้ PEAP	7.29	109.75	0.00	25.61	31.24	67.09

จากผลการทดสอบประสิทธิภาพของระบบในรูปแบบที่ 4 ในขณะที่รับ-ส่งข้อมูลของโปรโตคอล TCP และ UDP พบว่าประสิทธิภาพโดยรวมในการรับ-ส่งข้อมูลมีประสิทธิภาพเป็นไปในทิศทางเดียวกันกับรูปแบบที่ 2 แต่ประสิทธิภาพของ Data lose 66-71% ซึ่งสูงมากกว่า โปรโตคอล TCP

จากผลการทดสอบประสิทธิภาพของระบบทั้ง 5 แบบการทดสอบ พบว่า รูปแบบการทดสอบที่ 1 มีประสิทธิภาพโดยรวมสูงที่สุด และรูปแบบการทดสอบที่ 5 มีประสิทธิภาพโดยรวมต่ำที่สุด โดยโปรโตคอล TCP จะไม่มีการสูญเสียข้อมูล (Data lose) ในทั้ง 5 แบบการทดสอบ

และเมื่อเปรียบเทียบชั้นความปลอดภัยพบว่า ชั้นความปลอดภัยที่ 1 ของโปรโตคอล TCP และ UDP จะมีประสิทธิภาพโดยรวมสูงที่สุด ในขณะที่ชั้นความปลอดภัยที่ 6 จะมีประสิทธิภาพโดยรวมต่ำที่สุด

บทที่ 5

สรุปผลการวิจัย อภิปรายผล และข้อเสนอแนะ

การวิจัยเรื่องแบบจำลองสถานการณ์สำหรับการประเมินประสิทธิภาพในการประมวลผลของความปลอดภัยในเครือข่ายไร้สาย มาตรฐาน IEEE802.11g สามารถสรุปผลโดยมีรายละเอียดตามหัวข้อต่าง ๆ ดังนี้

1. สรุปผลการวิจัย
2. อภิปรายผลการวิจัย
3. ข้อเสนอแนะ
 - 3.1 ข้อจำกัดของการวิจัย
 - 3.2 ข้อเสนอแนะสำหรับการนำผลการวิจัยไปใช้งาน
 - 3.3 ข้อเสนอแนะสำหรับการวิจัยต่อไป

1. สรุปผลการวิจัย

จากผลการทดสอบประสิทธิภาพของระบบทั้ง 5 รูปแบบ โดยใช้ ซอร์ฟแวร์ Traffic generator ในการทดสอบระบบและ ซอร์ฟแวร์ Wireshark ในการวัดประสิทธิภาพของระบบ โดยวัดผลจาก ความเร็วในการรับ-ส่งข้อมูล เวลาที่ใช้ในการส่งข้อมูลจำนวน 100 MB และปริมาณการสูญหายของข้อมูลในขณะส่งข้อมูล (Data lose) บนโปรโตคอล TCP และ UDP ที่ชั้นความปลอดภัยทั้ง 7 ชั้น สรุปได้ว่า

1. ในขณะรับ-ส่งข้อมูลของโปรโตคอล TCP และ UDP ในทุกรูปแบบทดสอบ พบว่าความเร็วและเวลาในการรับ-ส่งข้อมูล มีประสิทธิภาพต่ำกว่ามาตรฐาน IEEE 802.11g ทุกรูปแบบทดสอบ
2. ความเร็วและเวลาในการรับ-ส่งข้อมูล ของโปรโตคอล UDP มีประสิทธิภาพสูงสุดในรูปแบบทดสอบที่ 3
3. ไม่พบ Data lose บนโปรโตคอล TCP ในขณะรับ-ส่งข้อมูลในทุกรูปแบบการทดสอบทดสอบ
4. Data lose บนโปรโตคอล UDP ในรูปแบบทดสอบที่ 4 มีค่าสูงกว่ารูปแบบทดสอบอื่นๆ โดยค่าที่สูงสุดอยู่ที่ 87%
5. ประสิทธิภาพโดยรวมบนโปรโตคอล TCP ทั้ง 5 รูปแบบการทดสอบ ในแต่ละชั้นความปลอดภัยเป็นไปในทิศทางเดียวกัน คือ รูปแบบการทดสอบที่ 3 มีประสิทธิภาพสูงสุดถึง 23-28Mbps รองลงมาคือ รูปแบบการทดสอบที่ 1, 5, 2 และ 4 ตามลำดับ และชั้นความปลอดภัยที่ 1 มีประสิทธิภาพสูงสุด รองลงมาคือ ชั้นความปลอดภัยที่ 2, 3, 4, 5, 7 และ 6 ตามลำดับ

6. ประสิทธิภาพพบโดยรวมโปรโตคอล UDP ทั้ง 5 รูปแบบการทดสอบ ในแต่ละชั้นความปลอดภัยมีรูปแบบของประสิทธิภาพคล้ายคลึงกัน กล่าวคือ รูปแบบการทดสอบที่ 3 มีประสิทธิภาพสูงสุด รองลงมาคือ รูปแบบการทดสอบที่ 4, 5, 1 และ 2 ตามลำดับ ยกเว้นชั้นความปลอดภัยที่ 6 ซึ่ง รูปแบบการทดสอบที่ 4 มีประสิทธิภาพสูงสุด รองลงมาคือ รูปแบบการทดสอบที่ 3, 5, 1 และ 2 ตามลำดับ พบว่ารูปแบบการทดสอบที่ 3-5 มีประสิทธิภาพสูงถึง 50-60 Mbps ซึ่งมากกว่าโปรโตคอล TCP ประมาณ 50-85% และ ชั้นความปลอดภัยที่ 1 มีประสิทธิภาพสูงสุด และชั้นความปลอดภัยที่ 6 มีประสิทธิภาพต่ำสุด

2. อภิปรายผลการวิจัย

การอภิปรายผลของแบบจำลองสถานการณ์สำหรับการประเมินประสิทธิภาพของความปลอดภัยในเครือข่ายไร้สาย มาตรฐาน IEEE 802.11g สามารถแบ่งการอภิปรายผลการวิจัยได้ดังนี้

2.1 เมื่อพิจารณาผลทดสอบประสิทธิภาพการรับ-ส่งข้อมูลของโปรโตคอล TCP และ UDP พบว่าโปรโตคอล TCP และ UDP มีประสิทธิภาพต่ำกว่ามาตรฐาน IEEE 802.11g ทุกรูปแบบทดสอบ เนื่องจากสภาพแวดล้อมมีผลต่อประสิทธิภาพ เช่น สัญญาณรบกวน นอกจากนี้ ข้อมูลที่ถูกส่งเป็นรูปแบบของ IP Protocol หรือ TCP/IP ซึ่งข้อมูลที่ต้องการส่งจริงจะมี Header อยู่ด้วยเพื่อกำกับบอกอยู่ทุก Packet ดังนั้นประสิทธิภาพในการรับ-ส่งข้อมูลจึงต่ำกว่ามาตรฐาน IEEE 802.11g ที่รับ-ส่งข้อมูลได้ที่ 54 Mbps

2.2 เมื่อพิจารณา รูปแบบการทดสอบทั้ง 5 รูปแบบ โปรโตคอล TCP จะไม่มีการสูญหายข้อมูลในระหว่างการรับ-ส่งข้อมูล เนื่องจากโปรโตคอล TCP มีการรับส่งข้อมูลที่ไม่คำนึงถึงปริมาณข้อมูลที่จะส่งไป แต่จะแบ่งข้อมูลเป็นส่วนย่อย ๆ ก่อน แล้วจึงจะส่งไปยังปลายทางอย่างต่อเนื่องเป็นลำดับข้อมูล ในรูปแบบการทดสอบที่ข้อมูลส่วนใดส่วนหนึ่งสูญหายไป ก็จะสามารถส่งข้อมูลส่วนนั้นใหม่อีกครั้งจนสำเร็จ ส่วน โปรโตคอล UDP จะไม่รับประกันความน่าเชื่อถือและลำดับของข้อมูล อย่างที่ TCP รับประกัน ซึ่งหมายความว่าข้อมูลอาจมาถึงไม่เรียงลำดับ หรือสูญหายระหว่างทางได้

2.3 เมื่อพิจารณา ชั้นความปลอดภัยที่ 1 ของโปรโตคอล TCP และ UDP พบว่า ชั้นความปลอดภัยดังกล่าวไม่มีการเข้ารหัสความปลอดภัย จึงมีประสิทธิภาพโดยรวมสูงที่สุด ในขณะที่ชั้นความปลอดภัยที่ 6 มีประสิทธิภาพโดยรวมต่ำที่สุด เนื่องจากมีการเข้ารหัสข้อมูลแบบ Advance Encryption Standard (AES) 128-bit ซึ่งเป็นการเข้ารหัสที่มีความซับซ้อนมาก แต่ถ้าพูดถึงเรื่องความปลอดภัยยังน้อยกว่า ชั้นความปลอดภัยที่ 7 ซึ่งเป็นชั้นที่มีความปลอดภัยมากที่สุด เนื่องจากจะต้องมี Radius Server ที่มี PKI หรือใบรับรองเพื่อใช้ในการตรวจสอบเท่านั้น ซึ่งเป็นไปตามทฤษฎีของระบบรักษาความปลอดภัยในเครือข่ายไร้สาย

3. ข้อเสนอแนะ

3.1 ข้อจำกัดของการวิจัย

การดำเนินการวิจัยมีข้อจำกัดหลายอย่างสำหรับการทดลอง เช่นสภาพแวดล้อมที่จำกัดซึ่งไม่มีอยู่ในเงื่อนไขในการควบคุม และปัจจัยเกี่ยวกับสิ่งแวดล้อมที่สำคัญมากสำหรับเครือข่ายไร้สาย อีกประการหนึ่งก็คือ การส่งผ่านคลื่นตามความถี่วิทยุและฮาร์ดแวร์ซึ่งก็มีผลต่อการทดลอง

3.2 ข้อเสนอแนะสำหรับการนำผลการวิจัยไปใช้งาน

3.2.1 ข้อเสนอแนะสำหรับการนำรูปแบบทดสอบไปใช้งาน

- รูปแบบทดสอบที่ 1 เหมาะสำหรับการใช้งานในลักษณะที่ต้องการรับ-ส่ง ข้อมูลปริมาณมากหรือมีประสิทธิภาพสูง และสนใจเรื่องความครบถ้วนของการรับ-ส่งข้อมูล แต่มีการรับ-ส่งข้อมูล แบบ point to point และเครื่องที่ใช้ในการรับข้อมูลต้องมีสายสัญญาณ (LAN) เชื่อมต่ออยู่ในระบบ (WLAN to LAN)

- รูปแบบทดสอบที่ 2 เหมาะสำหรับการใช้งานในลักษณะที่ต้องการรับ-ส่ง ข้อมูลปริมาณปานกลาง และมีการรับ-ส่งข้อมูล แบบ point to point แต่ไม่ต้องใช้สายสัญญาณ (LAN) เชื่อมต่อระบบ (WLAN to WLAN)

- รูปแบบทดสอบที่ 3-5 ไม่แนะนำให้ใช้โปรโตคอล UDP ในการรับ-ส่งข้อมูล และเหมาะสำหรับการใช้งานในลักษณะ Multi Point โดยข้อมูลที่ต้องการรับ-ส่ง ของรูปแบบทดสอบที่ 3 ควรเป็นข้อมูลทั่วไปขนาดปานกลาง ส่วนรูปแบบการทดสอบที่ 4-5 เหมาะสำหรับการรับ-ส่ง ข้อมูลที่มีปริมาณน้อย และรูปแบบการทดสอบที่ 4 ใช้ WLAN ในการรับ-ส่งข้อมูล แต่รูปแบบการทดสอบที่ 5 ต้องใช้ทั้ง WLAN และ LAN เพื่อรับ-ส่งข้อมูล

3.3.2 ข้อเสนอแนะสำหรับการนำ ชั้นความปลอดภัยไปใช้งาน

- ชั้นความปลอดภัยที่ 1 เหมาะสำหรับการใช้งานในลักษณะที่ต้องการรับ-ส่ง ข้อมูลปริมาณมากหรือมีประสิทธิภาพสูง แต่ไม่สนใจเรื่องความปลอดภัยของข้อมูล เช่น การ Streaming ต่างๆ

- ชั้นความปลอดภัยที่ 2 เหมาะสำหรับการใช้งานในลักษณะที่ต้องการรับ-ส่ง ข้อมูลปริมาณมากหรือมีประสิทธิภาพสูง และต้องการกำหนดเครื่องคอมพิวเตอร์ในการเข้าใช้งาน เช่น การประชุม

- ชั้นความปลอดภัยที่ 3-6 เหมาะสำหรับการใช้งานในลักษณะที่ต้องการรับ-ส่ง ข้อมูลทั่วไป แต่ให้ความสนใจเรื่องความปลอดภัยในระดับมาตรฐานที่อุปกรณ์ Wireless Access Point กำหนดมาให้ เหมาะสำหรับการใช้งานในองค์กรขนาดเล็ก หรือการใช้งานตามบ้านทั่วไป

- ชั้นความปลอดภัยที่ 7 เหมาะสำหรับการใช้งานในลักษณะที่ต้องการรับ-ส่ง ข้อมูลทั่วไป แต่ให้ความสนใจเรื่องความปลอดภัยในระดับสูง ในชั้นความปลอดภัยนี้ จะต้องมีการ Server ที่เป็น Radius ในการตรวจสอบสิทธิ์ในการใช้งาน และอุปกรณ์ ในการสร้างหรือกำหนด

Certificate เพื่อยืนยันตัวตนของผู้ที่เป็นเจ้าของ ซึ่งเหมาะกับองค์กรขนาดกลางไปจนถึงองค์กรขนาดใหญ่

3.3 ข้อเสนอแนะสำหรับการวิจัยต่อไป

การวิจัยนี้มีข้อเสนอแนะอันจะเป็นประโยชน์ต่อผู้วิจัยที่ต้องการนำผลของการวิจัยไปออกแบบ พัฒนาหรือนำไปใช้วิจัยต่อ ดังนี้

3.3.1 งานวิจัยนี้มีข้อจำกัดเรื่องจำนวนของ Wireless Access Point ที่มีเพียง 1 เครื่องเท่านั้น ดังนั้นหากต้องการทำการวิจัยต่อยอดสามารถเพิ่มจำนวน Wireless Access Point ให้มากกว่า 1 เครื่อง

3.3.2 งานวิจัยนี้ใช้มาตรฐานความปลอดภัย IEEE802.11g ซึ่งมีความเร็ว 54 Mbps หากผู้ที่สนใจต้องการศึกษาต่อยอดสามารถเปลี่ยนมาตรฐานความปลอดภัยที่มีความเร็วมากขึ้นเป็นมาตรฐานความปลอดภัย IEEE802.11n ซึ่งมีความเร็วมากกว่า 100 Mbps





บรรณานุกรม

- จตุชัย แพงจันทร์ และอนุชิต วุฒิพรพงษ์. (2546). *เจาะระบบNetwork ฉบับสมบูรณ์*. นนทบุรี: ไอดีซี อินโฟ ดิสทริบิวเตอร์ เซ็นเตอร์.
- จตุชัย แพงจันทร์ และอนุชิต วุฒิพรพงษ์.(2551). *เจาะระบบNetwork 2nd Edition*. นนทบุรี: ไอดีซี อินโฟ ดิสทริบิวเตอร์ เซ็นเตอร์.
- ชูศรี วงศ์รัตน์.(2534). *สถิติเพื่อการวิจัย*. พิมพ์ครั้งที่ 3. กรุงเทพฯ: เจริญพร.
- ศาลทศ พัดฟูทรัพย์.(2549). *การทดสอบความปลอดภัยของเครือข่ายไร้สาย* สารนิพนธ์ วท.ม. (สาขาเทคโนโลยีสารสนเทศ) กรุงเทพฯ: บัณฑิตวิทยาลัย
สถาบันเทคโนโลยีพระจอมเกล้าพระนครเหนือ.ถ่ายเอกสาร.
- ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์แห่งประเทศไทย. Wireless Security
[Online] Available form: <http://www.thaicert.org/paper/wireless.php>
- สุธี พงศาสกุลชัย และณรงค์ ลำดี. (2551). *การสื่อสารข้อมูลและเครือข่ายคอมพิวเตอร์*. กรุงเทพฯ: เคทีพี คอมพ์ แอนด์ คอนซัลท์.
- อำนาจ มีมงคล และอรอนพ ชันธิกุล.(2547). *ออกแบบและติดตั้งเครือข่าย Wireless LAN*. นนทบุรี: ไอดีซี อินโฟ ดิสทริบิวเตอร์ เซ็นเตอร์.
- Baghaei & Hunt. (July 2004). *Security performance of loaded IEEE 802.11b wireless networks*, Science direct Journal on Selected Areas in Computer Communications, pp 1746-1756.
- Chandran-Wadia Mahajan & Iyer.(2002). *Throughput Performance of the Distributed and Point Coordination Functions of an IEEE 802.11 Wireless LAN*, K.R. School of Information Technology, Department of Electrical Engineering, Indian Institute of Technology, Bombay, www.it.iitb.ac.in/~sri/papers/dot11-iccc02.pdf.
- Gurkas, Zaim & Aydin.(Nov 2006). *Security Mechanisms And Their Performance Impacts On Wireless Local Area Networks*, IEEE Journal on Selected Areas in Local Computer Network, pp 123-127.
- IP Traffic Test & Measure, Available form: <http://www.zti-telecom.com>, [Online]
- Linksys WAP54G Wireless Access point, Available form: www.linksys.com, [Online]
- Northrup & Thomas.(2004). *Implementing and Administering security in a Microsoft Windows Server 2003 Network*: Microsoft Press,
- Williamson.(2001). *Internet Traffic Measurement*, Department of Computer Science University of Calgary, Nov
- Wireshark Network Analyzer, Available form: <http://www.wireshark.org>, [Online]



ภาคผนวก ก
ผลการทดสอบสำหรับการประเมินประสิทธิภาพของความปลอดภัยในเครือข่ายไร้สาย
มาตรฐานIEEE802.11g

ผลการทดสอบสำหรับการประเมินประสิทธิภาพของความปลอดภัยในเครือข่ายไร้สาย มาตรฐาน IEEE 802.11g

1. ความเร็วในการรับ-ส่งข้อมูล (Mbps) ของเครือข่ายไร้สาย มาตรฐาน IEEE 802.11g

ตารางที่ 1 ความเร็วในการรับ-ส่งข้อมูลบนระบบเครือข่ายไร้สาย (WLAN) ไปยังเครือข่ายมีสาย (LAN) แบบ หนึ่งต่อหนึ่ง (Single Point) Mbps ของ โปรโตคอล TCP

รูปแบบทดสอบ	ครั้งที่									
	1	2	3	4	5	6	7	8	9	10
1. ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายมีสาย (LAN) แบบ หนึ่งต่อหนึ่ง (Single Point) Mbps										
ชั้นความปลอดภัยที่ 1: ไม่มีระบบรักษาความปลอดภัยหรือ เชื่อมโยงเครือข่ายด้วยSSID	27.85	28.78	29.00	29.13	27.51	26.42	27.69	27.65	27.32	26.99
ชั้นความปลอดภัยที่ 2: ตรวจสอบโดยใช้ MAC Address	24.80	25.07	25.00	24.79	24.81	24.92	25.01	24.63	24.58	24.90
ชั้นความปลอดภัยที่ 3: ตรวจสอบโดยใช้ WEP 64 บิต	23.94	23.40	23.32	23.40	23.39	23.56	23.49	23.94	24.06	23.48
ชั้นความปลอดภัยที่ 4: ตรวจสอบโดยใช้ WEP 128 บิต	23.21	23.50	23.10	23.66	23.59	23.76	23.42	23.84	23.51	23.44
ชั้นความปลอดภัยที่ 5: ตรวจสอบโดยใช้ WPA-PSK Version1	24.03	23.11	23.12	23.50	23.22	23.28	23.26	23.01	23.97	23.68
ชั้นความปลอดภัยที่ 6: ตรวจสอบโดยใช้ WPA-PSK Version2	21.71	20.40	19.98	20.20	21.65	20.99	20.78	22.25	20.57	20.61
ชั้นความปลอดภัยที่ 7: ตรวจสอบโดยใช้ PEAP	20.32	21.79	21.77	20.53	20.90	21.65	21.00	21.23	21.17	21.01

ตารางที่ 2 ความเร็วในการรับ-ส่งข้อมูลบนระบบเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายไร้สาย (WLAN) แบบ หนึ่งจุด (Single Point) Mbps ของ โปรโตคอล TCP

รูปแบบทดสอบ	ครั้งที่									
	1	2	3	4	5	6	7	8	9	10
2. ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายไร้สาย (WLAN) แบบ หนึ่งจุด (Single Point) Mbps										
ชั้นความปลอดภัยที่ 1: ไม่มีระบบรักษาความปลอดภัยหรือ เชื่อมโยงเครือข่ายด้วยSSID	12.29	12.39	12.35	12.03	12.97	12.24	12.45	12.93	12.66	12.31
ชั้นความปลอดภัยที่ 2: ตรวจสอบโดยใช้ MAC Address	12.67	12.30	12.69	12.64	12.16	12.47	12.35	12.17	12.36	12.22
ชั้นความปลอดภัยที่ 3: ตรวจสอบโดยใช้ WEP 64 บิต	11.68	11.86	11.56	11.29	11.00	11.97	11.35	11.19	11.23	11.89
ชั้นความปลอดภัยที่ 4: ตรวจสอบโดยใช้ WEP 128 บิต	10.75	10.73	11.16	11.17	11.37	10.98	10.82	11.03	10.92	11.12
ชั้นความปลอดภัยที่ 5: ตรวจสอบโดยใช้ WPA-PSK Version1	10.10	10.34	10.83	10.22	10.55	10.18	10.68	10.28	10.43	10.04
ชั้นความปลอดภัยที่ 6: ตรวจสอบโดยใช้ WPA-PSK Version2	7.07	7.98	7.36	7.47	8.09	7.74	8.15	8.38	8.44	7.72
ชั้นความปลอดภัยที่ 7: ตรวจสอบโดยใช้ PEAP	10.23	10.38	10.41	10.63	10.69	10.11	10.31	10.28	9.97	10.39

ตารางที่ 3 ความเร็วในการรับ-ส่งข้อมูลบนระบบเครือข่ายไร้สาย (WLAN) ไปยังเครือข่ายมีสาย (LAN) แบบ หลายจุด (Multiple Point) Mbps ของ โปรโตคอล TCP

รูปแบบทดสอบ	ครั้งที่									
	1	2	3	4	5	6	7	8	9	10
3. ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายมีสาย (LAN) แบบ หลายจุด (Multiple Point) Mbps										
ชั้นความปลอดภัยที่ 1: ไม่มีระบบรักษาความปลอดภัยหรือ เชื่อมโยงเครือข่ายด้วยSSID	28.28	28.71	28.15	29.10	28.53	27.70	28.94	27.41	27.84	27.75
ชั้นความปลอดภัยที่ 2: ตรวจสอบโดยใช้ MAC Address	24.56	25.66	26.80	26.55	26.24	26.33	27.26	25.71	26.33	25.72
ชั้นความปลอดภัยที่ 3: ตรวจสอบโดยใช้ WEP 64 บิต	26.46	24.90	24.16	25.95	24.46	25.02	24.98	24.88	26.53	26.44
ชั้นความปลอดภัยที่ 4: ตรวจสอบโดยใช้ WEP 128 บิต	24.71	24.32	23.98	24.21	25.28	25.53	23.74	24.15	24.46	24.49
ชั้นความปลอดภัยที่ 5: ตรวจสอบโดยใช้ WPA-PSK Version1	25.00	22.85	24.18	24.99	24.79	24.32	24.67	24.62	24.31	24.90
ชั้นความปลอดภัยที่ 6: ตรวจสอบโดยใช้ WPA-PSK Version2	20.21	22.89	23.61	22.11	20.67	22.13	24.51	21.83	22.07	24.28
ชั้นความปลอดภัยที่ 7: ตรวจสอบโดยใช้ PEAP	23.21	23.29	23.14	23.37	23.41	22.48	23.22	22.81	22.33	22.41

ตารางที่ 4 ความเร็วในการรับ-ส่งข้อมูลบนระบบเครือข่ายไร้สาย (WLAN) ไปยังเครือข่ายไร้สาย (WLAN) แบบ หลายจุด (Multiple Point) Mbps ของ โปรโตคอล TCP

รูปแบบทดสอบ	ครั้งที่									
	1	2	3	4	5	6	7	8	9	10
4. ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายไร้สาย (WLAN) แบบ หลายจุด (Multiple Point) Mbps										
ชั้นความปลอดภัยที่ 1: ไม่มีระบบรักษาความปลอดภัยหรือเชื่อมโยงเครือข่ายด้วยSSID	11.79	12.28	11.79	11.86	11.69	11.12	11.54	10.98	11.31	11.54
ชั้นความปลอดภัยที่ 2: ตรวจสอบโดยใช้ MAC Address	12.18	11.98	11.80	11.11	10.91	10.87	11.02	11.21	11.05	11.32
ชั้นความปลอดภัยที่ 3: ตรวจสอบโดยใช้ WEP 64 บิต	11.09	11.01	11.09	10.47	11.49	11.82	10.78	11.00	10.72	11.01
ชั้นความปลอดภัยที่ 4: ตรวจสอบโดยใช้ WEP 128 บิต	11.40	10.37	10.64	10.45	10.07	10.56	10.21	10.89	10.47	11.00
ชั้นความปลอดภัยที่ 5: ตรวจสอบโดยใช้ WPA-PSK Version1	10.35	10.57	10.49	10.66	10.08	10.13	10.37	10.83	10.91	10.56
ชั้นความปลอดภัยที่ 6: ตรวจสอบโดยใช้ WPA-PSK Version2	6.33	7.19	7.25	7.05	7.80	7.56	7.31	6.74	7.57	7.68
ชั้นความปลอดภัยที่ 7: ตรวจสอบโดยใช้ PEAP	9.82	9.63	10.03	9.86	9.74	9.85	10.00	9.84	10.20	10.02

ตารางที่ 5 ความเร็วในการรับ-ส่งข้อมูลบนระบบเครือข่ายไร้สาย (WLAN) ไปยังเครือข่ายมีสาย (LAN) และไร้สาย (WLAN) Mbps ของโปรโตคอล TCP

รูปแบบทดสอบ	ครั้งที่									
	1	2	3	4	5	6	7	8	9	10
5. ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายมีสาย (LAN)และไร้สาย (WLAN) Mbps										
ชั้นความปลอดภัยที่ 1: ไม่มีระบบรักษาความปลอดภัยหรือเชื่อมโยงเครือข่ายด้วยSSID	17.51	17.81	17.11	16.89	17.45	17.37	17.79	17.00	16.99	17.77
ชั้นความปลอดภัยที่ 2: ตรวจสอบโดยใช้ MAC Address	17.28	17.14	16.88	17.13	16.53	17.08	16.87	16.99	17.12	17.09
ชั้นความปลอดภัยที่ 3: ตรวจสอบโดยใช้ WEP 64 บิต	16.35	16.22	16.43	16.46	16.31	15.98	16.66	16.40	16.51	16.35
ชั้นความปลอดภัยที่ 4: ตรวจสอบโดยใช้ WEP 128 บิต	14.93	14.80	15.07	15.61	15.72	14.98	15.11	15.34	15.80	15.77
ชั้นความปลอดภัยที่ 5: ตรวจสอบโดยใช้ WPA-PSK Version1	15.11	15.08	14.57	15.22	14.89	15.68	15.17	15.23	14.99	15.30
ชั้นความปลอดภัยที่ 6: ตรวจสอบโดยใช้ WPA-PSK Version2	12.91	12.27	13.32	11.03	11.32	12.53	11.27	11.71	12.48	11.34
ชั้นความปลอดภัยที่ 7: ตรวจสอบโดยใช้ PEAP	14.10	14.75	14.63	14.68	14.57	14.47	14.67	14.71	14.80	14.40

ตารางที่ 6 ความเร็วในการรับ-ส่งข้อมูลบนระบบเครือข่ายไร้สาย (WLAN) ไปยังเครือข่ายมีสาย (LAN) แบบ หนึ่งต่อหนึ่ง (Single Point) Mbps ของ โปรโตคอล UDP

รูปแบบทดสอบ	ครั้งที่									
	1	2	3	4	5	6	7	8	9	10
1. ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายมีสาย (LAN) แบบ หนึ่งต่อหนึ่ง (Single Point) Mbps										
ชั้นความปลอดภัยที่ 1: ไม่มีระบบรักษาความปลอดภัยหรือเชื่อมโยงเครือข่ายด้วยSSID	30.77	32.25	30.43	29.83	29.91	29.74	29.33	31.00	31.42	31.21
ชั้นความปลอดภัยที่ 2: ตรวจสอบโดยใช้ MAC Address	27.50	27.89	27.29	27.52	27.19	28.26	27.78	27.17	26.79	26.92
ชั้นความปลอดภัยที่ 3: ตรวจสอบโดยใช้ WEP 64 บิต	26.63	26.22	25.47	25.76	25.40	25.39	26.58	26.36	26.22	25.90
ชั้นความปลอดภัยที่ 4: ตรวจสอบโดยใช้ WEP 128 บิต	25.29	25.03	25.18	26.10	26.21	25.26	25.56	26.02	25.19	25.21
ชั้นความปลอดภัยที่ 5: ตรวจสอบโดยใช้ WPA-PSK Version1	25.53	24.70	25.14	25.54	25.10	24.93	25.52	25.35	25.29	24.50
ชั้นความปลอดภัยที่ 6: ตรวจสอบโดยใช้ WPA-PSK Version2	23.95	24.74	24.21	23.81	24.78	23.35	24.51	24.42	25.62	23.89
ชั้นความปลอดภัยที่ 7: ตรวจสอบโดยใช้ PEAP	25.23	24.18	26.07	24.78	25.26	24.91	25.40	24.83	23.97	24.62

ตารางที่ 7 ความเร็วในการรับ-ส่งข้อมูลบนระบบเครือข่ายไร้สาย (WLAN) ไปยังเครือข่ายไร้สาย (WLAN) แบบ หนึ่งจุด (Single Point) Mbps ของ โปรโตคอล UDP

รูปแบบทดสอบ	ครั้งที่									
	1	2	3	4	5	6	7	8	9	10
2. ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายไร้สาย (WLAN) แบบ หนึ่งจุด (Single Point) Mbps										
ชั้นความปลอดภัยที่ 1: ไม่มีระบบรักษาความปลอดภัยหรือ เชื่อมโยงเครือข่ายด้วยSSID	29.70	28.37	29.27	27.60	30.17	26.74	29.01	28.92	29.11	29.13
ชั้นความปลอดภัยที่ 2: ตรวจสอบโดยใช้ MAC Address	14.88	15.02	14.88	15.13	15.24	14.72	14.75	15.13	14.99	15.41
ชั้นความปลอดภัยที่ 3: ตรวจสอบโดยใช้ WEP 64 บิต	14.20	14.28	14.41	14.06	14.52	14.39	14.55	14.22	14.59	14.62
ชั้นความปลอดภัยที่ 4: ตรวจสอบโดยใช้ WEP 128 บิต	13.43	14.15	14.24	13.98	13.87	14.07	13.75	13.69	13.42	13.78
ชั้นความปลอดภัยที่ 5: ตรวจสอบโดยใช้ WPA-PSK Version1	12.35	13.42	12.74	12.85	13.72	12.14	12.09	12.98	12.74	12.86
ชั้นความปลอดภัยที่ 6: ตรวจสอบโดยใช้ WPA-PSK Version2	10.03	12.61	9.89	9.98	10.23	10.11	12.53	13.02	11.91	10.65
ชั้นความปลอดภัยที่ 7: ตรวจสอบโดยใช้ PEAP	11.89	12.00	11.97	12.21	12.40	11.80	11.81	12.46	11.98	12.37

ตารางที่ 8 ความเร็วในการรับ-ส่งข้อมูลบนระบบเครือข่ายไร้สาย (WLAN) ไปยังเครือข่ายมีสาย (LAN) แบบ หลายจุด (Multiple Point) Mbps ของ โปรโตคอล UDP

รูปแบบทดสอบ	ครั้งที่									
	1	2	3	4	5	6	7	8	9	10
3. ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายมีสาย (LAN) แบบ หลายจุด (Multiple Point) Mbps										
ชั้นความปลอดภัยที่ 1: ไม่มีระบบรักษาความปลอดภัยหรือ เชื่อมโยงเครือข่ายด้วยSSID	62.48	55.51	64.94	61.92	61.85	57.87	54.62	60.89	54.69	64.46
ชั้นความปลอดภัยที่ 2: ตรวจสอบโดยใช้ MAC Address	52.35	59.71	60.10	58.05	61.96	59.62	58.61	60.08	55.70	59.89
ชั้นความปลอดภัยที่ 3: ตรวจสอบโดยใช้ WEP 64 บิต	56.67	57.32	56.03	55.98	56.41	56.31	56.10	53.98	54.74	55.07
ชั้นความปลอดภัยที่ 4: ตรวจสอบโดยใช้ WEP 128 บิต	55.86	55.06	56.71	54.10	54.49	53.23	55.76	57.10	54.68	55.53
ชั้นความปลอดภัยที่ 5: ตรวจสอบโดยใช้ WPA-PSK Version1	55.58	57.05	56.64	54.94	54.37	57.89	52.41	56.09	55.84	54.17
ชั้นความปลอดภัยที่ 6: ตรวจสอบโดยใช้ WPA-PSK Version2	51.36	45.88	47.11	44.62	50.01	45.61	45.17	50.46	43.87	47.79
ชั้นความปลอดภัยที่ 7: ตรวจสอบโดยใช้ PEAP	53.46	59.38	54.25	55.17	56.17	58.08	51.43	57.06	54.02	57.65

ตารางที่ 9 ความเร็วในการรับ-ส่งข้อมูลบนระบบเครือข่ายไร้สาย (WLAN) ไปยังเครือข่ายไร้สาย (WLAN) แบบ หลายจุด (Multiple Point) Mbps ของ โปรโตคอล UDP

รูปแบบทดสอบ	ครั้งที่									
	1	2	3	4	5	6	7	8	9	10
4. ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายไร้สาย (WLAN) แบบ หลายจุด (Multiple Point) Mbps										
ชั้นความปลอดภัยที่ 1: ไม่มีระบบรักษาความปลอดภัยหรือ เชื่อมโยงเครือข่ายด้วยSSID	49.28	52.86	52.42	54.23	57.32	57.31	61.22	60.35	57.33	50.01
ชั้นความปลอดภัยที่ 2: ตรวจสอบโดยใช้ MAC Address	58.52	57.55	58.32	49.67	57.81	50.53	51.32	49.58	52.87	52.89
ชั้นความปลอดภัยที่ 3: ตรวจสอบโดยใช้ WEP 64 บิต	52.53	48.36	51.07	51.51	53.09	48.74	51.80	54.04	48.50	52.36
ชั้นความปลอดภัยที่ 4: ตรวจสอบโดยใช้ WEP 128 บิต	51.21	47.93	47.82	48.88	48.98	51.00	47.53	50.31	47.42	49.46
ชั้นความปลอดภัยที่ 5: ตรวจสอบโดยใช้ WPA-PSK Version1	44.58	55.41	45.90	50.48	51.79	53.25	52.76	49.83	50.20	53.96
ชั้นความปลอดภัยที่ 6: ตรวจสอบโดยใช้ WPA-PSK Version2	31.40	53.89	44.17	42.75	47.06	54.35	48.68	50.79	51.21	54.54
ชั้นความปลอดภัยที่ 7: ตรวจสอบโดยใช้ PEAP	42.06	50.12	57.69	53.98	58.16	56.58	53.02	54.63	54.17	48.02

ตารางที่ 10 ความเร็วในการรับ-ส่งข้อมูลบนระบบเครือข่ายไร้สาย (WLAN) ไปยังเครือข่ายมีสาย (LAN) และไร้สาย (WLAN) Mbps ของโปรโตคอล UDP

ชั้นความปลอดภัย	ครั้งที่									
	1	2	3	4	5	6	7	8	9	10
5. ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายมีสาย (LAN) และไร้สาย (WLAN) Mbps										
ชั้นความปลอดภัยที่ 1: ไม่มีระบบรักษาความปลอดภัยหรือ เชื่อมโยงเครือข่ายด้วยSSID	54.32	53.13	47.35	53.00	55.65	56.90	57.45	57.10	55.23	57.26
ชั้นความปลอดภัยที่ 2: ตรวจสอบโดยใช้ MAC Address	49.61	49.39	55.12	53.55	51.83	50.81	54.92	50.92	53.72	51.83
ชั้นความปลอดภัยที่ 3: ตรวจสอบโดยใช้ WEP 64 บิต	49.85	46.19	50.65	53.36	51.02	47.16	49.29	50.14	51.94	46.82
ชั้นความปลอดภัยที่ 4: ตรวจสอบโดยใช้ WEP 128 บิต	49.16	41.94	48.83	46.08	48.78	47.80	45.76	41.29	43.92	43.83
ชั้นความปลอดภัยที่ 5: ตรวจสอบโดยใช้ WPA-PSK Version1	44.16	46.03	51.01	52.66	49.15	46.68	50.00	49.23	52.21	50.79
ชั้นความปลอดภัยที่ 6: ตรวจสอบโดยใช้ WPA-PSK Version2	47.18	46.86	45.74	46.13	48.18	46.18	43.27	41.89	43.21	41.41
ชั้นความปลอดภัยที่ 7: ตรวจสอบโดยใช้ PEAP	49.54	53.46	53.71	48.36	53.83	53.31	48.78	50.31	51.24	49.62

2. ปริมาณข้อมูลที่ได้รับได้ เมื่อส่งข้อมูลจำนวน 100 MB ของเครือข่ายไร้สาย มาตรฐาน IEEE 802.11g

ตารางที่ 11 ปริมาณข้อมูลที่ได้รับบนระบบเครือข่ายไร้สาย (WLAN) ไปยังเครือข่ายมีสาย (LAN) แบบ หนึ่งต่อหนึ่ง (Single Point) Mbps ของโปรโตคอล TCP

รูปแบบทดสอบ	ครั้งที่									
	1	2	3	4	5	6	7	8	9	10
1. ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายมีสาย (LAN) แบบ หนึ่งต่อหนึ่ง (Single Point) Mbps										
ชั้นความปลอดภัยที่ 1: ไม่มีระบบรักษาความปลอดภัยหรือ เชื่อมโยงเครือข่ายด้วยSSID	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00
ชั้นความปลอดภัยที่ 2: ตรวจสอบโดยใช้ MAC Address	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00
ชั้นความปลอดภัยที่ 3: ตรวจสอบโดยใช้ WEP 64 บิต	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00
ชั้นความปลอดภัยที่ 4: ตรวจสอบโดยใช้ WEP 128 บิต	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00
ชั้นความปลอดภัยที่ 5: ตรวจสอบโดยใช้ WPA-PSK Version1	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00
ชั้นความปลอดภัยที่ 6: ตรวจสอบโดยใช้ WPA-PSK Version2	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00
ชั้นความปลอดภัยที่ 7: ตรวจสอบโดยใช้ PEAP	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00

ตารางที่ 12 ปริมาณข้อมูลที่ได้รับบนระบบเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายไร้สาย (WLAN) แบบ หนึ่งจุด (Single Point) Mbps ของโปรโตคอล TCP

รูปแบบทดสอบ	ครั้งที่									
	1	2	3	4	5	6	7	8	9	10
2. ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายไร้สาย (WLAN) แบบ หนึ่งจุด (Single Point) Mbps										
ชั้นความปลอดภัยที่ 1: ไม่มีระบบรักษาความปลอดภัยหรือ เชื่อมโยงเครือข่ายด้วยSSID	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00
ชั้นความปลอดภัยที่ 2: ตรวจสอบโดยใช้ MAC Address	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00
ชั้นความปลอดภัยที่ 3: ตรวจสอบโดยใช้ WEP 64 บิต	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00
ชั้นความปลอดภัยที่ 4: ตรวจสอบโดยใช้ WEP 128 บิต	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00
ชั้นความปลอดภัยที่ 5: ตรวจสอบโดยใช้ WPA-PSK Version1	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00
ชั้นความปลอดภัยที่ 6: ตรวจสอบโดยใช้ WPA-PSK Version2	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00
ชั้นความปลอดภัยที่ 7: ตรวจสอบโดยใช้ PEAP	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00

ตารางที่ 13 ปริมาณข้อมูลที่ได้รับบนระบบเครือข่ายไร้สาย (WLAN) ไปยังเครือข่ายมีสาย (LAN) แบบ หลายจุด (Multiple Point) Mbps ของ โปรโตคอล TCP

รูปแบบทดสอบ	ครั้งที่									
	1	2	3	4	5	6	7	8	9	10
3. ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายมีสาย (LAN) แบบ หลายจุด (Multiple Point) Mbps										
ชั้นความปลอดภัยที่ 1: ไม่มีระบบรักษาความปลอดภัยหรือ เชื่อมโยงเครือข่ายด้วยSSID	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00
ชั้นความปลอดภัยที่ 2: ตรวจสอบโดยใช้ MAC Address	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00
ชั้นความปลอดภัยที่ 3: ตรวจสอบโดยใช้ WEP 64 บิต	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00
ชั้นความปลอดภัยที่ 4: ตรวจสอบโดยใช้ WEP 128 บิต	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00
ชั้นความปลอดภัยที่ 5: ตรวจสอบโดยใช้ WPA-PSK Version1	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00
ชั้นความปลอดภัยที่ 6: ตรวจสอบโดยใช้ WPA-PSK Version2	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00
ชั้นความปลอดภัยที่ 7: ตรวจสอบโดยใช้ PEAP	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00

ตารางที่ 14 ปริมาณข้อมูลที่ได้รับบนระบบเครือข่ายไร้สาย (WLAN) ไปยังเครือข่ายไร้สาย (WLAN) แบบ หลายจุด (Multiple Point) Mbps ของโปรโตคอล TCP

รูปแบบทดสอบ	ครั้งที่									
	1	2	3	4	5	6	7	8	9	10
4. ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายไร้สาย (WLAN) แบบ หลายจุด (Multiple Point) Mbps										
ชั้นความปลอดภัยที่ 1: ไม่มีระบบรักษาความปลอดภัยหรือเชื่อมโยงเครือข่ายด้วยSSID	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00
ชั้นความปลอดภัยที่ 2: ตรวจสอบโดยใช้ MAC Address	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00
ชั้นความปลอดภัยที่ 3: ตรวจสอบโดยใช้ WEP 64 บิต	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00
ชั้นความปลอดภัยที่ 4: ตรวจสอบโดยใช้ WEP 128 บิต	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00
ชั้นความปลอดภัยที่ 5: ตรวจสอบโดยใช้ WPA-PSK Version1	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00
ชั้นความปลอดภัยที่ 6: ตรวจสอบโดยใช้ WPA-PSK Version2	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00
ชั้นความปลอดภัยที่ 7: ตรวจสอบโดยใช้ PEAP	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00

ตารางที่ 15 ปริมาณข้อมูลที่ได้รับบนระบบเครือข่ายไร้สาย (WLAN) ไปยังเครือข่ายมีสาย (LAN) และไร้สาย (WLAN) Mbps ของโปรโตคอล TCP

รูปแบบทดสอบ	ครั้งที่									
	1	2	3	4	5	6	7	8	9	10
5. ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายมีสาย (LAN)และไร้สาย (WLAN) Mbps										
ชั้นความปลอดภัยที่ 1: ไม่มีระบบรักษาความปลอดภัยหรือเชื่อมโยงเครือข่ายด้วยSSID	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00
ชั้นความปลอดภัยที่ 2: ตรวจสอบโดยใช้ MAC Address	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00
ชั้นความปลอดภัยที่ 3: ตรวจสอบโดยใช้ WEP 64 บิต	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00
ชั้นความปลอดภัยที่ 4: ตรวจสอบโดยใช้ WEP 128 บิต	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00
ชั้นความปลอดภัยที่ 5: ตรวจสอบโดยใช้ WPA-PSK Version1	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00
ชั้นความปลอดภัยที่ 6: ตรวจสอบโดยใช้ WPA-PSK Version2	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00
ชั้นความปลอดภัยที่ 7: ตรวจสอบโดยใช้ PEAP	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00

ตารางที่ 16 ปริมาณข้อมูลที่ได้รับบนระบบเครือข่ายไร้สาย (WLAN) ไปยังเครือข่ายมีสาย (LAN) แบบ หนึ่งต่อหนึ่ง (Single Point) Mbps ของโปรโตคอล UDP

รูปแบบทดสอบ	ครั้งที่									
	1	2	3	4	5	6	7	8	9	10
1. ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายมีสาย (LAN) แบบ หนึ่งต่อหนึ่ง (Single Point) Mbps										
ชั้นความปลอดภัยที่ 1: ไม่มีระบบรักษาความปลอดภัยหรือเชื่อมโยงเครือข่ายด้วยSSID	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00
ชั้นความปลอดภัยที่ 2: ตรวจสอบโดยใช้ MAC Address	100.00	100.00	100.00	100.00	100.00	98.90	100.00	100.00	100.00	100.00
ชั้นความปลอดภัยที่ 3: ตรวจสอบโดยใช้ WEP 64 บิต	100.00	100.00	100.00	99.30	100.00	100.00	100.00	100.00	100.00	100.00
ชั้นความปลอดภัยที่ 4: ตรวจสอบโดยใช้ WEP 128 บิต	98.20	100.00	100.00	100.00	100.00	100.00	100.00	98.30	100.00	100.00
ชั้นความปลอดภัยที่ 5: ตรวจสอบโดยใช้ WPA-PSK Version1	100.00	100.00	100.00	100.00	98.80	100.00	100.00	97.40	100.00	100.00
ชั้นความปลอดภัยที่ 6: ตรวจสอบโดยใช้ WPA-PSK Version2	100.00	100.00	100.00	100.00	100.00	100.00	98.80	100.00	100.00	100.00
ชั้นความปลอดภัยที่ 7: ตรวจสอบโดยใช้ PEAP	100.00	98.70	100.00	100.00	100.00	100.00	97.60	100.00	100.00	100.00

ตารางที่ 17 ปริมาณข้อมูลที่ได้รับบนระบบเครือข่ายไร้สาย (WLAN) ไปยังเครือข่ายไร้สาย (WLAN) แบบ หนึ่งจุด (Single Point) Mbps ของโปรโตคอล UDP

รูปแบบทดสอบ	ครั้งที่									
	1	2	3	4	5	6	7	8	9	10
2. ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายไร้สาย (WLAN) แบบ หนึ่งจุด (Single Point) Mbps										
ชั้นความปลอดภัยที่ 1: ไม่มีระบบรักษาความปลอดภัยหรือ เชื่อมโยงเครือข่ายด้วยSSID	91.50	86.20	90.30	90.40	89.10	90.60	90.70	87.50	91.60	91.80
ชั้นความปลอดภัยที่ 2: ตรวจสอบโดยใช้ MAC Address	89.78	82.41	89.11	90.10	88.60	89.70	82.30	84.33	86.51	80.50
ชั้นความปลอดภัยที่ 3: ตรวจสอบโดยใช้ WEP 64 บิต	84.30	77.70	87.50	87.00	85.60	89.10	83.50	73.50	74.10	73.90
ชั้นความปลอดภัยที่ 4: ตรวจสอบโดยใช้ WEP 128 บิต	89.90	87.40	81.20	81.30	82.20	78.20	83.40	79.90	79.70	84.70
ชั้นความปลอดภัยที่ 5: ตรวจสอบโดยใช้ WPA-PSK Version1	87.60	88.40	81.80	80.90	83.20	81.10	82.10	87.80	84.10	82.40
ชั้นความปลอดภัยที่ 6: ตรวจสอบโดยใช้ WPA-PSK Version2	89.70	87.50	88.30	82.70	80.20	81.90	86.10	85.40	81.20	87.40
ชั้นความปลอดภัยที่ 7: ตรวจสอบโดยใช้ PEAP	89.80	88.30	84.73	86.71	80.50	87.30	83.20	83.23	82.30	84.75

ตารางที่ 18 ปริมาณข้อมูลที่ได้รับบนระบบเครือข่ายไร้สาย (WLAN) ไปยังเครือข่ายมีสาย (LAN) แบบ หลายจุด (Multiple Point) Mbps ของโปรโตคอล UDP

รูปแบบทดสอบ	ครั้งที่									
	1	2	3	4	5	6	7	8	9	10
3. ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายมีสาย (LAN) แบบ หลายจุด (Multiple Point) Mbps										
ชั้นความปลอดภัยที่ 1: ไม่มีระบบรักษาความปลอดภัยหรือ เชื่อมโยงเครือข่ายด้วยSSID	62.20	65.10	63.00	69.80	63.60	62.10	64.90	64.20	60.70	61.10
ชั้นความปลอดภัยที่ 2: ตรวจสอบโดยใช้ MAC Address	64.74	67.75	59.81	66.80	62.80	64.90	60.00	65.30	65.40	65.10
ชั้นความปลอดภัยที่ 3: ตรวจสอบโดยใช้ WEP 64 บิต	56.60	54.90	52.70	55.20	47.10	51.80	52.60	47.80	54.00	50.60
ชั้นความปลอดภัยที่ 4: ตรวจสอบโดยใช้ WEP 128 บิต	68.80	62.80	62.50	69.20	57.90	65.20	65.60	63.70	58.70	66.70
ชั้นความปลอดภัยที่ 5: ตรวจสอบโดยใช้ WPA-PSK Version1	59.80	61.30	62.60	62.10	57.50	59.80	58.70	59.70	53.10	54.30
ชั้นความปลอดภัยที่ 6: ตรวจสอบโดยใช้ WPA-PSK Version2	64.70	61.20	56.70	57.60	65.00	53.10	57.20	55.10	60.90	66.50
ชั้นความปลอดภัยที่ 7: ตรวจสอบโดยใช้ PEAP	65.40	61.31	62.33	59.12	58.77	62.10	65.20	58.50	59.87	60.15

ตารางที่ 19 ปริมาณข้อมูลที่ได้รับบนระบบเครือข่ายไร้สาย (WLAN) ไปยังเครือข่ายไร้สาย (WLAN) แบบ หลายจุด (Multiple Point) Mbps ของโปรโตคอล UDP

รูปแบบทดสอบ	ครั้งที่									
	1	2	3	4	5	6	7	8	9	10
4. ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายไร้สาย (WLAN) แบบ หลายจุด (Multiple Point) Mbps										
ชั้นความปลอดภัยที่ 1: ไม่มีระบบรักษาความปลอดภัยหรือ เชื่อมโยงเครือข่ายด้วยSSID	46.35	47.58	42.87	57.80	36.57	35.05	35.98	60.90	38.03	47.63
ชั้นความปลอดภัยที่ 2: ตรวจสอบโดยใช้ MAC Address	43.12	44.80	39.20	41.10	40.37	38.33	32.70	41.20	43.50	44.30
ชั้นความปลอดภัยที่ 3: ตรวจสอบโดยใช้ WEP 64 บิต	28.11	26.91	28.64	24.20	24.40	23.30	25.60	24.60	20.40	33.87
ชั้นความปลอดภัยที่ 4: ตรวจสอบโดยใช้ WEP 128 บิต	52.80	38.79	32.75	31.77	33.78	35.75	33.79	32.88	24.04	31.18
ชั้นความปลอดภัยที่ 5: ตรวจสอบโดยใช้ WPA-PSK Version1	39.50	34.70	43.12	39.60	31.50	33.80	32.60	37.64	31.98	29.10
ชั้นความปลอดภัยที่ 6: ตรวจสอบโดยใช้ WPA-PSK Version2	21.55	38.45	27.07	18.99	24.93	32.42	31.24	28.86	37.62	29.42
ชั้นความปลอดภัยที่ 7: ตรวจสอบโดยใช้ PEAP	38.80	29.60	41.95	38.76	42.11	40.20	42.50	31.20	33.50	39.82

ตารางที่ 20 ปริมาณข้อมูลที่ได้รับบนระบบเครือข่ายไร้สาย (WLAN) ไปยังเครือข่ายมีสาย (LAN) และไร้สาย (WLAN) Mbps ของโปรโตคอล UDP

ชั้นความปลอดภัย	ครั้งที่									
	1	2	3	4	5	6	7	8	9	10
5. ระบบเครือข่ายที่มีเครือข่ายไร้สาย (WLAN) ส่งข้อมูลไปยังเครือข่ายมีสาย (LAN) และไร้สาย (WLAN) Mbps										
ชั้นความปลอดภัยที่ 1: ไม่มีระบบรักษาความปลอดภัยหรือ เชื่อมโยงเครือข่ายด้วยSSID	62.02	68.20	68.33	68.90	61.29	69.61	69.20	67.10	62.00	62.34
ชั้นความปลอดภัยที่ 2: ตรวจสอบโดยใช้ MAC Address	67.77	71.30	62.40	62.10	69.60	74.40	63.50	60.14	62.35	65.50
ชั้นความปลอดภัยที่ 3: ตรวจสอบโดยใช้ WEP 64 บิต	62.50	50.90	55.80	54.80	54.40	69.00	57.90	57.70	62.20	54.30
ชั้นความปลอดภัยที่ 4: ตรวจสอบโดยใช้ WEP 128 บิต	72.21	68.30	69.80	57.72	67.94	70.21	68.88	66.20	63.30	60.60
ชั้นความปลอดภัยที่ 5: ตรวจสอบโดยใช้ WPA-PSK Version1	59.75	56.80	63.10	64.80	59.13	58.50	69.80	70.70	60.50	62.30
ชั้นความปลอดภัยที่ 6: ตรวจสอบโดยใช้ WPA-PSK Version2	67.90	68.00	61.90	61.90	58.39	71.70	61.07	60.60	69.55	47.36
ชั้นความปลอดภัยที่ 7: ตรวจสอบโดยใช้ PEAP	69.50	63.22	64.70	68.89	59.11	70.41	68.40	63.21	59.70	71.10



ภาคผนวก ข
การตั้งค่าในอุปกรณ์สำหรับการทดสอบระบบ

การตั้งค่าในอุปกรณ์สำหรับการทดสอบระบบ

ในการตั้งค่าในอุปกรณ์สำหรับการทดสอบประสิทธิภาพของความปลอดภัยในเครือข่ายไร้สาย มาตรฐาน IEEE802.11g สามารถทำการตั้งค่าโดยแบ่งออกเป็นส่วนต่างๆได้ดังนี้

1. เครื่องคอมพิวเตอร์สำหรับการส่งข้อมูล

การตั้งค่าเครื่องคอมพิวเตอร์สำหรับการส่งข้อมูล	
ชื่อคอมพิวเตอร์	A001
IP Address บน Wireless การ์ด	192.168.0.101
ซอฟต์แวร์	1. Windows XP Service Pack3
	2. IP Traffic Generator
	3. Wireshark

ตารางที่ ข-1 การตั้งค่าเครื่องคอมพิวเตอร์สำหรับการส่งข้อมูล

2. เครื่องคอมพิวเตอร์สำหรับการรับข้อมูลเครื่องที่ 1

การตั้งค่าเครื่องคอมพิวเตอร์สำหรับการรับข้อมูลเครื่องที่ 1	
ชื่อคอมพิวเตอร์	A002
IP Address บน Wireless การ์ด	192.168.0.102
IP Address บน LAN การ์ด	192.168.0.112
ซอฟต์แวร์	1. Windows 7 Pack1
	2. IP Traffic Generator

ตารางที่ ข-2 การตั้งค่าเครื่องคอมพิวเตอร์สำหรับการรับข้อมูลเครื่องที่ 1

3. เครื่องคอมพิวเตอร์สำหรับการรับข้อมูลเครื่องที่ 2

การตั้งค่าเครื่องคอมพิวเตอร์สำหรับการรับข้อมูลเครื่องที่ 2	
ชื่อคอมพิวเตอร์	A003
IP Address บน Wireless การ์ด	192.168.0.103
IP Address บน LAN การ์ด	192.168.0.113
ซอฟต์แวร์	1. Windows 7 Pack1
	2. IP Traffic Generator

ตารางที่ ข-3 การตั้งค่าเครื่องคอมพิวเตอร์สำหรับการรับข้อมูลเครื่องที่ 2

4. Wireless Access Point

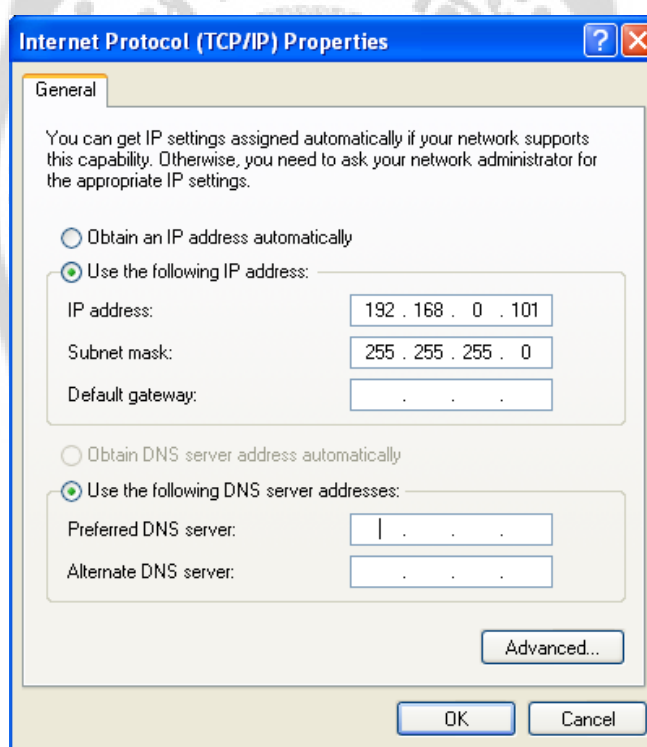
การตั้งค่าเครื่อง Wireless Access Point	
ชื่อ	AP01
IP Address	192.168.0.1
SSID	tsunami
ระบบความปลอดภัย	1. No Security
	2. MAC-Address
	3. WEP 64 bit
	4. WEP 128 bit
	5. WPA-PSK Version1
	6. WPA-PSK Version2
	7. PEAP

ตารางที่ ข-4 การตั้งค่าเครื่อง Wireless Access Point

5. RADIUS Server

การตั้งค่าเครื่องคอมพิวเตอร์ Radius Server	
ชื่อคอมพิวเตอร์	RADIUS01
IP Address	192.168.0.200
ซอฟต์แวร์	1. Windows Server 2003 Service Pack2
	2. Active Directory Service (AD)
	3. Certificate Authority Service (CA)
	4. Internet Authentication Service (IAS)

ตารางที่ ข-5 การตั้งค่าเครื่อง Wireless Access Point



ภาพประกอบ ข-1 การตั้งค่า IP Address สำหรับเครื่องส่งข้อมูล

The screenshot shows the 'IP Generator - Parameters' window. The 'Destination Parameters' section has 'IP Address or Host Name' set to '192.168.0.102' for Connection #01, and 'NO_ADDRESS' for all other connections. The 'Protocol' is set to 'TCP' and the 'Port' is '2010' for all connections. The 'Type' is 'Packet generator' and 'Parameters' are set to 'Parameters #01' for Connection #01 and 'Parameters #02' through 'Parameters #16' for the others. The 'Enabled' status is 'Enabled' for all connections.

Connection	IP Address or Host Name	Protocol	Port	Type	Parameters	Enabled
Connection #01	192.168.0.102	TCP	2010	Packet generator	Parameters #01	Enabled
Connection #02	NO_ADDRESS	TCP	2009	Packet generator	Parameters #02	Enabled
Connection #03	NO_ADDRESS	TCP	2009	Packet generator	Parameters #03	Enabled
Connection #04	NO_ADDRESS	TCP	2009	Packet generator	Parameters #04	Enabled
Connection #05	NO_ADDRESS	TCP	2009	Packet generator	Parameters #05	Enabled
Connection #06	NO_ADDRESS	TCP	2009	Packet generator	Parameters #06	Enabled
Connection #07	NO_ADDRESS	TCP	2009	Packet generator	Parameters #07	Enabled
Connection #08	NO_ADDRESS	TCP	2009	Packet generator	Parameters #08	Enabled
Connection #09	NO_ADDRESS	TCP	2009	Packet generator	Parameters #09	Enabled
Connection #10	NO_ADDRESS	TCP	2009	Packet generator	Parameters #10	Enabled
Connection #11	NO_ADDRESS	TCP	2009	Packet generator	Parameters #11	Enabled
Connection #12	NO_ADDRESS	TCP	2009	Packet generator	Parameters #12	Enabled
Connection #13	NO_ADDRESS	TCP	2009	Packet generator	Parameters #13	Enabled
Connection #14	NO_ADDRESS	TCP	2009	Packet generator	Parameters #14	Enabled
Connection #15	NO_ADDRESS	TCP	2009	Packet generator	Parameters #15	Enabled
Connection #16	NO_ADDRESS	TCP	2009	Packet generator	Parameters #16	Enabled

ภาพประกอบ ข-2 การตั้งค่า IP ปลายทางแบบ กรณี Single Point ของโปรโตคอล TCP สำหรับ
เครื่องส่งข้อมูล

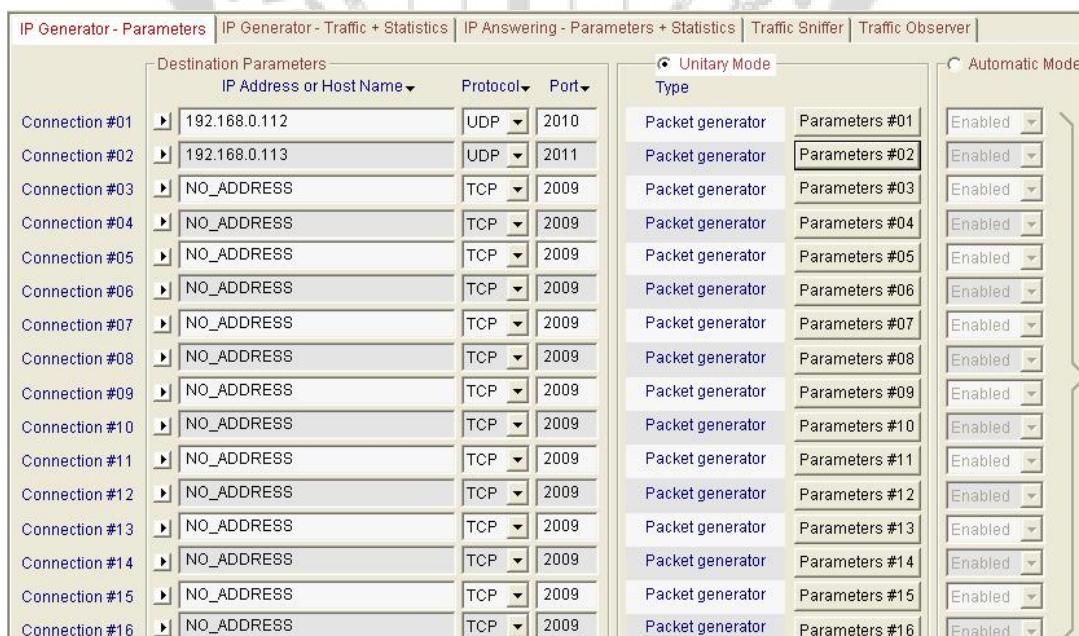
The screenshot shows the 'IP Generator - Parameters' window. The 'Destination Parameters' section has 'IP Address or Host Name' set to '192.168.0.112' for Connection #01, '192.168.0.113' for Connection #02, and 'NO_ADDRESS' for all other connections. The 'Protocol' is set to 'TCP' and the 'Port' is '2010' for Connection #01, '2011' for Connection #02, and '2009' for all other connections. The 'Type' is 'Packet generator' and 'Parameters' are set to 'Parameters #01' for Connection #01, 'Parameters #02' for Connection #02, and 'Parameters #03' through 'Parameters #16' for the others. The 'Enabled' status is 'Enabled' for all connections.

Connection	IP Address or Host Name	Protocol	Port	Type	Parameters	Enabled
Connection #01	192.168.0.112	TCP	2010	Packet generator	Parameters #01	Enabled
Connection #02	192.168.0.113	TCP	2011	Packet generator	Parameters #02	Enabled
Connection #03	NO_ADDRESS	TCP	2009	Packet generator	Parameters #03	Enabled
Connection #04	NO_ADDRESS	TCP	2009	Packet generator	Parameters #04	Enabled
Connection #05	NO_ADDRESS	TCP	2009	Packet generator	Parameters #05	Enabled
Connection #06	NO_ADDRESS	TCP	2009	Packet generator	Parameters #06	Enabled
Connection #07	NO_ADDRESS	TCP	2009	Packet generator	Parameters #07	Enabled
Connection #08	NO_ADDRESS	TCP	2009	Packet generator	Parameters #08	Enabled
Connection #09	NO_ADDRESS	TCP	2009	Packet generator	Parameters #09	Enabled
Connection #10	NO_ADDRESS	TCP	2009	Packet generator	Parameters #10	Enabled
Connection #11	NO_ADDRESS	TCP	2009	Packet generator	Parameters #11	Enabled
Connection #12	NO_ADDRESS	TCP	2009	Packet generator	Parameters #12	Enabled
Connection #13	NO_ADDRESS	TCP	2009	Packet generator	Parameters #13	Enabled
Connection #14	NO_ADDRESS	TCP	2009	Packet generator	Parameters #14	Enabled
Connection #15	NO_ADDRESS	TCP	2009	Packet generator	Parameters #15	Enabled
Connection #16	NO_ADDRESS	TCP	2009	Packet generator	Parameters #16	Enabled

ภาพประกอบ ข-3 การตั้งค่า IP ปลายทางแบบ กรณี Multiple Point ของโปรโตคอล TCP สำหรับ
เครื่องส่งข้อมูล



ภาพประกอบ ข-4 การตั้งค่า IP ปลายทางแบบ กรณี Single Point ของโปรโตคอล UDP สำหรับ
เครื่องส่งข้อมูล



ภาพประกอบ ข-5 การตั้งค่า IP ปลายทางแบบ กรณี Multiple Point ของโปรโตคอล UDP สำหรับ
เครื่องส่งข้อมูล

Mode 1: Using the Internal Data Generator

Step1: Select the traffic generator type
First of all, select the traffic generator which is going to be used on this connection.

Packets Generator Parameters

Packets number (0 to 99,999,999) (0 = infinite value)

Packet Contents (00 to FF hexa byte)

☐ Fix

☒ Random min max

☐ Alternate value-1 value-2

☐ Increasing / Decreasing min max step

Law: data volume to send

☐ Mathematical law Edit...

Uniform law
Range: [9.77 KB, 2.38 MB]

Filename

Browse

File to send

Loop counter (1 to 99) Idle time between each loop (0 to 99 s)

Step2: Specify Data Size and packets parameters
In this step, define Data Size and packets parameters as well as the delay between each sent packet.

UDP Data Size (1 to 65,507 bytes)

☐ Fix

☒ Random min max

☐ Alternate size-1 size-2

☐ Increasing / Decreasing min max step

Inter Packet Delay (0 to 9,999 ms)

☒ Fix (See Forewarnings menu please)

☐ Random min max

☐ Alternate value-1 value-2

☐ Increasing / Decreasing min max step

☐ Mathematical law Edit...

Step 3 (Optional): Activate a throughput limit
When one of these two options is selected, "IP Traffic - Test & Measure" generates the traffic in best effort to respect the throughput chosen.

☐ Use value Mean Throughput (8 to 999,999 Kb/s)

☒ Inter Packet Delay automatically adjusted by IP Traffic

☐ TCP or UDP Data Size automatically adjusted by IP Traffic

☐ Use value (except for TCP connection) Mean Packet Throughput (1 to 99,999 Pkts/s)

ภาพประกอบ ข-6 การตั้งค่าพารามิเตอร์ข้อมูล ใน generate สำหรับเครื่องส่งข้อมูล

Wireless Network Connection Properties

Networking Sharing

Connect using:

☒ Intel(R) Wi-Fi Link 5100 AGN

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

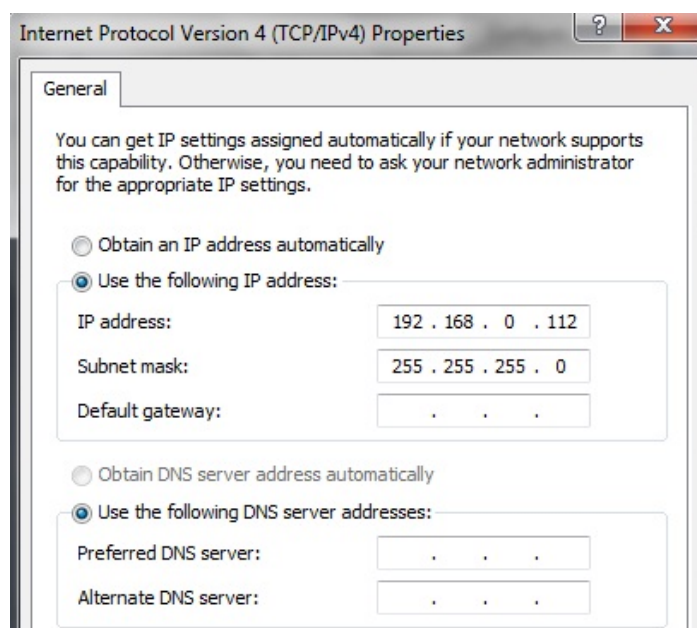
☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

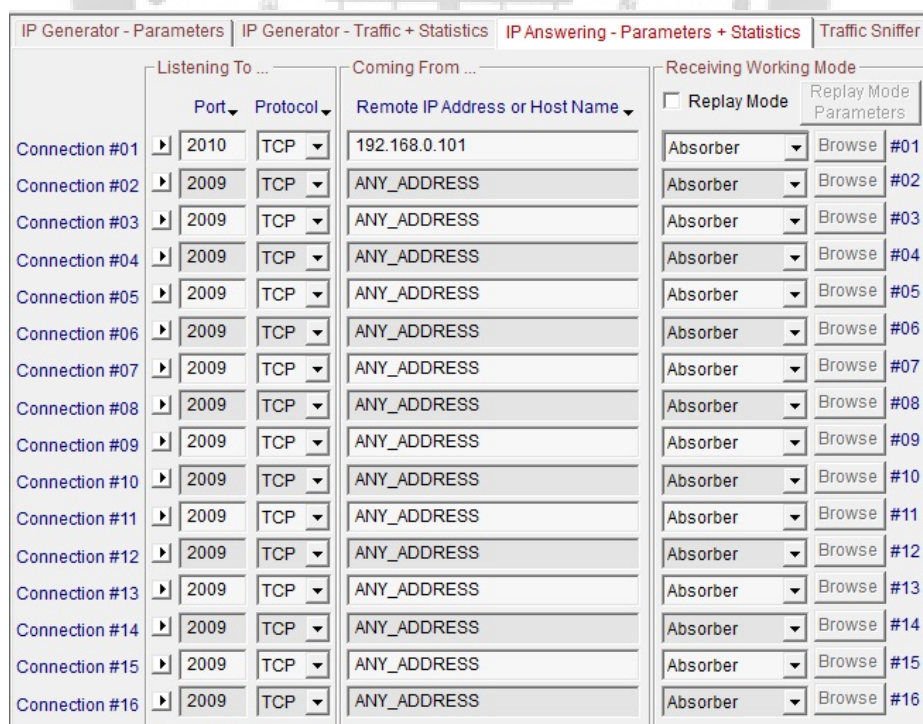
Preferred DNS server:

Alternate DNS server:

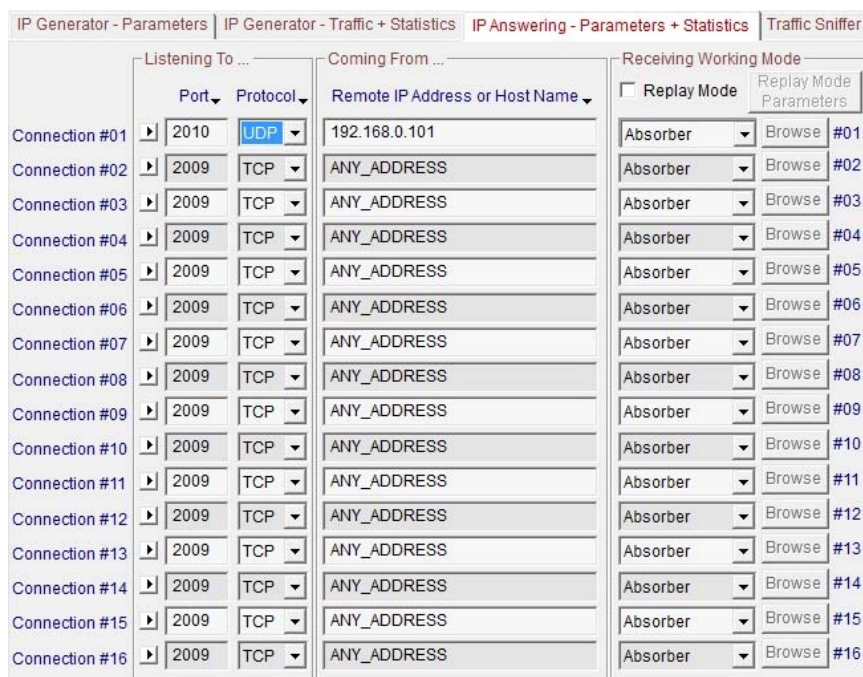
ภาพประกอบ ข-7 การตั้ง IP Address บน Wireless การ์ดสำหรับเครื่องรับข้อมูลเครื่องที่ 1



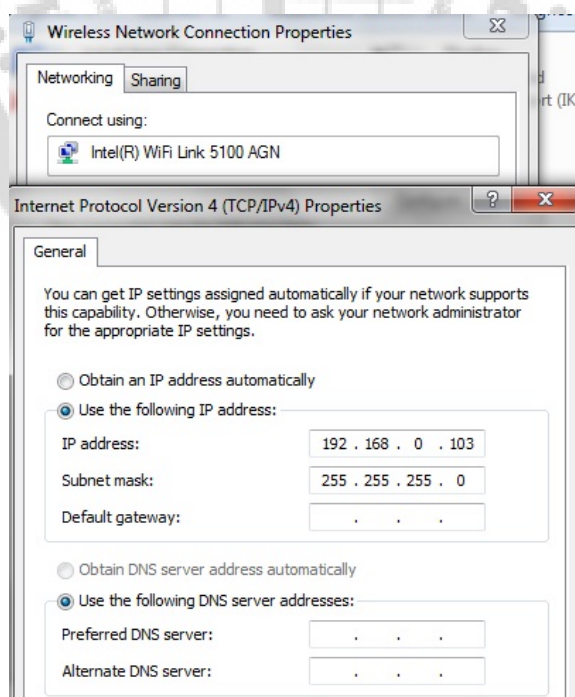
ภาพประกอบ ข-8 การตั้ง IP Address บน LAN การ์ดสำหรับเครื่องรับข้อมูลเครื่องที่ 1



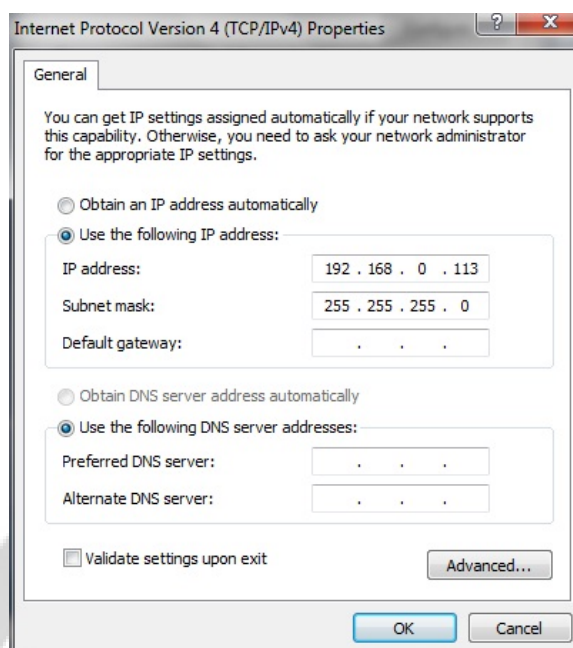
ภาพประกอบ ข-9 การตั้งค่า IP ต้นทาง ของโปรโตคอล TCP สำหรับเครื่องรับข้อมูลเครื่องที่ 1



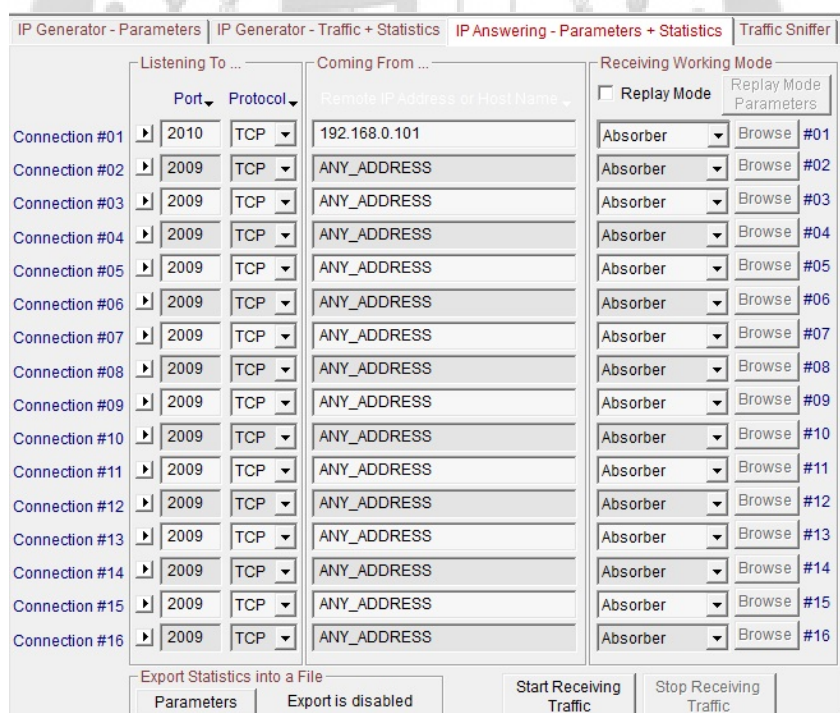
ภาพประกอบ ข-10 การตั้งค่า IP ต้นทาง ของโปรโตคอล UDP สำหรับเครื่องรับข้อมูลเครื่องที่ 1



ภาพประกอบ ข-11 การตั้ง IP Address บน Wireless การ์ดสำหรับเครื่องรับข้อมูลเครื่องที่ 2



ภาพประกอบ ข-12 การตั้ง IP Address บน LAN การ์ดสำหรับเครื่องรับข้อมูลเครื่องที่ 2



ภาพประกอบ ข-13 การตั้งค่า IP ต้นทาง ของโปรโตคอล TCP สำหรับเครื่องรับข้อมูลเครื่องที่ 2

IP Generator - Parameters		IP Generator - Traffic + Statistics		IP Answering - Parameters + Statistics		Traffic Sniffer	
Listening To ...		Coming From ...		Receiving Working Mode			
	Port	Protocol	Remote IP Address or Host Name	☐ Replay Mode Replay Mode Parameters			
Connection #01	2010	UDP	192.168.0.101	Absorber	Browse	#01	
Connection #02	2009	TCP	ANY_ADDRESS	Absorber	Browse	#02	
Connection #03	2009	TCP	ANY_ADDRESS	Absorber	Browse	#03	
Connection #04	2009	TCP	ANY_ADDRESS	Absorber	Browse	#04	
Connection #05	2009	TCP	ANY_ADDRESS	Absorber	Browse	#05	
Connection #06	2009	TCP	ANY_ADDRESS	Absorber	Browse	#06	
Connection #07	2009	TCP	ANY_ADDRESS	Absorber	Browse	#07	
Connection #08	2009	TCP	ANY_ADDRESS	Absorber	Browse	#08	
Connection #09	2009	TCP	ANY_ADDRESS	Absorber	Browse	#09	
Connection #10	2009	TCP	ANY_ADDRESS	Absorber	Browse	#10	
Connection #11	2009	TCP	ANY_ADDRESS	Absorber	Browse	#11	
Connection #12	2009	TCP	ANY_ADDRESS	Absorber	Browse	#12	
Connection #13	2009	TCP	ANY_ADDRESS	Absorber	Browse	#13	
Connection #14	2009	TCP	ANY_ADDRESS	Absorber	Browse	#14	
Connection #15	2009	TCP	ANY_ADDRESS	Absorber	Browse	#15	
Connection #16	2009	TCP	ANY_ADDRESS	Absorber	Browse	#16	
Export Statistics into a File Parameters Export is disabled				Start Receiving Traffic Stop Receiving Traffic			

ภาพประกอบ ข-14 การตั้งค่า IP ต้นทาง ของโปรโตคอล UDP สำหรับเครื่องรับข้อมูลเครื่องที่ 2

LINKSYS®
A Division of Cisco Systems, Inc. Firmware Version: 3.04 - HyperWAP v1.0c

Setup Wireless-G Access Point WAP54G

Setup | Wireless | Administration | Status

Network Setup | AP Mode

Network Setup

Device Name: AP01

Configuration Type: Static IP

IP Address: 192 . 168 . 0 . 1

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway:

Save Settings Cancel Changes

Help...

CISCO SYSTEMS

ภาพประกอบ ข-15 การตั้งค่า Device Name และ IP Address

LINKSYS®
A Division of Cisco Systems, Inc. Firmware Version: 3.04 - HyperWAP v1.0c

Wireless Wireless-G Access Point WAP54G

Setup | Wireless | Administration | Status

Basic Wireless Settings | Wireless Security | Wireless MAC Filter | Advanced Wireless Settings

Basic Wireless Setting

Mode: Mixed

Network Name (SSID): tsunami

Channel: 6 - 2.437GHz

SSID Broadcast: Enabled

Current Encryption: No Encryption

Status: SES Inactive

Reset Security

Help...

CISCO SYSTEMS

ภาพประกอบ ข-16 การตั้งค่า ชั้นความปลอดภัยที่ 1: ไม่มีระบบรักษาความปลอดภัยหรือ เชื่อมโยง
เครือข่ายด้วย SSID เพียงอย่างเดียว

LINKSYS®
A Division of Cisco Systems, Inc.

Firmware Version: 3.04 - HyperWAP v1.0c

Wireless-G Access Point WAP54G

Wireless

Setup Wireless Administration Status

Basic Wireless Settings | Wireless Security | Wireless MAC Filter | Advanced Wireless Settings

Wireless MAC Filter

Access Restriction

Enable

☐ Prevent PCs listed below from accessing the wireless network
☒ Permit PCs listed below to access the wireless network

MAC Addresses 1~25

(Enter the MAC Addresses in this format: xxxxxxxxxx)

MAC 01	70:1A:04:D2:BB:13	MAC 14	
MAC 02	00:16:EA:EF:54:24	MAC 15	
MAC 03	00:21:5D:24:CC:58	MAC 16	
MAC 04		MAC 17	
MAC 05		MAC 18	
MAC 06		MAC 19	
MAC 07		MAC 20	
MAC 08		MAC 21	
MAC 09		MAC 22	
MAC 10		MAC 23	
MAC 11		MAC 24	
MAC 12		MAC 25	

Help...

ภาพประกอบ ข-17 การตั้งค่า ชั้นความปลอดภัยที่ 2: ตรวจสอบโดยใช้ MAC Address

LINKSYS®
A Division of Cisco Systems, Inc.

Firmware Version: 3.04 - HyperWAP v1.0c

Wireless-G Access Point WAP54G

Wireless

Setup Wireless Administration Status

Basic Wireless Settings | Wireless Security | Wireless MAC Filter | Advanced Wireless Settings

Wireless Security

Security Mode: WEP

Encryption: 40 / 64-bit (10 hex digits)

Passphrase: Generate

Key 1: 1234567890

Key 2: D452592BB2

Key 3: 1824BC6ED8

Key 4: 4A52D18211

TX Key: 1

Help...

CISCO SYSTEMS

ภาพประกอบ ข-18 การตั้งค่า ชั้นความปลอดภัยที่ 3: ตรวจสอบโดยใช้ WEP 64 บิต

LINKSYS®
A Division of Cisco Systems, Inc. Firmware Version: 3.04 - HyperWAP v1.0c

Wireless-G Access Point WAP54G

Wireless

Setup | Wireless | Administration | Status

Basic Wireless Settings | Wireless Security | Wireless MAC Filter | Advanced Wireless Settings

Wireless Security

Security Mode: WEP

Encryption: 104 / 128-bit (26 hex digits)

Passphrase: Generate

Key 1: 12345678901234567890123456

Key 2:

Key 3:

Key 4:

TX Key: 2

Help...

CISCO SYSTEMS

ภาพประกอบ ข-19 การตั้งค่า ชั้นความปลอดภัยที่ 4: ตรวจสอบโดยใช้ WEP 128 บิต

LINKSYS®
A Division of Cisco Systems, Inc. Firmware Version: 3.04 - HyperWAP v1.0c

Wireless-G Access Point WAP54G

Wireless

Setup | Wireless | Administration | Status

Basic Wireless Settings | Wireless Security | Wireless MAC Filter | Advanced Wireless Settings

Wireless Security

Security Mode: WPA-Personal

Encryption: AES

Passphrase: b1fll0l0bx4xe0j

Key Renewal: 300 seconds

Help...

Save Settings Cancel Changes

CISCO SYSTEMS

ภาพประกอบ ข-20 การตั้งค่า ชั้นความปลอดภัยที่ 5: ตรวจสอบโดยใช้ WPA-PSK Version1

LINKSYS®
A Division of Cisco Systems, Inc.

Firmware Version: 3.04 - HyperWAP v1.0c

Wireless-G Access Point WAP54G

Wireless

Setup | Wireless | Administration | Status

Basic Wireless Settings | Wireless Security | Wireless MAC Filter | Advanced Wireless Settings

Wireless Security

Security Mode: WPA2-Personal

Encryption: AES

Passphrase: b1f1l0i0bx4xe0j

Key Renewal: 300 seconds

Save Settings Cancel Changes

Help...

CISCO SYSTEMS

ภาพประกอบ ข-21 การตั้งค่า ชั้นความปลอดภัยที่ 6: ตรวจสอบโดยใช้ WPA-PSK Version2

LINKSYS®
A Division of Cisco Systems, Inc.

Firmware Version: 3.04 - HyperWAP v1.0c

Wireless-G Access Point WAP54G

Wireless

Setup | Wireless | Administration | Status

Basic Wireless Settings | Wireless Security | Wireless MAC Filter | Advanced Wireless Settings

Wireless Security

Security Mode: RADIUS

RADIUS Server: 192 . 168 . 0 . 200

RADIUS Port: 1812

Shared Secret: 1234

Encryption: 104 / 128-bit (26 hex digits)

Passphrase: Generate

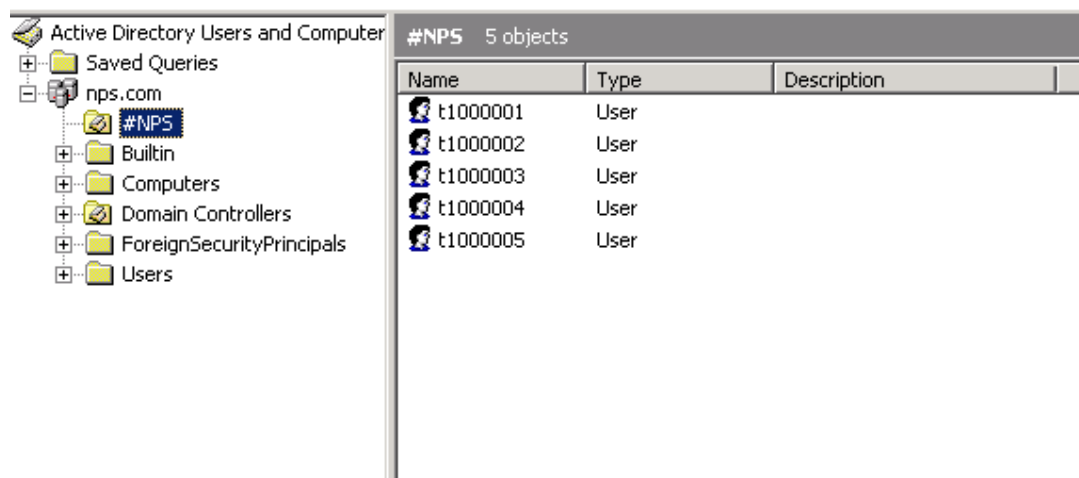
Key 1:

Key 2:

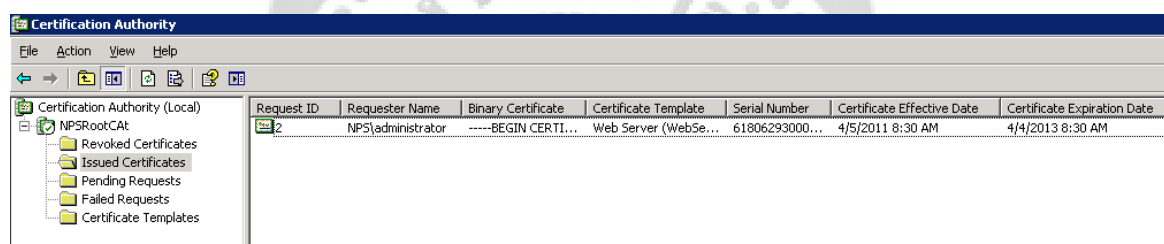
Key 3:

Help...

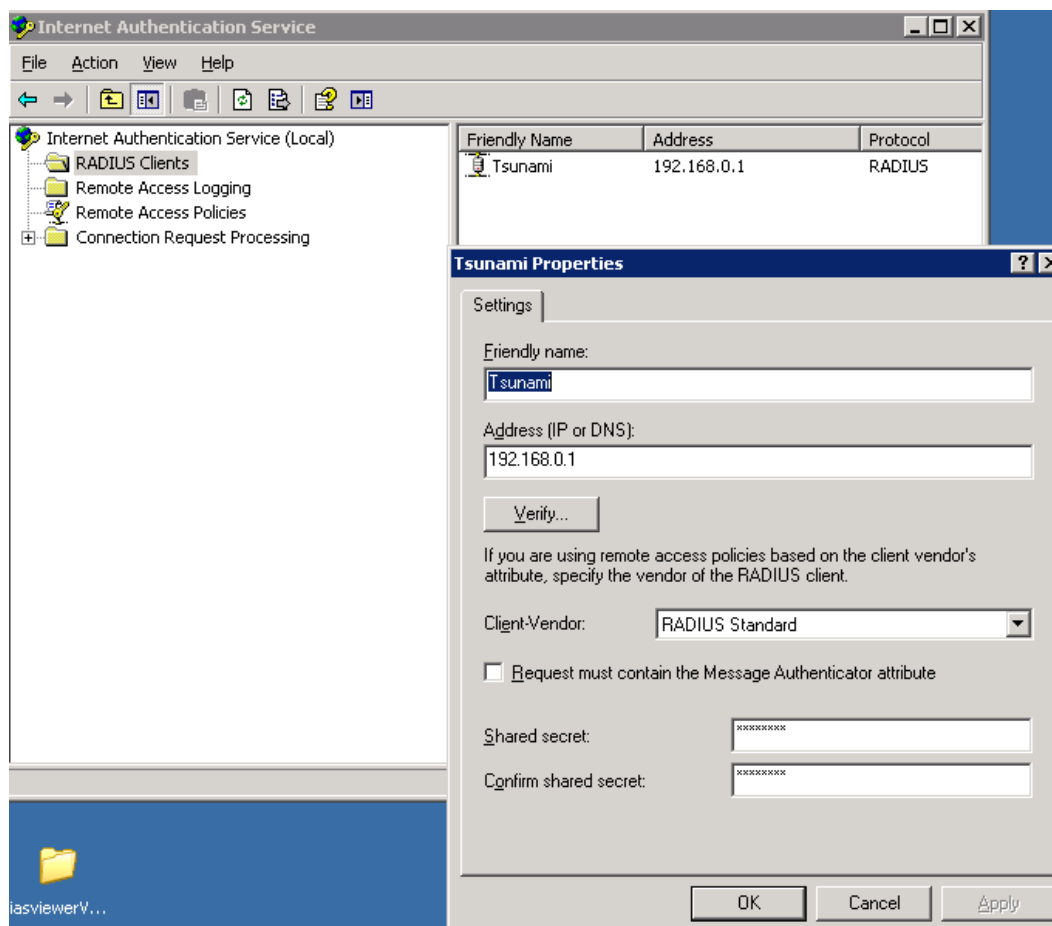
ภาพประกอบ ข-22 การตั้งค่า ชั้นความปลอดภัยที่ 7: ตรวจสอบโดยใช้ PEAP



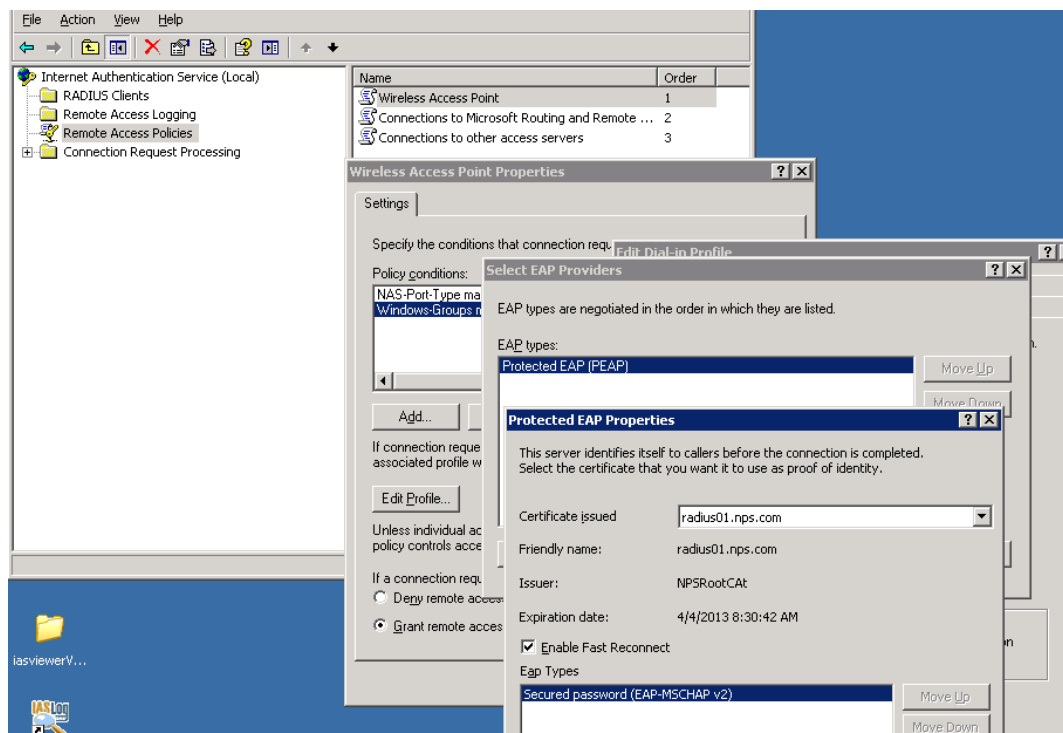
ภาพประกอบ ข-23 การตั้งค่า Active Directory User and Computer



ภาพประกอบ ข-24 การตั้งค่า Certification Authority



ภาพประกอบ ข-25 การตั้งค่า Radius Client ใน เครื่อง Radius Server โดยใช้ Internet Authentication Service (IAS)



ภาพประกอบ ข-26 การตั้งค่า Wireless Policy ใน เครื่อง Radius Server



ประวัติย่อผู้ทำสารนิพนธ์

ชื่อ ชื่อสกุล	ณัฐพงษ์ สำเนียงงาม
วันเดือนปีเกิด	23 มิถุนายน 2523
สถานที่เกิด	กรุงเทพมหานคร
สถานที่อยู่ปัจจุบัน	255/322 รัชดาเพรสทีจคอนโด ซ.ลาดพร้าว 48 ถ.ลาดพร้าว แขวงสาม เสนนอก เขตห้วยขวาง กรุงเทพฯ 10320
ตำแหน่งหน้าที่การงานปัจจุบัน	วิศวกรระบบ
สถานที่ทำงานปัจจุบัน	บริษัท ไทยเบฟเวอเรจ จำกัด (มหาชน)
ประวัติการศึกษา	
พ.ศ. 2547	วศ.บ. (วิศวกรรมคอมพิวเตอร์) จาก มหาวิทยาลัยนเรศวร พิษณุโลก
พ.ศ. 2554	วศ.ม. (การจัดการทางวิศวกรรมเทคโนโลยีสารสนเทศและการสื่อสาร) จาก มหาวิทยาลัยศรีนครินทรวิโรฒ